Ara — Den weltweit dezentralisiert Infrastruktur für Zahlungen, Benutzerkennung, Webhosting, Streamen, und Besitz von Dateien und Inhalte (Entwurf)

Eric Jiang, Charles Kelly, Joseph Werle, Tony Mugavero, Vanessa Kincaid

Zuletzt aktualisiert 14. November 2018 (teilweise**)

Abstrakt

Das Internet ist zu einem Schatten seiner selbst geworden, dominiert von nur einigen großen Unternehmen, die die gesamte Autorität über alle Informationen ausüben, indem sie kontrollieren, wie es um die Welt fließt, wie viel es kostet und wie und wann es konsumiert werden kann. Ara ist eine dezentrale Plattform und eine Reihe von Protokollen, um dies zu beheben. Durch die Lizenzierung und den Verkauf von digitalen Dateien und Inhalten mit einem neuartigen Eigentumsnachweissystem bedient Ara die globale Datenlieferung und unterstützt den Erwerb dieser Assets mit dem nativen Ara-Token. Und dabei benutzt die Ara-Plattform außerdem ein allgegenwärtiges und verteiltes Benutzer-ID- und Wallet-System, das es den Benutzern ermöglicht, das Eigentum an ihren persönlichen Informationen zu behalten. In der Tat ist Ara ein neues, modernes mentales Modell dafür, wie Information im Internet gehostet und bereitgestellt werden und wie Konsumenten sie nutzen und dafür bezahlen. Es führt zu einem neuen Paradigma, nicht nur für Unternehmen, sondern auch für die Konsumenten, da sie durch das Hosting und die Teilnahme am Netzwerk einen Beitrag zu dem System leisten können, um Belohnungen zu verdienen. Peer-to-Peer (P2P) Datenaustausch, Blockchain-Technologie für Besitz und Lizenzierung sowie verteiltes Computing sind in einem einzigen effizienten und dezentralen System zusammengefasst.

Zahlreiche Mitgliederbereiche profitieren von Ara. Verbraucher können ihren ungenutzten Speicher, ihre Bandbreite und ihre Rechenleistung nutzen, um Ara-Token, die vergleichbar mit Airbnb für Computer sind, zu verdienen und diese Token verwenden, um Inhalte zu kaufen. Unternehmen sparen, indem Sie diese Informationen Personen durch P2P-Technologie bereitstellen, was wiederum die Kosten für die Konsumenten und andere Unternehmen senkt. Jeder kann als Rechenzentrum im Netzwerk teilnehmen, um Belohnungen zu verdienen. Digitale Urheber, Gaming- und Softwareentwickler, Film- und Fernsehstudios sowie Verlage verwenden Ara-Token, um lizenzierte Inhalte im Netzwerk zu veröffentlichen, und verdienen mehr für ihre Arbeit, indem sie größere Umsatzanteile generieren und den Rest für die Hosting-Kosten an ihre Fans weitergeben. Es ist ein Rundum-Gewinn. Die Konsumenten werden belohnt, die Verleger verdienen mehr, und die Unternehmen verbessern ihre Profite. Dies alles geschieht auf eine dezentrale und netzneutrale Weise, sodass keine zwischengeschalteten Unternehmen ein einzelnes Geschäft drosseln können, das Ihnen Informationen und Inhalte liefert.

** Dies ist eine Teilaktualisierung des Whitepapers vom Juni 2018. Ein ausführlicheres Update wird in den kommenden Monaten veröffentlicht.

Hinweis: Ara steht unter aktiver Forschung und Entwicklung. Dieses Papier unterliegt Änderungen. Die neueste Version ist erhältlich unter https://ara.one. Bitte wenden Sie sich mit allen Kommentaren und Vorschlägen an hello@ara.one.

Inhaltsverzeichnis

1. Einführung **2**
1.1 Hintergrund . . . 2
1.2 Übersicht . . . 3
1.3 Plattform-Services . . . 3

2. Plattform-Übersicht **5**
2.1 AraID . . . 5
2.1.1 Dezentralisierte Identität . . . 5
2.2 Dezentralisiertes Content-Delivery-Netzwerk (DCDN) . . . 6
2.2.1 Ara-Dateisystem (Ara File System (AFS) . . . 7
2.2.2 Token-Verwendung . . . 7
2.3 Ara Protokoll Suite . . . 8
2.3.1 Belohnungen und Anreize . . . 8
2.3.2 Dateilieferung (File Delivery) . . . 9
2.3.3 Smart-Verträge . . . 9

3. Zukünftige Entwicklung **12**
3.1 Module . . . 12
3.2 Ara Namen-System (ANS) . . . 12

4. Danksagung **12**

Akronyme **13**

Literatur **13**

Anhang **15**

I. Reife Ara-Plattform Token-Wirtschaft (Entwurf) **15**
Übersicht . . . 15
Das Ara-Token . . . 15
Funktion . . . 16
Markt-Dynamiken . . . 16
Anreizstruktur . . . 17
Netzwerkeffekte . . . 17
Verweise . . . 18

II. DCDN Kostenanalyse by Lester Kim **19**
Gewinnmaximierung des Uploaders . . . 19
Kostenminimierung des Distributors . . . 21
Beispiel . . . 23
Verweise . . . 24

III. Erwartete Ara-Prämien-Analyse by Lester Kim **26**
Netzwerkmodell . . . 26
Beispiel . . . 27
Verweise . . . 27

1. Einführung

1.1 Hintergrund

Die Hypermedia-Landschaft ist heutzutage veraltet. Aggregatoren und App-Stores verstärken den Griff auf Content (Inhalts)-Ersteller. Traditionelle Content-Delivery-Netzwerke sind ineffizient und teuer; Cloud-Computing ist auf wenige ausgewählte Gatekeeper zentralisiert; und Daten werden nicht von denen gespeichert, die sie besitzen, sondern von denen, die davon profitieren. Content-Publisher und Schöpfer sind gezwungen, die Preise zu überhöhen, um die Kosten für dieses langsame und teure System auf Konsumenten auszulagern, was zu verloren Wert sowohl für Publisher, als auch die Konsumenten und Urheber führt.

Mit Video, das bis 2021 über 80% des gesamten Internetverkehrs ausmacht [3], steigen die Kosten für Inhalte weiterhin an, da die Dateigrößen und die Kosten für die Bereitstellung dieses Inhalts steigen. 4K-, VR- und AAA-Spiele tragen alle zu diesem Trend bei. Die Verbraucher zahlen nicht nur mehr für Transaktionsinhalte und Abonnements, sondern sie müssen sich mit einem komplexen und missbräuchlichen Werbesystem auseinandersetzen, um freie Inhalte anzuschauen. Diese Faktoren verstärken das Problem der Produktpiraterie, das den Besitzern von Inhalten Verluste in Milliardenhöhe verursacht [16][12][4], und führen zum Einsatz von Tools wie Ad-Blocker, mit denen Werbung übersprungen oder entfernt werden können. Dadurch werden Adblocker-Blocker und teurere Abonnementdienste geschaffen, da die Konsumenten Anzeigen vermeiden und Inhaltsinhaber versuchen, verlorene Einnahmen zurückzugewinnen. Es ist ein Teufelskreis.

Peer-to-Peer (P2P) - Dateiverteilungsarchitekturen entstanden als Antwort auf diese Ineffizienzen, die sich von Hybridlösungen mit zentralisierten Servern wie Napster bis hin zu vollständig dezentralisierten Lösungen wie Gnutella und schließlich BitTorrent entwickelten. Heutzutage ist die P2P-Dateibereitstellung so kostengünstig, dass Unternehmen wie Microsoft sie verwenden, hier anstatt ihrer eigenen Azure-Infrastruktur, um an Kosten für die Windows 10-Verteilung zu sparen.

Während P2P-Filesharing-Netzwerke kosteneffizient sind, gab es in der Vergangenheit immer wieder Trittbrettfahrer, Piraterie, Hacker und Schwarzmärkte, beim Einsatz in öffentlichen Umgebungen. Es gab kein Vertrauen darauf, dass derjenige, der Inhalte hochlädt auch dazu berechtigt ist, und es gibt keine Möglichkeit, zu überprüfen, ob der Inhalt so ausgestreut (seeded) wird, wie es der Inhaltseigentümer vorgesehen hat. Es gab außerdem keine Belohnung für das Speichern und Teilen von Inhalten, so dass den Nutzern kein Anreiz gegeben wurde, Seeds im Liefersystem zu bleiben. Peers beuteten Inhalte für sich selbst aus und nahmen nicht weiter am Seeding dieser Inhalte an andere Peers teil. Um dem gerecht zu werden, begannen P2P-Architekturen Anreizmechanismen wie Tauschstrategien, Reputationssysteme und Eigenwährungen zu integrieren. Aber auch diese Mechanismen haben ihren Anteil an Problemen und sind anfällig für Sybil- und Whitewashing-Angriffe.

1.2 Übersicht

In diesem Whitepaper präsentieren wir Ara: eine Community-gesteuerte, dezentralisierte und verteilte Computing- und Content-Auslieferungs-Plattform. Ara ermöglicht jedem Gerät auf der Welt, durch die Nutzung seiner ungenutzten Verarbeitungs-, Speicher- und Bandbreitenkapazität sofort Teil eines globalen Supercomputers, einer Datenbank und eines Übertragungsnetzwerkes zu werden. Zusammengefasst bilden diese Geräte das Ara-Netzwerk, ein Ökosystem, in dem jeder teilnehmen und davon profitieren kann.

Grundsätzlich besteht das Netzwerk aus einer sich überschneidenden Gemeinschaft von Konsumenten, Service-Anforderern, Serviceanbietern und Softwareentwicklern, die jeweils eigene Anreize zur Übernahme haben. Mit Ara steht Serviceanforderern eine riesige Reserve an Rechenressourcen zusammen mit einer ständig wachsenden Bibliothek verteilter Services zur Verfügung. Serviceanbieter, die bereits für ihre Geräte, sei es ein Smartphone, ein Laptop oder eine Spielekonsole, bezahlt haben, können damit beginnen, ungenutzte Ressourcen zu vermieten. Die einzige Voraussetzung, um Belohnungen zu verdienen, besteht darin, eine kleine Einzahlung zu leisten, die als Zugriff auf dem Konto fungiert. Dieser Zugriff kann jederzeit zurückgezogen werden, ist jedoch erforderlich, um Belohnungen zu verdienen und einzulösen. Softwareentwickler können die beispiellose Skalierung von Aras Ökosystem nutzen, um heftige Rechenaufgaben zu bewältigen und neuartige verteilte Services zu erstellen, an denen Anforderer und Anbieter teilnehmen können. In der Zwischenzeit können die Konsumenten ihrem täglichen Leben genauso wie immer nachgehen, während sie dafür belohnt werden, die Shows zu sehen und die Musik anzuhören, die sie lieben.

Jeder, der über unbenutzte Computerressourcen verfügt, kann sofort als Service-Erbringer fungieren, um Belohnungen für die Verteilung von Inhalten zu erhalten. Wer nach Remote-Ressourcen sucht, kann die dezentralen Services von Ara anfordern und die Sicherheit, Dateiverfügbarkeit und Liefergeschwindigkeiten zu einem Bruchteil der Kosten nutzen im Vergleich zu herkömmlichen Cloud-Computing-Service-Anbietern. Damit Ara die Kosten für den Kauf und die Verwaltung von Infrastruktur wegfallen, können Content-Ersteller aller Art davon profitieren, sei es der Indie-Künstler, der sein neues Album selbst veröffentlichen kann, ohne über ein Plattenlabel zu gehen, bis zu einem großen Medienkonzern, der nicht mehr über Aggregatoren gehen muss, um sein Publikum zu erreichen. Ara vertraut den Ressourcen, die von Mitgliedern des Netzwerks bereitgestellt werden; je größer das Netzwerk anwächst, desto robuster und effizienter wird es.

1.3 Plattform-Services

Die Ara-Plattform besteht aus drei (3) Kerndiensten und -systemen:

1. **AraID:** AraID erstellt sichere, dezentralisierte und überprüfbare globale Identitäten für alle Agenten und Inhalte auf der Ara-Plattform und gibt somit die Kontrolle der Daten an ihre rechtmäßigen Eigentümer zurück.
2. **Dezentralisierte Identität (DCDN):** DCDN dient als Aras Netzwerk von zugrunde liegenden Peer-to-Peer-, sicheren verteilten Dateisystemen und Speichernetzwerken (AFSs), die Inhaltsintegrität, Anreize, Versionsverwaltung und

dezentralisierte Identitäten unterstützen.

3. **Protocol Suite:** Ara ist über eine sichere Protokoll-Suite verbunden, die eine vertrauensfreie Interoperabilität zwischen DCDN, AraID und der Ethereum Blockchain möglich macht.

2. Plattform-Übersicht

Das Konfliktfreies Datei-System-Netzwerk (Conflict-Free File System Network (CFSNet)) ist das Rückgrat von Aras Peer-to-Peer-verteiltem Dateisystem, AraID und Dezentralisiertes Content-Delivery-Netzwerk (Decentralized Content Delivery Network (DCDN)). Durch die Verwendung einer zugrundeliegenden Merkle-Baumstruktur und des Syncable Ledger of Exact Events Protokoll-Dateiformats (Syncable Ledger of Exact Events Protocol (SLEEP)) [1] adressiert CFSNet viele Probleme, die beim traditionellen Dateitransport, sowohl beim Client-Server als auch P2P, auftreten verbessert vorhandene Technologien wie IPFS durch kryptographisch abgesicherte Inhaltsintegrität sowie Versionsverwaltung und Versionsgeschichte. Das Netzwerk besteht aus isolierten Dateisystemen, die CFS genannt werden. Darüber hinaus implementiert jede CFS-Instanz eine Teilmenge der Datei-System Hierarchie-Standard (Filesystem Hierarchy Standard (FHS)) [8] unterstützenden Partitionen und ermöglichen es jedem Verzeichnis, als eigenständiges CFS-Archiv mit eigenen Zugriffsebenen zu existieren. Von diesen Partitionen benutzt AFS die Partitionen `/home` und `/etc`, um AFS-Inhalte beziehungsweise Metadaten zu speichern. Jede CFS-Partition ist im gesamten Netzwerk mit einem eindeutigen öffentlichen `Ed25519` 32-Byte-Schlüssel, der zum Zeitpunkt der Erstellung generiert wurde, öffentlich identifizierbar. Ein öffentlicher CFS-Schlüssel gewährt schreibgeschützten Zugriff auf das Dateisystem, wobei nur der Inhaber des privaten Schlüssels den darin enthaltenen Inhalt aktualisieren und veröffentlichen kann.

2.1 AraID

AraID ist verantwortlich für die Erstellung und Lösung von sicheren und verifizierbaren dezentralisierte Repräsentationen für alle Benutzer und Inhalte auf der Ara-Plattform. Voll kompatibel mit der W3C-Dezentralisierte Kennung (Decentralized Identifier (DID))-Spezifikation [15], verwendet AraID DID Deskriptor-Objekt oder kurz DDOs, um Benutzer und Inhalte darzustellen (siehe *Abbildung 1*). DDOs sind einfache JSON-LD-Dokumente, die Methoden für Authentifizierung und Autorisierung sowie andere Identitätsattribute definieren, einschließlich Serviceendpunkten und privaten Kommunikationskanälen, die vom Eigentümer kontrolliert werden [15]. Da DDOs niemals Persönlich identifizierbare Informationen (Personally-Identifiable Information (PII)) speichern [15], identifizieren diese Serviceendpunkte und Kommunikationskanäle sichere Methoden, um sie zu erhalten und ermöglichen somit Entitäten die Eigenständigkeit über ihre privaten Daten und Online-Identitäten.

2.1.1 Dezentralisierte Identität

Für alle Benutzer und Inhalte auf der Ara-Plattform wird eine AraID generiert in Form von:

- `did:ara:ee93189c629cdaf94 9fd57bac5b005b916936d2a5c6806 40fd1aedc8315730a0`

AraID implementiert eine Universelle Resolver-`Methode`, bezeichnet durch die zweite Komponente der DID (`ara` oben) als Teil des Dezentralisierten Identitäts-Fundierungssystems [11]. Diese `Methode`, die auch als Treiber bekannt ist, definiert, wie DIDs und DDOs innerhalb der Ara-Plattform aufgelöst werden. Im Gegensatz zu Internet-URIs benötigen DIDs keine zentrale Autorität für Registrierung oder Kontrolle und bilden eine bijektive Korrespondenz mit DDOs statt der nicht-injektiven, nicht-surjektiven Beziehung, die in TCP/IP und DNS gefunden wird.

Der Kern der AraID-Sicherheit wird kryptographisch unter Verwendung von Dezentralisierte Public-Key-Infrastruktur (Decentralized Public Key Infrastructure (DPKI)) [13] aufrechterhalten, wobei `Ed25519` öffentliche Schlüssel benutzt werden in sowohl dem `id` Teil des DID (`ee9318`... oben) und dem öffentlichen Schlüssel des CFS, in dem das dazugehörige DDO gespeichert wird. Diese Dokumente enthalten eine `publicKey` (öffentlicher Schlüssel) Eigenschaft, die verschiedene Schlüssel für digitale Signaturen, Verschlüsselung und andere kryptografische Operationen

enthält. Wenn eine Identität erstellt wird, wird dieses Array mit dem Schlüssel der Eigentümeridentität sowie dem öffentlichen Schlüssel des Ethereum-Kontos gefüllt.

Für AFS AraIDs wird ebenso der öffentliche Schlüssel der `/etc` Partition, die die dazugehörigen Metadaten enthält, gespeichert. Da der Schlüssel dafür in der AFS DDO gespeichert ist, kann er von jedem Anforderer, der die AFS DID hat, aufgelöst werden.

Jedes Mal, wenn eine neue Identität generiert wird, wird eine mnemonische Phrase verwendet, um das Schlüsselpaar auszustreuen (seed). Das Mnemonic wird an den Besitzer zur sicheren Aufbewahrung und zur einfachen Verwaltung des privaten Schlüssels zurückgegeben, wodurch Entitäten die Eigentümerschaft von DIDs leicht überprüfen und Konten ohne Einsatz des privaten Schlüssels wiederherstellen können.

Identitätsarchivierung und -auflösung

Wenn eine Identität erstellt wird, wird sie zunächst lokal geschrieben, so dass jede lokale Auflösung den Cache überprüfen kann, bevor sie auf das Netzwerk zurückfällt. Bevor jedoch eine Identität remote aufgelöst werden kann, muss sie zuerst archiviert werden. Ara betreibt Archivierungsknoten, deren Aufgabe es ist, diese Identitäten für zukünftige Auflösung zu speichern.

Ähnlich wie die Archivierer-Knoten führt Ara auch Auflösungsknoten aus, die für die Abfrage der Archivierer nach angeforderten DDOs zuständig sind. Auflösungsanfragen versuchen zuerst, Identitäten, die möglicherweise auf der Festplatte gespeichert sind, lokal aufzulösen, bevor sie ins Netzwerk gehen, um entfernte Archivierer, die die betreffende AraID archiviert haben, anzugehen.

```
{
    'ddo': {
        '@context': 'https://w3id.org/did/v1',
        'id': 'did:ara:ee9318...',
        'authentication;: [{
           'type': 'Ed25519SignatureAuthentication2018',
           'publicKey': 'did:ara:ee9318...#owner'
        }],
        'publicKey': [{
           'id': 'did:ara:ee9318...#eth',
           'type': 'Secp256k1VerificationKey2018',
           'owner': 'did:ara:ee9318...,
           'publicKeyBase58': 'H3C2AVvLMv6gmMNam...'
        }],
        'service': {
           'ens': 'https://etherscan.io/enslookup',
        }
        ...
    }
}
```

Abbildung 1: *Example DDO*

Ethereum-Konto

Jede Identität wird mit einem Ethereum-Konto und einer zugeordneten Ethereum-Wallet erstellt, die mit einem generierten Zufallsmnemonic, das während der Identitätsgenerierung generiert wurde, wiederhergestellt werden kann. Da der Ethereum-Account und die Identität selbst deterministisch mit diesem Mnemonic erstellt werden, kann ein Benutzer seine vollständige Identität einschließlich seines Ethereum-Accounts und seiner Wallet mit nur diesem Mnemonic wiederherstellen.

AraID wurde designt, um alle Konten zu unterstützen, die durch Kryptografie mit öffentlichen Schlüsseln gesichert sind. Es ist daher agnostisch für die Arten von Kryptowährungskonten, die es unterstützen kann, und es kann leicht mit jeder Art von Kryptowährungs-Wallets verknüpft werden.

2.2 Dezentralisiertes Content-Delivery-Netzwerk (DCDN)

DCDN ist Aras Lösung für skalierbare, dezentrale Hypermedia- und Digitale Asset Distribution. Im Kern besteht DCDN aus einem Netzwerk von Ara File Systems (AFSs), CFS-Implementierungen, die Inhalte und die dazugehörigen Metadaten enthalten.

2.2.1 Ara-Dateisystem (Ara File System (AFS)

AFS ist eine Art von CFS, die auf die spezifischen Anforderungen und Ziele von Ara zugeschnitten ist. AFS nutzt zwei bestehende Partitionen, die CFS implementiert, die `/home` und `/etc` Partitionen. Diese Partitionen, die als Untergruppe der FHS [8] implementiert sind, sind für die rohen Binärdaten bzw. die Metadaten des Inhalts verantwortlich. Auf die `/home` Partition kann nur zugegriffen werden, nachdem ein Benutzer den Inhalt von AFS erworben oder gewährt hat. Auf die `/etc` Partition jedoch, die die Metadaten enthält, kann unabhängig vom Inhalt zugegriffen werden. Der AFS-Besitzer kann ein Schema für die Metadaten definieren, so dass es von einem Anforderer analysiert werden kann. Das Protokoll erzwingt keinen strengen Standard, wie Metadaten strukturiert sein sollten, aber wir empfehlen Schema.org als Verweis auf bestehende Paradigmen, um die Interoperabilität zwischen dezentralen Diensten bestmöglich zu unterstützen.

Wenn ein AFS anfänglich erstellt wird, wird eine AraID mit einem zufälligen `BIP39` [5] 12-Wörter Mnemoniksatz erstellt. Die generierte DID wird als öffentlicher Schlüssel des AFS verwendet, und die entsprechende DDO `Authentifizierungs`-Eigenschaft wird so geändert, dass sie die DID des Eigentümers enthält. Auf diese Weise kann der Besitzer eines AFS von der Auflösung seiner DID ermittelt werden.

Ein AFS wird für alle in das System eingebrachten Inhalte erstellt. Dies kann eine einzelne Datei wie ein Film oder eine Sammlung von Dateien wie ein Spiel sein. Zur kryptografischen Überprüfung der Eigentumsrechte an Inhalten werden zwei Sätze von Byte-Puffern in die Ethereum-Blockchain geschrieben. Zuerst die `metadata.tree` Eingaben, die den serialisierten Merkle-Baum der in der Datenspeicherschicht enthaltenen Daten darstellen. Als zweites die `metadata.signatures` Datei, die Signaturen der Rootknoten des serialisierten Baums enthält.

2.2.2 Token-Verwendung

Zu Beginn bietet der Besitz von Ara-Tokens in Bezug auf DCDN die folgenden Funktionen:

1. Die Fähigkeit, Inhalte im Netzwerk zu kaufen und herunterzuladen.
2. Die Möglichkeit, an der P2P-Dateiübertragung teilzunehmen und Belohnungen für jeden Inhalt zu verdienen, indem eine Ara-Einzahlung eingereicht wird, die als Halt fungiert.

2.3 Ara Protokoll Suite

Die folgenden Unterabschnitte definieren die Kernprotokolle der Plattform, beschreiben jeden Teil des Systems im Detail und erklären die Interoperabilität zwischen ihnen.

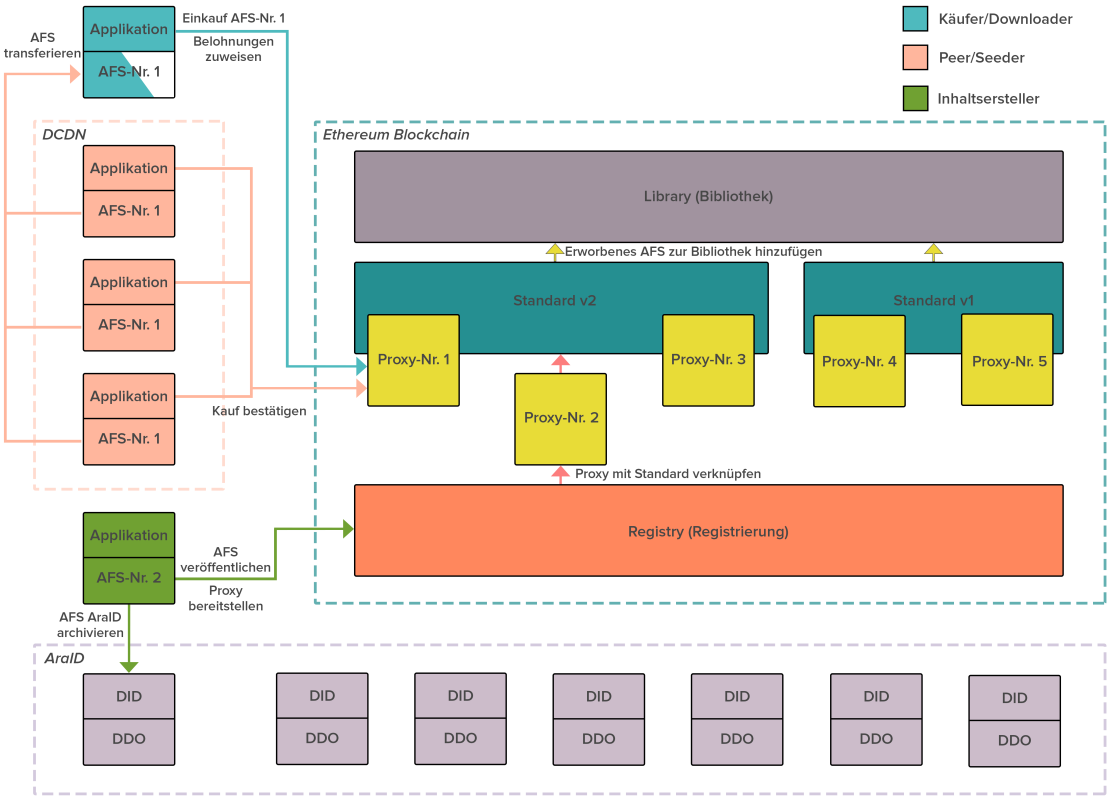

Abbildung 2: *Illustration des Ara-Protokolls*

2.3.1 Belohnungen und Anreize

Herkömmliche Peer-to-Peer-Filesharing-Systeme wie BitTorrent basieren auf altruistischem Verhalten und bieten keine effektiven Anreize [7] für Peers, so viel in das Netzwerk hochzuladen, wie sie herunterladen. Dadurch entsteht ein Ungleichgewicht, bei dem *Leechers* (Benutzer, die eine verteilte Datei herunterladen) einen *Schwarm* (alle Peers, die eine verteilte Datei herunterladen oder hochladen) leicht dominieren können. Dieses Ungleichgewicht, eine Form von Trittbrettfahrerproblem [6], ist in einem gesunden Netzwerk unerwünscht, da Leecher oft auf Kosten anderer von dem Netzwerk profitieren, ohne etwas im Austausch anzubieten. Ara implementiert ein Belohnungssystem als Anreizmechanismus, um diese Netzwerkineffizienz abzuschwächen und die Dateiverfügbarkeit zu verbessern, indem für jeden Download kleine Kosten berechnet werden und diese Kosten als Belohnung an jeden Peer verteilt werden, der den Download ausstreut. Abhängig vom Zahlungsmodell könnten diese Kosten als Belohnungszuweisung in die Gesamtkosten des Inhalts mitinbegriffen werden; für „kostenlose“ Inhalte können diese Kosten traditionelle Anzeigen oder Datensammlungen ersetzen (wie Nutzer heute für „kostenlose“ Inhalte bezahlen). Da jeder Download zu einer Belohnungsquelle

wird, können Netzwerkteilnehmer im Laufe der Zeit viel mehr von den Belohnungen verdienen, als sie vorab für den Download bezahlen.

2.3.2 Dateilieferung (File Delivery)

Dateilieferung ist der wichtigste Mechanismus, um das Inhaltslieferungs (Content-Delivery)-Netzwerk von Ara aufrecht zu erhalten und für die Teilnehmer, um Belohnungen zu verdienen. Das File-Delivery-Protokoll von Ara beginnt mit einem vierstufigen Handshake.

1. Alice, der Inhaltsanforderer, sendet eine Download-Anfrage für einen Inhaltsteil über ein Netzwerkerkennungsprotokoll (CFSNet implementiert mehrere Strategien, einschließlich mDNS und BitTorrent).
2. Bob, ein Lizenzprüfer und Inhaltslieferant, empfängt die Übertragung und antwortet mit seiner Dateiverfügbarkeit.
3. Alice wählt Peers aus dem Pool (dem Schwarm) von Antworten aus und sendet eine Nachricht mit ihrem öffentlichen Zwischenschlüssel zusammen mit ihrer DID.
4. Bob überprüft kryptografisch Alices Nachricht und dass sie eine Lizenz für das zugrunde liegende AFS erworben hat.

Sobald der Handshake abgeschlossen ist, beginnt die Dateiübertragung.

2.3.3 Smart-Verträge

Ara startet zunächst auf Ethereum mainnet, wo Smart-Verträge als zentraler Bestandteil der Protokollsuite von Ara dienen werden. Diese Smart-Verträge vermitteln und erleichtern die Interoperabilität zwischen DCDN, AraID und der Applikationsschicht und stellen sicher, dass alle nicht vorübergehenden Eigenschaften und Entitäten auf der Plattform in der Ethereum-Blockchain einschließlich der folgenden registriert sind:

- Veröffentlichte Inhalte
- Einkäufe
- Belohnungen
- Ara-Kontostand

Aras Smart-Vertragsarchitektur wurde im Hinblick auf Sicherheit und Modifizierbarkeit entwickelt. Um die sich ändernden Konzepte zu unterstützen, wie AFSs verkauft und gekauft werden sollten, wie Prämien behandelt und verteilt werden sollten und wie Zahlungen innerhalb des Systems verarbeitet und weitergeleitet werden sollten, setzt Ara einen `Proxy-Vertrag` für jedes veröffentlichte AFS ein. `Proxies` werden über einen `Registrierungsvertrag` bereitgestellt, wo sie einer bestimmten Version eines `AFS-Standards` zugeordnet sind, der die Geschäftslogik für AFS definiert. Während die Bereitstellung des gesamten `AFS-Standards` für jedes AFS kostspielig und schwierig zu aktualisieren wäre, das AFS würde im Wesentlichen an einen bestimmten Standard gebunden sein, ermöglicht die Proxy-Architektur die Bereitstellung eines einzelnen `Proxys` für die Lebensdauer eines AFS und Aktualisierungen, indem man ändert auf welche `AFS Standardversion` es sich bezieht. Proxy-Architektur stellt auch sicher, dass nur registrierte `Proxy`-Adressen (d. H. Gültiger AFS-Inhalt) zu Benutzerbibliotheken in dem `Bibliotheksvertrag` hinzugefügt werden können.

AFS Standard

Der `AFS-Standard` ermöglicht AFSs eine definierte, strukturierte und eigenständige Präsenz in der Ethereum-Blockchain. Es beinhaltet Methoden für Einkauf und Belohnungen, sowie Methoden, wie die `Baum-` und `Signatur`-Dateien von dem `Metadaten` SLEEP-Register gespeichert werden. Das `Metadaten` SLEEP-Register speichert Metadaten über Inhalte innerhalb eines AFS, inklusive Dateinamen, Größen und Zulassungen, während das `Inhalts` SLEEP-Register speichert den unverarbeiteten binären Inhalt der Dateien. Innerhalb des `Metadaten` Register, repräsentiert die `Baum`-Datei den seriellen Merkle-Baum, der die Daten im `Inhaltsregister` ausmacht, und die `Signaturendatei` speichert die signierten Stämme des serialisierten Baums. Während bei CFS diese Dateien auf der Disk gespeichert und von dieser gelesen werden, werden sie mit AFS in die Ethereum-Blockchain geschrieben und dar-

aus gelesen. Da AFSs mit diesem Standard über ihre eigene `Proxy` kommunizieren, können viele verschiedene `AFS-Standards` koexistieren, was Content-Ersteller erlaubt, den Standard auszuwählen, der ihren Anforderungen am besten entspricht.

Die Benutzung von `Proxies` trennt Logik vom Speicher, der `AFS-Standard` dient als logische Schicht für jedes AFS, das diese Version des Standards verwendet, und jede `Proxy` dient als Speicherschicht für ein einzelnes AFS. `AFS-Standards` müssen zumindest eine `AFS-Standard` Abstraktklasse einrichten, was die Implementierung von Preis-, Einkaufs-, Belohnungs- und Speicherfunktionen erzwingt.

Bei dem einfachsten (und Standard) AFS-Standard können Preise nur durch den `Besitzer` des AFS geändert werden. Beim Kauf wird dieser Preis von der Ara-Wallet des Käufers an die Ara-Wallet des Besitzers überwiesen. Der `Basis-ASF-Standard` erzwingt Unterstützung für Belohnungsbudgets, die vor dem Download abgegeben werden müssen. Sobald der Download abgeschlossen ist, wird das Budget zwischen den teilnehmenden Peers aufgeteilt, die dann ihre Prämien einlösen können, sofern sie den dafür erforderlichen Kontostand (Hold) nicht zurückgezogen haben.

Nach Ermessen von Inhaltsentwicklern können `AFS-Standards` auch eine Vielzahl von anpassbaren Commerce-Steuerelementen unterstützen:

1. **Lizenzgebühren**: Käufe können angepasst werden, um Erlöse auf viele verschiedene Ara-Konten nach Prozentaufteilung zu verteilen.
2. **Großeinkäufe**: Preise können basierend auf der gekauften Menge gestuft werden.
3. **Weiterverkaufsbedingungen**: Gekaufte Inhalte können mehrmals zu einem Mindestverkaufspreis weiterverkauft werden, wie vom Ersteller des Inhalts angegeben.
4. **Eigentumsübertragung**: Der Eigentümer eines AFS kann das Eigentumsrecht leicht auf eine andere Ethereum-Adresse übertragen.
5. **Vorbestellungen**: Inhalte können gekauft werden, bevor sie zum Download verfügbar sind. Käufer können im Voraus ein Prämienbudget einreichen, damit sie mit dem Herunterladen eines AFS beginnen können, sobald es verfügbar ist.
6. **Scarcity**: Inhaltsentwickler können eine maximale Anzahl von Verkäufen für einen AFS definieren, nach denen der AFS `ungelistet` und nicht mehr zum Kauf verfügbar ist.

Diese Commerce-Steuerelemente bieten Content-Entwicklern aller Art die Möglichkeit, ihre eigenen Geschäfts- und Umsatzmodelle zu definieren, die genau auf ihre Bedürfnisse und Spezifikationen zugeschnitten sind. Die Steuerungen können zu interessanten neuen Modellen kombiniert werden, die auf herkömmliche Art nur schwer zu realisieren wären. Zum Beispiel kann jemand, der gerne Musik remixt, die Tracks des ursprünglichen Künstlers mit definierten Wiederverkaufsbedingungen und minimalen Wiederverkaufspreisen kaufen, die Songs remixen und die remixten Versionen verkaufen, während er immer noch dem ursprünglichen Künstler auszahlt. Während früher die Kombination dieser Arten von Kontrollen eine riesige Menge an Zeit, Kapital und rechtlicher Beteiligung erfordert hätte, die für kleineren Ersteller von Inhalten wesentliche Zugangsbarrieren darstellten, stehen sie jetzt jedem kostenlos zur Verfügung.

Registry (Registrierung)

Als Teil der Proxy-Architektur dient der `Registry-Vertrag` zwei Hauptfunktionen:

1. Es dient als `Proxy`-Fabrik
2. Es rückverfolgt alle `AFS-Standard` Versionen

Wenn ein AFS zuerst herausgegeben wird, benutzt die `Registry` eine `Proxy` für dieses AFS und stellt eine Beziehung zwischen ihm und einem bestimmten `AFS-Standard` her. Die `Proxy` sieht die `Registry` ein für die Adresse ihres entsprechenden `AFS-Standards`. Dies geschieht

jedes Mal, wenn sie aufgerufen wird, und der Aufruf wird an diese Adresse delegiert, wo er verarbeitet und an die `Proxy` zurückgegeben wird.

Library (Bibliothek)

Das Ara-Netzwerk nutzt den `Bibliotheksvertrag`, um eine kanonische Wahrheitsquelle für AFSs zu erstellen, auf die ein Benutzer Zugriff hat, egal ob gekauft oder nicht. Wenn Inhalt gekauft wird, fügt die `Einkaufsfunktion` in dem `AFS-Standard` automatisch das AFSs DID in die Bibliothek des Einkäufers in dem `Bibliotheksvertrag` ein. Dies ermöglicht jedem Service, der Informationen über die Bibliothek eines Benutzers benötigt, den Vertrag nach diesen Informationen abzufragen. Das AFS DID, das in der Blockchain gespeichert ist, ermöglicht es jedem Service, den zugrunde liegenden Inhalt aufzulösen. Die `Bibliothek` erzwingt, dass nur registrierte `Proxies` ihre entsprechenden AFS zu einer Benutzerbibliothek hinzufügen können, um sicherzustellen, dass niemand die Bibliothek eines anderen Benutzers ohne deren Zustimmung manipulieren kann.

3. Zukünftige Entwicklung

3.1 Module

Die Ara-Plattform ist im Wesentlichen agnostisch zu den Arten verteilter Services, die darüber laufen können. Module sind verteilte und/oder dezentrale Dienste, die die Modul-APIs implementieren und innerhalb der Plattform synonym verwendet werden können. Ähnlich wie der Token-Standard ERC-20 es allen Token auf Ethereum ermöglicht, von anderen Anwendungen wiederverwendet zu werden [14], ermöglichen die Modul-APIs allen verteilten Services, die die Schnittstelle implementieren, auf der gesamten Plattform verwendet zu werden. Dies fördert die Bildung einer Entwicklergemeinschaft, die sich dem Aufbau eines Ökosystems verteilter Services widmet, von denen jeder die Möglichkeit hat, die Belohnungs-, Kauf- und Zahlungssysteme von Ara zu nutzen, was im Wesentlichen eine lohnende verteilte Servicewirtschaft bildet. Von Modulen, die das Belohnungssystem nutzen wollen, wird erwartet, dass sie eine zusätzliche Smart-Vertrag-API implementieren, in der sie ihren eigenen Belohnungsmechanismus und ihre eigene Methodik definieren. Jeder Smart-Vertrag des Moduls speichert seine eigene Belohnungszuordnung, die durch die Nutzung des verteilten Service angesammelt wurde, und verteilt sie entsprechend.

3.2 Ara Namen-System (ANS)

Ähnlich wie die Domain-Namen-System (Domain Name System (DNS)) [9] ist ANS eine dezentrale Möglichkeit, Zertifikate im Ara-Netzwerk zu registrieren, abzufragen, aufzurufen oder zu sperren. Während DNS als Teil der Anwendungsebene des Internets sitzt und von Menschen lesbare URLs in zugrundeliegende IP-Adressen auflöst, so dass ein Benutzeragent (z. B. ein Webbrowser) den angeforderten Inhalt erhalten und rendern kann, lösen ANS lesbare Namen in DIDs für die endgültige Auflösung in DDOs auf. ANS verwendet verdeckt den Identitäts-Archivierer und Resolver für die zweite Phase der Auflösung, um DDOs von DIDs bereitzustellen. ANS ist im Wesentlichen sowohl ein Archivierer als auch ein Resolver für menschlich lesbare URLs. Eine Beispielanwendung von ANS könnte das Bereitstellen von DDOs aus Hostnamen im Kontext eines auf Ara aufgebauten Webbrowsers sein.

Um zwischen den verschiedenen Datensatztypen zu unterscheiden, speichert jeder Datensatz einen `TYP`-Ressourceneintrag, ähnlich wie DNS seine eigenen Datensätze klassifiziert [17]. Das `TYP`-Feld wird durch einen numerischen Wert dargestellt, der es ermöglicht, zukünftig andere Arten von Datensätzen in ANS zu speichern. Die folgende Tabelle beschreibt den Datensatz `TYP`:

TYPE	Value	Description
USR	00	User
PCT	01	Published Content

Jeder Superknoten-Hub, der ANS umfasst, führt eine HyperDB-Instanz aus [2]. Eine verteilte, hochskalierbare Datenbank wie HyperDB bietet mehrere Funktionen, die sie für ein System wie ANS geeignet machen. Die erste ist HyperDBs Verwendung von tries: Suchbäume, wobei jeder Knoten ein Präfix zu seinen untergeordneten Knoten ist. Indem wir Namen mit tries speichern, können wir garantieren, dass selbst mit Tausenden von Einträgen in der Datenbank Lookups kostengünstig und schnell sind. Lookups in tries sind `O(n)` wo `n` die Länge des Schlüssels ist, nachdem gesucht wird. HyperDB verwendet auch Vektoruhren, die die Kausalität von Ereignissen innerhalb eines verteilten Systems verfolgen, um Fälle zu verhindern, in denen Knoten desynchronisiert werden [10].

4. Danksagung

Dieses Papier wurde ermöglicht durch Littlstar und Token Foundry. Ein besonderer Dank geht an Logan Dwight, Andrew Grathwohl und Brandon Plaster für ihre Beiträge.

Akronyme

AFS Ara File System. 1, 3, 5–7, 9–11

ANS Ara Name System. 12

CFS Conflict-Free File System. 5–7

CFSNet Conflict-Free File System Network. 5

DCDN Decentralized Content Delivery Network. 3–6

DDO DID Descriptor Object. 5–7, 12

DID Decentralized Identifier. 5–7, 11, 12

DNS Domain Name System. 5, 12

DPKI Decentralized Public Key Infrastructure. 5

FHS Filesystem Hierarchy Standard. 5, 7

PII Personally-Identifiable Information. 5

SLEEP Syncable Ledger of Exact Events Protocol. 5

Literatur

[1] Code for Science Buus, Ogden. Sleep - syncable ledger of exact events protocol. https://github.com/datproject/docs/blob/master/papers/sleep.pdf, Aug 2017.

[2] Mathias Buus. Hyperdb. https://github.com/mafintosh/hyperdb, Aug 2017.

[3] Cisco. Cisco visual networking index predicts global annual ip traffic to exceed three zettabytes by 2021. https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1853168, Jun 2017.

[4] Stewart Clarke. Piracy set to cost streaming players more than $50 billion, study says. http://variety.com/2017/tv/news/piracy-cost-streaming-players-over-50-billion-1202602184/, Oct 2017.

[5] Palatinus et al. Mnemonic code for generating deterministic keys. https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki, Sept 2013.

[6] Russell Hardin. The free rider problem. https://plato.stanford.edu/entries/free-rider, May 2003.

[7] Ahamad Jun. Incentives in bittorrent induce free riding. https://disco.ethz.ch/courses/ws0506/seminar/papers/freeriding_incentives.pdf, Aug 2005.

[8] The Linux Foundation LSB Workgroup. Filesystem hierarchy standard. https://refspecs.linuxfoundation.org/FHS_3.0/fhs-3.0.pdf, Mar 2015.

[9] Paul Mockapetris. Domain names - implementation and specification. https://tools.ietf.org/html/rfc1035, Nov 1987.

[10] Multiple. Vector clock. https://en.wikipedia.org/wiki/Vector_clock.

[11] Markus Sabadello. A universal resolver for self-sovereign identifiers. https://medium.com/decentralized-identity/a-universal-resolver-for-self-sovereign-identifiers-48e6b4a5cc3c, Nov 2017. Accessed on 2018-04-24.

[12] Stephen E. Siwek. The true cost of sound recording piracy in the us economy. https://www.riaa.com/wp-content/uploads/2015/09/20120515_SoundRecordingPiracy.pdf, Aug 2007.

[13] Rebooting the Web-of Trust. Decentralized public key infrastructure. http://www.weboftrust.info/downloads/dpki.pdf, Dec 2015. Accessed on 2018-04-19.

[14] Buterin Vogelsteller. Erc-20 token standard. https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md, Nov 2015.

[15] W3C. Decentralized identifiers. https://w3c-ccg.github.io/did-spec, Apr 2018. Accessed on 2018-05-01.

[16] Music Business Worldwide. Why does the riaa hate torrent sites so much? https://www.musicbusinessworldwide.com/why-does-the-riaa-hate-torrent-sites-so-much/, Dec 2014.

[17] Inc ZyTrax. Dns resource records (rrs). http://www.zytrax.com/books/dns/ch8/, Oct 2015.

Anhang

I. Reife Ara-Plattform Token-Wirtschaft (Entwurf)

Übersicht

Traditionelle Cloud-Dienste haben aufgrund ihrer Flexibilität, Agilität und Kosteneinsparungen gegenüber dem Erwerb und der Verwaltung von interner Infrastruktur an Bedeutung gewonnen. Viele Cloud-Dienste verwenden notorisch komplexe und obskure Preismodelle, die langfristige Verpflichtungen und Verträge beinhalten und sind oft individuell pro Kunde ausgehandelt, was die Flexibilität und Agilität, die sie ursprünglich bieten sollten, untergräbt [1]. In den letzten Jahren haben P2P-CDNs mit den aufkommenden SaaS-Hybridlösungen für die Videoübertragung an Bedeutung gewonnen. Während diese SaaSs eine hochskalierbare Lösung mit einem einfacheren Preismodell durch Nutzung der Maschinen von Video-Betrachtern etablieren, halten sie mehrere Zentralisierungsquellen aufrecht, nämlich durch ihr Geschäftsmodell und ihre Zuordnung von Nutzern als „Bürger zweiter Klasse“, wobei die Nutzung ihrer Maschinen ohne ihre Zustimmung oder finanziellen Ausgleich stattfindet. Ara bringt es noch einen Schritt weiter und belohnt die Netzwerkteilnehmer für die Nutzung ihrer Maschinen. Um die bestehenden klassischen Cloud-Infrastrukturkosten zu ersetzen, implementiert die Ara-Plattform ein natives Protokoll-Utility-Token: das Ara-Token. Dieses Token kann auf der Ara-Plattform verwendet werden, um kryptoökonomische Anreize für ein gesundes und ehrliches Netzwerkverhalten zu schaffen, um eine direktere Interaktion zwischen Inhaltskonsumenten und Erzeugern zu ermöglichen und die Akzeptanz der Plattform zu fördern. Der Ara-Token kann als Verkapselung des Wertes angesehen werden, den Mitglieder des Netzwerks bereitstellen, wobei jedes belohnte Token einen geringfügigen Anstieg des Netzwerk-Nutzens darstellt.

Das Ara-Token

Verteilte Dienste, die unter Verwendung von Aras SDKs, bekannt als Module, erstellt wurden, können im gesamten Ara-Netzwerk gekauft, verkauft, angefordert und erfüllt werden. Modulaufgaben werden an Peers im Netzwerk ausgelagert, die nach erfolgreichem Abschluss mit Ara-Token kompensiert werden können. Um einen offenen und wettbewerbsfähigen Markt zu fördern, ermöglicht es Ara Service-Anforderern, Belohnungszuweisungen oder Prämien für von ihnen angeforderte Dienste zu definieren, sowie Dienstanbietern eine Mindestprämie für die Annahme zu bestimmen. Ähnlich wie bei Amazon Mechanical Turk, einem Marktplatz für Crowdsourcing-Aufgaben, die menschliche Intelligenz erfordern, schafft Ara einen Marktplatz für die Auslagerung verteilter Rechen- oder Netzwerkaufgaben. Module können einmalige On-Demand-Aufgaben sein, wie z. B. verteilte Transkodierung, oder sie können sich ständig wiederholende Dienste sein, z. B. ein P2P-Multiplayer-Gamingserver.

Funktion

Der Ara-Token kann auf verschiedene Arten im gesamten Netzwerk verwendet werden.

- Verbraucher können Ara-Tokens für jede Art von Kauf verwenden, von digitalen Inhalten für Vergnügen bis zu neuen Modulen, an denen sie teilnehmen können
- Serviceanforderer können Ara-Token verwenden, um Jobanfragen einzuleiten und Prämien für den erfolgreichen Abschluss dieser Jobs festzulegen
- Serviceanbieter können Ara-Tokens als Verpflichtung zur Erfüllung einer Aufgabe gegen Belohnungen einzahlen (die Einzahlung kann auf Anfrage zurückerstattet werden, der Anbieter kann jedoch keine Belohnungen mehr verdienen)
- Entwickler können Ara-Token verwenden, um neue Module in das Netzwerk zu verteilen

Da sich jede dieser Rollen sich stark überschneiden, kann ein Serviceanbieter die gleichen Ara-Token als Belohnungen verwenden, indem er eine Aufgabe zum Kauf eines neuen Inhalts erfüllt, genau wie ein Entwickler Ara-Tokens verwenden kann, die durch Modulkäufe erworben wurden, um eine neue Jobanfrage zu initiieren.

Markt-Dynamiken

Da die Netzwerk-Mitglieder bei der Entscheidung, an welchen Aufgaben oder Dienstleistungen sie beteiligt sind, uneingeschränkt agieren können, bildet das Netzwerk einen freien Markt, in dem wirtschaftliche Gleichgewichte entstehen. Jedes Modul wird wahrscheinlich seine eigene Wirtschaft haben, die durch das Verhalten der Anforderer und Anbieter für die Jobs dieses bestimmten Moduls beeinflusst wird. Zum Beispiel können verteilte Video-Transcodierungen für Video-Produzenten eine charakteristische dringende Aufgabe sein, was zu einer Preis-Inelastizität der Nachfrage nach verteilten Video-Transcodierungen führt (d. H. Videoproduzenten ist es relativ gleichgültig, wie viel sie Serviceanbieter möglicherweise entlohnen müssen). Daher treiben die Marktformen eines Verkäufers, in denen Anbieter von verteilten Transcodediensten den Vorteil haben, die Belohnungszuweisung zu bestimmen, die Prämien in die Höhe. In ähnlicher Weise kann ein P2P-Gamingserver-Modul sehr gefragt sein, hat aber relativ wenige Dienstanbieter. Wiederum bildet sich ein Verkäufermarkt, und Prämien steigen an. Ein verbreitetes Modul zum maschinellen Lernen wird andererseits nur von wenigen Personen angefordert, hat jedoch viele geeignete Serviceanbieter. Aufgrund der relativ geringen Nachfrage werden viele Anbieter Chancen verpassen, wenn sie ihre Mindest-Prämienanforderung zu hoch ansetzen. Ein Käufermarkt bildet sich, und Prämien werden niedriger.

Es ist wichtig zu bemerken, dass Module keine Prämien festlegen müssen und kein standardisiertes Modell für die Einrichtung von Prämien existiert. Ziele sind, die Anreize von Serviceanforderern und Serviceanbietern auszurichten, alle Arten von Anreizmodellen zu unterstützen und die unterschiedlichen Fixkosten für Infrastruktur- und Netzwerkfähigkeiten weltweit zu berücksichtigen.

Anreizstruktur

Um besser zu verstehen, wie dieses Modell eine Angleichung der Anreize zwischen Serviceanforderern und -anbietern unterstützt, leiten wir eine allgemeine Beschreibung der wirtschaftlichen Interessen beider Parteien ab. Serviceanforderer möchten, dass ihre Anforderungen zu den geringsten Kosten erfüllt werden, während Serviceanbieter die größtmögliche Anzahl von Services mit dem höchsten Preis optimieren wollen. Mit anderen Worten, es ist im besten Interesse sowohl der Anforderer als auch der Anbieter, den Netzwerk-Nutzen zu maximieren, solange sich beide auf einen Preis einigen. Daher werden die Dienstleistungen, die Prämien und Arbeit am besten ausgleichen, am ehesten erfüllt, was zu einem Marktdruck führt, der sowohl Wettbewerbsvorteile als auch Innovationen bei der Gestaltung von verteilten Dienstleistungen fördert, um die Wirtschaftlichkeit zu verbessern.

Die Vielfalt verteilter Dienste, die auf der Plattform ausgeführt werden können, erfordert Flexibilität bei der Bestimmung der unit-of-work-rewarded (*UWR* (Arbeitseinheit-vergütet), die Basiseinheit der nachweisbaren Arbeit, mit der die Prämiengelder aufgeteilt und belohnt werden) und das Prämienmodell (die Bedingungen, nach denen die Prämien bezahlt werden). Ein P2P-Multiplayer-Gamingserver kann die Anzahl der Anfragen, die er erfüllt, als sein *UWR* benutzen, und ein Gameentwickler, der dieses Server-Modul aufruft, könnte entscheiden, dass ein Abonnement-basiertes, sich wiederholendes Prämienmodell am sinnvollsten ist. Andererseits kann ein verteilter Transcodierungsservice die Anzahl der pro Minute transcodierten Bytes als sein *UWR* verwenden, und ein Videoproduzent könnte eine Prämie pro Transcode auszahlen.

Serviceanbieter können Ara-Tokens einsetzen, um teilzunehmen und Prämien zu verdienen. Wie bei Prämien können Serviceanforderer einen Mindesteinsatz festlegen, den Anbieter ggf. hinterlegen müssen, um sich an dem Dienst zu beteiligen. Der Mindesteinsatzwert sollte ein Indikator für das Engagement sein, das der Service erfordert, und zusammen mit der Prämie zurückgegeben werden, sobald der Service erfolgreich abgeschlossen wurde. Zur Bestimmung von *UWR*, müssen Services ebenso einen Nachweis für die Überprüfung seiner Erfüllung definieren.

Alternativ können Dienstanbieter eine Abonnementgebühr für die Bereitstellung ihrer Ressourcen für einen Service festlegen. Diese dedizierten Anbieter werden als *Superknoten* bezeichnet, und ihre Einsätze werden in einem Smart-Vertrag bis zum Ende des Abonnements treuhänderisch verwaltet. Da Superknoten meist zuverlässiger sind als ihre nicht dedizierten Gegenüber, können sie die Marktdynamik durch die Festlegung ihrer Abonnementgebühren steuern. Superknoten in Bogotá könnten wegen höherer Hardware- und Internetkosten mehr als Superknoten in Los Angeles verlangen.

Netzwerkeffekte

Die Einführung neuer Inhalte in das Netzwerk beinhaltet den Aufruf von DCDN-Superknoten - Ara-Knoten, die für die Redundanz und Verfügbarkeit von Inhalten reserviert sind. Unter der Annahme, dass die Prämie für eine einzelne Datei konstant ist, wirkt sich der geringfügige Anstieg der Dateiverfügbarkeit von einem einzigen Peer auf die potenziellen Belohnungserträge aus dieser Datei für jeden Peer in DCDN (und

allen währungsbasierten P2P-File-Sharing-Systeme mit festen Anreizen [2]) kann mit Hilfe einer Untermodul-Einrichtefunktion modelliert werden, die intuitiv als eine Funktion betrachtet werden kann, die sinkende Erträge beschreibt. Aufgrund dieser Eigenschaft können DCDN-Superknoten ein Abonnement-Prämienmodell verwenden, um den steigenden Opportunitätskosten des Hosting von Inhalten entgegenzuwirken, wenn die Verfügbarkeit ansteigt.

Inhaltsherausgeber können so viele oder so wenige Superknoten in geografischen Standorten ihrer Wahl auf pro Inhaltsbasis aufrufen und abonnieren wie gewünscht. Publisher können daraufhin frei entscheiden, in welchem Umfang ihre Inhalte global verfügbar sein sollen. Dies ermöglicht den Support für den großen Medienverteiler, der alle verfügbaren Superknoten weltweit zur Unterstützung eines globalen Publikums aufrufen möchte, während es ebenso den Indie-Inhalts-Ersteller unterstützt, der seine primäre Zielgruppe als überwiegend europäisch identifiziert und beschließt, europäische Superknoten zu priorisieren. Content-Publisher legen außerdem die Belohnungszuordnung für jeden Inhaltsdownload fest. Somit existiert eine optimale Belohnungszuweisung und Superknotenverteilung, um den gewünschten Grad der Teilnahme (d. H. Dateiverfügbarkeit) zu erreichen.

Verweise

[1] Enterprise Strategy Group (2015, June), *Price Comparison: Google Cloud Platform vs. Amazon Web Services*, https://cloud.google.com/files/esg-whitepaper.pdf

[2] M. Salek, S. Shayandeh, and D. Kempe, *You Share, I Share: Network Effects and Economic Incentives in P2P File-Sharing Systems* https://arxiv.org/pdf/1107.5559.pdf

II. DCDN Kostenanalyse by Lester Kim

Einführung

Um die Streaming-Kosten für einen potenziellen Partner zu berechnen, müssen wir wissen, wie viele Daten B (in Byte) sie pro Zeiteinheit T (in Sekunden) an die Konsumenten liefern müssen. Lassen Sie uns N Gruppen von Uploaderknoten nehmen, wobei $N \in \mathbb{N}$. $\forall n \in \{1, ..., N\}$ die durchschnittliche Bandbreite von Gruppe n ist b_n(in Bytes/Sekunde pro Knoten). Lassen Sie q_n die Anzahl der Gruppen n Knoten sein. Lassen Sie $\mathbf{b} = [b_1...b_N]^\intercal$ sein und $\mathbf{q} = [q_1...q_N]^\intercal$. Somit ist die Anzahl der pro Sekunde gelieferten Bytes begrenzt durch $\frac{B}{T}$

$$g(\mathbf{q}) = \mathbf{b} \cdot \mathbf{q} = \frac{B}{T}. \tag{1}$$

Wir wollen den optimalem $\mathbf{q}^*$ finden, um die Distributionskosten zu verringern $C(\mathbf{q})$. Wenn, $\mathbf{p} = [p_1...p_N]^\intercal$ wobei p_n der Preis pro Knoten für Gruppe n ist, haben wir

$$C(\mathbf{q}) = \mathbf{p} \cdot \mathbf{q}. \tag{2}$$

Gewinnmaximierung des Uploaders

Um $\mathbf{p}$ zu bestimmen, lassen Sie uns das Verhalten einer gewinnmaximierenden Firma betrachten. f soll die Produktionsfunktion mit Energieeingabe E (in kWh) und -ausgabe q (in Knoten) sein. Wir modellieren diese Produktionsfunktion als

$$f(E) = AE^\alpha \tag{3}$$

wobei A ist der Faktor der Produktion (Knoten/kWh$^\alpha$) und $\alpha \in [0, 1]$ ist die Elastizität der Produktion (prozentuale Steigerung der Produktion gegenüber dem prozentualen Anstieg des Inputs) [1].

Lassen Sie P(in kWh/s) die Leistungssteigerung sein, wenn ein Knoten mit dem Hochladen von Daten beginnt. Dies beinhaltet das Senden von Daten mit der Netzwerkschnittstellensteuerung (Network Interface Controller (NIC)), aber kann auch das Einschalten der Maschine (entweder von aus oder aus dem Standby-Modus) beinhalten. Wenn jeder Knoten eine Leistung von P hat, dann kann für einige E ein einziger Knoten für $\frac{E}{P}$ Sekunden laufen. Jedoch hinsichtlich der Zeitbeschränkung und T um die Abeit zu beendigen, muss es $\frac{E}{PT}$ Knoten geben. Daher,

$$A = \frac{D}{(PT)^\alpha} \tag{4}$$

wobei D die gesamte Faktorproduktivität (in Knoten) ist [2].

Lassen Sie p der Preis eines Knotens sein und p_E der Preis von Energie (pro kWh). Die Profitfunktion der Firma π ist

$$\pi(q, E) = pq - p_E E. \tag{5}$$

Bandbreitenkosten werden ignoriert, da es sich um kurzfristige Fixkosten bei der Betrachtung von Sekunden im Gegensatz zu Monaten handelt[1].

Wir wollen den Gewinn des Unternehmens maximieren, wenn mindestens eine Ausgangsanforderung von q; vorliegt

$$\max_{q,E} \ \pi(q, E) \quad \text{s.t. } f(E) \geq q. \tag{6}$$

Um das zu lösen, nehmen wir unseren Lagrange zu

$$\mathcal{L}(q, E, \lambda) = pq - p_E E - \lambda(AE^{\alpha} - q). \tag{7}$$

Wir nehmen partielle Derivate und setzten sie auf Null

$$\frac{\partial \mathcal{L}}{\partial q} = p + \lambda = 0 \tag{8}$$
$$\frac{\partial \mathcal{L}}{\partial E} = -p_E - \lambda A \alpha E^{\alpha - 1} = 0 \tag{9}$$
$$\frac{\partial \mathcal{L}}{\partial \lambda} = q - AE^{\alpha} = 0. \tag{10}$$

Die Lösung dieser Bedingungen erster Ordnung ergibt

$$q^* = \left(\frac{\alpha A^{\frac{1}{\alpha}} p}{p_E} \right)^{\frac{\alpha}{1-\alpha}}. \tag{11}$$

Umgeschrieben (den Asterisk von q fallen lassen) ergibt dies

$$p = \frac{p_E}{\alpha} \Big(\frac{q^{1-\alpha}}{A} \Big)^{\frac{1}{\alpha}}. \tag{12}$$

Diese Formel läßt den Erzeuger wissen, was p sein sollte, um die gewünschte Anzahl von Knoten zu erhalten.

An (12) erkennen wir, dass der optimale Umsatz in Bezug auf q ist

[1] Sogar mit der Bandbreite inbegriffen, haben die Kosten pro Sekunde die gleiche Größenordnung wie die von Energie. In NYC, 50 MBps kosten 3 US$ x 10^{-5}/Sekunde [3].

$$pq = \frac{p_E}{\alpha}\left(\frac{q}{A}\right)^{\frac{1}{\alpha}}. \tag{13}$$

Kostenminimierung des Distributors

Da die Einnahmen für das Unternehmen Ausgaben für den Verbraucher (der Ersteller) sind, können wir (2) schreiben als

$$C(\mathbf{q}) = \frac{p_E}{\alpha}\sum_{n=1}^{N}\left(\frac{q_n}{A_n}\right)^{\frac{1}{\alpha}}. \tag{14}$$

Das Kostenminimierungsproblem des Erstellers ist

$$\min_{\mathbf{q}} \; C(\mathbf{q}) \quad \text{s.t. } g(\mathbf{q}) \geq \frac{B}{T}. \tag{15}$$

Der Lagrange ist

$$\mathcal{L}(\mathbf{q}, \lambda) = C(\mathbf{q}) - \lambda(g(\mathbf{q}) - \frac{B}{T}). \tag{16}$$

Die Konditionen Ordnung sind

$$\frac{\partial \mathcal{L}}{\partial \mathbf{q}} = \frac{\partial C}{\partial \mathbf{q}} - \lambda\frac{\partial g}{\partial \mathbf{q}} = 0 \tag{17}$$

$$\frac{\partial \mathcal{L}}{\partial \lambda} = \frac{B}{T} - g(\mathbf{q}) = 0. \tag{18}$$

Von (14), (4), und (1),

$$\frac{\partial C}{\partial \mathbf{q}} = \frac{p_E T\mathbf{P}}{\alpha^2} \circ (\mathbf{q}^{\circ(1-\alpha)} \oslash \mathbf{D})^{\circ\frac{1}{\alpha}} \tag{19}$$

$$\frac{\partial g}{\partial \mathbf{q}} = \mathbf{b} \tag{20}$$

wobei $(\mathbf{D}, \mathbf{P}) = ([D_1 ... D_N]^\intercal, [P_1 ... P_N]^\intercal)$. „$\circ$“, „$^\circ$“, „$\oslash$“ sind die Hadamard (nach Eingabe) Produkt, Leistung, beziehungsweise Division [4]. Also, $\forall m, n \in \{1, ..., N\}$

$$\frac{P_m^\alpha q_m^{1-\alpha}}{b_m^\alpha D_m} = \frac{P_n^\alpha q_n^{1-\alpha}}{b_n^\alpha D_n}. \tag{21}$$

Daher,

$$b_m q_m = \left(\frac{b_m D_m P_n^\alpha}{P_m^\alpha b_n D_n} \right)^{\frac{1}{1-\alpha}} b_n q_n. \tag{22}$$

Ergibt die Kombination (22) mit (18)

$$\boxed{\mathbf{q}^* = \frac{B\mathbf{b}^{\circ -1}}{T\kappa} \circ (\mathbf{b} \circ \mathbf{D} \oslash \mathbf{P}^{\circ \alpha})^{\circ \frac{1}{1-\alpha}}} \tag{23}$$

$$\boxed{C^* = \frac{p_E T}{\alpha} \left(\frac{B}{T\kappa^{1-\alpha}} \right)^{\frac{1}{\alpha}}} \tag{24}$$

wo

$$\kappa \equiv \sum_{m=1}^{N} \left(\frac{b_m D_m}{P_m^\alpha} \right)^{\frac{1}{1-\alpha}}. \tag{25}$$

Fall: $\alpha = 1$

Wenn, $\alpha = 1$ (23) und (24) werden

$$q_n^* = \begin{cases} \frac{B}{|\Upsilon| T b_n} & n \in \Upsilon \\ 0 & n \notin \Upsilon \end{cases} \tag{26}$$

$$C^* = \frac{p_E B P_n}{b_n D_n} \qquad \text{any } n \in \Upsilon \tag{27}$$

wo

$$\Upsilon \equiv \left\{ n \in \{1, ..., N\} \;\middle|\; n = \arg\max_{1 \le m \le N} \frac{b_m D_m}{P_m} \right\}. \tag{28}$$

$\forall n \in \Upsilon$, jeder Knoten in der Gruppe n würde $\frac{B}{|\Upsilon| q_n^*} (= b_n T)$ an Daten liefern und mindestens $\frac{p_E P_n T}{D_n}$ als Kompensation erhalten. Es gibt jedoch mehrere Lösungen zu $\mathbf{q}^*$. Beispielsweise kann für jede $n \in \Upsilon$ Gruppe n all die Arbeit mit Hilfe von $\frac{B}{T b_n}$ Knoten erledigen.

Beispiel

Lassen Sie uns ein Beispiel in NYC erarbeiten, wo

$$\alpha = 1 \tag{29}$$
$$B = 1 \text{ GB} \tag{30}$$
$$N = 2 \tag{31}$$
$$p_E = \$0.2321/\text{kWh [5]} \tag{32}$$
$$T = 1 \text{ s} \tag{33}$$
$$\mathbf{b} = \begin{bmatrix} 100 \text{ MB/s} \\ 1 \text{ MB/s} \end{bmatrix} \text{ [6]} \tag{34}$$
$$\mathbf{D} = \begin{bmatrix} 1 \text{ node} \\ 1 \text{ node} \end{bmatrix} \tag{35}$$
$$\mathbf{P} = \begin{bmatrix} 200 \text{ W} \\ 2 \text{ W} \end{bmatrix} \text{ [7][8]} \tag{36}$$

um Beispiele von $\mathbf{q}^*$ und C^* für einen Ersteller zu finden. Dann,

$$\mathbf{q}^* = \begin{bmatrix} 5 \text{ nodes} \\ 500 \text{ nodes} \end{bmatrix} \tag{37}$$
$$C^* \approx \$1.29 \text{ x } 10^{-4}. \tag{38}$$

Dies ist 155 bis 659 Mal (99,35% - 99,85%) günstiger als die On-Demand-Preise von AWS Cloudfront (0,020 US$/GB - 0,085 US$/GB) [9]. Jeder Knoten der Gruppe 1 würde 100 MB bearbeiten, während jeder Knoten der Gruppe 2, 1 MB handhaben würde. Jeder Knoten in Gruppe 1 und 2 würde mehr als 1,29 US$ x 10^{-5} beziehungsweise 1,29 US$ x 10^{-7} benötigen.

Um dies zu veranschaulichen, nehmen wir an, dass Netflix ein potentieller Partner ist. Im Jahr 2017 wurden täglich durchschnittlich mehr als 140 Millionen Stunden Netflix-Inhalte angesehen [10]. Ein Netflix-Video ist durchschnittlich eine GB/Stunde [11]. Auf der Ara-Plattform würden die jährlichen Ausgaben von 51,1 Exabyte [12] nur 6,6 Millionen US$ pro Jahr betragen (0,2106 US$ pro Sekunde). Wenn wir die Streamingkosten von Netflix auf 0,03 US$/GB schätzen [13], erhalten wir 1,5 Mrd. US$/Jahr (46,61 US$/Sekunde). Mit dem Ara-Netzwerk würde Netflix den Nettogewinn von 558,9 US$ im Jahr 2017 fast vervierfachen [14]. (Manhattan hat 1,66 Millionen Menschen [15] mit 287.008 Netflix-Nutzern[2], die 321,45 TB/Tag, 3,72

[2]Ende des ersten Quartals 2018 hatte Netflix 56,71 Millionen Abonnenten in den USA und 125 Millionen weltweit [16]. Es gibt 328 Millionen Menschen in den USA [17], so proportional gibt es 287.008 Netflix-Abonnenten in Manhattan.

GB/s streamen. Das erfordert 3,721 Knoten der Gruppe 2 bei einer Rate von 41,47 US$/Tag).

Verweise

[1] Wikipedia (2018, April 22), *Cobb–Douglas production function*, https://en.wikipedia.org/wiki/Cobb%E2%80%93Douglas_production_function

[2] Wikipedia (2018, June 5), *Total factor productivity*, https://en.wikipedia.org/wiki/Total_factor_productivity

[3] Spectrum (2017, December 29), *Broadband Label Disclosure*, p.2, https://www.spectrum.com/content/dam/spectrum/residential/en/pdfs/ policies/Broadband_Label_Disclosure_Charter_122917.pdf

[4] Wikipedia (2018, March 10), *Hadamard product (matrices)*, https://en.wikipedia.org/wiki/Hadamard_product_(matrices)

[5] Electricity Local (2018, June 19), https://www.electricitylocal.com/states/new-york/new-york

[6] Wikipedia (2018, June 19), *Bandwidth (computing)*, https://en.wikipedia.org/wiki/Bandwidth_(computing)

[7] Energuide.be (2018, June 19), *How much power does a computer use? And how much CO2 does that represent?*, https://www.energuide.be/en/questions-answers/how-much-power-does-a-computer-use-and-how-much-co2-does-that-represent/54/

[8] R. Sohan, A. Rice, A. W. Moore, and K. Mansley, "Characterizing 10 Gbps Network Interface Energy Consumption," *The 35th Annual IEEE Conference on Local Computer Networks (LCN) Short Papers*, University of Cambridge, Computer Laboratory, July 2010, https://www.cl.cam.ac.uk/ acr31/pubs/sohan-10gbpower.pdf.

[9] Amazon Web Services Pricing (2018, June 19), *Amazon Cloudfront Pricing*, https://aws.amazon.com/cloudfront/pricing

[10] L. Matney (2017, December 11), "Netflix users collectively watched 1 billion hours of content per week in 2017," *Techcrunch*, https://techcrunch.com/2017/12/11/netflix-users-collectively-watched-1-billion-hours-of-content-per-week-in-2017

[11] K. Hubby (2017, May 23), "The surprising amount of data Netflix uses," *The Daily Dot*, https://www.dailydot.com/debug/how-much-data-netflix-use/

[12] Wikipedia (2018, June 20), *Exabyte*, https://en.wikipedia.org/wiki/Exabyte

[13] D. Rayburn (2009, July), SStream This!: Netflix's Streaming Costs,"*Streaming Media (June/July 2009)*, http://www.streamingmedia.com/Articles/Editorial/Featured-Articles/Stream-This!-Netflixs-Streaming-Costs-65503.aspx

[14] Netflix (2018, January 1), p.40, https://ir.netflix.com/static-files/20c3228d-bf1f-4956-a169-c8b76911ecd5

[15] Wikipedia (2018, July 5), *Manhattan*, https://en.wikipedia.org/wiki/Manhattan

[16] Statistica (2018, July 5), *Number of Netflix streaming subscribers in the United States from 3rd quarter 2011 to 1st quarter 2018 (in millions)*, https://www.statista.com/statistics/250937/quarterly-number-of-netflix-streaming-subscribers-in-the-us/

[17] United States Census Bureau (2018, July 5), *U.S. and World Population Clock*, https://www.census.gov/popclock/

III. Erwartete Ara-Prämien-Analyse by Lester Kim

Netzwerkmodell

Lassen Sie uns das Ara-Netzwerk der Knoten als vollständiges Diagramm [1] darstellen, $G = (V, E)$ wobei V beinhaltet N Eckpunkte, wobei jeder Eckpunkt einen Knoten und E darstellt, mit $\frac{N(N-1)}{2}$ Ecken, wobei jede Ecke einen Kommunikationskanal zwischen zwei Knoten repräsentiert. Lassen Sie C eine Sammlung von Inhalten sein (in unserem Fall eine Reihe von digitalen Unterhaltungsdateien), die alle Knoten haben wollen, und lassen Sie die Untergruppe $S \subseteq V$ alle Knoten mit C (d.h. $S = \{v \in V : C \in v\}$) enthalten.

Lassen Sie die Zeit $t \in \mathbb{N}$. bei, $t = 0$,$|S| = 1$ sodass es nur ein $v_0 \in V$ gibt, das Inhalt C hat; daher gibt es nur einen Eckpunkt, der eine Kopie von C an andere Knoten in dem Netzwerk liefern kann. Nehmen wir an, dass alle anderen $N - 1$ Knoten C benötigen, und v_0 hat genug Bandbreite, um C an nur einen Knoten zu liefern. Von $t = 0$ bis, $t = 1$ $|S|$ erhöht sich von 1 auf 2. Generell, um Zeit, t

$$|S| = \begin{cases} 2^t & 0 \leq t < \log_2 N \\ N & t \geq \log_2 N. \end{cases} \tag{39}$$

Beachten Sie, dass $|S| = N$ mit $t = \lceil \log_2 N \rceil$ starten.

$\forall s \in S, s$ wird C an einige $v \in V \setminus S$ liefern, aber nur, wenn v an s einen Betrag p zahlt. Lassen Sie M das gesamte Netzwerkbudget für Lieferung von Entertainment sein. Gleichmäßige Aufteilung durch N Knoten ergibt $p = M/N$.

Bei, $t = 0$ der einzige $v_0 \in S$ erhält p von einigen $v_1 \in V \setminus S$. Dann, bei, $t = 1$ $v_0, v_1 \in S$ erhält jeder p von einigen $v_2, v_3 \in V \setminus S$. Bei jeglichen, $t < \lfloor \log_2 N \rfloor$ jeder der $|S| = 2^t$ Knoten in S erhält p von 2^t Knoten in $V \setminus S$. At, $t = \lfloor \log_2 N \rfloor$ $|S| > \frac{N}{2}$ es gibt also mehr Anbieter als Nachfrager für C. Wenn dies auftritt, $N - 2^t$ Knoten von S werden zufällig ausgewählt, um C zu liefern. Bei $t = \lceil \log_2 N \rceil,\ S = V$.

In diesem Model, verdient v_0 mindestens

$$\frac{M \lfloor \log_2 N \rfloor}{N}; \tag{40}$$

v_1 verdient mindestens $\frac{M(\lfloor \log_2 N \rfloor - 1)}{N}$; v_k verdient mindestens

$$\frac{M(\lfloor \log_2 N \rfloor - \lceil \log_2 (k+1) \rceil)}{N}. \tag{41}$$

Der größte k wie der v_k verdient mindestens $\frac{M}{N}$ wenn

$$\lfloor \log_2 N \rfloor - \lceil \log_2 (k+1) \rceil \geq 1 \tag{42}$$

was andeutet

$$\log_2 (k+1) \leq \log_2 \frac{N}{2}. \tag{43}$$

Daher ist der maximale Wert von, k um mindestens $\frac{M}{N}$ zu verdienen, ist $k = \lfloor \frac{N}{2} \rfloor - 1$. Durchschnittlich verdient jeder

$$\frac{M - \frac{M}{N}}{2^{\lceil \log_2 N \rceil - 1}} = \frac{M(1 - \frac{1}{N})}{2^{\lceil \log_2 N \rceil - 1}}. \tag{44}$$

Der Zähler ist $M - \frac{M}{N}$ ohne v_0s Entertainment-Budget, da es C um $t = 0$ hatte. Der Nenner ist, $2^{\lceil \log_2 N \rceil - 1}$ da bei, $t = \lceil \log_2 N \rceil - 1$ $|S| = 2^{\lceil \log_2 N \rceil - 1}$ und zu diesem Punkt, S aus allen Knoten besteht, die die Möglichkeit haben, während dieses Prozesses Belohnungen zu verdienen. Dies bedeutet, dass es $N - 2^{\lceil \log_2 N \rceil - 1}$ Knoten gibt, die in der Lage sind, Belohnungen zu verdienen.

Beispiel

Ungefähr 80% der Amerikaner haben Computer mit Internetzugang [2]. Da 327 Millionen Amerikaner in den USA leben [3], gibt es (0.8)(327M) = 261.6M Amerikaner, die Geräte haben, die mit dem Internet verbunden sind. Angenommen jeder hat ein Gerät, nehmen wir $N = 261.6$M. Der jährliche Unterhaltungsverbrauchswert in den USA beträgt 734 Milliarden US$ [4] [5]. Nehmen wir an, dass der größte Teil dieser Ausgaben für die kommenden Jahre digital sein wird, aber lassen Sie uns nur das Budget von 80% der Amerikaner mit Internetzugang berücksichtigen, so dass deren Ausgaben (0.8)(734B) = $587B betragen. Belassen Sie 10% der Ausgaben für die Deckung der Vertriebskosten. Dann, $M = (0.1)(\$587\text{B}) = \$58.7\text{B}$. Dann, $p = M/N = \$58.7\text{B}/261.6\text{M} = \$224.39$. Bis (44), ist der durchschnittliche jährliche Verdienst $437.35 pro Node. Bis (40), der höchste Verdienst von v_0 ist $6282.87. Daher veranschaulicht dieses Beispiel, dass die anfänglichen Peers, die Inhalte teilen, die meisten Belohnungen verdienen.

Verweise

[1] Wikipedia (2018, June 19), *Complete graph*, https://en.wikipedia.org/wiki/Complete_graph

[2] C. Ryan and J. M. Lewis, "Computer and Internet Use in the United States: 2015," *American Community Survey Reports* U.S. Census Bureau, September 2017 https://www.census.gov/content/dam/Census/library/publications/2017/acs/acs-37.pdf

[3] World Population Review (2018, June 18) *United States Population 2018* http://worldpopulationreview.com/countries/united-states-population/

[4] SelectUSA (2018, August 22), *MEDIA AND ENTERTAINMENT SPOTLIGHT*, https://www.selectusa.gov/media-entertainment-industry-united-states

[5] Bureau of Labor Statistics (2017, August 29), *CONSUMER EXPENDITURES–2016* https://www.bls.gov/news.release/cesan.nr0.htm