Wie sieht das Internet der Zukunft aus?

Dezentrale Soziale Netzwerke

TINF2019

Identität und Entscheidungsfindung

Identität

Es ist üblich, bei jeder Internetseite einen Account mit eigenen Zugangsdaten zu erstellen. Inzwischen ist es jedoch bei einigen Internetseiten möglich, sich stattdessen über Drittanbieter wie „Facebook“, „Twitter“ und „Google“ anzumelden, genannt „Social login“. Der Vorteil ist, dass ein Anwender sich nur noch die Anmeldedaten für einen Dienst merken muss, der Nachteil ist, dass dieser zentrale Dienst ein SPOF wird. Geht der Dienst außer Betrieb oder wird der Anwender von der Nutzung des Dienstes ausgeschlossen, wird ihm gleichzeitig der Zugriff auf alle anderen Internetseiten verwehrt, bei welchen er sich mithilfe des Dienstes bisher angemeldet hat.

Die Identitäten von Internetseiten werden heutzutage über die PKI verwaltet. Es gibt mehrere CAs, die im Besitz von vertrauenswürdigen Stammzertifikaten sind. Diese sind in der Lage, beliebige Zertifikate zu erstellen. Diese Zertifikate beweisen dem Anwender, dass es sich bei der aufgerufenen Internetseite um die richtige Seite handelt. Trotz der umfangreichen Sicherheitsvorkehrungen der CAs gab es bereits einzelne Vorfälle, wie zum Beispiel fälschlicherweise ausgestellte Zertifikate.

Es gibt bereits einzelne Lösungsansätze für die Probleme, die aus dem unbegrenzten Vertrauen in die CAs entstehen. Bei HPKP wird das Zertifikat beim ersten Besuch der Internetseite gespeichert, was verhindert, dass bei nachfolgenden Verbindungen sich ein Angreifer mit einem anderen Zertifikat als diese Internetseite ausgeben kann. HPKP wird inzwischen nicht mehr praktiziert, da böswillige Akteure den Mechanismus verwendeten, um den Zugriff auf kompromittierte Internetseiten langfristig zu verhindern.

Ein Ansatz für eine dezentrale Identitätenverwaltung ist das WoT, in welchem einzelne Anwender die Echtheit der Identitäten der ihnen bekannten Anwender bestätigen. Damit lässt sich ein Netzwerk von Identitäten realer Personen leicht aufbauen, jedoch könnte das System gestört werden, wenn mehrere Angreifer gemeinsam eine Identität falsch bestätigen.

Zusammengefasst lässt sich sagen, dass die bisher praktizierte Identitätsverwaltung funktioniert, jedoch einige Schwachstellen besitzt, deren Behebung weiterhin Gegenstand der Forschung ist.

Entscheidungsfindung in dezentralen Systemen

Bei dezentralen Strukturen stellt sich sofort die Frage, wer Entscheidungen trifft, wie diese umgesetzt werden und wer bei Verstößen durchgreift. Ein existierendes Beispiel für dezentrale Gruppen sind sogenannte DAOs, welche ein Beiprodukt der Popularisierung von Kryptowährungen sind. Diese DAOs entstehen meist in Form von Venture Capital Groups (Risikokapital). Gruppenmitglieder sollen anhand von Tokens “demokratisch” entscheiden können, wie und wo diese Investments gemacht werden sollen. Dabei gibt es verschiedene Ansätze, zum Beispiel proportional (n Tokens = n Stimmen; vgl. Shareholder) oder Fiat (n Tokens = 1 Stimme). Bei demokratischen Fiat-Abstimmungen kann aber ohne ein zentrales Kontrollorgan nicht sichergestellt werden, dass niemand mehrere Accounts besitzt. Außerdem ist nicht klar, wie sichergestellt werden kann, dass die demokratischen Entscheidungen auch umgesetzt werden. Des Weiteren ist niemand (oder alle) verantwortlich, wenn durch die Entscheidungen Gesetze gebrochen werden. Ein Kompromiss dazu ist "semi-decentralization", wie sie von Google in Form von Android verwendet wird. Dabei ist Android Open Source und kann von seiner Community weiterentwickelt werden. Jedoch behält Google große Teile der Entscheidungsmacht, um zum Beispiel durch den Play Store Sicherheit, Kompatibilität und Konsistenz zu gewährleisten.

DHBW
Duale Hochschule
Baden-Württemberg

Abkürzungen

- **SPOF:** Single Point of Failure
- **PKI:** Public Key Infrastructure
- **CA:** Certificate Authority
- **HPKP:** HTTP Public Key Pinning
- **WoT:** Web of Trust
- **DAO:** Decentralized Autonomous Organization

Weiterführende Literatur

- https://www.theguardian.com/technology/2022/aug/22/google-csam-account-blocked
- https://sslmate.com/resources/certificate_authority_failures
- https://community.letsencrypt.org/t/hacked-new-wordpress-sites-because-le-is-created/175284
- https://www.heise.de/hintergrund/Wachsende-Kritik-an-Public-Key-Pinning-fuer-HTTPS-3324703.html
- Chen, Y., Richter, J. I., & Patel, P. C. (2020). Decentralized Governance of Digital Platforms. In Journal of Management (Vol. 47, Issue 5, pp. 1305–1337). SAGE Publications.
- https://naavik.co/deep-dives/axie-infinity#axie-decon=

Kontakt

Duale Hochschule Baden-Württemberg

Marienstraße 20, 89518 Heidenheim
+49 7321 2722 0, info@dhbw-heidenheim.de

Wie sieht das Internet der Zukunft aus?

Dezentrale Soziale Netzwerke

TINF2019

Bereitstellung von Content

Interplanetary File System

Ein Ansatz, ein dezentrales System zu bilden, liefert das Interplanetary File System (IPFS). IPFS ist ein Protokoll, welches den Nutzern ermöglicht, Hypermedien über ein Peer-to-Peer-Netzwerk abzurufen. Die Medien werden dabei verteilt auf unterschiedlichen Systemen gespeichert. Wird ein neuer Inhalt dem System hinzugefügt, bekommt dieser einen eigenen Content Identifier (CID), über den dieses Medium abrufbar ist. Jeder Betrachter dieses Mediums speichert es temporär auf seinem eigenen Rechner. Somit wird er automatisch zu einem Provider, bis sein Cache geleert wird. Wenn der Content dauerhaft gespeichert werden soll, muss dieser vom Provider angepinnt werden.

Vorteile	Nachteile
▪ Medien werden automatisch auf mehreren Knoten gespeichert ▪ Das System funktioniert auch, wenn einzelne Knoten ausfallen ▪ Content wird automatisch archiviert	▪ Kein wirtschaftlicher Anreiz, Knoten bereitzustellen ▪ Illegaler Content ist schwer zu entfernen ▪ Privatsphäre nur durch Verschlüsselung

Wirtschaftlichkeit

Trotz der vielen Vorteile von IPFS hat es seit der Veröffentlichung im Jahr 2015 nur wenig an Traktion gewonnen. Knoten werden nach wie vor nur von Technologie-Enthusiasten betrieben; eine breite Verwendung bleibt aus. Einer der Hauptgründe hierfür ist die fehlende Wirtschaftlichkeit des Konzeptes: es gibt keinen Anreiz für User, die eigene Hardware als Knoten zur Verfügung zu stellen. Vor allem Anwendungen, die Langzeitspeicherung von großen Datenmengen benötigen, kommen daher zu kurz, da man sich nicht darauf verlassen kann, dass fremde Knoten den Content dauerhaft anpinnen.
Ein Lösungskonzept für dieses Problem ist Filecoin, eine Erweiterung zu IPFS, die das dauerhafte Bereitstellen von fremdem Content durch eine Kryptowährung belohnt. Die Transaktionen, in diesem Fall sogenannte Speicher- und Abrufdeals, werden wie bei anderen Kryptowährungen durch ein Blockchain-Netzwerk verifiziert. Dabei schickt ein Knoten periodisch den Nachweis, dass die Datei immer noch wie vom Deal vorgesehen gespeichert ist. Im Gegenzug wird dem Knoten Filecoin gutgeschrieben, die durch den User finanziert werden.

Dezentrale Dienste

Neben der Speicherung von Daten mit IPFS werden dezentrale Dienste benötigt, welche eine „serverseitige“ Logik abbilden. Dadurch können zentrale Anbieter vermieden werden, welche z. B. Nutzerdaten missbrauchen könnten. In einem Social Media-Netzwerk werden beispielsweise Übersetzer benötigt. Durch die große Anzahl an Kombinationen ist es unpraktikabel, auf Endgeräten einen Übersetzer für alle Sprachen zu installieren. Hierfür kann ein Blockchain-Netzwerk verwendet werden, welches Smart Contracts mit verschiedenen Übersetzungsalgorithmen ausführt. Die Ergebnisse werden anschließend zusammengetragen, um zu prüfen, ob die Übersetzungen übereinstimmen und somit das Ergebnis korrekt ist. Schließlich ergibt sich zusammen mit anderen Diensten und einem Frontend eine Decentralized Application (DApp), welche transparent und ohne zentrale Autorität auf einem Blockchain-Netzwerk ausgeführt werden kann.

DHBW
Duale Hochschule
Baden-Württemberg

Das Internet der fernen Zukunft

Sollten die Vorhaben von Visionären wie Elon Musk Früchte tragen, könnten sich in der fernen Zukunft neue interplanetare Märkte für das Internet eröffnen. Hierbei würde der bisherige zentralisierte Ansatz an seine Grenzen stoßen, da Anbieter umständlich und teuer Hardware zu neuen Frontieren wie dem Mars transportieren müssten und Latenzzeiten bisherige Protokolle obsolet machen. In einem solchem Szenario könnte das IPFS seinem Namen getreu einspringen und mit seiner hohen Verfügbarkeit, Resilienz, und dynamischer Speicherung von Content auf Basis der Nachfrage, glänzen.

Definitionen

» **Content Identifier (CID):** Hashwert der Datei. Jedes Medium im IPFS ist über eine CID identifizierbar.
» **InterPlanetary Name System (IPNS):** Name Server für Medien im IPFS. Damit lässt sich der neueste Stand einer Datei immer über denselben Link abrufen.
» **IPFS-Search:** Suchmaschine für Medien im IPFS
» **Smart Contract:** Eine Sammlung von Code und Daten, die von mehreren Knoten eines Blockchain-Netzwerks ausgeführt wird. Alle Knoten müssen das gleiche Ergebnis erzielen, damit es als valide anerkannt wird.

Weiterführende Literatur

» https://ipfs.tech
» https://docs.filecoin.io/about-filecoin/what-is-filecoin/
» Benet, J. (2014). IPFS - Content Addressed, Versioned, P2P File System (Version 1). ArXiv.
» Y. Psaras and D. Dias, "The InterPlanetary File System and the Filecoin Network," 2020 50th Annual IEEE-IFIP International Conference on Dependable Systems and Networks-Supplemental Volume (DSN-S)
» Scarton, C., & Specia, L. (2014). Exploring Consensus in Machine Translation for Quality Estimation. In Proceedings of the Ninth Workshop on Statistical Machine Translation. Association for Computational Linguistics.
» Weber, S., & Mehandru, N. (2021). The 2020s political economy of machine translation. In Business and Politics (Bd. 24, Issue 1, S. 96–112). Cambridge University Press (CUP).

Kontakt

Duale Hochschule Baden-Württemberg

Marienstraße 20, 89518 Heidenheim
+49 7321 2722 0, info@dhbw-heidenheim.de

Wie sieht das Internet der Zukunft aus?

Dezentrale Soziale Netzwerke

TINF2019

Dezentrales Metaverse

Aktuell sind bestehende Soziale Netzwerke dabei, sich zum Metaverse weiterzuentwickeln, wie z. B. Meta (ehem. Facebook). Hierbei bleiben die Probleme von klassischen, zentral verwalteten Sozialen Netzwerken bestehen. Würden die Metaversen dezentral organisiert werden, könnten einige der bei zentralen Systemen auftretenden Probleme vermieden werden. Doch wie könnte so ein Metaverse aufgebaut sein?

Metaverse – Ingame Architektur

Stellt man sich ein dezentrales Metaverse vor, kommt einem beim Nachdenken sofort die Frage in den Sinn, wie sich diese Dezentralisierung auf die Innen-Perspektive im Metaverse auswirkt. Da für eine Dezentralisierung des Metaverse dieses über verschiedene Server verteilt werden muss, bietet es sich an, das Metaverse räumlich in verschiedene Welten und Räume zu unterteilen, die jeweils auf verschiedenen Servern gehostet sein können. Antworten zur Frage über die Fortbewegung zwischen den Welten kann man in der aktuellen Fantasie-Literatur und Game-Welten finden. So wäre es denkbar, wie in Minecraft zwischen verschiedenen Spielmodi und Lobbys auf verschiedenen Servern hin- und herzuwechseln oder während des Spiels den physischen Server durch verschiedene Arten von Portalen, wie dem Teleporter aus Star-Trek oder dem Schrank aus Narnia zu wechseln. Diese könnten dann anhand verschiedener Eigenschaften, wie feste, variable oder zufällige Start- und Endpunkte und Berechtigungen konfiguriert werden. So ist vorstellbar, dass jeder Server selbst festlegt, ob auf diesen teleportiert werden kann und wie.

Die Fortbewegung von Spielern zwischen Welten führt meistens wie in der realen Welt dazu, dass Spieler mit Eigentum und Geld Handel treiben wollen. Dies kann dabei wie in der realen Welt mit zentralen Banken, verteilten Banken oder einem komplett dezentralen Bankguthaben auf Blockchain-Basis wie Bitcoin passieren. Dahingegen gestaltet sich die Definition von Eigentum in den verteilten virtuellen Welten ungleich schwieriger. Es stellt sich die Frage, ob Eigentum von Welt zu Welt mitgenommen werden kann, oder ob es einfach kopiert und vervielfältigt werden kann. Mögliche Lösungsansätze dazu bieten das "Web of Trust", NFTs, dezentrale Eigentumszertifikatsstellen oder eine oder mehrere Blockchain-Netzwerke, die als Eigentumsnachweis verwendet werden könnten.

Dezentrales Metaverse – Technische Architektur

Neben der Ingame-Architektur muss natürlich auch die technische Architektur eines dezentralen Metaverse betrachtet werden. Dabei kann auch wieder einiges aus der bestehenden Game- und Internet-Welt übernommen werden. So wäre es möglich, dass die verschiedenen Server, wie bei Minecraft, auf IP-Basis miteinander kommunizieren. Die Weiterleitung zwischen verschiedenen Servern könnte dabei über Links, die sich Ingame als Portale darstellen, erfolgen. Das kann unter anderem zur Entstehung von Suchmaschinen für Räume des Metaverse führen, die eine Liste von Welten anbieten. Damit der Zugriff auf Räume geschützt werden kann, muss natürlich auch über Zugangsrestriktionen und Identität nachgedacht werden.

Eine weitere relevante technische Fragestellung ist die der Software. Gibt es eine zentrale "Metaverse-Software" oder einen Standard mit mehreren Implementierungen? Wie sieht die Software-Architektur einer solchen Software aus? Frontend, Game-Engine und Backend?

DHBW
Duale Hochschule
Baden-Württemberg

Begriffsdefinition

Metaverse:
Der weitgefasste Begriff Metaverse bezieht sich auf einen virtuellen Raum, in dem Menschen mithilfe von Virtual-Reality-Technologien als Avatare miteinander interagieren können. Dabei schafft das Metaverse eine Konvergenz zwischen physischer Realität und virtuellem Raum im Kontext des vernetzten Digitalraums. Der Unterschied zu traditionellen Websites und sozialen Netzwerken liegt in der immersiven Erfahrung, die das Metaverse bietet. Verschiedenste Aktivitäten, wie arbeiten, einkaufen, spielen oder auch reisen sind im Metaverse möglich. Viele Experten und Expertinnen sehen hierin eine große Entwicklung des Internets. Nach dem Sprung vom Desktop zum Smartphone könnte der Sprung vom Smartphone ins Metaversum bevorstehen. Dabei können auch verschiedene Entitäten entstehen, die jeweils die Bezeichnung Metaversum erhalten.

Quelle:
https://onlinemarketing.de/lexikon/definition-metaverse

Weiterführende Literatur

- Duan, H. et al. (221). Metaverse for Social Good. In Proceedings of the 29th ACM International Conference on Multimedia. MM ’21: ACM Multimedia Conference. ACM.
- Yang, Q. et al. (2022). Fusing Blockchain and AI With Metaverse: A Survey. In IEEE Open Journal of the Computer Society (Bd. 3, S. 122–136). Institute of Electrical and Electronics Engineers (IEEE).
- Mozumder et al. (2022). Overview: Technology Roadmap of the Future Trend of Metaverse based on IoT, Blockchain, AI Technique, and Medical Domain Metaverse Activity. In 2022 24th International Conference on Advanced Communication Technology (ICACT). IEEE.

YouTube Video:
The Metaverse is Already Here

YouTube Video:
The Metaverse and How We'll Build It Together

Kontakt

Duale Hochschule Baden-Württemberg

Marienstraße 20, 89518 Heidenheim
+49 7321 2722 0, info@dhbw-heidenheim.de

Alle Informationen finden Sie unter: **www.dhbw.de**