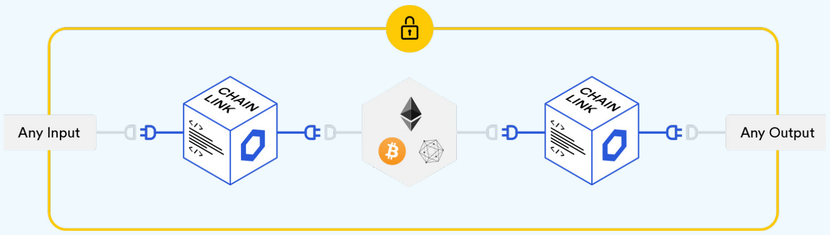
Smart Contracts & die Echtwelt

Ermöglicht sichere Ein- und Ausgaben für Smart Contracts und Kompatibilität unter verschiedenen Blockchains

Smart Contracts sind unverfälschbare, Ende zu Ende gesicherte und hochverfügbare digitale Verträge (Contracts) die automatisch vollzogen werden. Damit ein Contract sicher und verlässlich vollzogen wird, müssen die Ein- und Ausgaben ebenso gesichert sein. Mithilfe von Chainlink können Smart Contracts auf sichere Weise mit Daten aus der Echtwelt gefüttert werden.



Übersicht

Generell können Blockchains und Smart Contracts nicht ohne weiteres mit externen Systemen kommunizieren. Damit ist das Potential der Smart Contracts strikt auf die Funktionen innerhalb der Blockchain begrenzt, sodass Zahlungen und Echtwelterreignisse unerreichbar bleiben.

Um diese Limitierung zu überbrücken gibt es sogenannte "Oracles". Sie liefern Daten von einem System in das andere. Das Problem von den heutigen Oracles jedoch ist dass sie zentrale Instanzen sind und die Kontrolle von solch einem System fällt wieder in die Hände von einem Mittelsmann, genau das was die Blockchain eigentlich lösen soll und vertrauen zwischen fremden Parteien schaffen soll.

Hier kommt Chainlink (ICO in 2017, Live seit Mitte 2019) ins Spiel, Chainlink wurde von der Firma SmartContract.com (gegründet in 2014) als Open Source Projekt gestartet und gilt als das erste dezentrale Oracle System dass jede Form von Daten, Events oder Bezahlsystemen extern mit Blockchains verbindet. Dadurch kann trotz Einfluss externer Daten die Sicherheit und Integrität der Blockchain gewahrt werden.

Die Verweise aus den nachfolgenden Seiten sind von http://chain.link[1] http://smartcontract.com[2].

Was Chainlink zu bieten hat

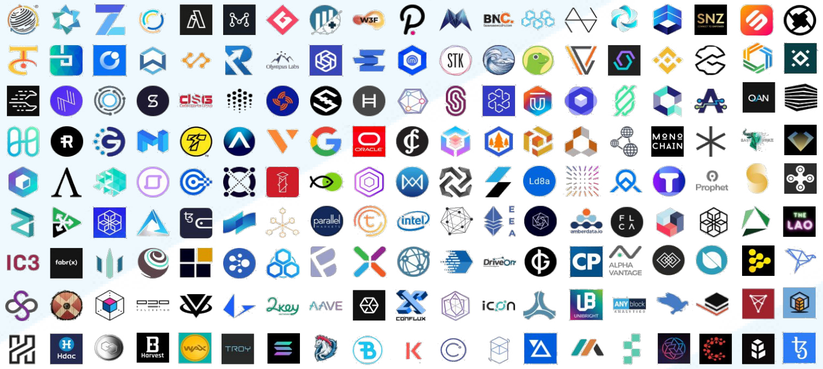
Smart contracts benötigen eine Middleware um auf Daten aus der Echtwelt zugreifen zu können. Diese Daten haben direkten Einfluss auf das Resultat des Smart Contracts. Deshalb ist es wichtig das diese Inputs extrem sicher und genau funktionieren.

Egal ob es sich um ein kleines Startup oder einen riesen Konzern handelt, Chainlink als dezentrales Oracle Netzwerk Middleware kann deinen Smart Contract verifizierbar sicher und genau mit Daten wie Events, Finanzinfo oder Zahlungen füllen.

- Entwickler aus jeder Industrie können in wenigen Schritten ihren eigenen 'Chainlink' aufsetzen, um jegliche API an Smart Contracts verkaufen zu können während die Datenanbieter selbst ihre Daten weiterhin über ihre üblichen Schnittstelle verkaufen. Für das Erstellen eines Chainlink können Entwickler für etwas bezahlt werden das tausende Smart Contract benötigen.
- Große Unternehmen können mithilfe von Chainlink existierende APIs auf dem Smart Contract Markt monetarisieren. Einfach und schnell Daten und APIs mit Hilfe von Chainlink über eine Menge neuer Plattformen verkaufen. Unzählige Smart Contracts könnten dadurch Zugriff auf deine Services bekommen.

Partnerschaften und Integrationen

- 30+ Price Feeds auf dem Ethereum Mainnet, genutzt von 14+ DeFi Applikationen in Produktion.
- 100+ Integrationen, wie z.B Polkadot[3], Tezos[4], Synthetix[5], Aave[6], vv[7], Web3[8] und weitere.
- Kollaborationen mit großen Enterprise Firmen wie Google[9], Oracle[10], SWIFT[11].
- Verfügbar in mehreren großen Entwicklungsumgebungen wie zum Beispiel der beliebten Truffle Suite die Ethereum Entwickler hauptsächlich nutzen.
- Chainlink arbeitet zusammen Intel, Microsoft, IBM und anderen[12] an dem 'Hyperledger Avalon' Framework, welches sichere Off-Chain Berechnungen mithilfe von Intel SGX erlaubt.

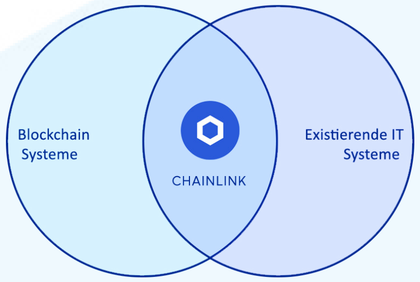


VOLLSTÄNDIGE LISTE an Partnern, Kollaborationen, Frameworks und Kunden von Chainlink oder SmartContract.com unter https://chainlinkecosystem.com [13]

Anwendungsfälle

Zugriff auf externe Daten erlaubt eine ganze Welle an neuen Anwendungsfällen. Mit Daten gefüllte Smart Contracts sind von der Funktionalität her quasi ohne Limit.

- Geld und Finanzen
- Zahlungen
- Versicherung
- Lieferketten
- Regierungen und Behörden
- Enterprise Systeme
- Autorisierung und Identitätslösungen
- Dienstprogramme
- Glücksspiele



Ein Großteil der visionären Smart Contract Anwendungsfälle von denen du vielleicht gehört hast, benötigen im Hintergrund eigentlich Chainlink. Einfach weil die Daten die es für den Anwendungsfall braucht für die Blockchain selbst unerreichbar sind. Um ein paar Beispiele zu nennen: Derivative Smart Contracts von Rohstoffen (Google Prototyp). Automatische Balancierung des Portfolio durch traditionelle Indikatoren wie RSI oder EMA, Markt-Sentiment oder sogar die aktuelle Bitcoin Hashrate. Versicherungen die automatisch eine Entschädigung auszahlen wenn ein Flug zu spät kommt, verschiedene Kredit-produkte ohne Mittelsmann wie Banken die ein Kollateral automatisch errechnen bzw. Anfordern, automatischer Boni-Score. Cloud Lösungen mit Blockchains verbinden und mehr.

EIN SEHR EMPFEHLENSWERTER ARTIKEL ÜBER ANWENDUNGSFÄLLE FÜR SMART CONTRACTS DIE ÜBER TOKENISIERUNG HINAUSGEHEN: 44 ways to improve your smart contract[15]

*** Ein und Ausgabe steht für eine bestimmte Information oder einen bestimmten Auslöser. Zum Beispiel als Eingabe den Preis von einem Bitcoin oder als Ausgabe eine Zahlung in Paypal zu verschicken.**

*** Eine API erlaubt Programme und Webseiten miteinander kommunizieren zu lassen. TradingView benutzt z.B. Binance APIs um Preise zu ermitteln und in Charts darzustellen. Uber = APIs für Zahlungen, GPS, SMS und KYC geschaffen.**

Blockchains mit zentralisierten Datenfeeds zu füllen ist sinnlos Chainlink sorgt für dezentrale und unmanipulierbare Ein und Ausgaben für JEDE Blockchain

Dezentralisierung Erreichen

Ist es wirklich möglich die Wahrheit in einer Welt zu finden in der man einzelnen Quellen nicht vertrauen kann? Chainlink ermöglicht das indem es ein Netzwerk aus Oracles bildet. Anfragen werden von mehreren unabhängigen Node Betreibern gestellt die jeweils unterschiedliche unabhängige Datenquellen/APIs nutzen.

Dadurch dass mehrere Nodes und Quellen genutzt werden, wird statistisch die Chance auf wahrheitsgemäße Daten erhöht. Nodes werden außerdem durch Kriterien wie Reputation und vergangene Performance ausgewählt. Dadurch liegt es im Interesse der Node Betreiber hochqualitative Daten Quellen/APIs zu nutzen. **Dazu ein Beispiel wie es Schritt für Schritt abläuft findest du auf Seite 3** oder auf Chainlink market[15B].

Die Nutzung des LINK Token

Der LINK Token wird als Zahlung und Kollateral für die Sicherheit des Chainlink Netzwerkes genutzt. Wie der Token genutzt wird:

1. Zahlung an Node-Betreiber für das Liefern von Echtwelt-Daten an Smart Contracts.
2. Node-Betreiber nutzen LINK als Kollateral (Kaution/Sicherheit) das im Falle eines Ausfalls des Nodes oder nachweislich falschen Daten einbezogen und als Entschädigung an den Kunden ausgezahlt wird.

LINK ist ein ERC20 Token mit einem weiteren Standard, dem ERC677 obendrauf. ERC677 wurde spezielle von und für Chainlink entwickelt. Es bietet die Funktion "TransferAndCall" um innerhalb einer Transaktion zu bezahlen und Daten zu empfangen.

LINK ist ein Ethereum basierender Token aber für den Fall der Fälle kann er auf jede beliebige Blockchain transferiert werden. Chainlink ist demnach nicht von Ethereum abhängig.

Chainlink Token-Verteilung

Es gibt insgesamt 1 Milliarde LINK Token.

- 350 Mil. wurden beim Token-Sale verkauft.
- 350 Mil. um das ursprüngliche Netzwerk an Node-Betreibern zu Kickstarten (bevor es genug natürliche Nachfrage gibt - Huhn oder Ei Problem).
- 300 Mil. hält die Firma 'SmartContract Chainlink Ltd' für die Finanzierung der Entwicklung.

Warum nutzt man nicht ETH anstelle von LINK?

Es gibt mehrere Gründe die für die Nutzung von LINK gegenüber ETH sprechen:

- Bindet die finanzielle Motivation der Node Betreiber an den Wert des gesamten Chainlink Netzwerkes.
- Isoliert die Sicherheit und die Wirtschaftliche Bandbreite (LINK Stake) von äußeren Faktoren.
- Wenn ein größerer Netzwerkangriff stattgefunden hat, werden die LINK Tokens die als Kollateral eingesetzt wurden wertlos und schaden somit dem Angreifer. Dies gilt nicht für einen nicht verwandten Vermögenswert (ETH).
- Stablecoins würden auch nicht funktionieren, da sie entweder von Fiat unterstützt und somit Opfer von Zensur werden könnten oder auf Oracles angewiesen sind, um zu funktionieren.
- Die wachsende Nachfrage nach LINK in Kombination mit einem schrumpfenden Angebot (aufgrund von Staking) schafft eine positive Rückkopplungsschleife, in der die zunehmende Anwendung den Preis von LINK erhöht, wodurch die wirtschaftliche Bandbreite erhöht und eine stärkere Akzeptanz unterstützt wird.
- Chainlink ist blockchain-unabhängig und benötigt ein Token, das leicht zwischen Blockchains überbrückt werden kann.

Blockchain Unabhängig

Chainlink supportet JEDE Blockchain. LINK wurde als Ethereum Token generiert aber Chainlink kann Daten von jeder zu jeder Blockchain schicken.

Es gibt zwei Wege Chainlink zu integrieren:

1. Jeder Entwickler kann einen einfachen externen Adapter[16] schreiben um jeder Blockchain kompatibilität zu Chainlink zu geben. LINK Zahlungen und Staken finden dann jedoch weiter auf der Ethereum Blockchain statt.

2. Der LINK Token kann durch die Funktion "LockDeposit" auf andere Blockchains überbrückt werden. Damit kann Chainlink Funktionalität z.B auf kleineren Proof of Stake Blockchains nativ unterstützt werden ohne über Ethereum geroutet werden zu müssen.

Chainlink Smart Contracts auf neuen Blockchains auszurollen und den Token zu überbrücken ist schon komplexer und benötigt Blockchain-Übergreifende Kommunikation.

Bisher Chainlink kompatible Blockchains:

- Ethereum
- Tezos
- Polkadot
- Hedera Hashgraph
- Jede EVM-kompatible Blockchain
- Zilliqa
- Kava/Cosmos
- Bitcoin
- Einige mehr

Anpassbare Sicherheit und Daten

Chainlink's Flexibilität kommt größtenteils durch die sog. "Service Agreements" (SA) Jeder Entwickler kann ein Oracle Netzwerk aufbauen wie auch immer er es benötigt.

Anpassungen einer Reihe verschiedener Parameter:

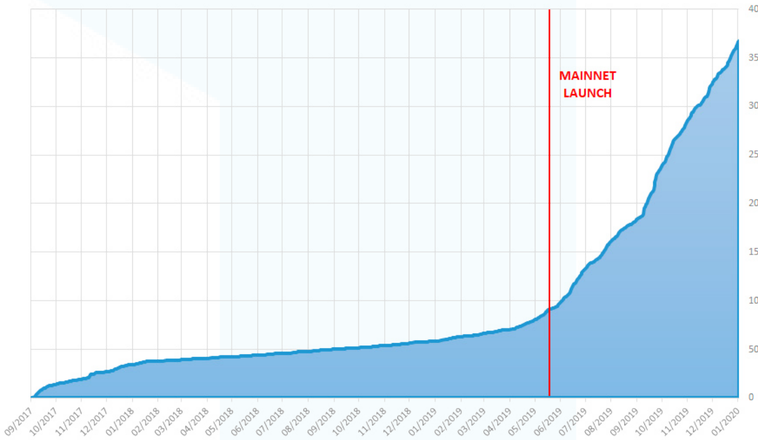
- Auswahl und Anzahl von Nodes
- Auswahl und Anzahl von Daten-Quellen
- Anzahl an LINK Token als Bezahlung
- Anzahl an LINK Token als Kollateral / Sicherheit als Anforderung
- Minimale Reputation
- Slashing Bedingung (Verlust des Stakes)
- Node Zertifizierung
- "Threshold Signatures"
- TEEs (Siehe weiter unten für eine Erklärung von TEE's)
- Mixicles

Node Reputation/Ranking*: Chainlink Nodes haben einen Reputations-Faktor. Chainlink Kunden/Endnutzer können festlegen wie hoch der Wert an Reputation sein muss für einen Node um für den jeweiligen 'Job' in Frage zu kommen. Reputation ergibt sich aus folgenden Werten:

- Node Verfügbarkeit (Online-Zeit)
- Korrektheitsgrad der Antwort
- Durchschnittliche Rückmeldezeit
- Gesamtzahl zugewiesener Anfragen
- Gesamtzahl von abgeschlossenen Anfragen
- Gesamtzahl von akzeptierten Anfragen
- Menge an Strafzahlungen
- Menge an LINK als Kollateral (LINK Stake)

Netzwerk Nutzung

Steigende Zahl von Chainlink betreffenden Smart Contracts zeigt ein deutliches Wachstum der Aktivität und Interesse von Entwicklern.



Total number of smart contract addresses that have ever received LINK vs. Date each contract recevied LINK for the first time.

Zugangsbeschränkte oder frei zugängliche, öffentliche oder private, jede Blockchain braucht eine vertrauenswürdige Oracle-Lösung um nützlich zu sein.

First-Mover Vorteil

- Erstes dezentrales Oracle Framework.
- Lang-bestehende Verbindungen zu Industrie Giganten wie Swift[17], Google[18], und Oracle[19],, führende Recherche Konsultanten wie Gartner[20] und Capgemini[21]) und Enterprise Konsortiums wie (IC3[22], EEA[23], Baseline protocol[24] und Hyperledger[25]).
- Netzwerk Effekt: Chainlink's große Nummer an Kunden, Nodes und Daten-Quellen macht Chainlink attraktiv.

Konkurrenz

- **Direkt**: Alternative dezentrale Oracles die nicht flexibel mit der dezentraliserung oder dem Datenformat sind oder plattformabhängig sind. Davon eingeschlossen sind Tellor[26], Witnet[27], Compound's OOS[28], Maker's OSM[29], Doracle[30] von iExec (hat Chainlink integriert) & Band.

- **Indirekt**: Zentrale Oracles wie Provable[31] (Partnerten mit Chainlink) und Rhombus[32].

Auftauchende Konkurrenz wird es schwer haben Marktanteil zu bekommen wenn die meisten dApps bereits ein dezentrales Oracle integriert hat das sich über Jahre bewiesen hat und einen riesigen Netzwerk Effekt mit zu bringt.

Open Source & Prüfbar

- Der Code ist Open Source (hier[33]).
- Entwicklung öffentlich einsehbar (hier[34]).
- Bug Belohnungs Programm (hier[34B])
- 4 unabhängige Audits:
  - 3 vom Haupt Contract (hier[35]).
  - 1 vom Aggregator Contract (here[36]).
  - 1 von Mixicles (in Bearbeitung).

Starke Community

- Die Chainlink Community (die Marines) sind eine der größten, besten unterrichteten und kreativsten Communities im Krypto-Umfeld, bekannt für eine riesige Menge an Memes und Kameradschaft.
- Offizielles discord[37] und gitter[38] um das Team zu erreichen.
- Ein offizielles Chainlink Community Programm existiert bereits in vielen Ländern und mehreren Kontinenten auf der ganzen Welt. Eine vollständige Liste findet sich hier[39].

Team

- Team[40] von über 25 Personen
- 6 Berater, unter anderem:
  - Tom Gonser (Docusign Gründer). Artikel[41]
  - Ari Juels (formalisierte[42] Proof of Work; RSA chief scientist[43]; IC3 Gründer[44])
  - Evan Cheng (Facebook[45] R&D Dir & LLVM Autor bei Apple)
  - Hudson Jameson (Ethereum Foundation[46])
  - Andrew Miller (Konsens Forscher[47])

- Momentan 11 offene Positionen. Karriere hier[48]
- Kein Hype vom Team, nur Professionalität.

*Info über die Konkurrenz und dem 'Coinbase oracle': Obwohl Coinbase ein großer und seriöser Akteur in diesem Bereich ist, ist der von ihnen angebotene Service ein Preis-Feed (kein allgemeines Oracle) und die Ergebnisse werden nicht auf die Blockchain geschrieben. Daher kann es weder als Blockchain-Oracle noch als Konkurrent im Oracle-Bereich betrachtet werden.

Chainlink konkurriert nicht mit Blockchain-Plattformen, sondern verbessert sie

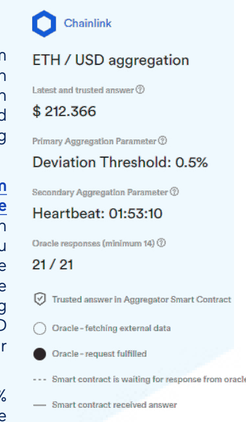
DeFi & Chainlink

DeFi (Decentralized Finance) ist derzeit einer der am schnellsten wachsenden Sektoren im dezentralen Ökosystem. DeFi besteht nicht nur aus dezentralen Börsen, sondern auch aus Kreditplattformen und Derivaten, die vollständig dezentral und vertrauenswürdig betrieben werden.

Bei Open Finance geht es nicht darum, ein neues System von Grund auf neu zu erstellen, sondern das bestehende System zu demokratisieren[54] und es mit offenen Protokollen und transparenten Daten gerechter zu gestalten. Das traditionelle Finanzsystem weist einige Nachteile auf, wie z.B. langsame grenzüberschreitende Überweisungen, hohe Gebühren, Zensur, Diskriminierung ("Sie können nur investieren, wenn Sie 1 Mio. USD besitzen"), Banken können Gelder einfrieren oder sogar wie in der Finanzkrise Banken zum Absturz bringen.

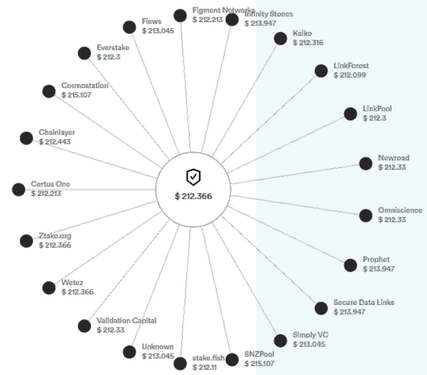
Das Geschäftsmodell für den DeFi-Sektor erfordert 100% sichere und genaue Preis-Feeds aller Vermögenswerte (Oracles werden in 90%+ aller Anwendungsgebiete von DeFi benötigt). In DeFi wie auch im Finanzwesen im Allgemeinen sind Sicherheit, Zuverlässigkeit und Reputation für die Rentabilität gleichermaßen von größter Bedeutung. Lesen Sie diesen **empfehlenswerten Artikel**[55] des Teams über DeFi.

Chainlink liefert derzeit die Referenzdaten für 36 Vermögenswerte oder Handelspaare wie EUR / USD. Diese Preis-Feeds werden bereits von Synthetix[56] (Top 2 an gesicherten USD), Aave[57](top #5), Ampleforth[58] und von dy/dx[59] (top #7) untersucht. Daten von: defipulse.com[60], exploring.link[61], Referenz ETH/USD[62], Liste aller bereitgestellten Feeds[63]



Live platforms using Chainlink

GESAMTWERT DURCH CHAINLINK GESICHERT
Stand 1.Mai 2020
158 M$



Synthetix
Synthetic Vermögenswerte
115 M$

Aave
Verleihen & Leihen
44 M$

DMM
DMM Vermögenswerte der realen Welt
8 M$

Ampleforth
Warengeld
5 M$

Loopring
DEX Protokoll
5 M$

BZX
DEX Protokoll
3 M$

Ein Blick auf die Technologie hinter Chainlink

Zusammen formen diese Innovativen Technologien die fortschrittlichste Oracle Technologie auf dem Markt

1. Privatsphäre & Überprüfbarkeit: Mixicles

Mixicles ist im Wesentlichen ein Mixer, der externe Oracles verwendet, um die Privatsphäre für öffentlich einsehbare Smart Contracts auf der Blockchain zu ermöglichen. Der Smart Contract ist in zwei Teile unterteilt, in denen die sensiblen Daten und die Geschäftslogik außerhalb der Blockchain bleiben und die private Abwicklung auf der Blockchain erfolgt. Mixicles ermöglichen:

- Die Geheimhaltung von Vertragsgeschäftslogik und externen Oracledaten, sowie dem endgültigen Ergebnis des Zahlungsempfängers.
- Finanzverträge sind **zwar nicht öffentlich einsehbar, für Aufsichtsbehörden jedoch überprüfbar**.
- Blockchain-Agnostizismus, wodurch Chainlink auch in Unternehmens-Blockchains verwendet werden kann.
- Eine neue Generation von Datenschutz berücksichtigenden und skalierbaren DeFi-Instrumenten.

***Mixicles sind zur Zeit in der Prüfung durch externe Firmen. Empfehlenswerter Artikel darüber hier[49].**

3. Trusted Computation Framework

Das Trusted Compute Framework (TCF) ist eine Möglichkeit für Unternehmen, vertrauenswürdige Ausführungsumgebungen (Trusted Execution Environments = TEEs) zu verwenden, um Off-Chain-Berechnungen für On-Chain-Verträge zu sichern. Chainlink stellt sicher, dass die gelieferten Daten verschlüsselt und manipulationssicher sind.

Die Berechnung erfolgt normalerweise On-Chain und ist sehr teuer. TCF ermöglicht es Verträgen stattdessen, komplexe Berechnungen von On-Chain- zu Off-Chain-Systemen (On-Premise oder in Cloud-VMs) zu verschieben und die Ergebnisse nach Abschluss wieder in der Kette zu veröffentlichen, während die Verifizierungs- und Attestierungsverifizierungseigenschaften beibehalten werden.

Chainlink ist Teil des "Hyperledger Avalon Trusted Compute Framework" von Intel, IBM, Microsoft, Alibaba Cloud und Banco Santander.
Siehe Intel Pressemitteilung[50] & Artikel[51].

2. Geringe Kosten und Skalierbar: 'Threshold Signatures'

In Chainlink werden „Threshold Signatures" (TS) implementiert, mit denen Nodes ihre Antworten außerhalb der Blockchain zusammenfassen können, wodurch die Transaktionskosten (Gas) erheblich reduziert und die Auswirkungen auf das Blockchain-Netzwerk minimiert werden.

Wie kann dies erreicht werden? Threshold Signatures ebnen den Weg zur Lösung des Oracle-Dilemmas: Man möchte, dass sich Hunderte, Tausende oder sogar Zehntausende von Zeugen auf einen Datenpunkt einigen, aber das ist aufgrund der wachsenden Anzahl erforderlicher Transaktionen teuer.

TS ermöglicht es Oracles untereinander Off-Chain zu kommunizieren. Es wird sich auf etwas gemeinsam geeinigt und dann zusammen eine einzelne Signatur erzeugt die als Antwort für die Anfrage abgeschickt wird. Artikel[52]

4. Staking Kollateral (Die eigene Hand ins Feuer legen)

Kurz gesagt, Staking ist, wenn Nodes, die Daten an einen Smart Contract liefern, eine vorbestimmte Menge an LINK als Sicherheit einsetzen.

- Wenn Nodes keinen zuverlässigen Datenpunkt liefern, ihn nicht rechtzeitig bereitstellen oder überhaupt keine Daten liefern, werden sie bestraft, indem ihr LINK-Kollateral gekürzt wird.
- Wenn Nodes stattdessen einen zuverlässigen, zeitnahen Datenpunkt für einen Oracle-Auftrag bereitstellen, wird ihnen eine Gebühr in LINK gezahlt. Sie können die Gebühren zurückziehen und ihre Sicherheiten behalten oder ihre Sicherheiten teilweise / vollständig zurückziehen. Bei böswilligen oder nicht reagierenden Nodes werden die Sicherheiten gekürzt und ihr Ruf wird ebenfalls als Strafe verringert. Artikel[53].

Auf diese Weise fördert das Chainlink-Netzwerk ehrliches Verhalten und bestraft böswilliges Verhalten von Nodes.

Chainlink und der Standardisierungsprozess

Chainlink ist an mehreren Initiativen beteiligt, um Blockchain-Technologien zu standardisieren

1. Enterprise Ethereum Alliance & Chainlink

Die Enterprise Ethereum Alliance (EEA)[64] ist eine von Mitgliedern betriebene Organisation zur Durchsetzung von Standards, deren Charta darin besteht, offene Blockchain-Spezifikationen zu entwickeln, die die Harmonisierung und Interoperabilität für Unternehmen und Verbraucher weltweit fördern. Chainlink ist seit 2017 Teil der EEA zusammen mit sehr bekannten Unternehmen. Im Januar 2020 schuf die **EEA die von Chainlink und anderen geleitete Taskforce "Mainnet Integration for Enterprises" - EMINENT**[65].

Der Schwerpunkt dieser Arbeitsgruppe liegt auf der Erstellung von Open Source-verfügbaren Referenzimplementierungen und Richtlinien für die Integration des Ethereum-Mainnets in Unternehmens- "Aufzeichnungssysteme". Mit anderen Worten, das Ziel ist es, einen Standard zu erreichen, der es ermöglicht, Business-Backends (CRMs & ERPs) mit dem Ethereum-Mainnet zu verbinden.

ENTERPRISE ETHEREUM ALLIANCE · cisco · CREDIT SUISSE · BBVA · Deloitte. · THOMSON REUTERS · intel · bp · HYPERLEDGER · J.P.Morgan · ING · UBS · Santander · Microsoft · AMD · +178 more

2. Baseline protocol & Chainlink

Das Baseline-Protokoll, das im März 2020 von Ernst & Young in Zusammenarbeit mit Microsoft, Consensys, AMD, Chainlink und anderen vorgestellt wurde, ist eine Open-Source-Initiative, die Fortschritte in Kryptografie, Blockchain und offenen Standards kombiniert, um sichere und private Geschäftsprozesse über das öffentliche Ethereum Mainnet zu niedrigen Kosten bereitzustellen. Das Protokoll bietet Unternehmen einen gemeinsamen Rahmen, der eine vertrauliche und komplexe Zusammenarbeit zwischen ihnen ermöglicht, ohne dass sensible Daten auf die Blockchain gelangen. Siehe Pressemitteilung hier[66].

EY · CONSENSYS · Microsoft · AMD

3. Hyperledger Avalon & Chainlink

Im Oktober 2019 stellte Hyperledger das Projekt „Hyperledger Avalon" vor. Es handelt sich um eine vom Ledger unabhängige Implementierung des Trusted Compute Framework. Ziel ist es, die On-Chain-Verarbeitung auf sichere Weise auf Off-Chain (Cloud) zu verlagern. Avalon wurde entwickelt, um die Nachteile der On-Chain-Berechnung (Skalierbarkeit und Vertraulichkeit) abzumildern. Es entlastet die Blockchain, erhöht die Leistung und behält gleichzeitig Integrität und Bezeugbarkeit bei. Chainlink arbeitet zusammen mit anderen Partnern wie IBM, Oracle, Microsoft und anderen an der Avalon-Spezifikation. Intel Pressemitteilung[67]

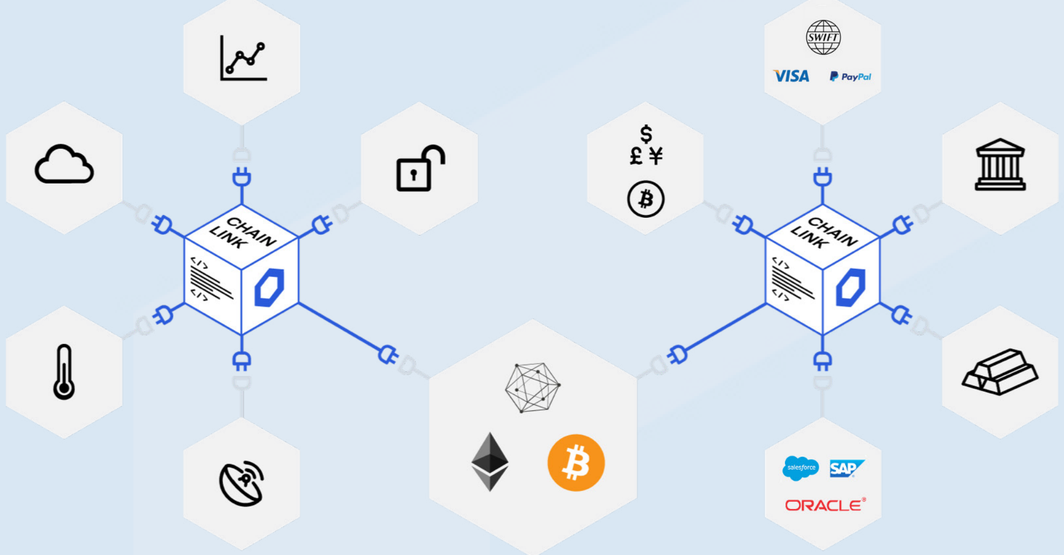
IBM · intel · Santander · Microsoft · ORACLE · Alibaba Cloud

*** Was ist TEE? Eine Trusted Execution Environment (TEE) ist ein hochsicherer, hardwarebasierter, isolierter Rechenbereich in modernen CPUs, der die Ausführung privater und attestierter Berechnungen ermöglicht, auf die Anwendungen, das Betriebssystem, der Manager virtueller Maschinen oder sogar der Computerbetreiber nicht zugreifen können.**

Einige interessante Highlights

- Oracle Corp wird Chainlink im dritten Quartal 2020 gemäß der Openworld 2020-Konferenz von Oracle integrieren. Die Folien gibt es hier[68] zu sehen.
- Chainlink ist seit langem Mitglied der IC3[70], (Initiative for Cryptocurrencies and Contracts), der führenden akademischen Forschungsinitiative für Distributed Ledger Technology und wurde von Ari Juels mitgegründet. Neben Chainlink sind JPMorgan, Microsoft, Cisco, Siemens und Intel weitere IC3-Mitglieder.
- Über ISDA (International Swaps & Derivatives Association): Im Januar 2020 wurde BAPI[71] angekündigt, eine bilaterale Plattform für Smart-Derivatives, die Technologien wie eine **Standard-ISDA-Vorlage**, Ethereum, OpenLaw, Chainlink und Kaleido verwendet. Es wurde von Carlos Matilla, Executive Director bei der Santander Investment Bank, mitentwickelt.
- Chainlink arbeitet derzeit mit SWIFT[72] dem globalen Standard für Interbank-Messaging. SWIFT wird von mehr als 11.000 Finanzinstituten in mehr als 200 Ländern und Territorien verwendet. Über 32 Millionen Nachrichten bewegen täglich Billionen von Dollar.
- Im Januar 2017 schrieb Professor Klaus Schwab, Gründer und Vorsitzender des Weltwirtschaftsforums, ein Buch mit dem Titel „Die vierte industrielle Revolution". In diesem Buch beschreibt er SmartContract.com als Wendepunkt für den "Shift in Action" unter "Bitcoin and the Blockchain". (Siehe hier[74]).
- Selbst zentralisierte Oracles wie "Provable" können ihre Daten weiterhin wie gewohnt verkaufen, indem sie einen externen Adapter erstellen und Daten als weitere verfügbare Quelle im Chainlink-Netzwerk verkaufen. Daher verdienen beide Geld mit dem Verkauf von Daten auf ihre reguläre zentrale Art und Weise sowie über das dezentrale Chainlink-Netzwerk.
- Es gibt 3 Arten von APIs: Private, Partner or public. Zwei sind passwortgeschützt. Chainlink liefert Daten von allen drei. Weder die direkten Konkurrenten Tellor noch Band können auf Daten von privaten oder Partner-APIs zugreifen.
- Chainlink ist den US-regulierte Handelsplattformen Coinbase, Gemini und Kraken gelistet, die New Yorker Anlegern das Handeln mit LINK anbietet. Die Gesetze zum Finanzrecht in NYC gehören zu den härtesten der Welt.
- Chainlink erwarb das von IC3 programmierte Oracle „Town Crier", um die Möglichkeiten seines dezentralen Oraclenetzwerks mit Unterstützung nativer TEEs (Trusted Execution Environments) zu erweitern. (Forbes Artikel[75] | Weitere Informationen[76] | * Was ist TEE?)
- Chainlink hat zwei wichtige Marktplätze:
  1. market.link[77], erstellt von LinkPool, ist ein Marktplatz, auf dem jeder seine Nodes, Adapter und die von ihm angebotenen Jobs auflisten kann. Jeder kann diese Liste von Nodes sehen und nach verschiedenen Kriterien filtern.
  2. honeycomb.market[78], von CLCG erstellt, ermöglicht Entwicklern ihre Smart Contracts und dezentralen Apps mithilfe mehrerer hochwertiger und geprüfter Chainlink-Nodes von Betreibern wie Certus.One, LinkForest & Cosmostation mit einer Vielzahl hochwertiger, kostenpflichtiger APIs verbinden. Testnet-APIs werden kostenlos angeboten.
- Selbst zentralisierte Oracles wie "Provable" können ihre Daten weiterhin wie gewohnt verkaufen, indem sie einen externen Adapter erstellen und Daten als weitere verfügbare Quelle im Chainlink-Netzwerk verkaufen. Daher verdienen beide Geld mit dem Verkauf von Daten auf ihre reguläre zentrale Art und Weise sowie über das dezentrale Chainlink-Netzwerk.
- Dies ist die einzige Bemerkung zu Chainlink als Investition: Chainlink war in den letzten 2,5 Jahren die Kryptowährung mit der besten Performance. Der ROI (Return on Investment) ist 1.700% höher als der durchschnittliche Altcoin und + 900% besser als Bitcoin. (Siehe hier[79]).

Jede Art von Eingabe. Jede Art von Ausgabe. Jede Art von Blockchain.

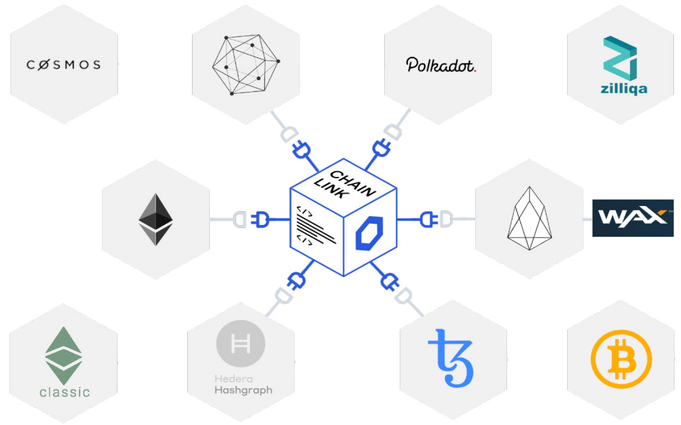


Mögliche Verbindung mit beliebiger Quelle eines Datenfeeds / API

Öffentliche und private Blockchains werden durch Chainlink unterstützt

Zahlungen überallhin senden Verbindung zu jeder Art von Backend-Systemen möglich

Von Chainlink unterstützte Blockchains



Chainlink anhand von Beispielen und häufig gestellten Fragen

Ein Beispiel für das Arbeiten mit Chainlink (mit Staking)

1. Bob braucht vertrauenswürdige Daten für seinen Smart Contract, also fragt er Chainlink ab.
2. Dann fordert Bob eine bestimmte Anzahl von Chainlink-Nodes unter Verwendung eines Smart Contracts an, der angibt, dass sie mindestens eine bestimmte Anzahl vorheriger Transaktionen erfüllen müssen, eine bestimmte Prozentzahl an Genauigkeit in ihrer Auftragshistorie haben und verlangen, dass von jedem einzelnen Node eine bestimmte Menge an LINK als Strafzahlung eingesetzt wird als Garantie dafür, dass sie ihren Teil der Arbeit wahrheitsgemäß erfüllen.
3. Bob legt außerdem fest, wie viel LINK er bereit ist, für den Datenabruf zu zahlen.
4. Alle Chainlink-Nodes, die Bobs Anforderungen entsprechen, bieten nun darum ein Oracle für seinen Smart Contract sein. Bob wählt diejenigen Oracles aus, die den niedrigsten LINK-Betrag als Transaktionsgebühr verlangen.
5. Die von Bob ausgewählten Nodes stellen die geforderten Daten bereit und ihre Antworten werden durch den von Bob ausgewählten Aggregationsvertrag zusammengetragen. Diese Daten werden nun an Bobs Smart Contract übermittelt, jeder Node wird in LINK bezahlt und die Strafzahlungen werden an all diejenigen Nodes vergeben, deren Daten nicht mit dem Konsens nicht überein gestimmt haben.
6. Die Nodes deren gelieferten Daten mit dem Konsens übereingestimmt haben, verfügen jetzt über mehr LINK, die sie für zukünftige Strafzahlungen behalten oder auf dem Markt verkaufen können.

Zwei wichtige Hinweise:

- Sobald Mixicles live ist (momentan in Überprüfung durch Dritte), werden der gesamte Prozess, die Vertragsgeschäftslogik und die externen, durch Oracles gelieferte Daten, sowie das endgültige Ergebnis des Zahlungsempfängers geheim gehalten, während sie durch **Aufsichtsbehörden weiterhin prüfbar** sind.
- Sobald die Threshold Signatures aktiv sind und nicht jeder Node seine Antwort in die Kette schreibt (hohe Kosten, und Überlastung des Netzwerks), wird ein Konsens außerhalb der Blockchain (Off-Chain) erreicht und Ergebnisse in nur einer Transaktion auf die Blockchain geschrieben.

FAQ - Häufig gestellte Fragen und Antworten

1. Ist Node-Ranking und Staking dasselbe?
Nein, jeder Node hat ein Ranking (Reputation), das durch seine frühere Leistung bestimmt wird. Das Einsetzen von LINK-Tokens ("Staking") ist eine zusätzliche Metrik, die von den Antragstellern bei der Auswahl der möglichen Nodes berücksichtigt wird. Wenn mehr LINK zum Staken verfügbar ist, erhöht sich die Wahrscheinlichkeit, dass ein Noden Wahrheitsgemäß handelt, aber auch das Ranking eines Nodes spielt dabei eine Rolle.

2. Würde mein LINK-Node nicht automatisch im Ranking steigen wenn ich einen riesen Menge an LINK halten würde?
Nein, das Node-Ranking berücksichtigt verschiedene Faktoren für die Reputation eines LINK-Nodes von denen das Staking und die eingesetzte Menge an LINK-Tokens nur einer der Parameter neben vielen anderen ist.

3. Was für Faktoren sind für das Node Ranking relevant?
Dies hängt von einer Vielzahl von Faktoren ab: Uptime, Richtigkeit/ Genauigkeit der Antworten, Gesamtzahl der zugewiesenen/ akzeptierten/ abgeschlossenen/ abgelehnten Anfragen, durchschnittliche Antwortzeit, Historie der Strafzahlungen und die Anzahl der eingesetzten LINKs.

4. Ist Staking schon live?
Nein, es wird wahrscheinlich nach anderen Hauptmerkmalen wie Mixicles & Threshold Signatures kommen. Netzwerke werden momentan durch den Ruf eines Nodes und die Opportunitätskosten für den Verlust zukünftiger Einnahmen gesichert, sollten Nodes in eigenem Interesse bzw. Böswillig handeln. Das Chainlink-Kernteam subventioniert Oracle-Netzwerke mit den Mitteln aus dem Token-Verkauf, um sicherzustellen, dass die Nodes richtig reagieren und ein Node in den frühen Tagen des Netzwerks wirtschaftlich betrieben werden kann.

5. Was sind die Erträge aus dem Staken?
Dies variiert von Node zu Node basierend auf dem Ranking (siehe Nr. 3), der Reputation, der Anzahl der eingesetzten LINKs und dem Volumen der empfangenen Jobs. Je zuverlässiger, genauer und schneller ein Node reagiert, desto wahrscheinlicher ist es, dass er aufgrund des höheren Auftragsvolumens und der höheren Gebühren, die erhoben werden können, höhere Renditen für seine eingesetzten LINK erzielt.

6. Gibt es Verträge bei denen keine LINK-Tokens eingesetzt werden müssen?
Ja, Verträge können eine beliebig festgelegte Anzahl an eingesetzten LINK-Tokens erforden (siehe Abschnitt "Anpassbare Sicherheit und Daten). Die eingesetzte Anzahl an LINK ist nur einer von mehreren Faktoren, die der Antragsteller/Ersteller in seinem Dienstleistungsvertrag verlangen kann. Es liegt an den Antragstellern, wie viel LINK für einen Job eingesetzt werden muss, und es ist Sache des Node-Operators zu entscheiden, welche Job er annehmen möchte.muss, und es ist Sache des Node-Operators zu entscheiden, welche Job er annehmen möchte.

CHAINLINK
SMART CONTRACTS & REAL WORLD

http://chain.link | http://smartcontract.com

COORDINATED BY: @CRYPTODAVID_ SPECIAL THANKS TO: @HAHUS | @CHAINLINKGOD | @DLTPANDU | @BAUMGART_V
@CHAINLINKP | @CRYPTOSPONGE3 | @CRYPTO___ORACLE | @KWSANTIAGO | @THELINKMARINE1 | @DAGCHADHEADROOM | THE INVISIBLE DESIGNER

Whitepaper[80]
Community: 'The missing piece to the god protocol'[81]
Community: 'An in-depth look at LINK token'[82]
Devs: Chainlink technical documentation[83]