

Der Internet Computer

IN KÜRZE

Eine nicht technische Einführung

Inhalt

Die Entstehung der Internet Computer Projekts	3
Die Erweiterung des dezentralisierten Internets Paradigmas	4
Blockchain Funktionalität auf einem "World Computer" Netzwerk	7
Die DFINITY Stiftung	9
Wie die "World Computer" Funktionalität zum Internet hinzugefügt ist	11
Warum im Netzwerk beheimatete Software immune gegen Cyberangriffe ist	14
Die Ökonomie des Internet Computer Netzwerks	18
Die offene Verwaltung (Governance) des Internet Computers	20
Wie Abstimmungsneuronen funktionieren	23
Wie Neuron Reife (maturity) funktioniert	24
Wie es ICP einer KI ermöglicht eigenständig Applikationen und Dienste zu bauen	25

Die Entstehung der Internet Computer Projekts

Das Internet Computer Projekt lässt sich bis ins Jahr 2014 zurückverfolgen, als Dominic Williams, ein früherer Pionier der Blockchain-Technologie, an Möglichkeiten arbeitete, diese erheblich schneller, effizienter und skalierbarer zu machen. Er war der Erste, der klassische verteilte Systeme Techniken auf die Blockchain übertrug. Er beschrieb in diesem Jahr erstmals eine Konstruktionsmethode um Token-Ledger unendlich skalierbar zu machen.

Binary Value Consensus

Input: Proposed $value_i \in \{0, 1\}$
Result: Correct nodes *decide* on a common value

```
1 Upon propose  $v_i$ 
2    $est_i \leftarrow v_i$ 
3    $r_i \leftarrow 0$ 
4   while true do
5      $r_i \leftarrow r_i + 1$ 
6     ABB.broadcast  $\langle est_i, r_i \rangle$ 
7     wait until  $accepted_i[r_i] \neq \emptyset$ 
8     Send  $\langle BVC.VOTE, vote \in accepted_i[r_i], r_i \rangle$  to all nodes
9     wait until  $|\{(v, -) \in votes_i[r_j], v \in accepted_i[r_i]\}| \geq n - f$ 
10     $coin \leftarrow common\_coin(r_i)$ 
11    if  $|\{v : \langle v, - \rangle \in votes_i[r_j], v \in accepted_i[r_i]\}| = 1$  then
12      if  $v = coin$  then  $decided_i \leftarrow TRUE$ 
13       $est_i \leftarrow v$ 
14    else
15       $est_i \leftarrow coin$ 
```

Annotations on the slide:

- Line 9: Byzantine quorum intersect
- Line 10: e.g. broadcast $ThresholdSign(r_j)$
- Line 12: Single Byzantine quorum value = coin, decide!!!
- Line 13: Converge on single Byzantine quorum value
- Line 15: Both 0 and 1 valid ... so coin ... coin value

Right side pseudocode:

```
1* Upon receive  $\langle BDA.VOTE, vote_j, r_j \rangle$  from  $N_j$ 
2* if  $|\{(., j) \in votes_i[r_j]\}| \geq 1$  then return
3*  $votes_i[r_j] \leftarrow votes_i[r_j] \cup \langle vote_j, j \rangle$ 
```

Seine Forschungsarbeit führte dazu, dass er sich der frühen Ethereum-Community anschloss, bevor das Ethereum-Blockchain-Netzwerk gestartet wurde. Diese Ethereum Community arbeitete darauf hin, ein Netzwerk zu schaffen, das eine neue Art von autonomer Software ausführen würde. Diese, heute Smart Contracts genannte Software sollte die für die Entwicklung von DeFi-Diensten (dezentralisierte Finanzdienste) genutzt werden.

Dominic erkannte bald, dass die Prinzipien dieser neuen Smart-Contract-Technologie revolutionär ist und mit ausreichendem Forschungs- und Entwicklungsaufwand viel breiter angewendet werden könnten. Es könnte ein neues Netzwerk geschaffen werden, das eine Weiterentwicklung der Smart-Contract-Software ausführt und mit welcher jede Art von Applikation implementiert werden könnte. So könnten zum Beispiel soziale Netzwerke,

Unternehmenssysteme und KI-Modelle erstellt werden, die vollständig auf so einem Netzwerk betrieben werden.

Diese neue „netzwerk-basierte“ Backend-Software würde wesentliche Vorteile gegenüber der herkömmlichen Backend-Software haben, die auf Servermaschinen mit traditioneller IT-Infrastruktur läuft. Zum Beispiel wäre so gebaute Softwarelösungen immun gegen den üblichen Formen von Cyberangriffen und, innerhalb der Redundanz und Fehlertoleranz des Netzwerks, nicht abschaltbar. Zudem würde sie die Entwicklung und Wartung von Webanwendungen und anderen Internetdiensten erheblich vereinfachen.

Darüber hinaus wären Webanwendungen und Internetdienste, die mit dieser netzwerk-basierten Software gebaut sind, souverän, da sie auf einem dezentralen Netzwerk betrieben würden, und nicht auf proprietärer Infrastruktur eines Unternehmens wie zum Beispiel Cloud-Anbieter. Solche Software könnte auch so konfiguriert werden, dass sie „autonom“ unter der exklusiven Kontrolle digitaler Governance-Systeme läuft, was den Weg für eine neue Generation transparenter und demokratischer Internetdienste ebnen könnte, die direkt von ihren Nutzergemeinschaften kontrolliert würden.

Das Hauptziel eines solchen Netzwerks bestünde darin, das dezentrale öffentliche Internet mit einer „Weltcomputer“-Funktionalität zu erweitern. Während die ursprüngliche Funktion des Internets darin besteht, Softwaresysteme unabhängig vom Standort einfach zu verbinden, würde diese neue Funktionalität es ermöglichen, Software in der Art einer öffentlichen, durch das Netzwerk erschaffene, Cloud-Computing-Plattform auszuführen. In Fällen, in denen private Netzwerkplattformen für eine Anwendung besser geeignet wären, könnten angepasste Versionen der Technologie verwendet werden, um Sicherheit, Resistenz und andere vorteilhafte Eigenschaften zu erzielen.

Die Entwicklung dieser Technologie wurde zu einem grossen Vorhaben, das jahrelange Arbeit und grosse Teams hochqualifizierter Forscher und Ingenieure involvierte.

Die Erweiterung des dezentralisierten Internets Paradigmas

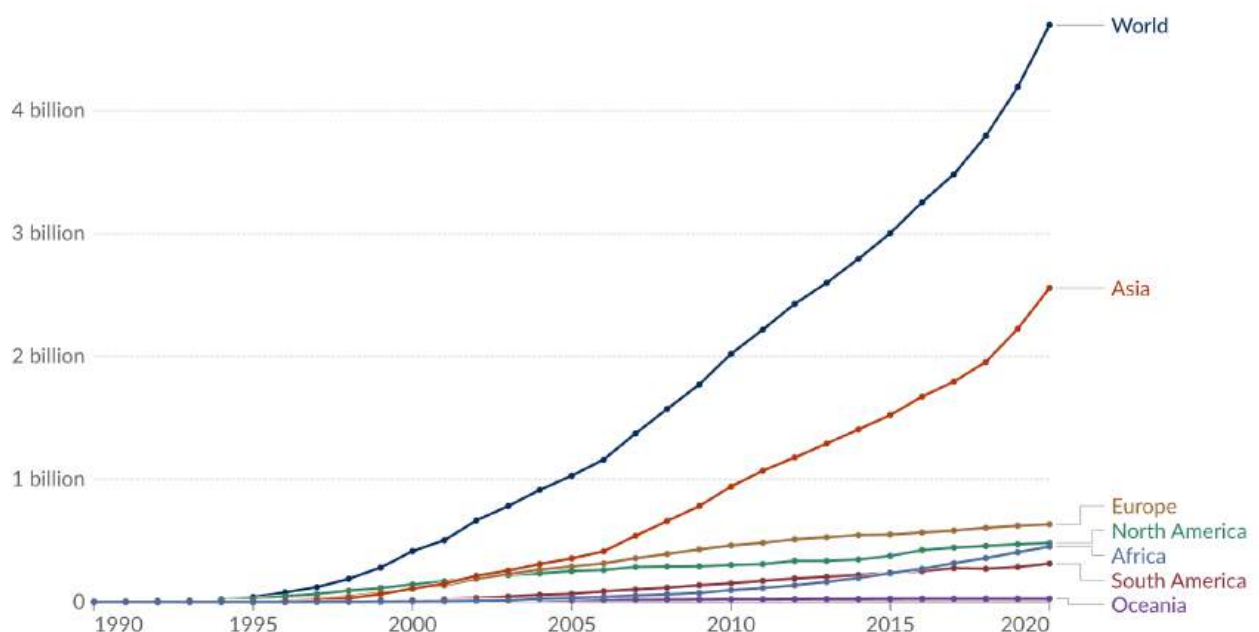
Das modernen Internet wurde am 1. Januar 1983 geboren, durch die Aktualisierung der Netzwerkprotokolle des früheren, ARPANET genannten Netzwerks. Die dem Internet zu grundlegenden Netzwerkprotokolle sind dezentral und gingen auf frühe Arbeiten zu paketvermittelten Netzwerken

aus den 1960er Jahren zurück. Diese zielten darauf ab, Kommunikationsnetzwerke für Computer zu entwickeln, die einem nuklearen Angriff standhalten könnten.

Das Ziel des Internets war es, Software unabhängig davon zu verbinden, wo sie läuft, und das auf eine hochgradig robuste und einfache Weise. Heute verbindet das Internet unsere Webbrowser mit Webservern, sodass wir Inhalte im World Wide Web konsumieren können. Es leitet unsere E-Mails weiter, überträgt unsere Chatnachrichten in Echtzeit, streamt Videos und erfüllt viele weitere Aufgaben.

Der offene und dezentrale Charakter des Internets war der Schlüssel zu seinem Erfolg. Da kein einzelner Akteur das Internet kontrolliert oder besitzt, kann es als eine globale öffentliche Infrastruktur dienen, die der gesamten Menschheit dient.

Jeder kann die physische Infrastruktur des Internets erweitern, beispielsweise als Internetdienstanbieter (ISP), welcher durch den Verkauf von Zugang an andere Gewinne erzielt. Die offene und dezentrale Natur des Internets bedeutet, dass solche Akteure keine Erlaubnis einholen müssen, um mit ihrer Infrastruktur das Internet auszubauen. Sie müssen auch nicht befürchten, dass jemand ihren Anschluss an das Internet widerrufen könnten, was den Wert ihrer Investitionen zerstören würde. Als in den 1990er Jahren die Nachfrage nach Internetzugang und Bandbreite exponentiell zunahm, traten schnell neue Anbieter in den Markt der Internet Infrastruktur ein, und das Internet wuchs rasch um die Nachfrage ohne Engpässe zu bewältigen.



Internet-Adaption nach 1990 (die erste Website ging am 6. August 1991 online)

Diese Faktoren führten in den 1990er Jahren zu einer massiven Welle der Internetadoption. Das Internet wurde schnell zur bevorzugten Method der Kommunikation zwischen Computern und begann, einen riesigen globalen Marktplatz für Waren, Dienstleistungen und Informationen zu ermöglichen, an dem jeder teilnehmen konnte.

Die Welt erforscht nun andere Möglichkeiten, wie dezentrale Netzwerke nützliche Funktionalitäten schaffen können. Im Jahr 2008 wurde mit Bitcoin eine neue Art eines „zustandsbasiertem dezentralem Netzwerkes“ eingeführt, das auf dem Internet lief.

In einem zustandsbasierten dezentralen Netzwerk verwalten die Teilnehmer gemeinsam geteilte Daten. Diese können nur auf die vom Protokoll des Netzwerks definierte Art und Weise modifiziert werden können. Im Fall von Bitcoin handelt es sich bei den geteilten Daten um ein Verzeichnis (Ledger) von Bitcoins, die als „digitales Gold“ fungieren. Diese Verzeichnis kann nur durch das Schicken von korrekt authentifizierter „Transaktionen“ an das Netzwerk geändert werden, die Bitcoin zwischen Adressen im Verzeichnis verschieben.

Zustandsbasierte dezentrale Netzwerke werden durch Netzwerkprotokolle mit speziellen mathematischen Eigenschaften geschaffen. Diese verhindern, dass die Netzwerke manipuliert werden und verleihen ihnen eine unglaubliche Widerstandsfähigkeit verleihen. Deshalb können Bitcoins nicht gestohlen werden, ohne das entsprechende Authentifizierungsmaterial ihrer Besitzer zu stehlen. Ebenso konnte das Netzwerk sogar in seinen kontroversen Anfangsjahren nicht abgeschaltet werden.

Dominic hatte das Ziel, auf diesem Ansatz aufzubauen und ein öffentliches Netzwerk zu schaffen, das in der Lage ist, weltweite Berechnungen auszuführen und so die Funktionalität der Internets entscheidend zu erweitern.

Dies würde ein mächtiger Paradigmawechsel bedeuten: Während das Internet heute Software verbindet, kann es selbst keine Software ausführen und keine Daten speichern. Folglich verbindet uns das Internet mit Dingen wie sozialen Mediendiensten und Unternehmensanwendungen, die Teil unseres täglichen Lebens sind, aber die Dienste selbst laufen nicht in der dezentralen Netzwerkumgebung. Stattdessen laufen sie auf zentralisierten, proprietären, privaten Recheninfrastrukturen wie den Cloud-Diensten grosser Technologieunternehmen, wo sie mit der Technologie der traditionellen IT entwickelt werden.

Obwohl diese zentralisierte Infrastruktur für viele Zwecke geeignet ist, würden viele Dienste besser auf der „Weltcomputer“-Funktionalität laufen. DFINITY ging auf dieses Bedürfnis ein, indem es am 10. Mai 2021 Internet-

Computer-Netzwerk startete, mehreren Jahren der Entwicklung der notwendigen Technologien.

Seither wurde der Internet Computer von Unternehmern und Unternehmen auf der ganzen Welt genutzt, um alles Mögliche zu entwickeln und zu betreiben – von dezentralen sozialen Medien über Spiele, Sharing Economy Applikationen, Unternehmensanwendungen, Finanzsysteme, KI-Modelle und mehr.

Ein neuer Anwendungsfall beinhaltet fortschrittliche KI-Modelle, die in der Lage sind, eigenständig massgeschneiderte Webanwendungen und Internetdienste zu erstellen, indem sie die einzigartigen Eigenschaften der Internet-Computer-Umgebung nutzen. In diesem neuen Paradigma können souveräne, netzwerkansässige Anwendungen einfach durch Gespräche mit der KI erstellt und weiterentwickelt werden. Ebenso kann die vollständige Eigentümerschaft und Kontrolle über den zugrunde liegenden Softwarecode und alle Daten erlangt werden.

Blockchain Funktionalität auf einem "World Computer" Netzwerk

Die netzwerkansässige Backend-Software, die der Internet Computer beheimaten kann, bietet einen erweiterten Funktionsumfang im Vergleich zur Smart-Contract-Software, wie sie traditionellen Blockchains wie Ethereum kennen.

Smart-Contract-Software zeichnet sich dadurch aus, dass sie manipulationssicher ist. Es ist garantiert, dass sie ihre korrekte Logik mit den korrekten Daten ausführt. Sie ist unabschaltbar, da sie stets auf Anfrage ausgeführt wird. Sie kann autonom sein, da sie unabhängig von menschlicher Kontrolle existieren kann – entweder indem sie nicht aktualisiert werden kann oder nur durch ein dezentrales digitales Governance-System, das die Wünsche einer Gemeinschaft unabhängiger Akteure umsetzt. Diese Eigenschaften ermöglichen es, Smart Contracts auf Blockchains wie Ethereum und Solana zu nutzen, um dezentrale Finanzsysteme (DeFi) zu schaffen, die tokenisierte Werte verarbeiten.

Die Rechenkapazität der Smart-Contract-Software auf solchen Netzwerken ist jedoch äusserst begrenzt, und sie kann nur winzige Datenmengen verarbeiten. Dies reicht jedoch aus, um DeFi-Anwendungen zu implementieren, die im Wesentlichen Buchhaltungsinformationen verwalten und einfache damit verbundene Prozesse ausführen. Dennoch kosten es oft mehrere Dollar pro Ausführungskosten bei diesen Anwendungen. Solche

Berechnungen werden durch die Einreichung von Transaktionen ausgelöst, die Nutzer mithilfe von Krypto-Wallets erstellen.

Während solche traditionellen Blockchains dazu beigetragen haben, DeFi voranzutreiben, sind sie in der Praxis – selbst wenn sie als die „skalierbarsten“ und „effizientesten“ vermarktet werden – nicht in der Lage, einfache Inhalte wie ein mit einem Telefon aufgenommenes Foto zu speichern. Zum Beispiel werden Bilder im Zusammenhang mit NFTs oft nicht auf der Blockchain selbst gespeichert, sondern auf Cloud-Diensten.

Es herrscht weit verbreitete Verwirrung über die Fähigkeiten solcher Blockchains, da „Web3“-Projekte wie soziale Medienplattformen und Spiele häufig behaupten, auf Blockchains aufgebaut zu sein, deren Ökosysteme sie oft finanziell unterstützen. In der Praxis bedeutet dies jedoch, dass die Web3-Dienste auf zentralisierter Big-Tech-Cloud-Infrastruktur mit traditioneller IT-Technologie aufgebaut sind, und nur die zugehörigen Token und DeFi-Logik auf den genannten Blockchains verwaltet werden.

Im Vergleich dazu beheimatet der Internet Computer tatsächlich vollständige Dienste wie soziale Netzwerke, Unternehmensanwendungen und KI.

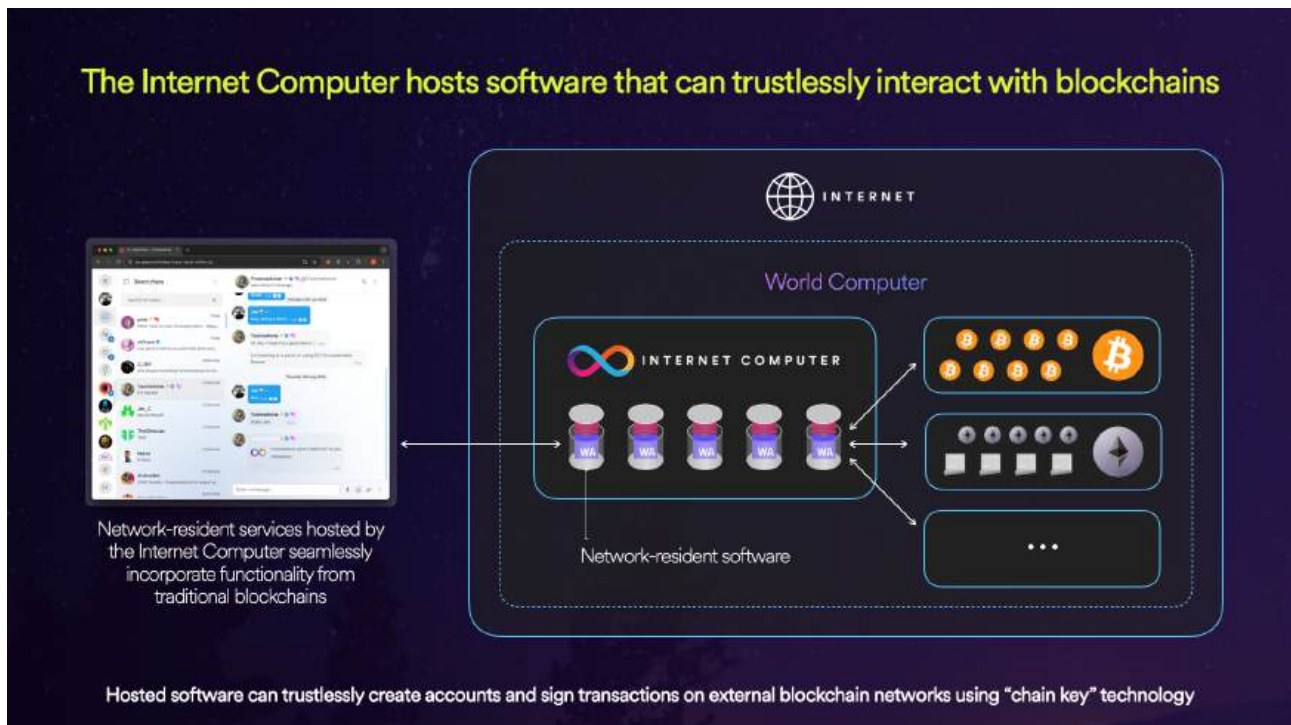
Diese neue Form von netzwerkansässiger Software bietet enorme Vorteile in Bezug auf Geschwindigkeit, Effizienz und Kapazität im Vergleich zu traditionellen Smart Contracts – gemessen in mehreren Größenordnungen – und unterstützt auch wichtige neue Funktionen. Zum Beispiel bezahlt die auf ihm beheimatete Software das Netzwerk für die konsumierte Rechenleistung und kann HTTP-Anfragen verarbeiten und dadurch direkt interaktiven Web-Inhalte den Nutzern bereitstellen. Nutzer können nahtlos mit der Software interagieren, ohne sich bewusst zu sein, dass diese in einem dezentralen Netzwerk und nicht von einem Server beheimatet ist.

Im Gegensatz dazu können traditionelle Smart Contracts keine Web-Inhalte bereitstellen. Nutzer, die direkt mit Smart Contracts interagieren möchten, müssen Berechnungen manuell auslösen, indem sie Krypto-Wallets verwenden, um einzelne Transaktionen zu erstellen, die so konfiguriert sein müssen, dass sie die Kosten für die teure Berechnung des Smart Contracts bezahlen.

Der Internet Computer nutzt fortgeschrittene Mathematik und Informatik, um seine dezentrale Plattformfunktionalität zu schaffen. Er baut auf den von Blockchains eingeführten Prinzipien auf, interpretiert jedoch die Protokolle und Technologie neu, um einen Weltcomputer zu schaffen.

Eine spezielle „Chain-Key“-Funktionalität des Netzwerks ermöglicht es netzwerkansässigem Code, Konten auf traditionellen Blockchains zu

erstellen und signierte Transaktionen einzureichen, ohne einen privaten Schlüssel zu verwalten, der gestohlen werden könnte (tatsächlich interagieren die Knoten des Netzwerks direkt mit Bitcoin- und Ethereum-Knoten).



Dies ermöglicht es, vertrauenslose digitale Zwillinge von Token auf traditionellen Blockchains zu erstellen. Dadurch kann beispielsweise DeFi-Funktionalität zu Netzwerken wie Bitcoin hinzugefügt werden, die Smart Contracts nicht nativ unterstützen. Gleichzeitig können Web3-Dienste, die auf zentralisierter Infrastruktur aufgebaut wurden, vollständig dezentralisiert werden, um sie manipulationssicher, unabschaltbar, autonom und zensurresistent zu machen. Durch diese Funktionalität werden traditionelle Blockchains Teil eines einzigen Weltcomputers.

Die DFINITY Stiftung

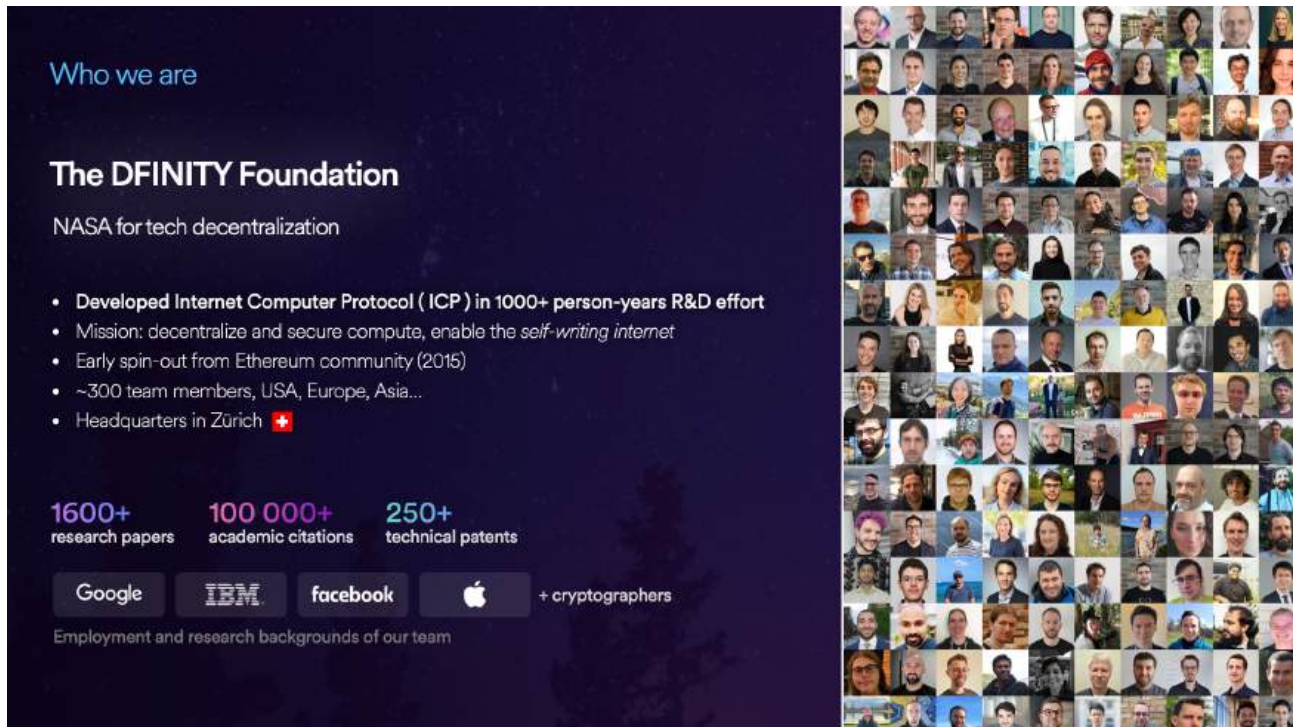
Im Jahr 2016 wurde das DFINITY-Projekt von einem durch Risikokapital finanzierten Inkubator für dezentrale Computerprojekte mit Sitz in Palo Alto, Kalifornien, unterstützt.

Als die Gründung anstand, stellte sich heraus, dass eine neutrale, gemeinnützige Organisation besser geeignet wäre als ein Start-up-Unternehmen, um die Internet-Funktionalität auszubauen. Daher wurde im Oktober 2016 die DFINITY Stiftung in der Schweiz gegründet.

DFINITY schätzt, dass bis 2024 mehr als 1.000 Personenjahre an Forschungs- und Entwicklungsarbeit in die Entwicklung und Verbesserung des Internet

Computers geflossen sind – eine Tätigkeit, die in grossem Masstab fortgeführt wird.

Die DFINITY Stiftung hat ihre Aktivitäten durch das Stiftungskapital von „ICP“-Tokens finanziert. Diese Tokens leiten ihren Wert aus den wirtschaftlichen Mechanismen ab, die das Internet-Computer-Netzwerk zugrundeliegen.



The screenshot displays the 'Who we are' section of the DFINITY Foundation website. The text includes:

- Who we are**
- The DFINITY Foundation**
- NASA for tech decentralization
- Developed Internet Computer Protocol (ICP) in 1000+ person-years R&D effort
- Mission: decentralize and secure compute, enable the *self-writing internet*
- Early spin-out from Ethereum community (2015)
- ~300 team members, USA, Europe, Asia...
- Headquarters in Zürich 🇨🇭

Key statistics are listed below:

- 1600+ research papers
- 100 000+ academic citations
- 250+ technical patents

Logos for Google, IBM, facebook, and Apple are shown, along with the text '+ cryptographers'. Below the logos, it says 'Employment and research backgrounds of our team'. To the right of the text is a large grid of approximately 100 small portrait photos of team members.

Im Februar 2017 verkaufte die DFINITY Stiftung erstmals ICP-Tokens in ihrem „Seed“-Public-ICO (Initial Coin Offering). Während dieses Ereignisses wurden fast 25 % aller ICP-Tokens an Hunderte anonymer Mitglieder der Öffentlichkeit zu je 3 Cent verkauft.

Obwohl die Blockchain-Industrie damals noch viel kleiner war als heute, ermöglichten die vergleichsweise geringen aufgebrauchten Mittel der DFINITY Stiftung seine Forschungs- und Entwicklungsaktivitäten schnell auszuweiten. Eine zweite öffentliche ICO-Finanzierungsrunde war geplant, konnte jedoch aufgrund regulatorischer Änderungen nicht stattfinden.

DFINITY führte daraufhin zwei private Finanzierungsrunden im Jahr 2018 durch, die als „Strategic“ und „Presale“-Runden bezeichnet wurden. Dabei wurden über 110 Millionen Dollar von mehr als 100 hochkarätigen Hedgefonds, Risikokapitalfirmen und vermögenden Einzelpersonen eingeworben.

DFINITY nutzte Forschungszentren in Kalifornien und Zürich. Das frühe Team kombinierte technisches Talent aus der frühen Krypto-Szene Kaliforniens mit

führenden Ingenieuren, Forschern und Kryptographen, die aus Organisationen wie Google stammten.

Im Jahr 2018 erweiterte DFINITY seine Forschungs- und Entwicklungsaktivitäten in Zürich und zog berühmte und angesehene Kryptographen vom IBM Forschungszentrum in Rüschlikon an, darunter Jan Camenisch, welcher CTO von DFINITY wurde, sowie zahlreiche Ingenieure und Forscher von Google, das seinen zweitgrössten Campus ausserhalb von Mountain View in Zürich unterhält, und ebenso Wissenschaftler der ETH Zürich. Infolge dieser Expansion sind mittlerweile mehr als die Hälfte der DFINITY-Mitarbeiter in der Schweiz ansässig.

Ein herausragendes Merkmal des Projekts ist die Fähigkeit, Pioniere der frühen Krypto-Szene mit hochqualifizierten und angesehenen technischen Fachkräften aus High-Tech- und Forschungsbereichen zu vereinen. Dies war entscheidend für die Verwirklichung der „Weltcomputer“-Vision.

DFINITY ist heute weltweit bekannt für seine fortschrittlichen Forschungs- und Ingenieursfähigkeiten.

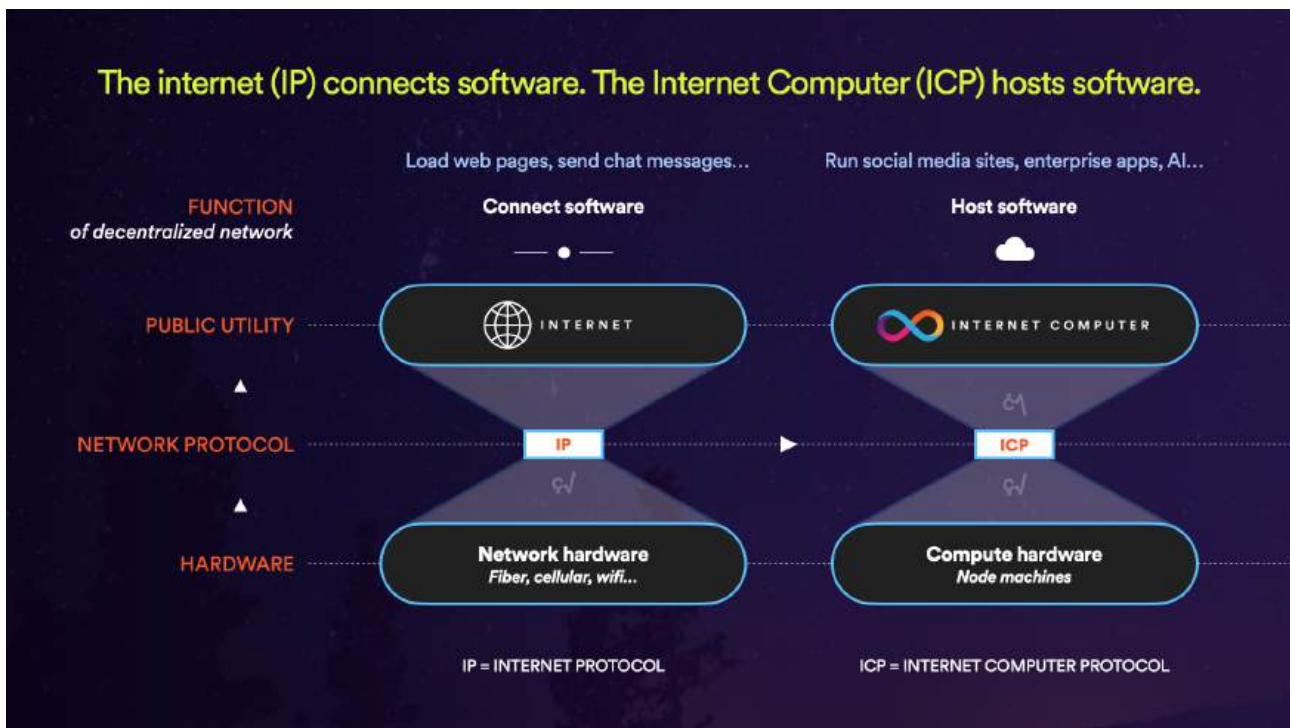
Wie die “World Computer” Funktionalität zum Internet hinzugefügt ist

Das Internet ist das ursprüngliche dezentrale Netzwerk, das durch ein Netzwerkprotokoll namens IP („Internet Protocol“) geschaffen wurde. Ein Netzwerkprotokoll ist eine sorgfältig definierte Sprache, die es durch das Netzwerk verbundenen Geräten ermöglicht, miteinander zu kommunizieren und dadurch Funktionalitäten zu schaffen.

IP kombiniert physische Netzwerkhardware und Verbindungen von unabhängigen Teilnehmern, um ein hochgradig widerstandsfähiges öffentliches Netzwerk zu schaffen, das auch dann weiter funktioniert, wenn ein erheblicher Teil der einzelnen Teilnehmer ausfällt, indem es Datenflüsse umleitet. Unterschiedlichste Netzwerkhardware kann ins Internet integriert werden, von Mobilfunktransceivern in Telefonen über Ethernet-Switches von Internetdienstanbietern (ISP) bis hin zu WLAN-Routern in Haushalten und Unterseekabeln aus Glasfaser. Diese heterogene Hardware wird zu einer robusten globalen Umgebung verwoben, die Software verbindet, unabhängig davon, wo diese ausgeführt wird.

Der Internet Computer orientiert sich am Modell des Internets, zielt jedoch darauf ab, die Funktionalität der öffentlichen Internets zu erweitern, sodass diese auch Software und Daten beheimaten kann.

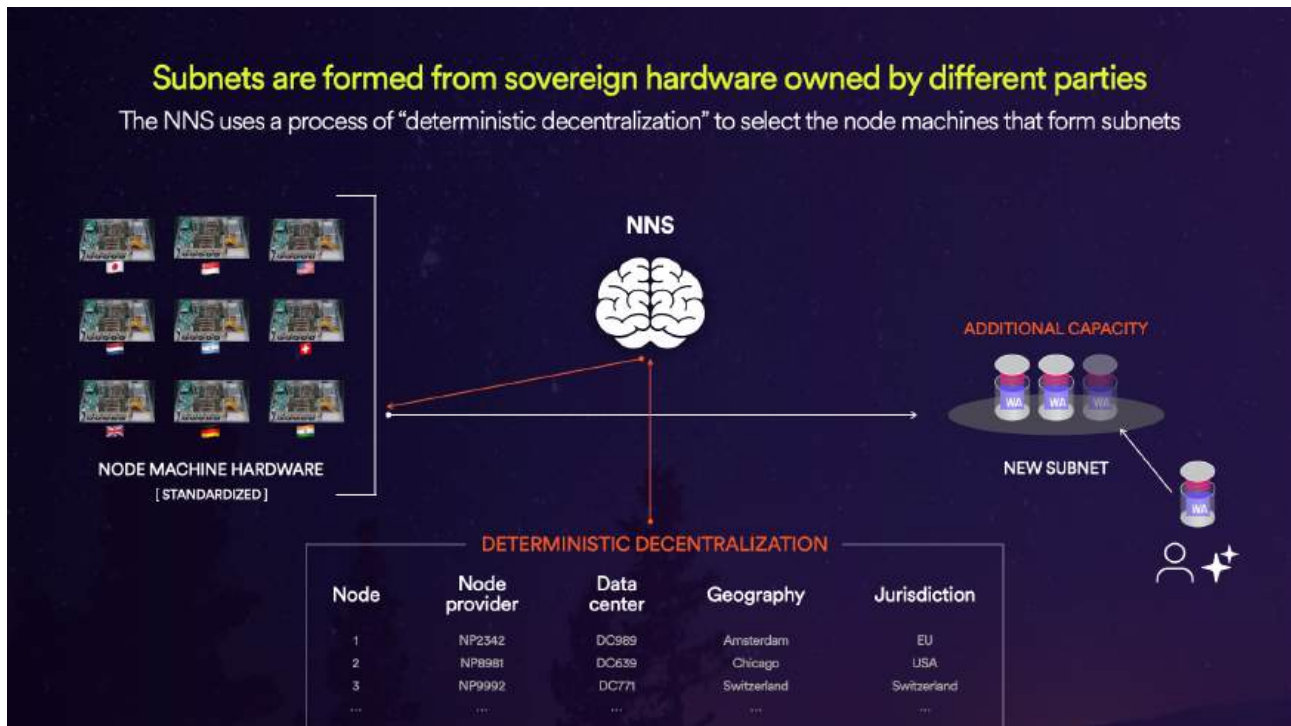
Ein Netzwerkprotokoll namens ICP („Internet Computer Protocol“) läuft über das Internet und kombiniert spezielle „Node-Maschinen“, die von unabhängigen „Node-Anbietern“ (in der Regel Unternehmen) in verschiedenen Rechenzentren auf der ganzen Welt betrieben werden. Zum Zeitpunkt der Erstellung dieses Textes gibt es mehr als 130 Node-Anbieter, die Node-Hardware besitzen und professionell betreiben. ICP verbindet diese Hardware, um eine öffentliche „Weltcomputer“-Funktionalität zu schaffen.



Node-Maschinen werden gemäss öffentlichen standardisierten Spezifikationen gebaut. Dies ermöglicht es, sie zu kombinieren und Berechnungen sowie Daten zu replizieren, ohne dass leistungsschwächere Maschinen bei hoher Netzwerkauslastung zurückfallen. Node-Maschinen ähneln Servercomputern, sind jedoch so gestaltet, dass sie besser für die Ausführung des ICP-Protokolls geeignet sind. Sie verzichten auf teure Hardware-Redundanz, da die Verteilung und Replikation von Daten und Berechnungen diese unnötig macht.

Innerhalb des Internet-Computer-Netzwerks organisiert das ICP-Protokoll diese Node-Maschinen in sogenannte „Subnets“. Das Netzwerk erstellt Subnets, indem es Node-Maschinen von unterschiedlichen Anbietern kombiniert, die in verschiedenen Rechenzentren in unterschiedlichen geografischen Regionen und Rechtsgebieten betrieben werden. Dies dient dazu, die zugrunde liegende Hardware „deterministisch“ zu dezentralisieren, sodass die mathematischen Eigenschaften des Protokolls die erforderlichen Sicherheits- und Widerstandsfähigkeitsniveaus mit minimaler Replikation gewährleisten können. Dies maximiert die Effizienz.

Jedes Subnet beheimatet einen Teil der gesamten netzwerkansässigen Softwareeinheiten, und das Netzwerk erhöht seine Kapazität, indem es neue Subnets erstellt.



Die Softwareeinheiten sind wie bereits erwähnt eine Weiterentwicklung von Smart Contracts und werden „Canisters“ genannt, da sie Logik (in Form von WebAssembly-Bytecode) und Daten (in Form von persistenten Speicherseiten) bündeln). Canisters laufen in einer radikal neuen Form von „serverloser Cloud“-Umgebung. Sofern die Zugriffsberechtigungen dies erlauben, können Softwareeinheiten andere Softwareeinheiten direkt aufrufen, unabhängig davon auf welchen Subnets diese beheimatet sind.

Wichtig ist, dass das ICP-Protokoll sicherstellt, dass die in einem Subnet beheimatete Software korrekt und fehlerfrei weiterläuft, selbst wenn einige der Knoten im Subnet ausfallen, fehlerhaft sind, oder aktiv durch einen Gegner manipuliert werden. Diese Eigenschaft nennt sich in der Fachsprache „Byzantinische Fehlertoleranz“.

Ausserdem verleiht die von dem ICP-Protokoll eingesetzte Informationstechnologie den Subnetzen (und dem gesamten Netzwerk) eine technische Eigenschaft namens „Byzantinische Fehlertoleranz“. Diese garantiert, dass selbst wenn ein Gegner des Netzwerks, wie ein imaginärer „Dr. Evil“, physische Kontrolle über einen Teil der Knoten in einem Subnetz erlangt, deren Berechnungen und Daten beliebig korrumpiert und ihre Interaktionen mit anderen Knoten manipuliert, die anderen Softwareeinheiten, die auf dem Subnetz laufen, weiterhin vollständig korrekt

funktionieren und keine ihrer Berechnungen oder Daten in irgendeiner Weise beeinträchtigt oder verfälscht werden.

Das Internet-Computer-Netzwerk ist hochdynamisch und kann Subnet-Knoten hinzufügen und entfernen, ohne die Ausführung der beheimateten Software zu unterbrechen. Wenn das Netzwerk mehr Kapazität benötigt, werden Knoten zu neuen Subnets geformt. Wenn ein Subnet durch die bereits beheimatete Software überlastet ist, wird das Subnet in zwei Subnets aufgeteilt, die die Last zwischen sich aufteilen.

Die Mathematik und Informatik, die all dies in der Praxis möglich machen, ist äusserst komplex. ICP ist modular konzipiert und implementiert, sodass Ingenieure und Forscher innerhalb ihrer Fachbereiche Beiträge leisten können, ohne im Detail zu verstehen, wie alle Teile funktionieren, und dennoch die vollständigen mathematischen Eigenschaften verifiziert werden können. Dieser Ansatz im Protokolldesign hat es ICP ermöglicht, das bisher fortgeschrittenste Netzwerkprotokoll zu werden.

Eine neue Art von dezentraler Computerplattform ist somit entstanden, die serverlose Software, Berechnungen und Daten in großem Maßstab beheimaten kann, immun gegen Cyberangriffe und unabschaltbar ist, mittels HTTP interagieren kann, und flexibel genug ist, KI-Modelle auszuführen.

Warum im Netzwerk beheimatete Software immune gegen Cyberangriffe ist

Die Backend-Software und Daten in der traditionellen IT sind hochgradig anfällig, und ein gewisses Mass an Unsicherheit und Risiko bleibt bestehen, selbst wenn die besten Cybersicherheitstechnologien und -praktiken eingesetzt werden. Selbst eine aktive Verwaltung durch Sicherheitsteams, die Firewalls, Anti-Malware und Systeme zur Überwachung von Eindringversuchen einsetzen, reicht nicht aus, um Sicherheit zu erlangen. Jederzeit kann ein Fehler dazu führen, dass Hacker in Systeme eindringen, vertrauliche Daten extrahieren oder Systeme mit Ransomware verschlüsseln, was potenziell zu dauerhaftem System- und Datenverlust führt. Die globalen Kosten der Cyberkriminalität nähern sich inzwischen 10 Billionen US-Dollar pro Jahr.

Der Internet Computer adressiert diese Herausforderungen, indem er eine „Weltcomputer“-Funktionalität mit Sicherheits- und Widerstandsgarantien bietet, die sich aus dem mathematischen Design des ICP-Protokolls ableiten. Innerhalb der „Fehlergrenzen“ des Protokolls garantiert der Internet Computer, dass die von ihm beheimatete Software manipulationssicher ist (in dem Sinne, dass sie immer ihre Logik korrekt mit ihren korrekten Daten

ausführt) und unabschaltbar ist (in dem Sinne, dass sie jederzeit auf ihre Logik mit ihren Daten ausführen kann).

Die Architektur basiert auf zwei Schlüsselprinzipien, um netzwerkansässige Software immun gegen traditionelle Formen von Cyberangriffen zu machen und sie unabschaltbar zu machen.

Das erste Schlüsselprinzip besteht darin, jede Einheit der netzwerkansässigen Software in einer global verteilten „virtuellen Ausführungsumgebung“ auszuführen. Dies ist vergleichbar mit der Art und Weise, wie Webbrowser die Software in den angezeigten Webseiten in sogenannten “Sandboxen” isoliert ausführen. So können Hacker keinen Code erstellen, der auf die Geräte der Nutzer zugreifen und Schaden anrichten kann.

Der Internet Computer platziert die gesamte von ihm beheimatete netzwerkansässige Software sowie alle zugehörigen Berechnungen und Daten in ein ähnliches Framework – mit der Innovation, dass die virtuelle Ausführungsumgebung eine vollständige serverlose Cloud-Computing-Plattform bietet.

Vielleicht wenig überraschend teilen sich der Internet Computer und Webbrowser Technologien. Der Internet Computer führt Software auf einer modifizierten Version der „WebAssembly“-virtuellen Maschine aus. Diese virtuelle Maschine wird auch von modernen Webbrowsern verwendet, um sicher Software innerhalb von Webseiten mit nativer Geschwindigkeit auszuführen, beispielsweise für Zwecke wie Videodekodierung.

Eine interessante historische Anmerkung ist, dass WebAssembly von einem der frühesten Mitglieder des DFINITY-Teams (Andreas Rossberg) mitentwickelt wurde. Von Anfang an war vorgesehen, dass WebAssembly nicht nur sicher Software in Webbrowsern ausführt, sondern auch für performante Backend-Software geeignet ist. Um die gesamte virtuelle Ausführungsumgebung zu schaffen, fügt der Internet Computer WebAssembly viele zusätzliche Komponenten hinzu, beispielsweise APIs, mit denen Software andere Software aufrufen kann, Berechtigungen und andere Konfigurationen festlegen und HTTP-Anfragen bearbeiten.

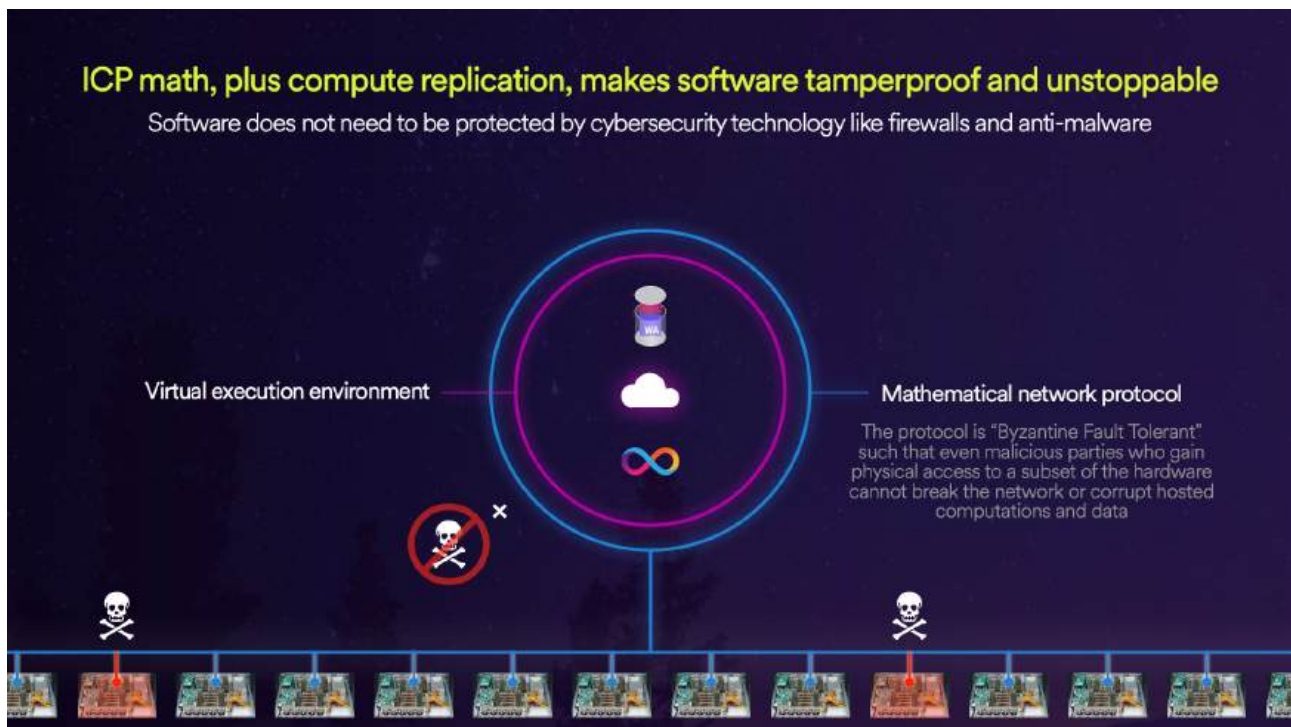
Obwohl der Internet Computer öffentlich ist und keine Barrieren für das Hochladen bösartiger Software bestehen, kann bösartige Software weder auf den Node-Maschinen noch an anderer auf dem Internet Computer beheimateter Software Schaden anrichten.

Das zweite Schlüsselprinzip besteht darin, die virtuelle Ausführungsumgebung in einem „zustandsbasierten dezentralen Protokoll“ einzubetten. Wie zuvor erläutert, ist der „Zustand“ im Fall von

Bitcoin das Verzeichnis (Ledger) der Bitcoins, und im Fall des Internet Computers ist der „Zustand“ die gesamte virtuelle Ausführungsumgebung, die die Cloud-Computing-Umgebung beheimatet.

Netzwerkprotokolle erfordern oft, dass Teilnehmer einige Daten im Zusammenhang mit ihren Interaktionen speichern. Zum Beispiel ermöglicht TCP („Transmission Control Protocol“, ein Teil der IP-Protokollfamilie) zwei Software-Instanzen, einen zuverlässigen bidirektionalen Datenstrom über das Internet aufrechtzuerhalten, den Entwickler über Softwarebibliotheken nutzen können, um Aufgaben wie das Streaming von Videos oder das Übertragen von Chatnachrichten auszuführen. Die Bibliotheken, die das Protokoll implementieren, müssen kontextbezogene Daten im Zusammenhang mit dem Stream speichern.

Ein zustandsbasiertes dezentrales Protokoll unterscheidet sich dadurch, dass viele Teilnehmer durch ihre Interaktionen mit anderen Teilnehmern sowie die kontextbezogenen Informationen und Berechnungen, die sie gemäss den Regeln des Netzwerkprotokolls durchführen, gemeinsam eine Kopie eines globalen „Zustands“ pflegen (der bei allen Teilnehmern konsistent ist).



Ein wesentlicher Erfindungsschritt dabei ist, dass selbst wenn einzelne Teilnehmer die Regeln des Protokolls nicht einhalten oder aktiv versuchen, andere Teilnehmer zu stören, die von korrekt agierenden Teilnehmern gepflegte Kopie des Zustands nicht korrumpiert wird und konsistent bleibt. Das bedeutet, dass fehlerhaft agierende Teilnehmer, die das Bitcoin-Netzwerk hosten, keine neuen Bitcoins erzeugen oder bestehende Bitcoins stehlen können, selbst wenn sie bösartig wären. Ebenso können Teilnehmer

im Internet-Computer-Netzwerk nicht in ihm beheimatete Software manipulieren oder in Berechnungen und Daten eingreifen.

Die Stärke dieses Ansatzes besteht darin, dass Hacker die Regeln der Mathematik nicht brechen können, um beispielsweise $2+2=5$ gültig zu machen. Solange der Anteil der fehlerhaften Teilnehmer die mathematisch definierten Fehlergrenzen des Netzwerks nicht überschreitet, bleibt die Plattform, die durch das Netzwerk geschaffen wurde, manipulationssicher und unabschaltbar. Diese Eigenschaft wird auf die beheimatete Software sowie deren Berechnungen und Daten übertragen, da diese Teil des Zustands sind, genauso wie ein Bitcoin Teil des Zustands des Bitcoin-Verzeichnisses ist.

Ein offensichtliches Risiko solcher Systeme besteht darin, dass ein „Dr. Evil“ neue fehlerhafte Teilnehmer (hier: Node-Maschinen) zum Netzwerk hinzufügen könnte, bis der Anteil der fehlerhaften Teilnehmer die Fehlergrenzen überschreitet. Das Netzwerk ist jedoch so gestaltet, dass die „Node-Anbieter“, die Node-Maschinen besitzen und betreiben, identifiziert werden, und sie in einer Weise zu Subnets kombiniert werden, die eine Überschreitung der Fehlergrenze verhindert.

Die traditionelle IT-Infrastruktur ist ein ganz anderes Konstrukt. Hier läuft Software direkt auf Computern und nicht innerhalb einer virtuellen Ausführungsumgebung innerhalb eines mathematisch sicheren Protokolls. Ein Hacker kann Software ausnutzen, um auf das Betriebssystem eines Computers oder andere Software zuzugreifen, Daten zu extrahieren oder Ransomware zu installieren.

Im Gegensatz dazu garantiert der Internet Computer, dass netzwerkansässige Software sowie deren Daten und Berechnungen nicht untergraben werden können und stets aufrufbar sind.

Dies wurde in der Praxis bewiesen. Zum Zeitpunkt der Erstellung dieses Textes laufen zum Beispiel Web3-Soziale-Netzwerke auf dem Internet Computer die viele tausend Nutzer haben. Diese haben es in den letzten zwei Jahren Nutzern ermöglicht, Kryptowährungs-Tokens in ihren Konten zu verwalten, sodass sie diese bequem mittels Instant-Messaging übertragen können. Alles diese Dienste liefen störungsfrei, obwohl zahlreiche staatlich finanzierte Hacker-Gruppen versuchten, Kryptowährungen von Internetdiensten zu stehlen. Das obwohl die Dienste ohne Sicherheitsteams oder traditionelle Formen der Cybersicherheit wie Firewalls und Anti-Malware betrieben werden.

Der Internet Computer stellt einen bahnbrechenden Fortschritt in der Sicherung von Softwarelogik und Daten dar.

Die Ökonomie des Internet Computer Netzwerks

Wie das Internet selbst zielt auch der Internet Computer darauf ab, als globale öffentliche Infrastruktur zu funktionieren, die niemand besitzt oder kontrolliert. Um sich selbst zu tragen, müssen dezentrale Netzwerke wirtschaftliche Modelle integrieren, welche Finanzierung und Betrieb der unterliegenden physischen Hardware unterstützen.

Das Internet schafft eine selbsttragende Wirtschaft durch sogenannte „Peering-Beziehungen“. In ihrer offensichtlichsten Form bezahlen Parteien andere Parteien, um ihre Geräte und Netzwerke mit dem Internet zu verbinden. Zum Beispiel könnte ein Endnutzer einen Mobilfunkanbieter bezahlen, um sein Telefon mit dem Internet zu verbinden, und ein Unternehmen könnte einen Internetdienstanbieter (ISP) bezahlen, um sein Büro zu verbinden. Der ISP wiederum könnte einen Internet-Backbone-Anbieter bezahlen, um ihm zusätzliche Konnektivität bereitzustellen, der möglicherweise wiederum für den Anschluss an Unterseekabel bezahlt.

(Manchmal nimmt der wirtschaftliche Nutzen solcher Peering-Beziehungen andere Formen an, insbesondere im Kern des Internets. Einige grosse Technologieunternehmen betreiben beispielsweise selbst Unterseekabel und erlauben Telekommunikationsunternehmen, sich kostenlos daran anzuschließen, wobei sie wirtschaftlichen Nutzen durch garantierten und beschleunigten Zugang zu ihren Diensten für Milliarden von Nutzern erzielen. Gleichzeitig beinhalten mehrseitige Peering-Beziehungen häufig eine Art von Sachleistung, bei der jede Partei Redundanz zu ihren Routen hinzufügt, sodass keine offensichtlichen Zahlungen erfolgen.)

Das Internet kann ein peering-basiertes Wirtschaftsmodell nutzen, um seine zugrunde liegende Infrastruktur zu finanzieren, da sein Zweck darin besteht, Software zu verbinden. Der Zweck des Internet Computers ist es jedoch, Software zu beheimaten, und er verwendet deshalb ein anderes wirtschaftliches Modell, um den Wertfluss von beheimateter Software zu denen, die die zugrunde liegende Hardware betreiben, zu lenken. Dies geschieht über Tokenisierung.

Ein Ledger von „ICP“-Tokens (benannt nach dem Protokoll) wird vom Internet-Computer-Netzwerk betrieben. Diese Tokens erhalten ihren Wert durch verschiedene Nachfragequellen, die sich aus dem Nutzen ergeben, den sie bieten. Dies ermöglicht es dem Netzwerk, die Token als Belohnung für die korrekte Betreuung von Node-Maschinen an die Node-Anbieter auszugeben.

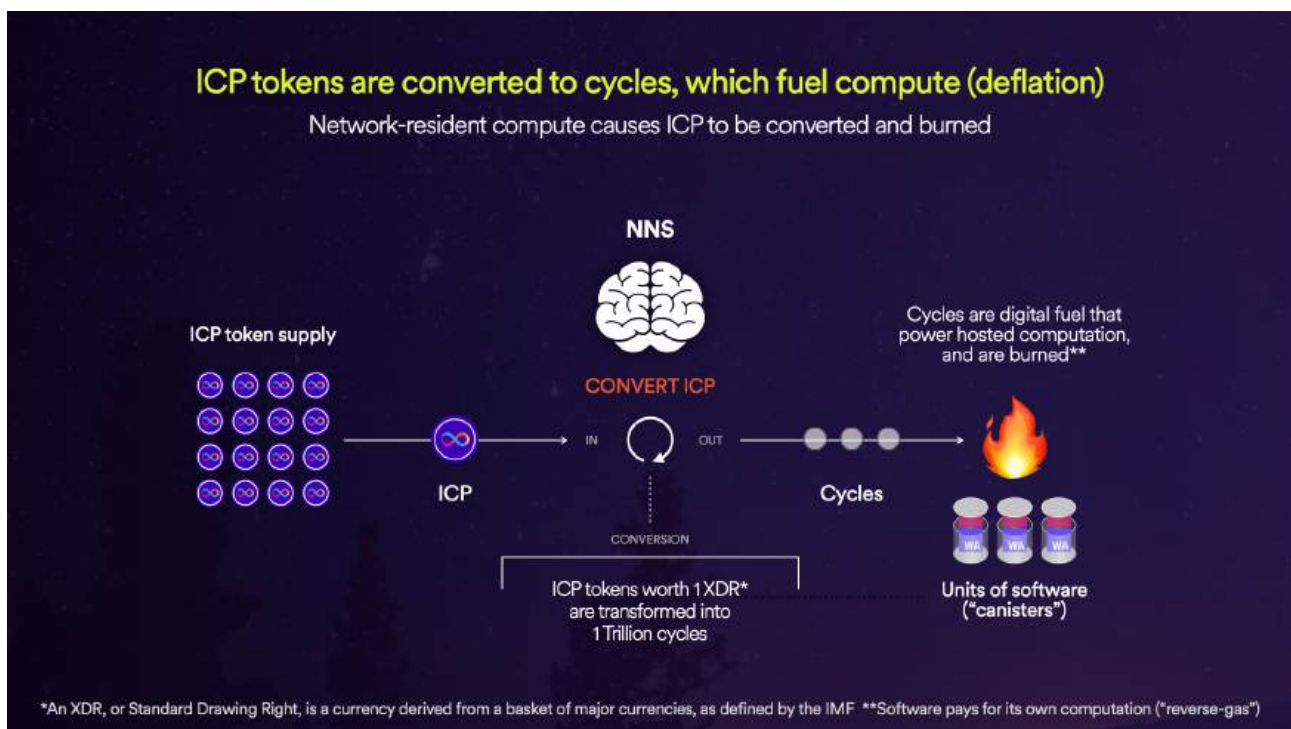
Node-Anbietern haben feste Kosten, die durch die Anschaffung ihrer Node-Maschinen-Hardware, deren Betrieb in einem Rechenzentrum und die Verwaltung ihrer Infrastruktur entstehen. Da der Preis von Krypto-Tokens

volatil sein kann, modulieren die Protokolle des Netzwerks die Anzahl der an Node-Anbietern ausgegebenen Tokens, um sicherzustellen, dass ihre finanziellen Belohnungen stabil bleiben, gemessen an Fiat-Währungen. Dies ermöglicht es den Node-Anbietern, ihre Geschäfte auf stabile Weise zu betreiben.

Eine wichtige Nachfragequelle, die dazu beiträgt, den ICP-Tokens Wert zu verleihen, ist, wie Software, die auf dem Netzwerk beheimatet ist, betrieben wird. Software auf dem Netzwerk muss mit einem digitalen Treibstoff namens „Cycles“ versorgt werden. Diesen verbraucht sie, wenn sie Berechnungen ausführt und Daten speichert, ähnlich wie ein Elektroauto mit Strom aufgeladen wird und diesen dann verbrennt, wenn es fährt.

Der Internet Computer bietet die Möglichkeit, ICP-Tokens im Wert von 1 XDR (einer vom IWF definierten virtuellen Währung) in 1 Billion Cycles umzuwandeln. Dadurch werden die Kosten für die Berechnungen im Netzwerk stabil und vorhersagbar. Kontinuierlich konvertieren Personen von ihnen erworbene ICP-Tokens in Cycles um ihre im Netzwerk beheimatete Software zu betreiben. Diese Cycles werden dann verbraucht und verschwinden dauerhaft.

Zusätzliche Nachfragequellen für ICP-Tokens ergeben sich aus deren Rolle als Kryptowährung und ihrer Nutzung in der Form des „Stakings“, die die Teilnahme an der Governance des Netzwerks ermöglicht.



Die vier Hauptzwecke der ICP-Tokens sind daher:

1. Bereitstellung des Ausgangsmaterials für einen digitalen Treibstoff namens „Cycles“ um Software im Internet-Computer-Netzwerk zu betreiben.
2. Bereitstellung eines Mechanismus, mit dem der Internet Computer Node-Anbieter, die das Netzwerk hosten, belohnen kann.
3. Vermittlung der Teilnahme an der Netzwerk-Governance und Schaffung von Anreizen für Teilnehmer.
4. Anwendung als programmierbarer Wertspeicher und Tauschmedium (Kryptowährung).

Die offene Verwaltung (Governance) des Internet Computers

Es wäre äusserst schwierig, ein globales dezentrales Netzwerk ohne eine Form von Verwaltung (Governance) zu schaffen, da einige der Aufgaben den Einsatz von Intelligenz (menschlicher oder anderer Art) erfordern.

Obwohl das Internet grösstenteils dezentral ist, gibt es einige zentrale Abhängigkeiten in Bezug auf die Governance, darunter eine gemeinnützige Organisation in den USA namens „Internet Corporation for Assigned Names and Numbers“ (ICANN). Zu ihren Aufgaben gehört unter anderem die Organisation der Vergabe von Internetadressen, die von Computern verwendet werden, und benutzerfreundlicher Domainnamen.

Zentralisierte Abhängigkeiten innerhalb dezentraler Netzwerke sind Schwachstellen, die die Neutralität, Sicherheit und Zensurresistenz beeinträchtigen können. Aus diesem Grund läuft der Internet Computer unter der Kontrolle eines vollständig automatisierten und offenen dezentralen Governance-Systems, das als „Network Nervous System“ (NNS) bezeichnet wird und das gesamte Netzwerk orchestriert.

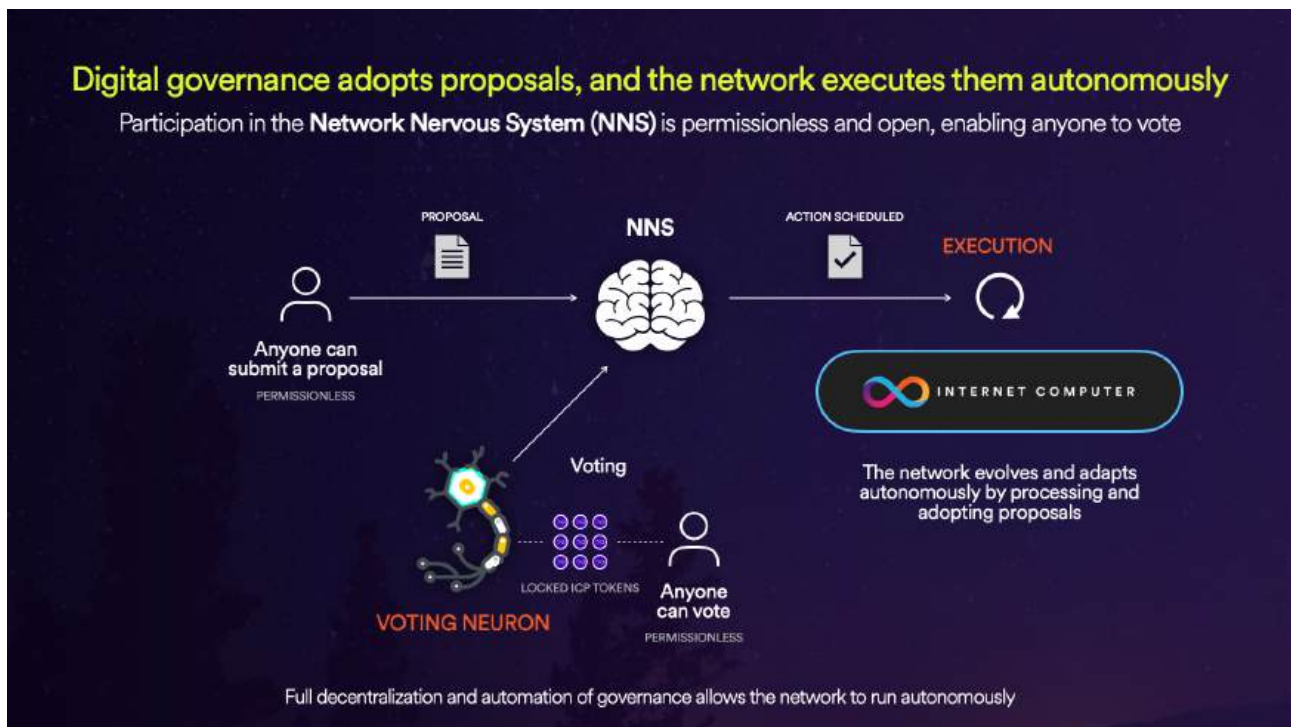
Das NNS wird von einem ausgeklügelten Software-Framework geschaffen, das direkt im Netzwerk beheimatet ist und nahtlos in die zugrunde liegenden ICP-Protokolle integriert ist.

Da die Node-Maschinen, die das Netzwerk bilden, blind das ICP-Protokoll verarbeiten, folgen sie auch automatisch den Anweisungen des NNS. Dies ermöglicht es dem NNS, die Governance und das Management des Netzwerks ohne zentrale Akteure zu realisieren.

Das NNS ist offen und dezentral und funktioniert wie eine Art DAO („Decentralized Autonomous Organization“). Dadurch kann der Internet

Computer vollständig autonom laufen und sich gleichzeitig dynamisch anpassen und weiterentwickeln.

Jeder kann Vorschläge an das NNS schicken, Diese Vorschläge beschreiben die Aktionen, die das Netzwerk ausführen soll. Jeder Vorschlag gehört zu einem standardisierten Thema und hat einen spezifischen Typ, der genau definiert, welche Informationen bereitgestellt werden müssen. Vorschläge lösen Aktionen aus, wie zum Beispiel die Vergabe einer kryptografischen Identität an einen neuen Node-Anbieter, der dem Netzwerk beitreten möchte, Anpassungen der Netzökonomie, Updates der Node-Maschinen-Software, die das ICP-Protokoll im gesamten Netzwerk verarbeitet (dies ist der Mechanismus, durch den das Netzwerk regelmässig auf neue Versionen von ICP aktualisiert wird), die Schaffung zusätzlicher Kapazität durch die Erstellung neuer Subnets, das Aufteilen überlasteter Subnets und viele andere Funktionen, einschließlich der Aufnahme externer Daten, die dem Netzwerk helfen, zu funktionieren.



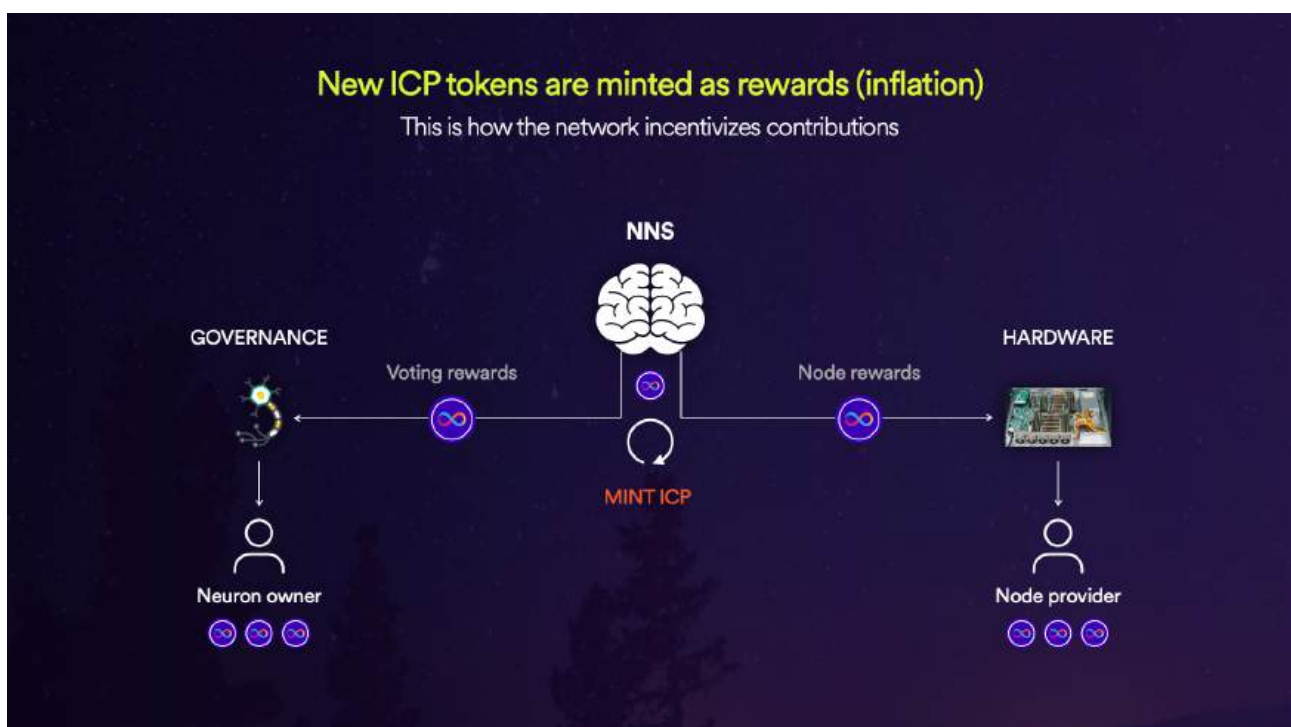
Das Design des NNS ermöglicht es, Vorschläge schnell und sicher zu entscheiden. Da die Vorschläge, die das NNS annimmt, automatisch vom Netzwerk ausgeführt werden, kann sich das Netzwerk schnell an sich ändernde Umstände anpassen, wie beispielsweise eine steigende Nachfrage, und sich eigenständig weiterentwickeln, indem Verbesserungen rasch integriert werden. Zum Zeitpunkt der Erstellung dieses Textes nimmt das NNS täglich Dutzende von Vorschlägen an, was den Grad widerspiegelt, in dem das Netzwerk hochdynamisch und selbstgesteuert läuft.

Da das NNS offen ist, kann grundsätzlich jeder Vorschläge einreichen und an Abstimmungen über Vorschläge teilnehmen, was die offenen und demokratischen Ziele des Netzwerks widerspiegelt.

Eine Herausforderung bei jedem solchen Governance-System besteht darin, Wege zu finden, um sicherzustellen, dass die Teilnehmer ehrlich und verantwortungsvoll abstimmen, sowie Möglichkeiten, böswillige Akteure daran zu hindern, einfach in großer Zahl beizutreten, um ehrliche Parteien zu überstimmen. Dies könnte dazu führen, dass das Netzwerk schädliche Aktionen ausführt, wie zum Beispiel alle Daten zu löschen.

Dieses Problem wird durch Abstimmungs-„Neuronen“ gelöst. Um über NNS-Vorschläge abzustimmen, ist es notwendig, anonyme Neuronen innerhalb des NNS zu erstellen und mit Abstimmungsmacht auszustatten, indem ICP-Tokens darin deponiert werden. Folglich setzen alle, die über Vorschläge abstimmen, ihre ICP-Tokens einem Risiko aus, indem sie diese deponieren.

Wenn schädliche Vorschläge angenommen werden, wird dies dazu führen, dass der Wert der in Neuronen deponierten ICP-Tokens fällt, und umgekehrt, was einen Anreiz für Neuronenhalter schafft, für Massnahmen zu stimmen, die langfristige Vorteile bringen, da die ICP-Tokens, die sie in ihren Neuronen deponiert haben, nicht sofort ausgelöst werden können.



Das NNS bietet Anreize um an der Governance teilzunehmen als auch um Nodes bereit zustellen. Das hast dazu geführt, dass enorme Mengen an Kapital von ehrlichen Parteien in Neuronen deponiert wurden. Dies macht es für böswillige Parteien unerschwinglich teuer, genügend ICP-Tokens zu erwerben, um durch Abstimmungen über Vorschläge schädlichen Einfluss

auszuüben, selbst wenn sie finanzielle Anreize dazu haben (zum Beispiel, weil sie auf fallende ICP-Token-Werte spekuliert haben und das Netzwerk schädigen möchten, um ihre Wetten profitabel zu machen).

Wie Abstimmungsneuronen funktionieren

Um an der Governance des Internet Computers teilzunehmen müssen „Abstimmungsneuronen“ innerhalb des NNS erstellt werden. Neuronen sind eigenständige Objekte, die nicht zum Übertragen oder Verkaufen vorgesehen sind. Neuronen schaffen starke Anreize, die zur Teilnahme an der NNS-Governance ermutigen und gleichzeitig sicherstellen, dass das gesamte Governance-System wie vorgesehen funktioniert.

Teilnehmer des NNS können ihre Neuronen so konfigurieren, dass sie vollständig automatisch abstimmen, indem sie den Stimmen von ihnen ausgewählten anderen Neuronen. Letztere gehören typischerweise zu Führungspersönlichkeiten und Experten innerhalb des Internet-Computer-Ökosystems.

Neuroneneigentümer können das Abstimmen auch so konfigurieren, dass sie der Mehrheitsstimme eines Quorums anderer Neuronen folgen. Sie können jederzeit auswählen, welchen Neuronen sie folgen möchten, oder zum manuellen Abstimmen zurückkehren. Das Folgen kann für jedes der verschiedenen Governance-Themen, die das NNS unterstützt, unterschiedlich konfiguriert werden, wodurch die Stimme präzise an diejenigen delegiert werden kann, die über die entsprechende Expertise verfügen. Das NNS fungiert somit als fortgeschrittene „automatisierte dynamische Demokratie“, die weltweit ihresgleichen sucht.

Viele Teilnehmer an der NNS-Governance erstellen ihre Neuronen und bringen damit Kapital ein, um Belohnungen auf die hier beschriebene Weise zu erhalten. Da diese Neuronenhalter typischerweise das tägliche Abstimmen aus Gründen der Bequemlichkeit an Experten delegieren, bietet dies enorme Sicherheit und Stabilität, während die letztendliche Stimmhoheit bei der Gesamtheit der Neuronenhalter verbleibt.

Der Einfluss, den ein einzelnes Neuron ausüben kann, sowie die Höhe der Belohnungen, die es letztendlich verdienen kann, hängen proportional von der relativen Größe seiner Stimmgewichte ab.

Das Stimmgewicht jedes Neurons hängt von seiner Konfiguration zum Zeitpunkt der Abstimmung ab, insbesondere von:

der Anzahl der in ihm deponierten ICP-Tokens,

seiner aktuellen „Auflösungsverzögerung“ (dissolve delay), die bestimmt, wie lange es dauern würde, die deponierten ICP-Tokens freizugeben, nachdem das Neuron in den „Auflösungsmodus“ versetzt wird,

seinem „Alter“, einem virtuellen Attribut, das als das geringere von den folgenden zwei Werten berechnet wird: der seit der Erstellung des Neurons vergangene Zeit und der Zeit, die vergangen ist seit es in Auflösungsmodus gesetzt wurde.

Das Stimmgewicht eines Neurons wird mit folgender Formel berechnet:

Stimmgewicht = deponierte ICP-Tokens x Bonus für die
Auflösungsverzögerung x Altersbonus

(Einschränkungen beinhalten, dass die maximale konfigurierbare Auflösungsverzögerung 8 Jahre beträgt, und dass Neuronen nur abstimmen können, wenn die Auflösungsverzögerung mindestens 6 Monate beträgt. Das maximal berechnete Alter beträgt 4 Jahre. Der Bonus für die Auflösungsverzögerung beginnt bei 1,0 für 6 Monaten Verzögerung und steigt auf 2,0 für 8 Jahren. Der Altersbonus beginnt bei 1,0 für null Tagen Alter und steigt auf 1,25 für 4 Jahren.)

Für jede Stimme, die ein Neuron über einen Vorschlag abgibt, erhöht das NNS sein „Reife“-Attribut (maturity) als Belohnung. Die Reife der Neuronen, können sie später verwendet werden, um neue ICP-Tokens zu erstellen.

Wie Neuron Reife (maturity) funktioniert

Jedes Neuron verfügt über ein Attribut namens „Reife“ (maturity), das mit dem Gewicht eines physischen Objekts vergleichbar ist. Da die Reife ein Attribut ist, kann sie nicht vom Neuron getrennt werden (d.h., sie ist beispielsweise kein Token, das separat übertragen oder gehalten werden kann). Das NNS erhöht die Reife von Neuronen als Belohnung für das Abstimmen über Vorschläge.

Alle 24 Stunden verfügt das NNS über eine Gesamtanzahl von Reifepunkten, die es unter den abstimmenden Neuronen verteilen möchte, wie es die Protokolle des Internet Computers definieren. Um die Verteilung fair zu gestalten, teilt das NNS die Reifepunkte proportional zum Stimmgewicht der Neuronen auf, die abgestimmt haben.

Neuroneneigentümer können ihre Reifepunkte maximieren, indem sie sicherstellen, dass ihre Neuronen über jeden Vorschlag abstimmen, sie ihr Stimmgewicht durch das Deponieren weiterer ICP-Tokens erhöhen, die

Auflösungsverzögerungen erhöhen oder warten, bis das berechnete Alter des Neurons das maximale Alter von 4 Jahren erreicht.

Sobald Neuronen Reife erlangt haben, können sie verwendet werden, um neue ICP-Tokens für ihre Eigentümer zu erzeugen.

Der genaue Prozess hängt grundsätzlich vom aktuellen Design des NNS ab, das sich verändern und weiterentwickeln kann, wenn das Netzwerk aktualisiert wird, um seine Tokenomics zu verbessern. Im aktuellen Design kann ein Neuron mit Reife verwendet werden, um ein neues Neuron abzuspalten (spawn), das dann neu geprägte ICP-Tokens enthält.

Wenn ein neues Neuron abgespalten wird, entspricht die Anzahl der in ihm deponierten neuen ICP-Tokens in etwa den Reifepunkten, die vom Ursprungsneuron „verbraucht“ wurden. Die Auflösungsverzögerung des neuen Neurons ist null, wodurch die neuen ICP-Tokens sofort abgerufen werden können, wenn dies gewünscht wird.

Der Erzeugungsprozess dauert eine Woche vom Anfang bis zum Ende. Das bedeutet, dass der Eigentümer eines Neurons nicht vorhersagen kann, wie der Preis der neuen ICP-Tokens auf den Märkten sein wird, auf denen sie gehandelt werden, wenn sie verfügbar sein werden. Darüber hinaus hängt die Anzahl der erzeugten ICP-Tokens davon ab, wie sich der Preis während des Erzeugungsprozesses entwickelt.

Steigt der Preis während des Erzeugungsprozesses, wird eine etwas größere Anzahl neuer ICP-Tokens erzeugt, und fällt er eine etwas kleinere Anzahl, mit einer Varianz von +/- 5 %. Dies ermutigt Neuronenbesitzer, Einkommen in Form von ICP-Tokens nur dann zu generieren, wenn die Märkte, auf denen sie gehandelt werden, stabil und gesund sind.

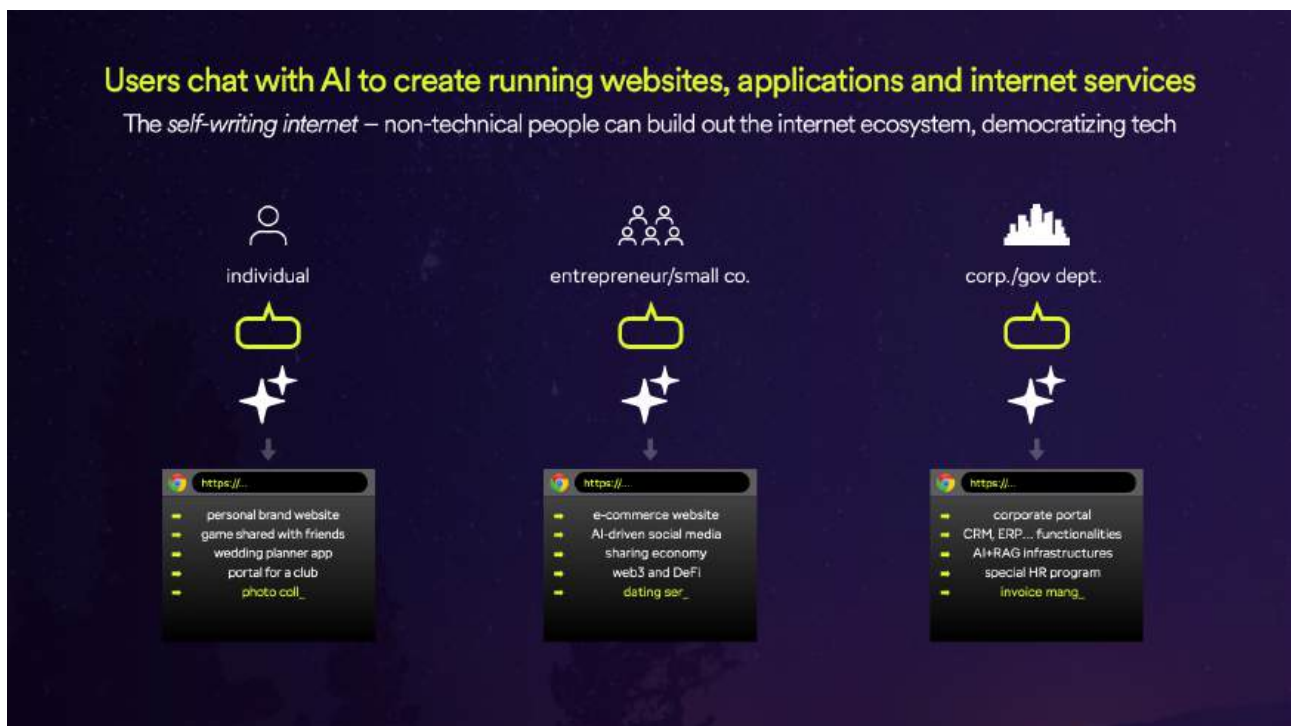
Wie es ICP einer KI ermöglicht eigenständig Applikationen und Dienste zu bauen

Ein zentraler aufkommender Zweck des Internet Computers und der ICP Technologie im Allgemeinen besteht darin, fortschrittliche KI-Modelle zu befähigen, massgeschneiderte Webanwendungen und Internetdienste auf der Grundlage einfacher Anweisungen, die über eine Texteingabeschnittstelle erfolgen, zu erstellen und weiterzuentwickeln.

Die Anwendungsbreite ist enorm. Ein Individuum könnte beispielsweise eine persönliche Marken-Website, einen Hochzeitsplaner oder ein Spiel erstellen, das es mit Freunden teilt. Ein Startup-Unternehmer könnte einen Web3-Dienst für die Sharing Economy oder eine E-Commerce-Website entwickeln,

während ein grösseres Unternehmen ein Unternehmensportal mit CRM- oder ERP-Funktionalitäten oder sogar KI-Infrastrukturen erstellen könnte. Die so erstellten massgeschneiderten Anwendungen und Dienste sind vollständig souverän. Das bedeutet, dass ihr Ersteller den zugrundeliegenden Softwarecode und die enthaltenen Daten besitzt und nicht dem Risiko eines Kunden-Lock-ins ausgesetzt ist, das bei der Nutzung proprietärer Infrastrukturen wie Cloud-Dienste oder SaaS-Plattformen auftreten könnte.

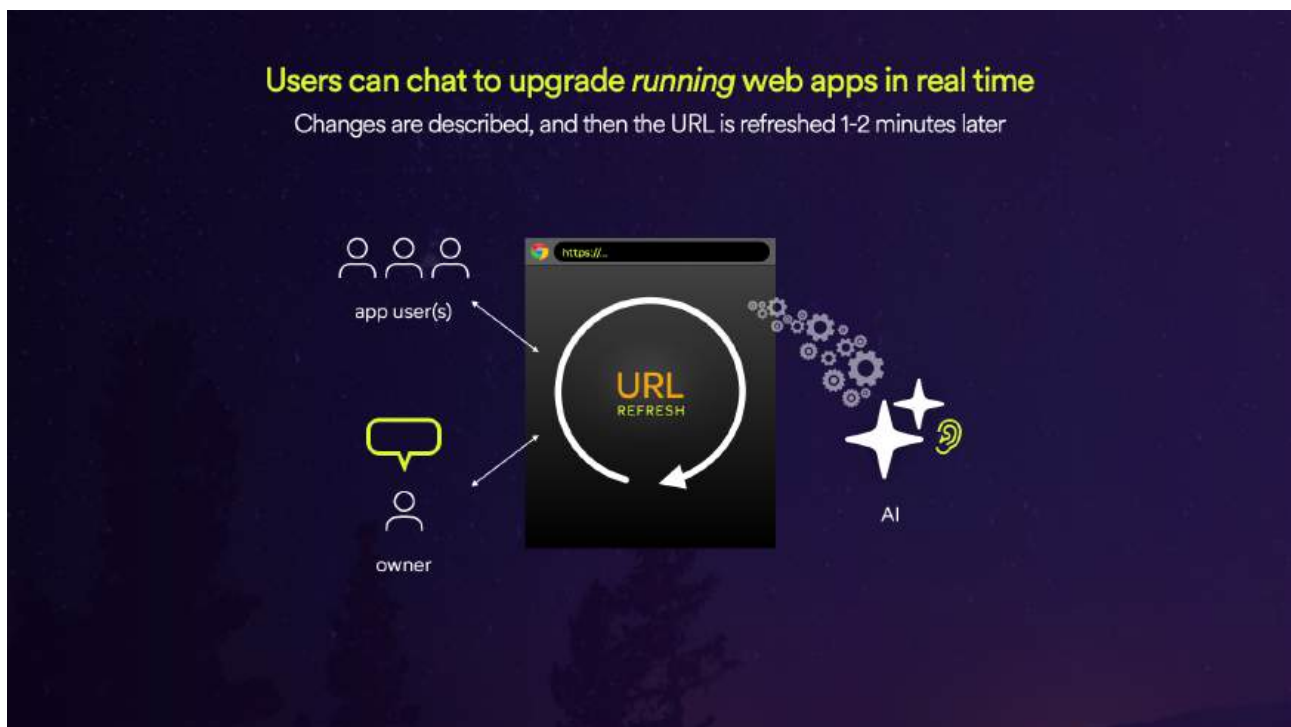
Wenn KI serverlose Software für den Internet Computer schreibt, um Anwendungen gemäss den über die Texteingabe erfolgten Anweisungen zu erstellen oder zu aktualisieren, kann diese „kompiliert“ und mit einem einzigen Schritt ins Netzwerk hochgeladen werden. Dies steht im Gegensatz zur traditionellen IT, bei der Updates Software und Konfigurationen umfassen, die über zahlreiche Plattformkomponenten wie Datenbanken und Webserver verteilt werden müssen. Solche Updates beinhalten oft Aufgaben wie Cloud-Orchestrierung sowie die Konfiguration von Backup- und Sicherheitssystemen. Diese Vorgänge dauern wesentlich länger als die Geschwindigkeit eines Chats und erfordern iterative Problemlösungen.



Obwohl KI immer leistungsfähiger wird, bleibt die Tatsache bestehen, dass sie zur Zeit noch „halluzinieren“ und Fehler machen kann. Dies stellt eine weitere Herausforderung dar, wenn KI Dienste in einer traditionellen IT-Umgebung verwalten muss. Beim Internet Computer hingegen ist Software automatisch manipulationssicher – genauso wie das Netzwerk. Das bedeutet, dass ein Fehler der KI nicht die Tür zu traditionellen Cyberangriffen öffnet. Im Gegensatz dazu könnte ein Fehler in der traditionellen IT katastrophale Konsequenzen haben.

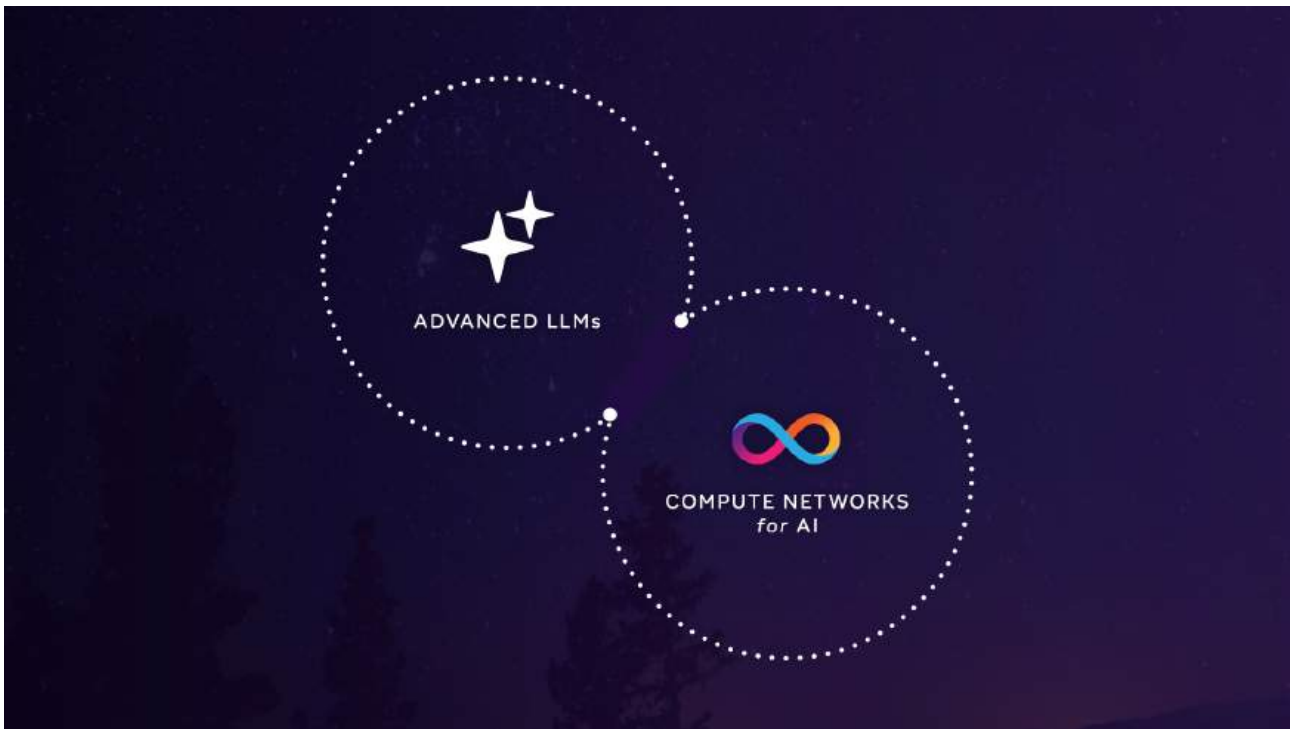
Ähnliche Herausforderungen ergeben sich, wenn KI Dienste aktualisieren soll, die auf traditioneller IT aufgebaut sind. Traditionelle IT wurde in der Regel darauf ausgelegt, seltene und komplexe Upgrades zu unterstützen, die oft Synchronisationsänderungen über mehrere Plattformkomponenten erfordern, anstatt schnelle Upgrades im Minutentakt als Reaktion auf Chat-Eingaben zu ermöglichen. Darüber hinaus beinhalten Software-Upgrades üblicherweise Datenmigrationen, und Fehler können zu Datenverlust führen.

Der Internet Computer unterstützt ein Paradigma namens „orthogonale Persistenz“, das im Wesentlichen den Unterschied zwischen Logik und Daten teilweise aufhebt. Softwareentwickler definieren die Logik, und die referenzierten Daten bleiben automatisch bestehen, ohne dass sie in eine Datenbank oder Datei kopiert werden müssen (dies liegt daran, dass Software innerhalb von persistenten Speicherseiten läuft).



Eine spezielle domänenspezifische Sprache namens Motoko wurde entwickelt, um die leistungsstarken Funktionen der Internet-Computer-Umgebung zu nutzen und die orthogonale Persistenz so anzupassen, dass sie die eigenständige Erstellung von Code und Anwendungen durch KI besser unterstützt.

Zu diesen Anpassungen gehört es, Datenmigrationen, die mit Upgrades verbunden sind, extrem effizient zu gestalten, sodass KI Upgrades für Anwendungen und Dienste in Echtzeit durchführen kann. Darüber hinaus stellen Programmiersprachfunktionen sicher, dass beim Aktualisieren von Software die notwendige Migrationen von gespeicherten Daten als Teil des Software-Update-Codes beschrieben werden. Sollte ein Fehler auftreten, der



zu Datenverlust führen könnte, wird die Aktualisierung fehlschlagen, was die Sicherheit zusätzlich erhöht.

Folien stammen von:

deck.internetcomputer.org

deck.icp.ai