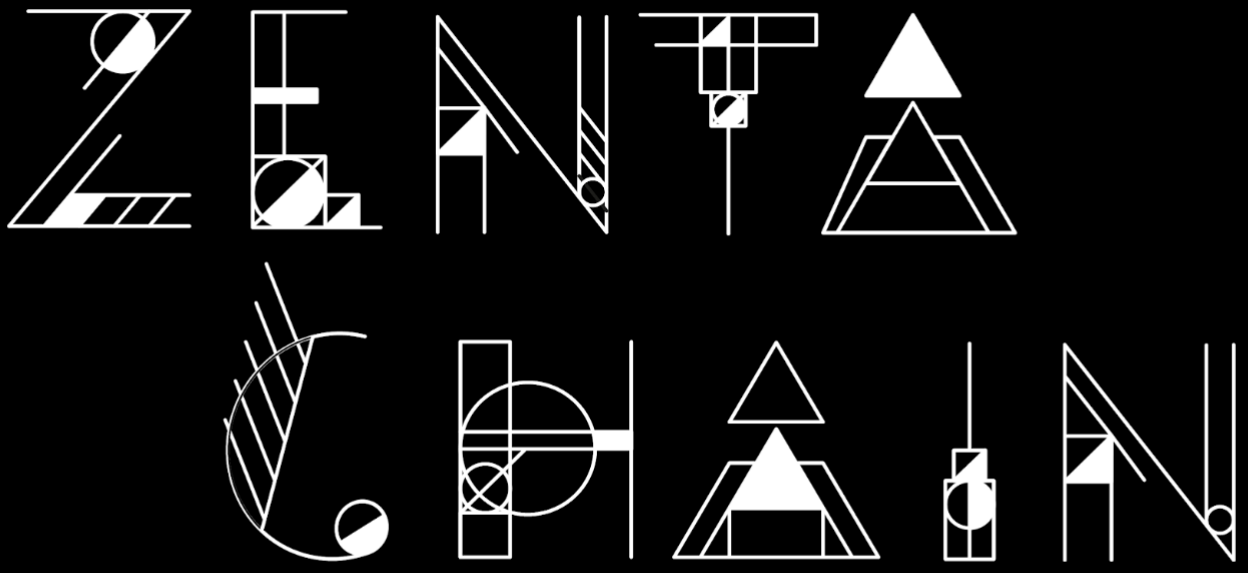


Weißbuch

“ die Zukunft beleuchtet das Potenzial der Gegenwart ”

Version: 1.2

WHITEPAPER-BEITRAGENDE

Zentachain.io

BESONDERS DANKE an Zentachain und Freunde!
E-mail:Team@zentachain.io

Entwickelt für Sicherheit, Anonymität und Offline-Kommunikation

Zentachain.io
(Datum:21.08.2020, Version 1.2)

Preface:

Die digitale Revolution hat die Welt, in der wir leben, umgeschrieben. Wir leben bereits in einer neuen Version unserer Zukunft. Wie Barbrook 2006 sagte: "Die Bedeutung der neuen Technologien liegt nicht darin, was sie hier und jetzt leisten können, sondern darin, was fortgeschrittenere Modelle eines Tages leisten könnten. Die Gegenwart wird als die Zukunft im Embryo verstanden - und die Zukunft beleuchtet das Potential der Gegenwart". Die digitale Transformation leistet einen größeren Beitrag zu unserer Zukunft. Die Menschen sind heute mehr als je zuvor von der Technologie abhängig. Seit der Erfindung des Personalcomputers und in jüngerer Zeit auch des Smartphones scheint fast die ganze Welt miteinander verbunden zu sein. Wir können uns eine Welt ohne digitale Kommunikation und Interaktionen, soziale Medien, nutzergenerierte Websites und freie Online-Enzyklopädien nicht vorstellen. Die Bedeutung des Internets, der Fasern, die uns alle verbinden, nimmt zu. Jetzt haben Sie Zugang zur Welt, und die Welt hat Zugang zu Ihnen. Die weitere Digitalisierung kann als eine positive Entwicklung angesehen werden, weil sie die gesamte Arbeitsweise verändert und dadurch nutzbarer und effizienter macht. Sie erhöht die Mobilität und Produktivität und verringert den Bedarf an einem eigenen Arbeitsplatz. Aber die digitale Revolution hat auch eine dunkle Seite, und genau das ist es, was Zentachain vor Unternehmen schützt, die Ihre Dateien und Dokumente auf einem zentralen Server speichern. Zentalk schützt Ihre Kontakthistorie vor großen Unternehmen, die all diese Informationen verkaufen können, weil sie Ihre Nachrichtenhistorie haben. Die Kryptographie ermöglicht Zentachain die Authentifizierung von Kommunikationen über nicht vertrauenswürdige Kanäle, solange die geheimen Schlüssel nicht offengelegt werden oder sich auf einer zentralen Plattform befinden. Für Zentachain ist es wichtig, den Informationsaustausch über das Internet und die dezentrale Speicherung von vertraulichen Daten zu schützen. Das Zentachain-Team arbeitet mit großer Präzision bei der Kommunikation und Speicherung und achtet sehr auf Anonymität und Verschlüsselung, um sie auf das höchste Sicherheitsniveau zu bringen. Die wichtigsten Modelle sind in der Lage, Daten zu verschlüsseln und auf dem eigenen Gerät des Benutzers zu hosten. Zentalk ist eine hybride, dezentralisierte Messaging-Anwendung ohne Cloud-Storage. Es verfügt über ein eigenes Netzwerk, das Zentamesh-Netzwerk, das es den Benutzern ermöglicht, in einer großen Zahl von Bereichen ohne Zugang zum Internet miteinander zu

kommunizieren. Zentalk enthält den Blake2-Algorithmus. Zentachain wird eine eigene Blockkette namens Zenta starten. Wir haben die Zenta-Blockkette so konzipiert, dass eine Offline-Kommunikation über das Zentamesh-Netzwerk möglich ist. Zentalk-Benutzer können Zentanode im Zentamesh-Netzwerk haben, um mit Zenta belohnt zu werden. Zentachain Labs erwägt mehrere Optionen für den Aufbau seiner Zenta-Blockkette, darunter: Cosmos (BPOS), Polkadot (Parachain & Blake2 & NPOS) und Ethereum (POW & POS). Das Ökosystem enthält alle Elemente, die für die Erstellung und das Hosting skalierbarer dezentraler Datenbanken, verteilter Dienste und dezentraler Speicherung in der Peer-2-Peer-Cloud erforderlich sind.

INHALT

1. Problem
2. Vision
3. Was macht Zentachain großartig?
4. Die Wirtschaft von Zenta
5. Ein lösungswürdiges Problem
6. Daten-Hacking und Datenschutzverletzungen
7. Privatsphäre
8. Zentralisierte Nachrichtenübermittlung
9. Zentralisierte Clouds
10. Über Zentachain
11. Zentachain-Ökosystem
12. Kommunikation
13. Zentalk
14. Zentalk & Tor-Netzwerk
15. Zentalk & Algorithmus & Verschlüsselung
16. Kryptoanalyse
17. Zentamesh Network & Zentanodes
18. Zentavault
19. Zentagate

1. Problem

- Notwendigkeit der sicheren Interaktion und Speicherung digitaler Daten - Eigentum der Initiatoren.
- Lösung des Problems des unberechtigten Zugriffs auf Daten und der Manipulation von Informationsflüssen.
- Schutz vor Hackern - unbefugter Zugriff und Diebstahl von Informationen, Aufzeichnung, Sammlung und Verkauf von Benutzerdaten.
- Nutzen Sie die Vorteile der Netzneutralität für Benutzerinformationen
- Gewährleistung von Dateneigentum, Datensicherheit und Kommunikation
- Eigentum und Sicherheit von Cloud-Storage
- Jede Aktion, die ein Benutzer auf einem Gerät ausführt, das auf einem digitalen Medium geliefert wird, wird potenziell aufgezeichnet und in einer Datenbank oder einem Dateiserver gespeichert. Es ist wahrscheinlich, dass diese Daten nicht richtig verschlüsselt oder anonymisiert sind.
- Server- oder cloudbasierte Kommunikationsanwendungen.
- Daten und Prozesse der Kommunikationshistorie, die von großen Unternehmen verschlüsselt werden und nie verschlüsselt wurden, oder der Benutzer muss eine Funktion in der Anwendung manuell starten, um die Verschlüsselung durchzuführen.
- Anwendungen, die sich gegenseitig ausspionieren, um in Programmen

  Rechte für den Zugriff auf Benutzerdaten und -informationen zu erhalten.

2. Vision

Zentachain ist ein dezentralisiertes Ökosystem, das für den Austausch und die Speicherung von neutralen Daten und Transaktionen im Netz aufgebaut ist. Das Ökosystem wird von seinen Nutzern gepflegt und ist gegen verschiedene Formen von Cyberangriffen und Hacking immun. Darüber hinaus liegen praktikable Lösungen für Sicherheits- und Dateneigentumsfragen vor. Zentachain ist ein Open-Source-Projekt. Zentachain will das fehlende Glied werden zwischen dezentralisierte, cloud-basierte Mesh-Netzwerkdienste wie IPFS (https://ipfs.io) und dynamische Routing- und Adressierungsprotokolle wie DNS und HTTPS. Es läuft darauf hinaus, dass Zentachain Labs das IPFS-Peer-to-Peer-Hypermedia-Protokoll mit fortschrittlicher Block-Chain-Technologie und einem eigenen Mesh-Netzwerk namens Zentameshnet aufrüsten wird.

Das Web wird nicht nur hochsicher, dezentralisiert und dauerhaft, sondern auch schneller und übersichtlicher werden. Zentachain wird es ermöglichen, große Datenmengen mit IPFS zu adressieren und mittels einer Blockketten-Transaktion dauerhafte und unveränderliche IPFS-Links auf das Zenta-Ledger zu setzen. Dies ermöglicht die Zeitstempelung und Sicherung der Inhalte, ohne dass die Daten auf Zenta selbst abgelegt werden müssen. Zentachain bringt die Freiheit und Unabhängigkeit der Kommunikation zu reduzierten Kosten. Das Ökosystem wird Inhalte so bereitstellen, dass die Nutzer viel Geld und Informationen sparen können.

Netzwerke mit hohen Latenzzeiten sind eine echte Eintrittsbarriere für die Entwicklungsländer. Zentachain bietet belastbaren Datenzugriff, Unabhängigkeit von niedrigen Latenzzeiten oder Backbone-Konnektivität. Zentachain ist wirklich dezentralisiert, ohne Ausnahmen, und wird das Ökosystem so gestalten, dass es niemals den Überblick über seine Nutzer behält und niemals IP-Adressen oder persönliche Informationen aufzeichnet. Das Ökosystem verfügt weder über diese Informationen, noch kann es Transaktionen mit einem bestimmten Nutzer oder einer bestimmten Identität in Verbindung bringen.

Zentachain's Vision basiert weitgehend auf Kommunikation und konzentriert sich darauf. Zentachain verwendet auch extreme Daten- und

Kommunikationsverschlüsselung: Es werden mehrere Verschlüsselungen angewendet. Zentalk wird nicht nur eine Kommunikationsanwendung sein, wie Sie sie heute kennen. Zentachain strebt dies an und weiß, dass die Zeit gekommen ist, in einem starken Offline-zu-Offline-Bereich zu kommunizieren. Wenn Sie mit Ihren Daten und Informationen für so genannte kostenlose Anwendungen bezahlen, verlangt Zentachain im Gegensatz zu den heutigen Kommunikationen und Anwendungen keine persönlichen Informationen vom Benutzer. Zentachain bezahlt den Benutzer mit seiner eigenen Zenta-Verschlüsselungswährung, die das Netzwerk unterstützt.

Sicherheit & Business

Zentacore enthält die gesamte Geschäftslogik im Ökosystem. Es enthält Modelle für die Offline-Kommunikation - Regieren und Konsens - und die Zentameshnet-Regierung. Zentacore wird eine der Sperrkettentechnologien wie NPOS, BPOS, DPOS oder Blake2 verwenden. Zentachain wird die Skalierbarkeit durch den Einsatz dieser Art von Technologie und Blockkette erheblich verbessern. Zentachain verfügt über einen Testmechanismus zur Partitionierung von Daten im Netzwerk. Um das Zentralisierungsproblem zu lösen, wird der Wert von n durch die Anzahl der Knoten in der Blockkette bestimmt, wobei jede Person, die stimmberechtigte Anteile hält, was Vertreter von n Bits (typischerweise n=101) ergibt. Je höher die Anzahl der Knoten, desto höher der Wert von n, und die Vertreter von n n Knoten haben die gleichen Rechte.

3. Was macht Zentachain großartig?

Die Zentachain ermöglicht es den Benutzern, mit Zentalk & Zentavault innerhalb des Ökosystems zu kommunizieren und Daten zu speichern. Alle ausgeführten dezentralisierten Anwendungen werden anonym und sicher sein, es wird keine Spur von Benutzern oder damit verbundenen Transaktionen geben, um die Fähigkeiten von Zentachain zu beweisen und zu demonstrieren, das Team präsentiert einen ultra-sicheren dezentralisierten Boten.

Zentalk

Zentalk ist eine hochsichere, dezentralisierte, hybride Verschlüsselung und Peer-to-Peer-Messaging. Neben der Benutzerfreundlichkeit finden Sie unter der Haube modernste Verschlüsselung mit AES-256, Diffie-Helman-, RSA- und El-Gamal-Sicherheit. Zentalk ist dezentralisiert, es hat keinen Serverpunkt. Zentachain garantiert totale Anonymität und Offline-Kommunikation zwischen Sender und Empfänger unter Verwendung von Zentanodes, einschließlich der Blake2-Hash-Funktion und dem Tor-Netzwerk.

Zentavault

Zentavault ist ein verschlüsselter und verteilter Hochgeschwindigkeits-Dienst zur Dateiübertragung und -speicherung. Im Gegensatz zu herkömmlichen Datenspeichersystemen speichert Zentavault nichts auf dem Gerät des Benutzers. Zentavault fungiert als Verschlüsselungsbereitstellungswerkzeug mit der Fähigkeit, Inhalte zu verschlüsseln und dynamisch und sicher über das Interplanetare Dateisystem (IPFS) zu verteilen. IPFS ist ein verteiltes Peer-to-Peer-Dateisystem, das versucht, alle Computergeräte mit demselben Dateisystem zu verbinden. In gewisser Weise ähnelt das IPFS dem World Wide Web, aber man könnte es sich als einen einzigen BitTorrent-Schwarm vorstellen, der Objekte innerhalb eines einzigen Git-Repositorys austauscht.

Zentagate

„Die Zentamesh-Netzwerk-Plattform".
Zentachain nimmt Sicherheit und Anonymität sehr ernst. Wir haben Zentachain so entwickelt, dass es auf seinem eigenen privaten Zentamesh-Netzwerk läuft. Das Zentagate verbindet das Ökosystem, um Zentamesh-Netzwerke wie das Internet zu nutzen. Zentagate bietet zusätzliche AES-Verschlüsselung und eine Anti-Piraterie-Schicht, um sicherzustellen, dass der Benutzer sicher verbunden und geschützt ist. Zusätzlich zur Zugangskontrolle und zum ungesicherten Netzwerkrelais planen wir die Einführung eines dezentralisierten Dienstnamens. Dieser Dienst wird vom Zentagate verwaltet, das in der Lage sein wird, Daten und Transaktionen über Zentanodes in das Zentamesh-Netzwerk hinein und aus diesem heraus weiterzuleiten und umzuleiten, so dass der Benutzer in Verbindung bleiben kann, ohne Zugang zum Internet zu haben.

4. Die Wirtschaft von Zenta

Zenta Verteilung :
Kettenname: ZENTA
Symbol: CHAIN
Algorithmus:, POA,NPOS(Mainnet)
Gesamtangebot: 26.500.000

5. Ein lösungswürdiges Problem

Immer mehr Menschen machen sich Sorgen um die Privatsphäre in einer Zeit, in der alles, was wir tun, virtuell irgendwo in einem Computersystem aufgezeichnet und elektronisch kommuniziert wird. Die Notwendigkeit einer sicheren Interaktion und Speicherung digitaler Daten - es bestand schon immer die Gefahr, dass der Urheber einem unberechtigten Zugriff auf Daten und der Manipulation von Informationsflüssen ausgesetzt sein könnte, aber diese Gefahr wächst von Tag zu Tag. Hacker können Sie jetzt von vielen Ländern, verschiedenen Regionen und mehreren Standorten aus gleichzeitig angreifen. Als ob das noch nicht genug wäre, gibt es auch noch Multimilliarden-Dollar-Unternehmen, die die Nutzung, Sammlung und den Verkauf Ihrer Daten zu einem lukrativen Geschäft gemacht haben.
Sie verkaufen Ihre Standortgeschichte, Nachrichten, Fotos, Dokumente und sogar die Profile, die sie über Sie erstellt haben. Alles über Sie wird an all die korrupten und böswilligen Organisationen auf der ganzen Welt versteigert, die diese Daten haben wollen. Einige Telekommunikationsbetreiber sammeln möglicherweise Benutzerdaten und Aktionen. Ob sie reguliert sind oder nicht, man kann nie sicher sein, ob sie reguliert sind oder nicht. Vielleicht werden sie diese Daten eines Tages für "Bildungszwecke" verwenden.

Es ist durchaus möglich, dass diese Daten nicht in geeigneter Weise verschlüsselt oder anonymisiert sind. Die von Social-Media-Unternehmen und Messaging-Anwendungen angebotenen Dienste werden als "kostenloser Dienst" dargestellt, der den Verbraucher nichts kostet. Vielmehr ermutigen diese Unternehmen gewöhnliche Menschen dazu, alle ihre Daten und Inhalte online zu stellen, um sie zu speichern und an bösartige Organisationen zu verkaufen, von denen bekannt ist, dass sie sie manipulieren. Das bedeutet, dass Sie über Ihre Daten bezahlen, anstatt eine monatliche Gebühr für den Dienst zu entrichten.

6. Daten-Hacking und Datenschutzverletzungen

Die Zahl der Internetnutzer wächst sehr schnell (von 1,36 Milliarden im Jahr 2007 auf 3,57 Milliarden im Jahr 2017, ein Anstieg um mehr als 2 Milliarden Nutzer in den letzten zehn Jahren). Wir stellen fest, dass unser tägliches Leben zunehmend virtualisiert wird und dass unsere Gefühle, Gedanken und persönlichen Informationen sich über das Internet verbreiten und dadurch anfällig für Piraterie werden.
Wir sind an einem Zeitpunkt angelangt, an dem alles und jeder zur Zielscheibe werden kann. Von persönlichen Angriffen, die durch Phishing, ClickJacking, Social Engineering und andere ähnliche Techniken ausgeführt werden, bis hin zu groß angelegten Infiltrationen in zentralisierte Unternehmensdatenbanken, die Hackern potenziell Zugang zu großen Mengen persönlicher Informationen ermöglichen. Während Ersteres in den meisten Fällen durch den gewissenhaften Einsatz sicherer Browsing-Praktiken vermieden werden kann, sind wir wegen des Umfangs der betroffenen Daten und der Tatsache, dass die Sicherheit unserer persönlichen Daten in diesem Fall völlig außerhalb unserer Kontrolle liegt, über Letzteres sehr besorgt.

6. Daten-Hacking und Datenschutzverletzungen

Die Zahl der Internetnutzer wächst sehr schnell (von 1,36 Milliarden im Jahr 2007 auf 3,57 Milliarden im Jahr 2017, ein Anstieg um mehr als 2 Milliarden Nutzer in den letzten zehn Jahren). Wir stellen fest, dass unser tägliches Leben zunehmend virtualisiert wird und dass unsere Gefühle, Gedanken und persönlichen Informationen sich über das Internet verbreiten und dadurch anfällig für Piraterie werden.
Wir sind an einem Zeitpunkt angelangt, an dem alles und jeder zur Zielscheibe werden kann. Von persönlichen Angriffen, die durch Phishing, ClickJacking, Social Engineering und andere ähnliche Techniken ausgeführt werden, bis hin zu groß angelegten Infiltrationen in zentralisierte Unternehmensdatenbanken, die Hackern potenziell Zugang zu großen Mengen persönlicher Informationen ermöglichen. Während Ersteres in den meisten Fällen durch den gewissenhaften Einsatz sicherer Browsing-Praktiken vermieden werden kann, sind wir wegen des Umfangs der betroffenen Daten und der Tatsache, dass die Sicherheit unserer persönlichen Daten in diesem Fall völlig außerhalb unserer Kontrolle liegt, über Letzteres sehr besorgt.

7. Privatsphäre

In den letzten zwei Jahrzehnten hat sich die Frage der Wahrung des Rechts auf Privatsphäre, hauptsächlich aufgrund der Auswirkungen des Internets auf unser tägliches Leben, von unserer physischen auf unsere digitale Umgebung ausgeweitet. Das berühmte Zitat "Wissen ist Macht" hat sich in der heutigen Welt zu "Daten sind Macht" entwickelt, da wir weiterhin unsere persönlichen Daten in sprichwörtlichen "Goldminen" preisgeben, die nicht nur Hacker und böswillige Einzelpersonen anziehen, sondern auch Unternehmen und Konglomerate, die sich anscheinend völlig im Rahmen des Gesetzes bewegen. Auf der einen Seite sind wir auf unsere Identitäten, Kreditkartennummern, digitalen Assets usw. ausgerichtet, während wir auf der anderen Seite unsere Informationen selbst weitergeben, im Austausch für eine komfortablere Benutzererfahrung. Obwohl Maßnahmen wie die

Allgemeine Datenschutzverordnung (GDPR) zum Schutz der Nutzer umgesetzt werden, werfen ihr Einfluss und der Grad ihrer Durchsetzung noch viele Fragen auf.

Die schwachen und machtlosen nationalen Verwaltungen haben dubiose Praktiken von Unternehmen zugelassen, die Daten von ihren Nutzern sammeln, so dass sie unsere Informationen nach eigenem Ermessen verarbeiten können. Einige der jüngsten Fälle von Datenschutzverstößen haben wir bereits im Kapitel über Datenschutzverletzungen in diesem Weißbuch erwähnt. Diese und andere ähnliche Vorfälle scheinen entweder in Vergessenheit zu geraten, ohne dass es entsprechende Auswirkungen und Reaktionen in der Öffentlichkeit gibt, oder sie schaffen manchmal eine Atmosphäre der Paranoia und des Misstrauens, die unserer zwischenmenschlichen Kommunikation abträglich ist. Aus diesem Grund ist es unbedingt erforderlich, dass wir uns unserer Persönlichkeitsrechte bewusst werden und nach neuen Ideen suchen, wie z.B. der Blockkette, um brennende Fragen der Privatsphäre anzugehen. Die Blockchain stellt die Werkzeuge zur Verfügung, die die Benutzer benötigen, um die Mittel, mit denen ihre persönlichen Daten verbreitet werden, vollständig zu kontrollieren. Es erlaubt höhere Anonymitätsgrade (einige erlauben sogar vollständige Anonymität) und die Möglichkeit, verschiedene Verschlüsselungsmethoden zum Schutz dieser Daten einzusetzen.

Sie entledigt sich anfälliger zentralisierter Datenbanken und ist immun gegen Datenveränderung und -manipulation. Letztlich handelt es sich um eine Plattform mit enormem Potenzial, um das durch das skrupellose Unterschlagungsverhalten der weltweit führenden Unternehmen verloren gegangene Vertrauen wieder herzustellen.

8. Zentralisierte Nachrichtenübermittlung

Die Präsenz des Internets in unserem täglichen Leben hat zugenommen, ebenso wie die Notwendigkeit einer effektiveren und umfassenderen Online-Kommunikation. In den folgenden Jahrzehnten gab es Fortschritte und das Aufkommen populärer Messaging-Anwendungen wie AIM, ICQ und PowW, die allmählich fortschrittlichere Funktionen wie privates Messaging, Mehrbenutzergruppen und Dateifreigabe beinhalteten.

In jüngster Zeit steht die Zunahme der Popularität von Messaging-Anwendungen in direktem Zusammenhang mit dem Anstieg der Smartphone-Nutzung. Desktop-Anwendungen wurden durch ihre mobilen Pendants ersetzt, so dass sofortigere und mobilere Kommunikationsmittel zur Verfügung stehen. Die Nutzerbasis ist exponentiell gewachsen, wobei die großen Dienstanbieter wie WhatsApp, Facebook, Messenger und WeChat allein über eine Milliarde aktive Nutzer pro Monat verzeichnen.

Die heutigen Messaging-Systeme sind jedoch alles andere als fehlerfrei. Die jüngsten Ereignisse haben ernsthafte Fragen zum Datenschutz aufgeworfen. Gegen Facebook (Eigentümer der beiden populärsten Messaging-Plattformen) wurde Anklage erhoben, weil es Nutzerdaten für politische Zwecke verkauft und die populärste Messaging-Anwendung im Blockbuster-Raum verwendet hat. Telegram hat sich bereit erklärt, seine Benutzerdaten an "zuständige Behörden" weiterzugeben, falls es eine gerichtliche Verfügung erhält. Dies ist ein Problem, das in direktem Zusammenhang mit der zentralisierten Architektur der bestehenden Messaging-Anwendungen steht. Eine solche Architektur ermöglicht es den Anwendungseigentümern, Inhalte zu nutzen, zu manipulieren und einzuschränken, so dass die Benutzer anfällig für potenziell schwerwiegende Verletzungen der Privatsphäre sind.

Die derzeitigen Messaging-Unternehmen scheinen dieses Problem durch die Implementierung von Ende-zu-Ende-Verschlüsselungslösungen anzugehen, aber auch diese Proximity-Implementierungen werfen Fragen über die Qualität und das tatsächliche Niveau der Verschlüsselung auf. Eine weitere Schwäche der heutigen

Messaging-Anwendungen ist ihre Anfälligkeit für Angriffe beim Austausch von SIM-Karten. Da die meisten Anwendungen eine Telefonnummer zur Registrierung erfordern, können Hacker potenziell auf den E-Mail-Inhalt ihres Benutzers zugreifen, indem sie den Betreiber davon überzeugen, die Nummer des Opfers auf eine in ihrem Besitz befindliche SIM-Karte zu übertragen.

9. Zentralisierte Clouds

Zentralisierte Wolken sind Dienste, die es ermöglichen, Daten auf entfernten Servern zu speichern und über das Internet auf sie zuzugreifen. Sie sind entweder kostenlos oder bezahlt und ihr Preis richtet sich im Allgemeinen nach der Vertragsdauer und der Lagerkapazität. Zentralisierte Clouds funktionieren durch den Einsatz virtualisierter Datenzentren, die über eine Web-Schnittstelle mit dem Benutzer verbunden werden können. Der Benutzer lädt Dateien ins Internet hoch, die dann auf Datenservern gespeichert werden.
Auf sie kann nur durch Angabe einer eindeutigen Kennung zugegriffen werden, die dann die Zusammenstellung von Metadaten auslöst, die es dem Benutzer ermöglichen, die Dateien anzuzeigen, zu ändern, zu übertragen oder zu synchronisieren. Um eine unterbrechungsfreie Datenwiederherstellung und -integrität zu gewährleisten, müssen Dateien auf mehr als einem Server gespeichert werden. Es gibt verschiedene Arten der zentralisierten Speicherung in der :
Öffentliche Speicherung in der Cloud - ist eine Umgebung mit gemeinsam genutzten Ressourcen, in der dem Kunden nur die genutzten Ressourcen in Rechnung gestellt werden und der Dienstanbieter für die Wartung der Cloud-Infrastruktur verantwortlich ist. Private Storage in the Cloud - ist in der Regel ein Vor-Ort-Service, der von einem einzigen Kunden/einer einzigen Organisation genutzt und vom Dienstanbieter gewartet wird. Hybride Cloud-Speicherung - ist eine Kombination aus öffentlicher und privater Cloud-Speicherung, die die Flexibilität bietet, sensible und öffentlich zugängliche Informationen auf verschiedenen Arten von Clouds zu speichern. Es ist klar, dass zentralisierte Wolken in letzter Zeit an Popularität gewonnen haben.

Die gestiegene Nachfrage nach Mobilität und Datenzugänglichkeit treibt die Nutzer von physischen Medien wie Festplatten und USB-Sticks weg. Trotz eines Schrittes in die richtige Richtung können zentralisierte Dienste jedoch immer noch auf Probleme stoßen. Zunächst einmal ist der Kunde nicht der Eigentümer der Daten. Die zentralisierte Serverarchitektur legt die Daten des Kunden in die Hände der Service Provider und macht sie zudem anfällig für Hacker und DDoS-Angriffe, die die Kontinuität des Datenzugriffs unterbrechen. Öffentliche Cloud-Dienste sind besonders anfällig für Angriffe, da sie eine gemeinsame Ressourcennutzung aufweisen, die ein böswilliges Eindringen über einen der Cloud-Clients ermöglicht. Gesetze und Vorschriften sind ein weiteres wichtiges Anliegen, da Datensicherheit und Datenschutz sensibel auf die sich ständig ändernden Regeln reagieren, die von Regierungen auf der ganzen Welt festgelegt werden. Für kleine Unternehmen, die komplexe Daten in der Cloud nutzen möchten, können die Kosten ein ernstes Problem darstellen, da die Anforderungen an die Bandbreite finanziell nicht tragbar sein können.

10. Über Zentachain

Zentachain präsentiert praktikable Lösungen für diese Probleme. Open Source, Inhalte, die nicht auf zentralisierten Servern gespeichert sind, und die Integration von Technologien wie Zentameshnet, Hyperborea und das Tor-Netzwerk zur Erhöhung der Sicherheit zeigen deutlich die Vorteile der Nutzung von Anwendungen, die auf dieser Plattform entwickelt wurden. Zentachain freut sich darauf, die Daten seiner Kunden mit einem vollständig sicheren Datenschutz - Ökosystem, gegen Einbrüche und alle Arten von Cyber-Angriffen - schützen zu können! Heute gilt jede Dienstleistung, die die Menschen nutzen, als vertrauliche Informationsquelle, die es Einzelhändlern und Organisationen ermöglicht, gezielte Verbraucherwerbung zu erhalten. Das Ziel von Zentachain ist es, Menschen und Unternehmen eine Möglichkeit zu bieten, sicher zu bleiben, ohne Angst haben zu müssen, ihre Daten abzuhören, auszuspionieren oder wiederherzustellen.

Zentachain verpflichtet sich, niemals Metadaten über seine Kunden zu speichern und wird Ihre IP-Adresse, E-Mail-Adresse oder Telefonnummer nicht aufzeichnen. Bei der Nutzung des Dienstes ist nichts erforderlich, mit Ausnahme unserer Zentalk-Anwendung, die Zentawallet mit einem Layer 2 zum Schutz der Zahlung zwischen Empfänger und Absender enthält. Wie bei allen unseren Dienstleistungen hat Zentachain keine Informationen über Ihre Identität, die Region, in der Sie leben, oder persönliche Daten über Sie. Zentachain kümmert sich nicht um diese persönlichen Gegenstände, denn unser einziges Ziel ist es, Dienstleistungen von Weltklasse anzubieten, die dem Verbraucher absolute Anonymität, Sicherheit und Privatsphäre bieten. Ein weiterer wichtiger Aspekt von Zentachain ist die Bereitstellung von Offline-Kommunikation über die dezentralisierte Zentalk-Anwendung (bietet internetfreie Kommunikation). Zentalk wird Quantenstärke mit mehreren kryptographischen Verschlüsselungen haben.

Das Zentachain-Ökosystem bietet mehrere Lösungen, dezentralisierte Anwendungen, um seinen eigenen hohen Wert zu erhalten und den Benutzer in seiner eigenen Blockchain zu schützen, und Zenta wird als Belohnung für diejenigen verwendet, die Zentanodes beherbergen. Zentanode-Eigentümer werden auf monatlicher Basis belohnt, was für den Erfolg des Zentameshnet-Netzwerks notwendig ist. Es ist identisch mit einem Bergbausystem, aber energieeffizienter und benutzerfreundlicher. Zentalk ist für moderne Kommunikation mit vielfältigen Möglichkeiten der Kommunikationsverschlüsselung da. Zentavault ist eine dezentralisierte IPFS-Cloud-Storage-Anwendung, die Daten verschlüsselt und sicher speichern kann, und ist die zweite Anwendung von Zentachain.

- **Anti-inflation**

Zentachain ist ein Anti-Inflationssystem und ein dezentralisiertes Netzwerk, das unter weitreichendem Schutz der Privatsphäre aufgebaut ist. Heute haben die meisten Kommunikationsanwendungen und Cloud-Speichersysteme die Erfassung von Benutzerdaten und vieles mehr als primäre Vision. Die Zentachain ist anders, sie belohnt den Benutzer und die Anhänger von Zentalk und Zentavult. Zentachain wird nie mit den Daten und Informationen der Nutzer leben können, sondern mit Produkten und einem Kommunikationssystem, das sich ganz auf den Schutz der Privatsphäre und seine eigene hochwirksame Sperrkette konzentriert.

- **Zenta-Auszeichnung**

Zentachain wird jeden Monat alle Zentanode-Inhaber im Netzwerk belohnen. Es wird keine Schwierigkeiten im Netzwerk geben, und die Belohnungen von Zenta werden festgelegt. Der Benutzer muss lediglich Zentanode starten. Wenn ein Benutzer die Verbindung unterbricht, wird Zentanode nicht mehr von Zenta belohnt, was bedeutet, dass der Benutzer Zentanode kontinuierlich ausführen muss.

- **Zentanode**

Die Knotenpunkte von Zentachain werden Zentanodes genannt. Zentanodes unterscheidet sich nicht von einem Knoten, Gerät oder Datenpunkt im Zentamesh-Netzwerk. Zentanodes wird nur auf unserer offiziellen Homepage zum Verkauf angeboten. Zentanodes wurden geschaffen, um Offline-Kommunikation über große Entfernungen zu ermöglichen. Alle Einnahmen aus den Zentanodes werden zur Unterstützung der Zenta-Blockkette verwendet.

- **Zentalk**

Zentalk ist eine dezentralisierte, hybride, verschlüsselte, ultra-sichere Peer-to-Peer (P2P)-Messaging-Anwendung. Die dezentrale Anwendung von Zentalk wird zunächst nicht als freie und vollständig öffentliche Open-Source-Anwendung veröffentlicht.

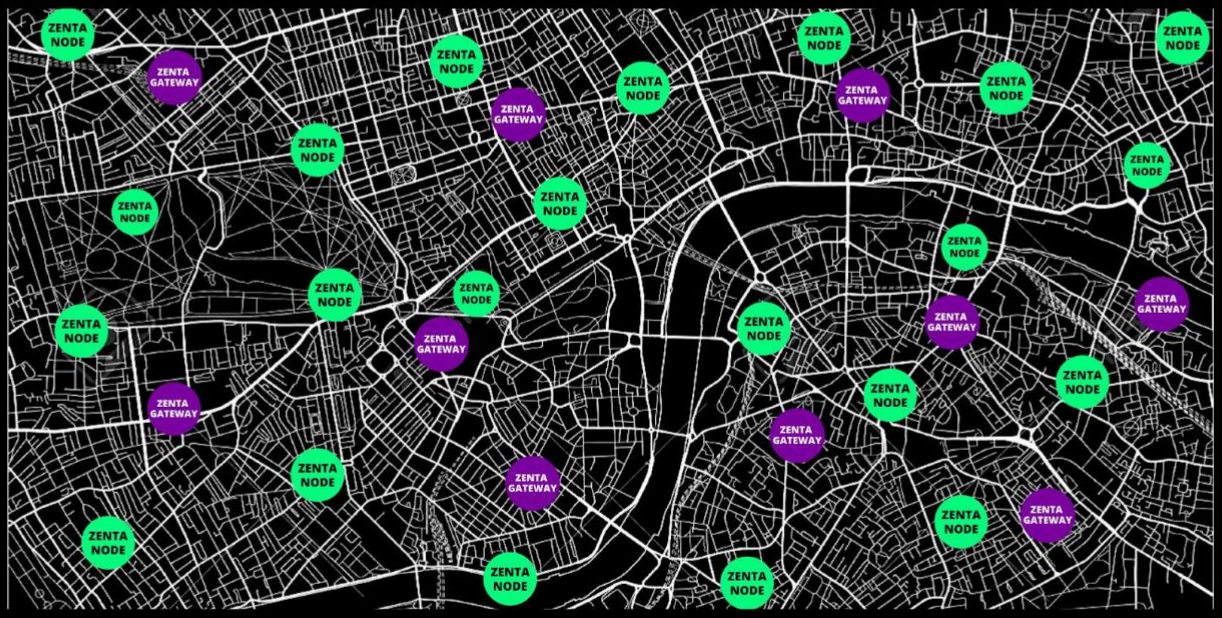
- **Zentavault**

Zentavault verlangt keine monatlichen Nutzungsgebühren, nur minimale Transaktionsgebühren für das Herunterladen von Daten. Zentavault ist ein Werkzeug zur Verschlüsselung und Dateiverteilung.

12. Kommunikation

Kommunikation bedeutet, dass zwei oder mehr Menschen problemlos miteinander reden und kommunizieren können. Die Kommunikation auf einer technologischen Plattform erfolgte zunächst über das Telefon. Und das Telefon ging als großer technologischer Durchbruch in die Geschichte ein, aber die Geschwindigkeit der Technologie hat von Tag zu Tag zugenommen, und es gibt heute unzählige Kommunikationsquellen. Ursprünglich boten Telefone Privatsphäre und Freiheit, aber die Entwicklung der Technologie hat den Zeitaufwand verringert. Weil die Kommunikation und das Gespräch zwischen zwei Menschen begann, von anderen gehört zu werden. Infolgedessen begann die Privatsphäre der Menschen zu verschwinden. Als jedoch Tag für Tag neue Technologien aufkamen, versuchte man, die Freiheit und Privatsphäre der Menschen wieder zu schützen, was jedoch nicht vollständig erreicht wurde. Für heute werden alle Gespräche und Korrespondenz auf die eine oder andere Weise verfolgt. Und leider ist dies nicht der Fall, wenn wir am Telefon oder mit irgendeinem Kommunikationsgerät sprechen, auch wenn wir glauben, dass unsere Gespräche nur zwischen uns und dem Gesprächspartner verborgen sind.

13. Zentalk



Zentalk ist eine dezentralisierte, hybride, verschlüsselte, ultra-sichere Peer-to-Peer (P2P)-Messaging-Anwendung.

Zentalk gewährleistet Datenschutz und Sicherheit durch die Integration von Zentamesh-Netzwerktechnologien. Das Zentamesh-Netzwerk (Zentameshnet) ist als eine der sichersten und zuverlässigsten Varianten der Vernetzung bekannt. Die Zentamesh-Netzwerktechnologie ist leistungsstark, verfügt über eine ausgezeichnete Lastverteilung und erfordert keine zentrale Verwaltung.

Das Zentamesh-Netzwerk ist eine Netzwerktopologie, in der jeder Knoten Daten für das Netzwerk weiterleitet. Zentachain implementiert .cjdns-Knoten, ein verschlüsseltes IPv6-Netzwerk mit Public-Key-Kryptographie für die Adresszuweisung und eine verteilte Hash-Tabelle für das Routing. Es erfordert keine Konfiguration und löst viele Sicherheits- und Skalierbarkeitsprobleme, die bestehende Netzwerke betreffen. Alle Zentamesh-Knoten kooperieren bei der Verteilung von Daten über das Netzwerk. Jedes Gerät, das Zentalk verwendet,

fungiert als Knoten im Zentamesh-Netzwerk. Diese Knoten haben die einzigartige Fähigkeit, sich auf verteilte Weise miteinander zu verbinden.

Das Zentamesh-Netzwerk leitet Nachrichten entweder mittels einer Injektions- oder einer Routing-Technik weiter. Beim Routing bewegt sich die Nachricht entlang der Route und springt von einer Zentanode zur anderen, bis sie ihr Ziel erreicht. Um die Verfügbarkeit aller Routen zu gewährleisten, ermöglicht das Netzwerk kontinuierliche Verbindungen durch selbstheilende Algorithmen, wie z.B. Shortest Path Bridging, und beschädigte oder fehlerhafte Routen werden rekonfiguriert. Die Selbstreparatur ermöglicht den Betrieb eines routingbasierten Netzwerks, wenn eine Zentanode ausfällt oder wenn eine Verbindung unzuverlässig wird. Folglich ist das Netzwerk absolut zuverlässig, da es im Zentanetzwerk oft mehr als einen Pfad zwischen einer Quelle und einem Ziel gibt. Obwohl dieses Konzept hauptsächlich in drahtlosen Situationen verwendet wird, kann es auch auf drahtgebundene Netzwerke und Software-Interaktion angewendet werden.

An example of the common meshed network technology, if you register a new Zentanode in your house like a new light bulb, the device pairs with the control center through a self-configured meshed network. Common mesh networks are typically wireless but Zentameshnet is the blockchain-based network topology and less infrastructure.

Zentalk provides technological privacy, this means only highly encrypted Metadata is shortly kept and afterward automatically unrecoverably removed. This is achieved through the integration of the Zentamesh network and its architecture. Zentalk sends and tunnels all messages and data through the Zentamesh network. This ensures that any messages shared between the sender and recipient being the highest levels of their privacy.

Im Zentamesh-Netzwerk ist jede Zentanode mit einem oder mehreren Knoten verbunden. Wenn mehrere Zentanodes miteinander verbunden sind, sprechen wir

von einem vollständigen Zentamesh-Netzwerk. Wenn eine Nachricht von Zentalk gesendet wird und die Daten durch das Zentamesh-Netzwerk gesendet werden, geht sie von einer Zentanode zur anderen, bis die Nachricht den gewünschten Empfänger erreicht hat. Aufgrund des Designs der Zentamesh-Netzwerkknoten wissen wir nicht, welcher Knoten welche Nachricht sendet oder empfängt. Die Kommunikation zwischen Absender und Empfänger bleibt somit anonym. Zentalk-Benutzer werden nicht mit der Übertragung einer einzigen Nachricht belohnt. Alle Zentanode-Inhaber werden mit Zenta belohnt. Das bedeutet, dass Sie eine Zentanode besitzen und sie ständig am Laufen halten müssen; außerdem ist sie sehr energieeffizient und benutzerfreundlich. Zentalk ist ein hochsicheres, verschlüsseltes Messaging-System, und jede Nachricht innerhalb und außerhalb des Netzwerks wurde so konzipiert, dass der Zentalk-Benutzer keine Fehler in seiner Privatsphäre machen kann. Zentalk lässt auch keine Sicherheitslücke offen, die Benutzer anfällig für Angriffe oder Hacker machen könnte. Zentalk wird verschiedene Arten der Verschlüsselung verwenden, da einige Verschlüsselungen anfällig sind; wir werden nur solche Verschlüsselungen verwenden, die für Zentalk wirklich sicher sind. Jede Verschlüsselung wird ihre eigene Rolle haben, und alle Verschlüsselungen, die wir verwenden werden, werden im Weißbuch aufgeführt sein. Zentalk wird Verschlüsselungen verwenden, die wirklich sicher gegen Angriffe von Quantencomputern sind.

Merkmale von Zentalk:

- Zentalk benötigt keine Google Play-Dienste
- Persönliche Informationen: No
- Einen Server / Cloud Server haben: No
- IP-Adressen sind geschützt: Ja mit dem Tor-Netzwerk
- Auf einem Server gespeicherte Nachrichten: Nie
- Nachrichten werden auf Ihrem eigenen Gerät verschlüsselt: Ja
- Daten werden auf ihren eigenen Geräten verschlüsselt: Ja
- Wiederherstellung von Benutzerkonten: Nein
- Sicherung: Nein
- Offline (Nutzung ohne Internet): Ja

- Google Tracker : Nein
- Datenunterstützung: Ja
- Telefonnummer: Nein
- E-Mail: Nein
- Bitte registrieren Sie sich: Nein
- Schützt Männer mitten in einem Angriff: Ja
- Gruppenchat: Ja
- Schlüssel-Sharing: Ja
- Nachrichten austauschen: Ja
- Zentawallet: Nein zuerst/letztes Ja Chat & Pay (Nur: Bitcoin, Ethereum, Zenta)
- Bitcoin-Zahlung im Zentamesh-Netzwerk: Ja
- Bitcoin-Zahlung mit Tor Routing: Ja
- Zenta-Belohnungen: Ja (Gastgeber Zentanode)
- Hash-Algorithmen: BLAKE2b
- Hybride Verschlüsselung: Ja (RSA, AES, DHKE, EL-Gamal)
- Verschlüsselung pro Block: 128 Bit
- Schlüsselgröße: 256 Bit
- RSS : Ja
- API: Ja
- Private Knoten: Ja Privater Gateway: Ja
- Verschlüsselte Zentanodes: Ja
- Zwiebel-Aktie : Ja
- Quantenresistenz: Ja
- Selbstzerstörung nach dem Lesen: Ja
- Einseitig gehackte Passwort-Unterschrift: Ja
- Stop Over Tracking durch andere Anwendungen
- Verwendung ohne SIM-Karte: Ja
- Zentalk-Benutzer im Bluetooth- oder Wi-Fi-Bereich können über Zentanode mit anderen Benutzern kommunizieren, auch wenn sie keinen Zugang zum Internet haben.

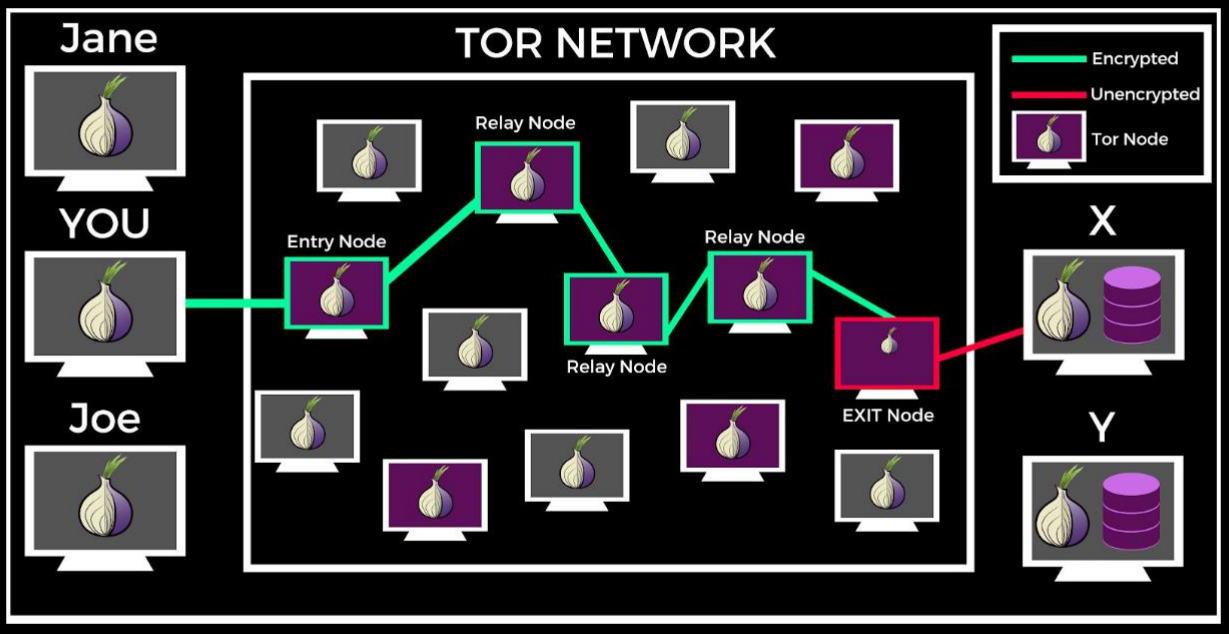
Viele Funktionen werden auch in Zukunft hinzugefügt werden.

14. Zentalk & Tor-Netzwerk

Tor ist freie und quelloffene Software, die für anonyme Kommunikation verwendet wird. Der Name ist von einem Akronym des ursprünglichen Software-

Projektnamens "The Onion Router" abgeleitet. Tor routet durch ein kostenloses, freiwilliges Netzwerk von über 7.000 Relays, um den Internetverkehr und den Standort eines Benutzers vor allen zu verbergen, die Netzwerküberwachung oder Verkehrsanalysen durchführen. Die Verwendung von Tor macht es schwieriger, die Internetaktivitäten eines Benutzers zu verfolgen: Dazu gehören "Website-Besuche, Online-Nachrichten, Sofortnachrichten und andere Formen der Kommunikation". Internet Service Provider (ISPs) in verschiedenen Ländern auf der ganzen Welt werden jedoch oft von ihren Regierungen gewarnt, Benutzer am Zugang zu Tor zu hindern. Infolgedessen wurden Tor-Brücken entwickelt, die es Benutzern ermöglichen, sich in Ländern, in denen dieser Zugang blockiert ist, mit dem Tor-Netzwerk zu verbinden. Indem einige der Gateway-Relais geheim gehalten werden, können Benutzer der Internet-Zensur entkommen, die auf der Blockierung öffentlicher Tor-Relais beruht. Tor blockiert einen Online-Dienst nicht, wenn auf ihn über Tor zugegriffen werden kann. Tor schützt die Privatsphäre eines Benutzers, verbirgt aber nicht die Tatsache, dass jemand es benutzt. Aber die Gateways verbergen die Tatsache, dass jemand Tor benutzt. Das Ziel von Tor ist es, die Privatsphäre seiner Nutzer sowie ihre Freiheit und Fähigkeit, vertrauliche Kommunikation zu führen, zu schützen, indem ihre Aktivitäten im Internet nicht überwacht werden. Wenn ein Nutzer Tor benutzt, können Online-Datensammler keine Verkehrsanalyse durchführen und keine Daten über die Gewohnheiten der Internetnutzer sammeln, wie zum Beispiel Google-Anzeigen. Daher werden Überwachungsorganisationen wie die NSA nicht in der Lage sein, Nutzer zu beobachten. Tor verschlüsselt die Daten mehrfach und schickt sie durch eine virtuelle Schaltung zufällig ausgewählter Tor-Relais, einschließlich der Ziel-IP-Adresse. Daher haben wir bei der Entwicklung der Zentalk-Messaging-Anwendung die Privatsphäre und Freiheit des Benutzers berücksichtigt. Zentalk garantiert die totale Anonymität der Kommunikation unter Verwendung des Tor-Protokolls. Benutzer können Zentalk einfach aktivieren und deaktivieren, ohne einen zweiten VPN-Provider oder Orbot installieren zu müssen.

Tor-Network



15. Zentalk & Algorithmus & Verschlüsselung

Kryptographie

Die Kryptographie oder Kryptologie ist die Anwendung und Untersuchung bestimmter Techniken zur sicheren Kommunikation zwischen Dritten, die als Angreifer bezeichnet werden. Allgemeiner ausgedrückt: Bei der Verschlüsselung werden Protokolle erstellt und analysiert, die verhindern, dass Dritte private Nachrichten von Einzelpersonen lesen können. Verschiedene Aspekte der Informationssicherheit, wie Datenvertraulichkeit, Datenintegrität und Authentifizierung, sind für die moderne Kryptographie wichtig. Die moderne Kryptographie existiert an der Schnittstelle zwischen den Disziplinen Mathematik, Informatik und Kommunikationswissenschaften. Zu den Anwendungen der Kryptographie gehören elektronischer Handel, intelligente Zahlungskarten, digitale Währung, Computerpasswörter und militärische Kommunikation.

Geschichte der Verschlüsselung

Circa 600 vor Christus: Die alten Spartaner verwendeten ein Gerät namens Skytale, um während der Schlachten geheime Nachrichten zu versenden. Es handelt sich um einen Lederriemen, der um einen Holzstab gewickelt ist. Die

Buchstaben auf dem Lederriemen sind bedeutungslos, wenn sie abgerollt sind, und die Botschaft macht nur Sinn, wenn der Empfänger einen gut dimensionierten Stab hat.

Um 60 vor Christus: Julius Cäsar erfindet ein Passwort, das an drei Stellen Zeichen ändert: A, D, B, E usw.

1553: Giovan Battista Bellaso stellt sich den ersten zu verwendenden Code - ein geeignetes Verschlüsselungs-Schlüsselwort - vor, den der Empfänger wissen muss, wenn er die Nachricht entschlüsseln will.

1854: Charles Wheatstone erfand die Playfair-Chiffre, die Buchstabenpaare anstelle von Einzelbuchstaben verschlüsselt und daher schwieriger zu entziffern ist.

1917: Ein Amerikaner, Edward Hebern, erfindet eine elektromechanische Maschine, bei der der Schlüssel in eine rotierende Scheibe eingebettet ist. Dies ist das erste Beispiel einer Rotormaschine. Sie kodiert eine Substitutionstabelle, die jedes Mal geändert wird, wenn ein neues Zeichen eingegeben wird.

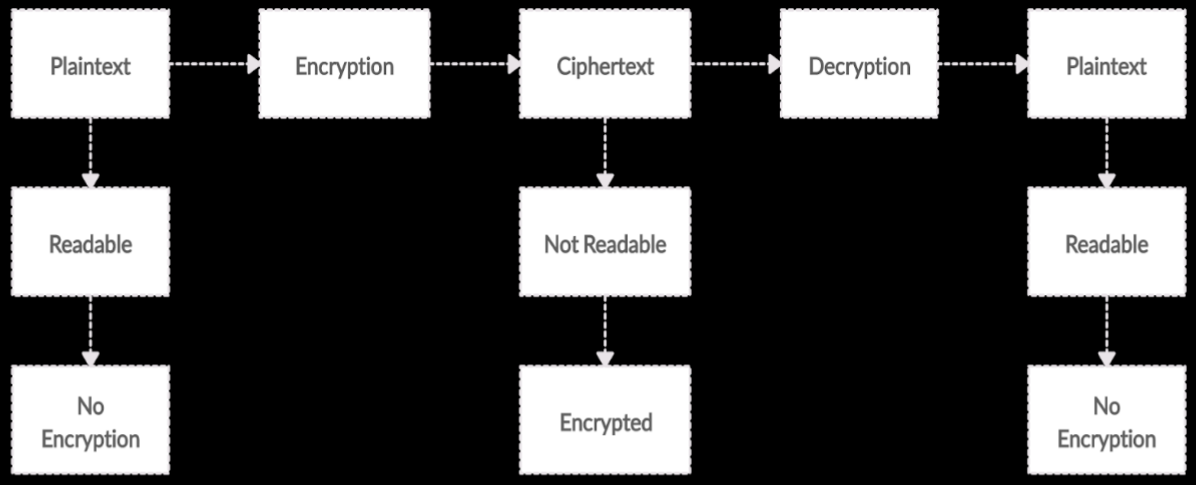
1918: Der deutsche Ingenieur Arthur Scherbius erfindet die Enigma-Maschine für den kommerziellen Gebrauch. Er arbeitet etwas mehr als ein Rotor, der von der Hebern-Maschine verwendet wird. Die deutsche Armee, die den Ingenieur kannte, begann damit, verschlüsselte Übertragungen zu versenden.

1932: Der polnische Kryptograph Marian Rejewski entdeckt die Funktionsweise von Enigma. Im Jahr 1939 teilt Polen diese Informationen mit dem französischen und britischen Geheimdienst, wodurch Kryptographen wie Alan Turing herausfinden konnten, wie man den Schlüssel, der sich jeden Tag ändert, knacken kann. Sie erwies sich als sehr wichtig für den Sieg im Zweiten Weltkrieg.

1945: Claude E. Shannon von den Bell Labs veröffentlicht einen Artikel mit dem Titel "Eine mathematische Theorie der Kryptographie". Dies ist der Ausgangspunkt der modernen Kryptographie.

Early 1970s: IBM bildet eine "Kryptographie-Gruppe", die einen Strichcode zum Schutz der Kundendaten des Unternehmens entwirft. Im Jahr 1973 übernahmen die Vereinigten Staaten ihn als nationalen Standard - den Data Encryption Standard (DES). Sie war in Gebrauch, bis sie 1997 entziffert wurde.

2000: Das DES wird durch den Advanced Encryption Standard, oder AES, ersetzt, der durch einen öffentlichen Wettbewerb gefunden wird. Heute ist AES weltweit gebührenfrei erhältlich und für die Verwendung in Verschlusssachen der US-Regierung zugelassen.



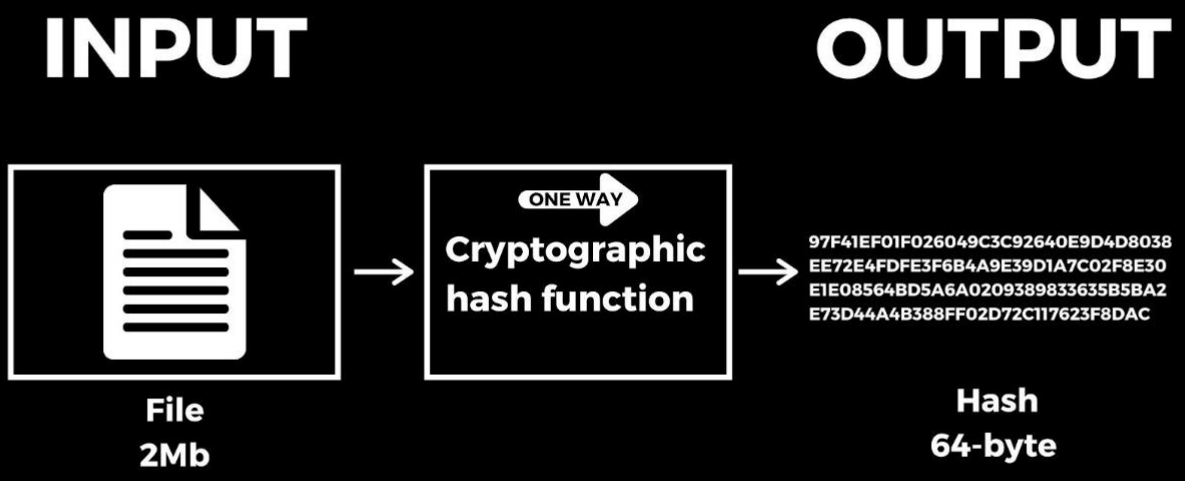
Hash-Funktionen

Hash-Funktionen sind die Bausteine der modernen Kryptographie. Eine Hash-Funktion ist ein kryptographischer Algorithmus, der verwendet wird, um große Daten mit zufälliger Größe in kleine Daten mit fester Größe zu transformieren. Die Datenausgabe des Hash-Algorithmus wird als Hash-Wert oder Digest bezeichnet. Die grundlegende Bedienung der Hash-Funktionen erfordert keine Tasten und funktioniert unidirektional. Unidirektionaler Betrieb bedeutet, dass es nicht möglich ist, die Eingabe von einer bestimmten Ausgabe aus zu berechnen.

- Die von einer Hash-Funktion zurückgegebenen Werte werden als Hash-Werte bezeichnet.
- Mit einer kryptografischen Hash-Funktion lässt sich leicht überprüfen, ob bestimmte Eingabedaten mit einem gegebenen Hash-Wert übereinstimmen.
- Eine Hash-Funktion ist jede Funktion, die verwendet werden kann, um Daten beliebiger Größe mit Daten fester Größe abzugleichen.
- Wenn die Eingabedaten unbekannt sind, ist es schwierig, sie durch Kenntnis des gespeicherten Hash-Wertes zu rekonstruieren.
- Hash-Funktionen haben keine Taste.
- Für langfristige Sicherheit werden 256 Bit oder mehr empfohlen.
- Das SHA-1 weist schwerwiegende Schwachstellen auf und sollte nach Möglichkeit nicht verwendet werden.
- Die SHA-2-Algorithmen sind noch nicht gebrochen, aber sie funktionieren nach dem gleichen Prinzip wie SHA-1.
- Die SHA256/512 Blake2b-Hash-Funktion und einige andere gelten als sicher.

  (Sie haben Quantenwiderstand für die nächsten 20-30 Jahre)

Hashing-Funktion



Verschlüsselung

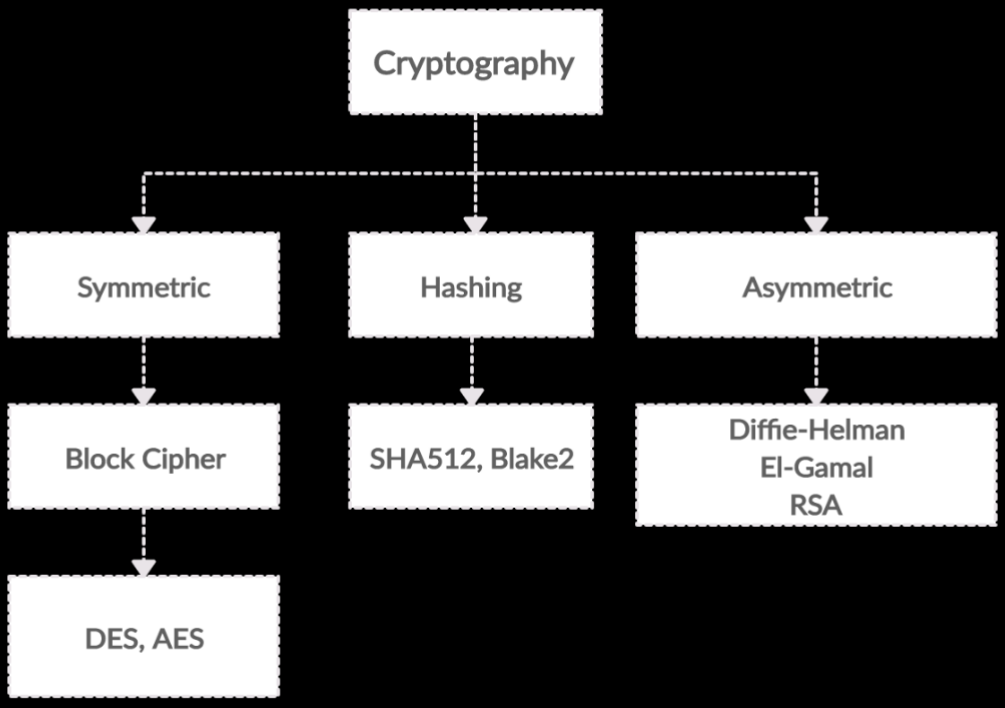
Verschlüsselung ist die Methode, mit der Text oder jede andere Art von Daten aus einer lesbaren Form in eine verschlüsselte Version umgewandelt wird, die von einer anderen Entität nur entschlüsselt werden kann, wenn sie Zugang zu einem Entschlüsselungsschlüssel hat. Die Verschlüsselung ist eine der wichtigsten Methoden zur Gewährleistung der Datensicherheit, insbesondere für den End-to-End-Schutz von Daten, die über Netzwerke übertragen werden.

Verschlüsselung ist im Internet weit verbreitet, um Benutzerinformationen zu schützen, die zwischen einem Browser und einem Server übertragen werden, einschließlich Passwörtern und anderen persönlichen Informationen, die privat bleiben müssen. Organisationen und Einzelpersonen verwenden auch häufig Verschlüsselung, um sensible Daten zu schützen, die auf Computern, Servern und mobilen Geräten wie Telefonen oder Tablets gespeichert sind.

Wie Verschlüsselung funktioniert

Bei der Verschlüsselung werden Algorithmen verwendet, um Ihre Informationen zu verschlüsseln. Die Nachricht wird dann an den Empfänger übermittelt, der sie mit Hilfe eines Schlüssels entschlüsseln kann. Es gibt viele Arten von Algorithmen, die alle verschiedene Arten der Verschlüsselung und dann der Entschlüsselung von Informationen beinhalten. Die heute weit verbreiteten Verschlüsselungsalgorithmen sind in drei Teile unterteilt: Hash-Funktionen, symmetrisch, asymmetrisch.

Kryotographie



Block-Verschlüsselung
Eine Blockchiffrierung nimmt einen Block von Klartextbits und erzeugt einen Block von Chiffretextbits, in der Regel von gleicher Größe. Die Größe des Blocks ist im vorgegebenen Schema festgelegt. Die Wahl der Blockgröße hat keinen direkten Einfluss auf die Stärke des Verschlüsselungssystems. Die Verschlüsselungsstärke hängt von der Länge des Schlüssels ab.

Block-Verschlüsselungsschemata:

- Es gibt eine große Anzahl von Blockverschlüsselungsschemata, die verwendet werden. Viele von ihnen sind öffentlich bekannt. Die beliebtesten und bekanntesten sind unten aufgeführt.

- Triple DES - Dies ist eine Schema-Variante, die auf wiederholten DES-Anwendungen basiert. Es handelt sich nach wie vor um eine angesehene Blockchiffre, aber sie ist weniger effektiv als die schnelleren verfügbaren Blockchiffren.

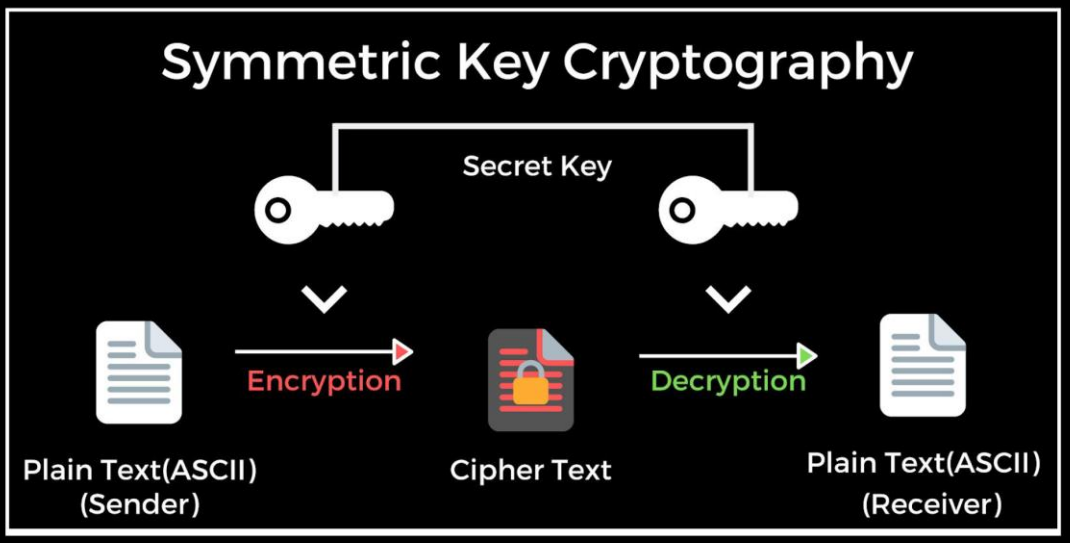
- Advanced Encryption Standard (AES) - Dies ist eine relativ neue Blockchiffre, die auf dem Rijndael-Verschlüsselungsalgorithmus basiert und den AES-Designwettbewerb gewonnen hat.

- IDEA - Dies ist eine ausreichend starke Blockchiffre mit einer Blockgröße von 64 und einer Schlüsselgröße von 128 Bit. Eine Reihe von Anwendungen verwenden die IDEA-Verschlüsselung, darunter auch frühe Versionen des PGP-Protokolls (Pretty Good Privacy). Die Verwendung von IDEA ist aufgrund von Patentfragen eingeschränkt..
- Twofish - Dieses Blockchiffrierungsschema verwendet eine Blockgröße von 128 Bit und einen Schlüssel variabler Länge. Sie gehörte zu den Finalisten der AES. Es basiert auf dem früheren Blowfish-Blockchiffrierungsschema mit einer Blockgröße von 64 Bit.
- Serpent - Ein 128-Bit-Blockcode und ein 128-, 192- und 256-Bit-Schlüssel, der auch Finalist im AES-Wettbewerb war. Sie ist langsamer, aber sicherer in der Ausführung als andere Blockchiffren.

Symmetrische Verschlüsselung

Symmetrische Verschlüsselung ist eine Art der Verschlüsselung, bei der ein einziger Schlüssel (ein geheimer Schlüssel) verwendet wird, um elektronische Informationen sowohl zu verschlüsseln als auch zu entschlüsseln. Entitäten, die mit symmetrischer Verschlüsselung kommunizieren, müssen den Schlüssel austauschen, damit er im Entschlüsselungsprozess verwendet werden kann. Diese Verschlüsselungsmethode unterscheidet sich von der asymmetrischen Verschlüsselung, bei der ein Schlüsselpaar, ein öffentliches und ein privates, zur Ver- und Entschlüsselung von Nachrichten verwendet wird. AES (Advanced Encryption Standard) ist einer der am weitesten verbreiteten symmetrischen Verschlüsselungsalgorithmen.

Symmetrische Verschlüsselung



AES-Verschlüsselung

Der am häufigsten verwendete symmetrische Algorithmus ist der AES (Advanced Encryption Standard), der ursprünglich unter dem Namen Rijndael bekannt war. Dies ist der vom U.S. National Institute of Standards and Technology im Jahr 2001 festgelegte Standard für die Verschlüsselung elektronischer Daten, der in der U.S. FIPS PUB 197 angekündigt wurde.Dieser Standard ersetzt DES,
der seit 1977 in Gebrauch war. Die AES-Chiffre hat eine Blockgröße von 128 Bit,

kann aber drei verschiedene Schlüssellängen haben, wie mit gezeigt:

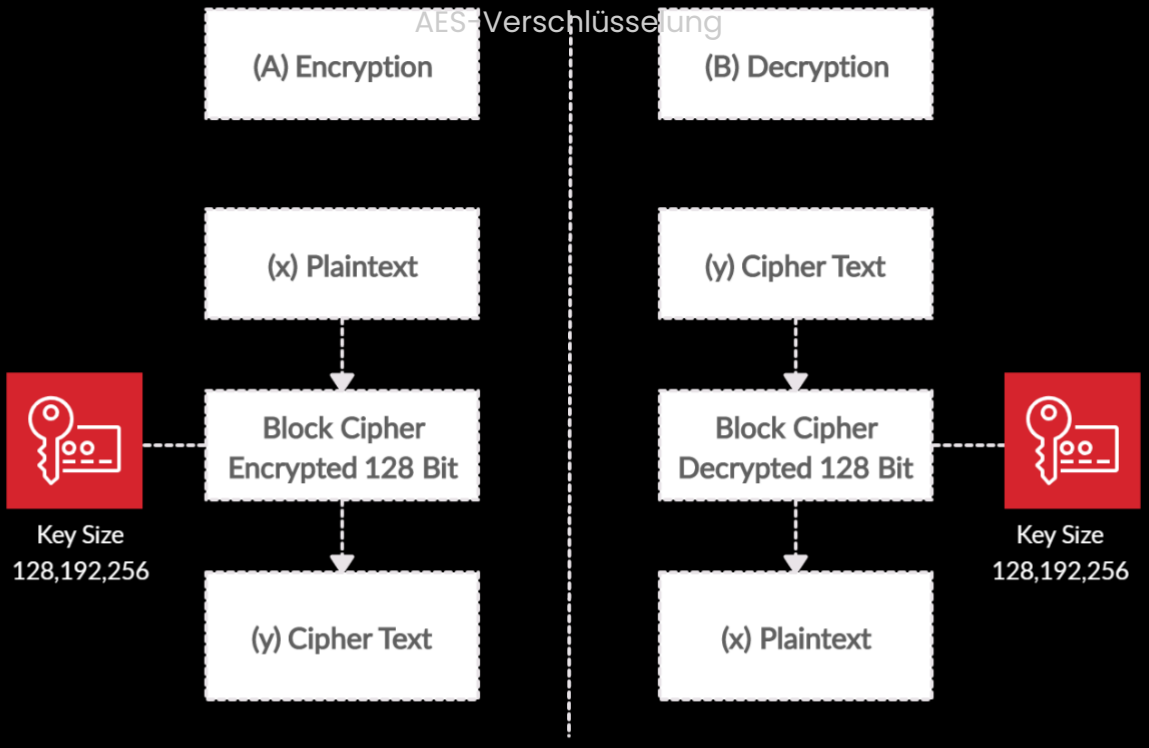
- AES - 128 Bit - (K)
- AES - 192 Bit - (K)
- AES - 256 Bit - (K)

Rundungs(R)-Zahlen basierend auf den Schlüssellängen:

- 128 Bit = 10 (R)
- 192 Bit = 12 (R)
- 256 Bit = 14 (R)

1. Bis heute gibt es keine Angriffe auf die AES-Verschlüsselung.

2. Das AES-System kann sehr effektiv sowohl in Software- als auch in Hardwarekomponenten implementiert werden.
3. Es bietet langfristig eine sehr gute Sicherheit gegen gewalttätige Angriffe.
4. Die AES wird seit Ende der 1990er Jahre intensiv untersucht
5. In der Praxis gibt es keinen Grund, die Verschlüsselung mit AES zu vervielfachen (DES benötigt heutzutage eine Mehrschlüssel-Verschlüsselung, auch TDES oder 3DES genannt).
6. Für die Ver- und Entschlüsselung wird derselbe geheime Schlüssel verwendet.
7. Alice und Bob haben die gleichen kryptografischen Fähigkeiten, da sie beide den gleichen Schlüssel haben, so dass alle Aktionen, die Alice ausführen kann (wie Ver- und Entschlüsselung) auch von Bob ausgeführt werden können und umgekehrt.
8. Eine höhere Anzahl von Umdrehungen führt zu einem sichereren System. Aber gleichzeitig bedeuten mehr Umdrehungen, dass die Ver- und Entschlüsselungsprozesse langsam und ineffizient sind.
9. Stärker und schneller als 3DES.
10. Software, die in C und Java implementiert werden kann.



Das Problem des Schlüsselaustauschs mit der ESA

Der symmetrische Schlüssel muss zwischen (A)Alice und (B)Bob auf einem sicheren Kanal ausgetauscht werden. Daher kann der Schlüssel nicht direkt über eine normale Verbindung gesendet werden, was der bequemste Weg wäre, und es ist eine andere Form der Übertragung erforderlich. Selbst für mittelgroße Netzwerke, wie z.B. ein Unternehmen mit 1000 Mitarbeitern, werden mehr als 2 Millionen Schlüssel benötigt, die über einen sicheren Kanal generiert und ausgetauscht werden müssen.

- Bei E-Commerce-Anwendungen ist es oft wichtig, zu beweisen, dass Alice tatsächlich eine Art Nachricht gesendet hat, z.B. durch die Bestellung einer Zentanode.
- Wenn wir nur symmetrische Kryptographie verwenden und Alice später ihre Meinung über den Kauf ändert, kann sie immer behaupten, dass Bob (der Verkäufer) die Bestellung irrtümlich erstellt hat. Die Verhinderung dieser Situation wird als "Nicht-Zurückweisung" bezeichnet und kann durch den Einsatz asymmetrischer Kryptographie (RSA, El-Gamal, DHKE) erreicht werden.

Asymmetrische Verschlüsselung

Asymmetrische Kryptographie, auch bekannt als Public-Key-Kryptographie, verwendet zwei verschiedene, aber mathematisch verwandte Schlüssel, einen öffentlichen und einen privaten. Der öffentliche Schlüssel kann mit jedem geteilt werden, während der private Schlüssel geheim gehalten werden muss. Der RSA-Verschlüsselungsalgorithmus ist der am weitesten verbreitete Algorithmus mit öffentlichem Schlüssel, zum Teil deshalb, weil sowohl der öffentliche als auch der private Schlüssel eine Nachricht verschlüsseln können; der Schlüssel, der dem zur Verschlüsselung einer Nachricht verwendeten Schlüssel entgegengesetzt ist, wird zur Entschlüsselung verwendet. Diese Funktion bietet nicht nur Vertraulichkeit, sondern auch eine Methode zur Gewährleistung der Integrität,

Zuverlässigkeit und Unberechenbarkeit der elektronischen Kommunikation und Daten durch die Verwendung digitaler Signaturen.

- Asymmetrische Kryptographie ist derzeit ein sehr begehrtes Werkzeug für viele Sicherheitsanwendungen.

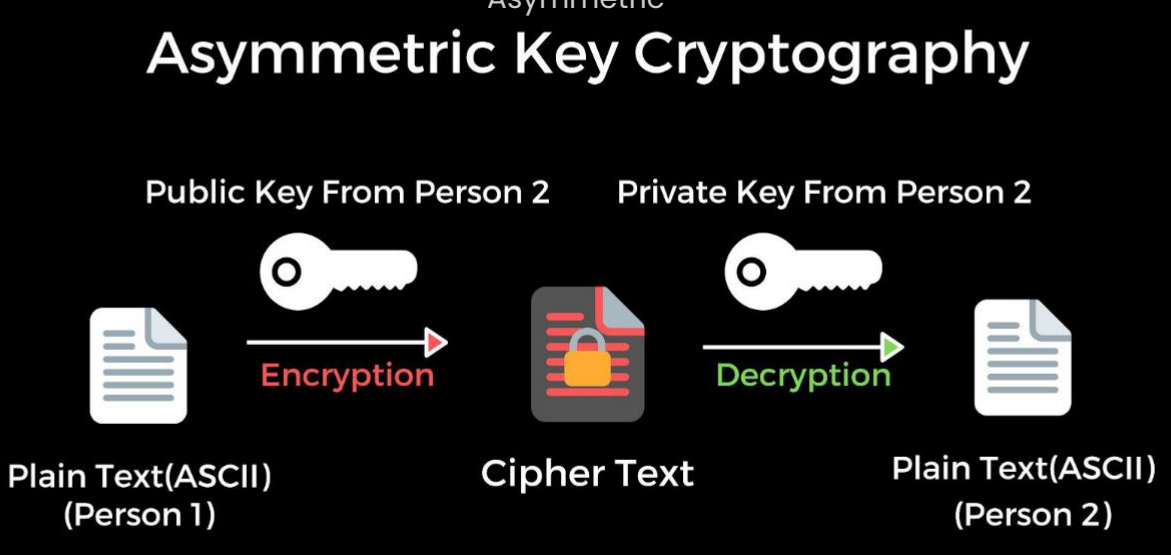
- Asymmetrische Kryptographie wird in der Workshop-Reihe "Public-Key Cryptography (PKC)" diskutiert.
- Es gibt asymmetrische Algorithmen, die ebenfalls auf unidirektionalen Funktionen basieren.

- Von besonderem Interesse sind Familien mit Einwegfunktionen: Hash-basiert und Code-basiert.
- Asymmetrische Algorithmen bieten dort Möglichkeiten, wo symmetrische Algorithmen den Austausch von Schlüsseln nicht erlauben, z.B. über unsichere Kanäle und digitale Signaturen.

- Asymmetrische Verfahren sind in der "wissenschaftlichen" Forschung seit etwa 2005 von großem Interesse.

- Das Interesse an diesen Methoden ist vor allem dadurch motiviert, dass es bisher keine Angriffe gegen asymmetrische Algorithmen auf der Basis von Quantencomputern gegeben hat.
- Er ist viel langsamer als Algorithmen wie AES oder 3DES (TDES). Dies ist auf den sehr hohen Rechenaufwand zurückzuführen, der für RSA (und alle anderen asymmetrischen Algorithmen) erforderlich ist.

Asymmetric



Rivest–Shamir–Adleman Encryption (RSA)

RSA (Rivest-Shamir-Adleman) ist eines der ersten Kryptographiesysteme mit öffentlichem Schlüssel und wird häufig für die sichere Datenübertragung verwendet. In einem solchen System ist der Verschlüsselungsschlüssel öffentlich und unterscheidet sich vom Entschlüsselungsschlüssel, der geheim (privat) gehalten wird. In RSA beruht diese Asymmetrie auf der praktischen Schwierigkeit, das Produkt zweier großer Primzahlen zu faktorisieren, dem "Faktorisierungsproblem". Das Akronym RSA setzt sich aus den Anfangsbuchstaben der Familiennamen von Ron Rivest, Adi Shamir und Leonard Adleman zusammen, die den Algorithmus 1977 erstmals öffentlich beschrieben haben.

Ein RSA-Benutzer erstellt und veröffentlicht dann einen öffentlichen Schlüssel, der auf zwei großen Primzahlen und einem Hilfswert basiert. Die Primzahlen müssen geheim gehalten werden. Jeder kann den öffentlichen Schlüssel zum Verschlüsseln einer Nachricht verwenden, aber nur jemand, der die Primzahlen kennt, kann die Nachricht entschlüsseln. Das Brechen der RSA-Verschlüsselung ist als RSA-Problem bekannt. Ob es so schwierig ist wie das Faktorisierungsproblem, bleibt eine offene Frage. Es gibt derzeit keine veröffentlichte Methode, um das System zu überwinden, wenn ein ausreichend großer Schlüssel verwendet wird.

RSA-Verschlüsselung und -Entschlüsselung

Um einen Klartext M mit einem öffentlichen RSA-Schlüssel zu verschlüsseln, stellen Sie einfach den Klartext durch eine Zahl zwischen 0 und N-1 dar und berechnen dann den Geheimtext C als:

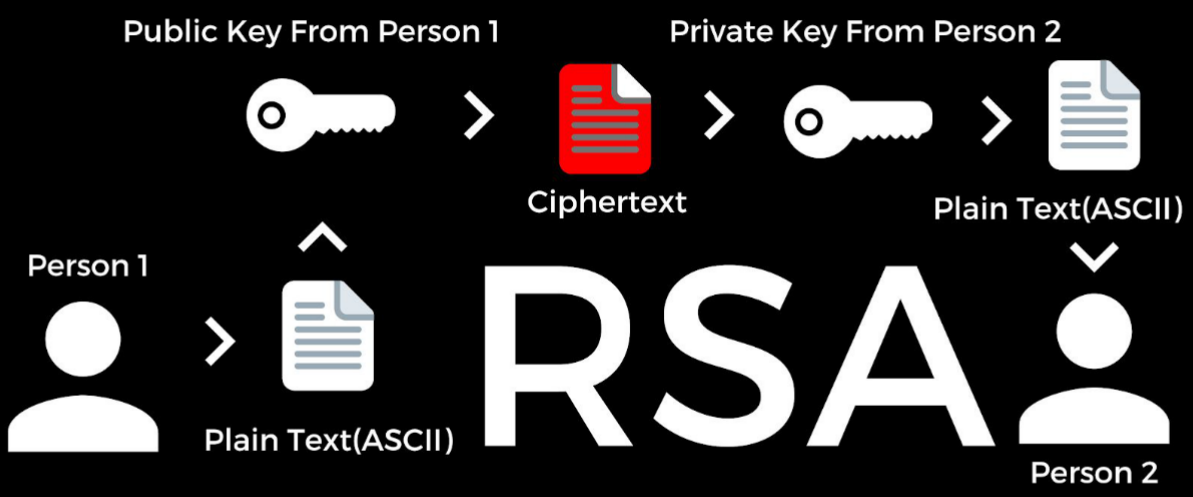
C = Me mod N

RSA-Entschlüsselung:

M Um einen Chiffretext C unter Verwendung eines öffentlichen RSA-Schlüssels zu entschlüsseln, berechnen wir einfach den Klartext M als:

M = Cd mod N

RSA-Encryption



Diffie-Hellman

Der Diffie-Hellman-Algorithmus ist eine der frühesten bekannten asymmetrischen Schlüsselimplementierungen und wird hauptsächlich für den Schlüsselaustausch verwendet. Obwohl symmetrische Schlüsselalgorithmen schnell und sicher sind, ist der Schlüsselaustausch immer ein Problem. Wir müssen einen Weg finden, um den privaten Schlüssel in alle Systeme zu bekommen. Der Diffie-Hellman-Algorithmus hilft dabei. Der Diffie-Hellman-Algorithmus wird verwendet, um einen sicheren Kommunikationskanal aufzubauen. Dieser Kanal wird von den Systemen verwendet, um einen privaten Schlüssel auszutauschen. Dieser private Schlüssel wird dann verwendet, um eine symmetrische Verschlüsselung zwischen den beiden Systemen durchzuführen. Aus diesem Grund verwenden wir den Austausch von DH-Schlüsselpaaren. Der Diffie-Hellman-Algorithmus ist anfällig für einen Man-in-the-Middle-Angriff.

Diffie-Hellman-Gruppen werden verwendet, um die Länge der Basisprimzahlen zu definieren, die während des Schlüsselaustauschprozesses verwendet werden. Es gibt drei Arten von Diffie-Hellman-Gruppen, die sich wie folgt zusammensetzen:

1. Dies ist die am wenigsten sichere Gruppe und stellt nur 768 Bit Schlagkraft zur Verfügung.
2. Diese Gruppe ist von mittlerer Stärke, mit 1024 Bits Schlagkraft. Diffie-Hellman-Gruppe.
3. Diese Gruppe wird auf der höchsten Ebene definiert, mit 2048 Bit Schlagkraft.

Diffie-Hellman Protocol

- Für das Diffie-Hellman-Protokoll in der Primzahl sollte p mindestens 2048 Bit betragen, um langfristige Sicherheit zu gewährleisten.
- Das Diffie-Hellman-Protokoll ist eine weit verbreitete Methode für den Schlüsselaustausch. Es basiert auf zyklischen Gruppen.

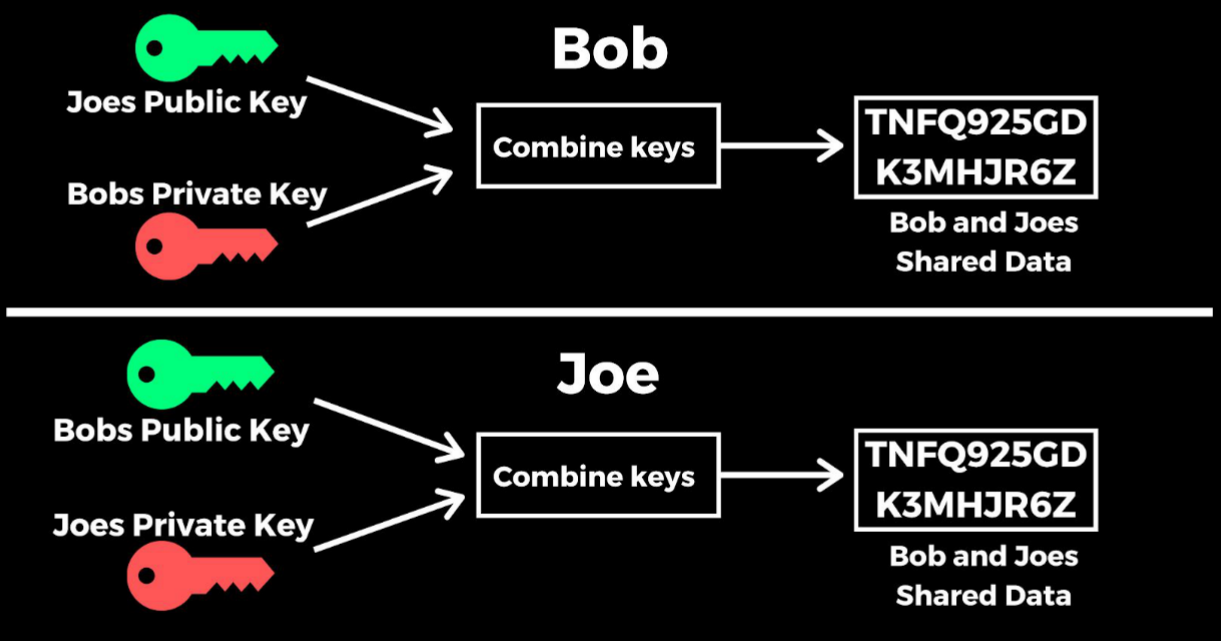
Diffie-Hellman-Hybridsysteme

Hybride Sitzungsschlüsselsysteme ähneln den Diffie-Hellman-Systemen, mit der Ausnahme, dass anstatt die verschiedenen Schritte zur Entwicklung eines Sitzungsschlüssels zu durchlaufen, Folgendes geschieht.

1. Teil A erzeugt einfach einen Sitzungsschlüssel, verschlüsselt ihn mit dem öffentlichen Schlüssel aus Teil B und sendet die verschlüsselte Nachricht an Teil B.
2. Teil B entschlüsselt dann die Nachricht mit seinem privaten Schlüssel, gibt den Sitzungsschlüssel in seine Software oder sein Single-Key-Telefon ein und beginnt das Gespräch oder den Datentransfer im schnelleren, temporären Single-Key-Modus.

Der eigentliche Prozess der Auswahl des temporären, zufälligen Sitzungsschlüssels ist für die Benutzer unsichtbar, weil er in dem mathematischen Algorithmus stattfindet, der in der Verschlüsselungssoftware enthalten ist, die jeder verwendet.

Diffie-Hellman



El-Gamal

Die El-Gamal-Verschlüsselung ist ein Kryptosystem mit öffentlichem Schlüssel. Es verwendet asymmetrische Schlüsselverschlüsselung für die Kommunikation zwischen zwei Parteien und die Verschlüsselung der Nachricht. Der Elgamal-Algorithmus wurde von Taher El-Gamal erfunden, der auf dem Schlüsselaustausch zwischen dem Diskreten Logarithmus-Problem und Diffie-Hellman-Schlüssel basiert. El-Gamal ist ein probabilistisches Verschlüsselungsverfahren, bei dem die Verschlüsselung von zwei identischen Nachrichten zu unterschiedlichen Chiffrierraten führt.

- El-Gamal hat den Nachteil, dass der Chiffriertext doppelt so groß ist wie der Klartext

- Jedes Mal, wenn derselbe Klartext verschlüsselt wird, ergibt sich ein anderer Chiffretext.

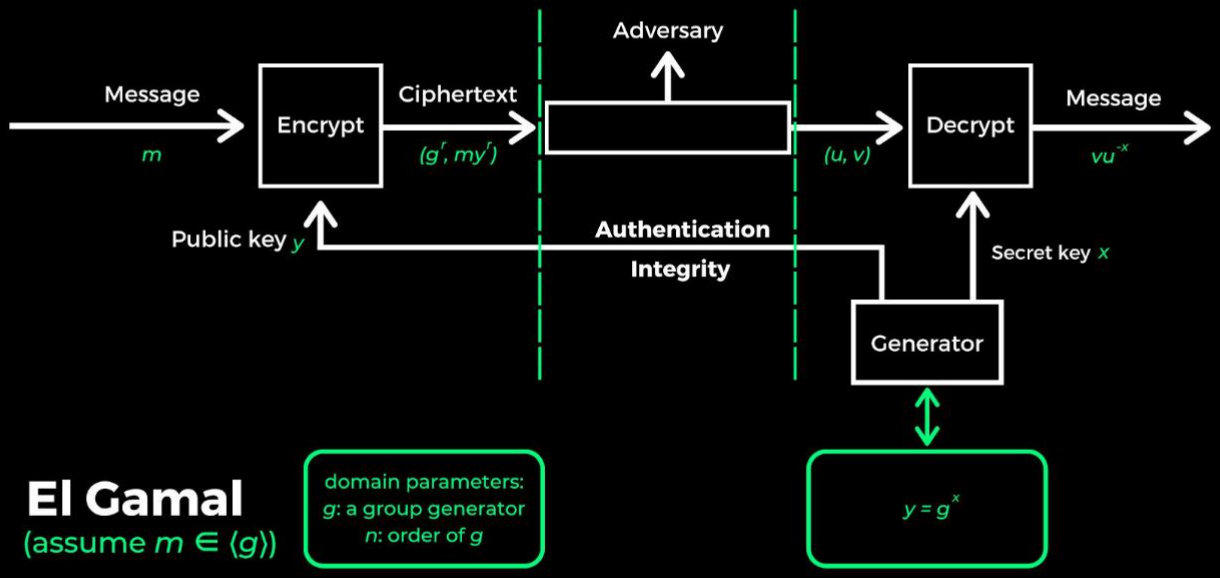
- El-Gamal kann sowohl zur Verschlüsselung als auch zur digitalen Signatur verwendet werden.
- El-Gamal basiert auf zyklischen Gruppen.
- Für die El-Gamal-Verschlüsselung sollte die Primzahl p mindestens 2048 Bit betragen.

El-Gamal-Protokoll

- Im Gegensatz zur DHKE ist keine vertrauenswürdige dritte Partei erforderlich, um die Primzahl und das primitive Element auszuwählen.
- Die Bauphase wird von den Parteien nur einmal durchgeführt.
- Die Verschlüsselungsphase und die Entschlüsselungsphase werden bei jedem Nachrichtenaustausch ausgeführt.

Alice braucht nur eine Nachricht zu senden, während das Diffie-Hellman-basierte Protokoll zwei Nachrichten erforder

El-Gamal



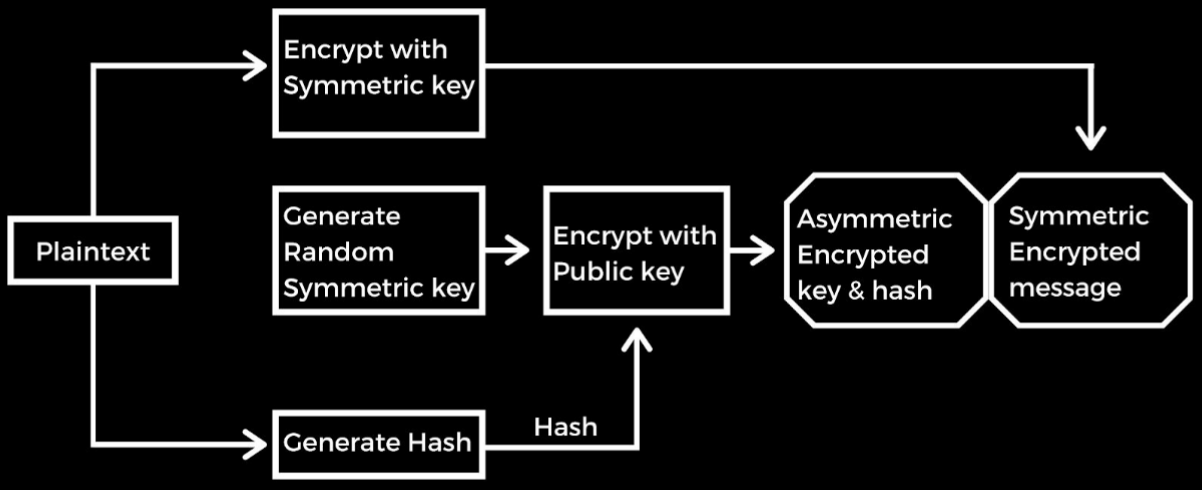
Hybrid-Verschlüsselungn

Hybride Verschlüsselung ist ein Verschlüsselungsmodus, der zwei oder mehr Verschlüsselungssysteme zusammenführt. Es beinhaltet eine Kombination von asymmetrischer und symmetrischer Verschlüsselung, um die Stärken jeder Verschlüsselungsform auszunutzen. Diese Stärken sind Schnelligkeit bzw. Sicherheit. Hybride Verschlüsselung gilt als hochsichere Art der Verschlüsselung, solange sowohl öffentliche als auch private Schlüssel vollständig gesichert sind. Ein hybrides Verschlüsselungssystem ist ein System, das den Komfort eines asymmetrischen Verschlüsselungssystems mit der Effektivität eines symmetrischen Verschlüsselungssystems kombiniert. Die Kombination der Verschlüsselungsmethoden hat mehrere Vorteile.

- Benutzer haben dann die Möglichkeit, mit hybrider Verschlüsselung zu kommunizieren.
- Asymmetrische Verschlüsselung kann den Verschlüsselungsprozess verlangsamen, aber mit der gleichzeitigen Verwendung von symmetrischer Verschlüsselung werden beide Verschlüsselungsformen verbessert.
- Dies führt zu einer erhöhten Sicherheit des Übertragungsprozesses sowie zu einer allgemeinen Verbesserung der Systemleistung.

- Erhöhte Rechenkomplexität, kryptographische Ziele wie Vertraulichkeit, Integrität und Authentizität können durch den Einsatz hybrider kryptographischer Ansätze erreicht werden.

Hybrid Encryption



SHA-256

Der SHA-256 ist eine der sequentiellen Hash-Funktionen des SHA-1 (kollektiv als SHA-2 bezeichnet) und stellt die leistungsstärkste verfügbare Funktion dar. Der SHA-256 ist nicht viel komplexer zu codieren als der SHA-1 und wurde bisher in keiner Weise kompromittiert. Der 256-Bit-Schlüssel macht sie zu einer guten Partnerfunktion für die SUP. Der SHA-256 ist eine Funktion, die eine Eingabe mit zufälliger Größe nimmt und eine Ausgabe mit fester Größe erzeugt.

Darüber hinaus hat das SHA-256 recht gute technische Parameter:

- Blockgrößenanzeige: 64 Bytes.
- Maximal zulässige Nachrichtenlänge: 33 Bytes.
- Merkmale der Größe des Message Digest: 32 Bytes.
- Die Standard-Wortgröße: 4 Bytes.
- Interner Positionslängenparameter: 32 Bytes.
- Die Anzahl der Iterationen in einem Zyklus: 64.
- Die durch das Protokoll erreichte Geschwindigkeit (MiB/s): ungefähr 140.

Die SHA-256-Hash-Funktion wird innerhalb des Bitcoin-Netzwerks hauptsächlich auf zwei Arten genutzt:

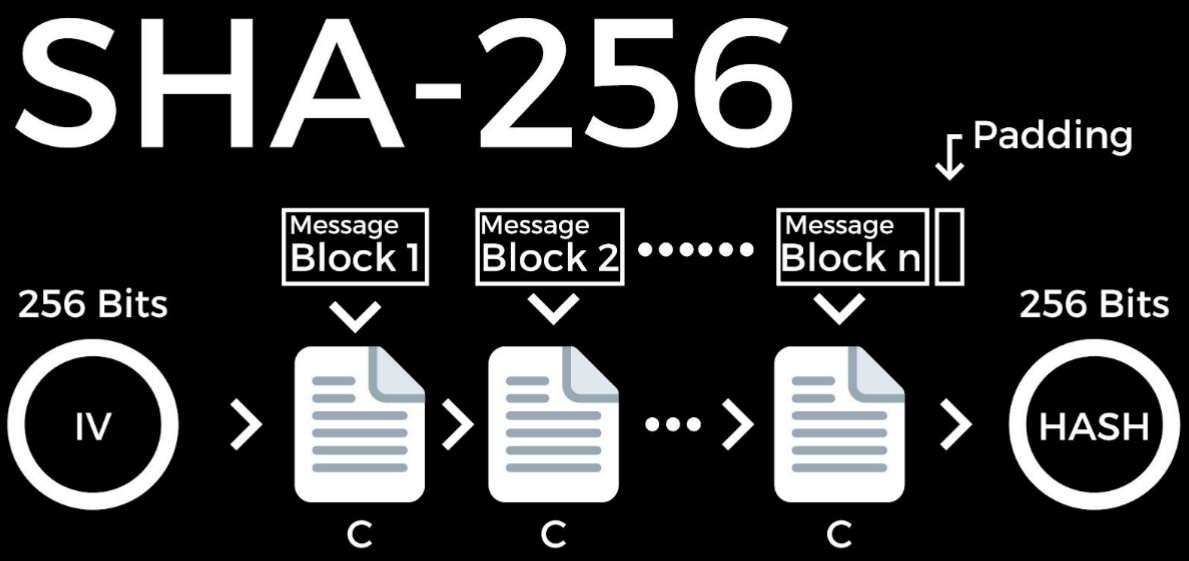
- Bergbau
- Erstellung von Bitcoin-Adressen

Was noch wichtiger ist:
Mit der Zeit nehmen Cyber-Angriffe dramatisch zu, da die Kosten für die Rechenleistung der Computer sinken. Bis 2025 wird die heutige digitale Signatur nicht mehr so sicher sein wie heute. Aus diesem Grund wird die Wahl des Algorithmus eine wichtige Entscheidung sein. Sie ist notwendig, weil kurzfristige temporäre Aktualisierungen die Sicherheit einfach gefährden können. Kein Hash-Algorithmus ist in der Lage, ein hohes Maß an Sicherheit aufrechtzuerhalten, nicht einmal für ein Jahrzehnt.

Das bedeutet nicht, dass Kryptographen untätig herumsitzen und auf ein Problem warten. Der Nachfolger von Sha-2, bekannt als SHA-3, ist bereits abgeschlossen. Wenn die Zeit für diesen Übergang gekommen ist, wird die Online-Technologiebranche in der Lage sein, SHA-3 als ihre nächste Wahl zu nutzen. Aber vielleicht wird es zu diesem Zeitpunkt einen ganz anderen Algorithmus geben.

Es dauert Jahre, neue kryptographische Standards zu erforschen und zu testen, bevor wir mit der Entwicklung von Software zur Unterstützung dieser Standards beginnen können. Nur wenn wir der Zeit voraus sind, können wir über beide Sicherheitsniveaus sprechen.

SHA-256



Blake2

Die kryptografische Hash-Funktion von BLAKE2 wurde von Jean-Philippe Aumasson, Samuel Neves, Zooko Wilcox-O'Hearn und Christian Winnerlein entworfen.

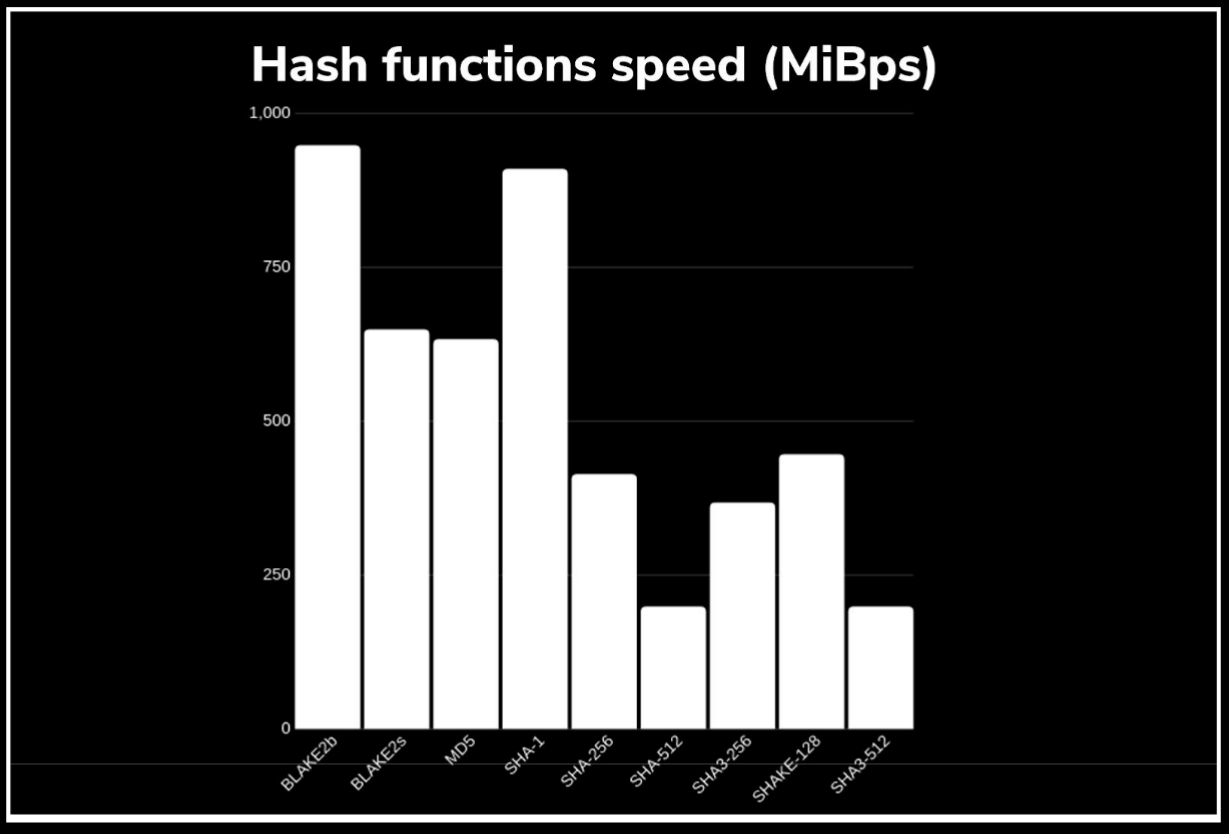
BLAKE2 ist eine schnellere kryptographische Hash-Funktion als MD5, SHA-1, SHA-2 und SHA-3, aber sie ist mindestens so sicher wie der neueste SHA-3-Standard. BLAKE2 wurde aufgrund seiner hohen Geschwindigkeit, Sicherheit und Einfachheit von vielen Projekten übernommen.

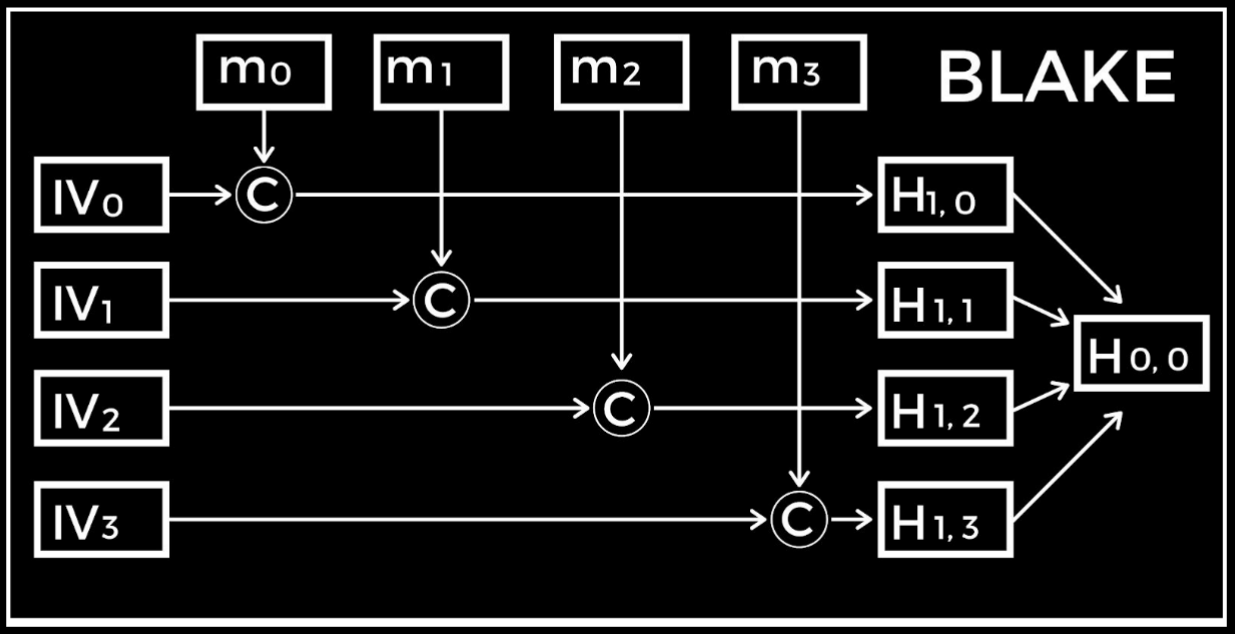
BLAKE2 ist in zwei Versionen erhältlich: BLAKE2b (oder einfach nur BLAKE2) ist für 64-Bit-Plattformen - einschließlich NEON-kompatibler ARMs - optimiert und erzeugt Vorschauen beliebiger Größe zwischen 1 und 64 Bytes BLAKE2s ist für 8- bis 32-Bit-Plattformen optimiert und erzeugt Zusammenfassungen beliebiger Größe zwischen 1 und 32 Bytes.

Die Leistung von BLAKE2 ist viel schneller als die von BLAKE, was vor allem auf die geringere Anzahl von Drehungen zurückzuführen ist. Bei langen Nachrichten wird erwartet, dass BLAKE2b und BLAKE2s etwa 25 % bzw. 29 % schneller sind, ohne Berücksichtigung der Einsparungen durch keine Konstanten, optimierte Rotationen oder Little-Endian-Konvertierung. Die parallelen Versionen BLAKE2bp und BLAKE2sp sollten bei langen Nachrichten 4- und 8-mal schneller sein als BLAKE2b und BLAKE2s, wenn sie mit mehreren Threads auf einer CPU mit 4 oder mehr Kernen implementiert werden (wie die meisten Desktop- und

Serverprozessoren: AMD FX-8150, Intel Core i5-2400S usw.) Wie bereits erwähnt, profitiert das parallele Hashing auch von fortschrittlichen Prozessortechnologien.

Abbildung 1: Vergleich der Geschwindigkeit verschiedener populärer Hash-Funktionen aus den "sandigen" eBACS-Messungen. SHA-3 und BLAKE2 haben keine bekannten Sicherheitsprobleme. SHA-1, MD5, SHA256 und SHA-512 sind anfällig für Dehnungen. SHA-1 und MD5 sind anfällig für Kollisionen. Das MD5 ist anfällig für Kollisionen mit dem gewählten Präfix.





Beispiel für einen Parameterblock aus BLAKE2b. Als Beispiel nehmen wir eine Instanz von BLAKE2b mit - 64 Bytes Digests, d.h. mit einer auf 40 gesetzten parametrischen Digestlänge, - einem 256-Bit-Schlüssel, d.h. mit einer auf 20 gesetzten parametrischen Schlüssellänge, - einem Salzsatz für die all-55 Zeichenkette, - einem Anpassungssatz für die all-ee Zeichenkette. BLAKE2b führt einen sequentiellen Hash der Daten durch, was bedeutet, dass die Baumparameter auf den für den sequentiellen Modus angegebenen Wert gesetzt werden:

Der Fanout und die maximale Tiefe werden auf 01 gesetzt, die maximale Blattlänge auf 000000000000, der Knotenversatz auf 000000000000, die Knotentiefe und die interne Hash-Länge auf 00. Der Parameterblock für diese Instanz von BLAKE2b ist: 40200101 00000000 00000000 00000000 00000000 00000000 00000000 00000000 55555555 55555555 55555555 55555555

Beispiel für einen Parameterblock von BLAKE2s. Als Beispiel nehmen wir eine Instanz von BLAKE2s mit - 32 Bytes Digests, d.h. mit einer auf 20 gesetzten Parameterdigestlänge, - keinem Schlüssel, d.h. mit einer auf 00 gesetzten Parameterschlüssellänge, - keinem Salz und keiner Anpassung, d.h. mit allen entsprechenden Bytes auf NULL gesetzt. BLAKE2s führt sequentielle Datenhashes durch, d.h. die Baumparameter werden auf den für den sequentiellen Modus angegebenen Wert gesetzt: Fanout und maximale Tiefe werden auf 01, die maximale Blattlänge auf 000000, der Knotenversatz auf 000000000000, die Knotentiefe und die interne Hash-Länge werden auf 00 gesetzt. Der Parameterblock für diese Instanz von BLAKE2s lautet: 20000101 00000000 00000000 00000000 00000000 00000000 00000000 00000000

Struktur und Terminologie:

	BLAKE2b	BLAKE2s
Bits in word	w = 64	w = 32
Rounds in F	r = 12	r = 10
Block bytes	bb = 128	bb = 64
Hash bytes	1 <= nn <= 64	1 <= nn <= 32
Key bytes	0 <= kk <= 64	0 <= kk <= 32
Input bytes	0 <= ll < 2**128	0 <= ll < 2**64
G Rotation constants	(R1, R2, R3, R4) = (32, 24, 16, 63)	(R1, R2, R3, R4) = (16, 12, 8, 7)

Blake2b-Größenanpassung der Bytes:

```
const (
  // The blocksize of BLAKE2b in bytes.
   BlockSize = 128
   // The hash size of BLAKE2b-512 in bytes.
   Size = 64
   // The hash size of BLAKE2b-384 in bytes.
   Size384 = 48
  // The hash size of BLAKE2b-256 in bytes.
   Size256 = 32
);
```

Ergebnisse der Verschlüsselungen:

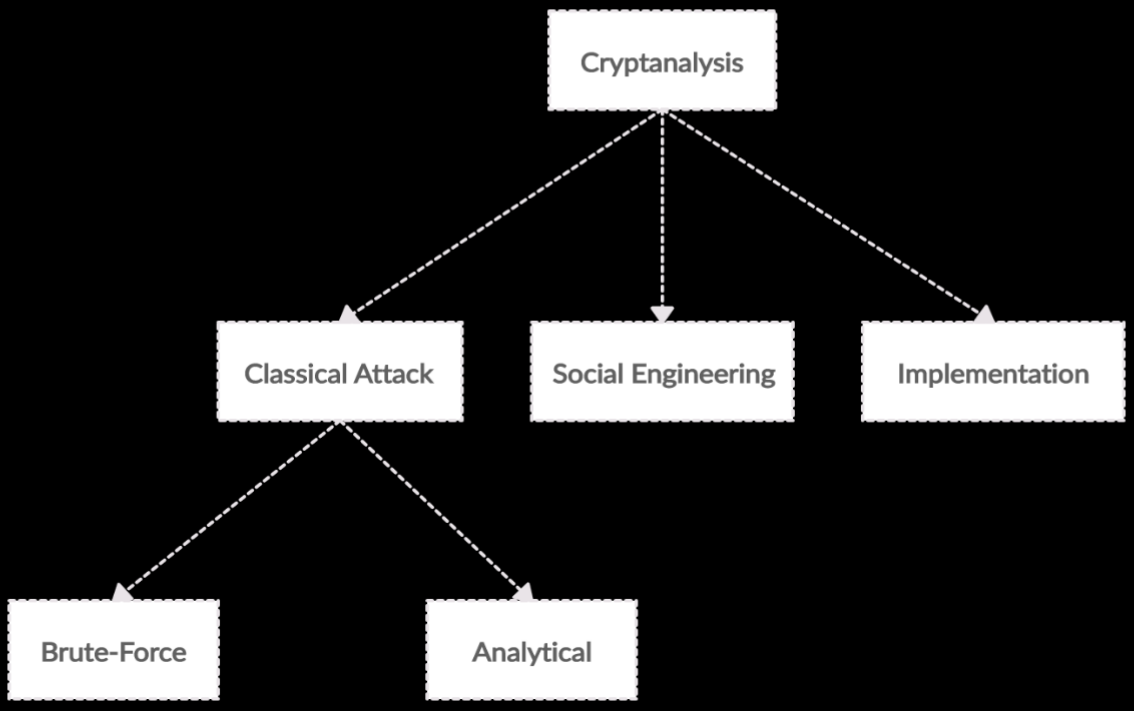
Wir haben all diese Verschlüsselungsmechanismen, Algorithmen und Mehrkomponenten-Verschlüsselung separat hinzugefügt. Wir haben auch die Hash-Funktion geschrieben, die für ihre Nutzung erforderlich ist, da alle Daten und IP-Adressen in Zentameshnet, Zentalk und Zentavult sehr sicher und gut geschützt sind und auf dem hohen Niveau arbeiten, das wir Ihnen präsentieren wollten. Noch wichtiger ist, dass andere Verschlüsselungsmethoden nicht mehr verwendet werden können, weil die Verschlüsselungsmechanismen heute entschlüsselt sind und es den Bits an Leistung mangelt. Darüber hinaus mangelt es einigen Verschlüsselungsalgorithmen bei einigen Anwendungen an Geschwindigkeit und Leistung; es ist absolut wichtig, die richtige Verschlüsselung und Hashes für die Anwendungen zu verwenden. Der Diffie-Hellman-Schlüsselaustausch deutet auf eine Schwäche gegenüber einem Angriff eines Mittelsmannes hin, weil er über den unsicheren Kanal verläuft. Die El-Gamal-Verschlüsselungs- und Entschlüsselungsphase findet bei jedem Nachrichtenaustausch statt, aber das Diffie-Hellman-Protokoll erfordert zwei Nachrichten, so dass eine Person nur eine Nachricht senden muss, und die Ver- und Entschlüsselungsphase wird bei jeder Nachrichtenänderung durchgeführt.

Hybride Verschlüsselung ist ein Verschlüsselungsmodus, der zwei oder mehr Verschlüsselungssysteme kombiniert. Da auch Zentalk dieses Verschlüsselungssystem verwendet, haben wir es Zentalk Hybrid Messaging Application genannt. Da es verschiedene Verschlüsselungen innerhalb und außerhalb des Netzwerks sichern muss, damit das System von selbst funktioniert, und nicht auf einen dritten Speicher in der Cloud zugreifen muss, ist El-Gamal eine ziemlich gute Lösung für digitale Signaturen. Die BLAKE2-Verschlüsselungshash-Funktion wird häufig verwendet, weil sie schneller als andere Hash-Funktionen ist und sich besser für dezentrale Anwendungen eignet. Deshalb haben wir uns für Blake2 entschieden. Eines der Hauptprobleme von AES besteht darin, dass es als symmetrischer Algorithmus erfordert, dass Verschlüsseler und Entschlüsseler denselben Schlüssel verwenden. Dies wirft ein entscheidendes Problem beim Schlüsselmanagement auf: Wie kann dieser geheime Schlüssel von größter Bedeutung an Hunderte von Empfängern in der ganzen Welt verteilt werden, ohne Gefahr zu laufen, dabei fahrlässig oder absichtlich kompromittiert zu werden? Die Antwort und Lösung ist eine Kombination aus symmetrischer und asymmetrischer Verschlüsselung und den kombinierten Stärken von AES und RSA. Es ist auch wichtig, eine hohe Bitstärke beider Verschlüsselungen zu verwenden. Die Hash-Funktionen des SHA-256 sind derzeit leistungsfähig genug, um in unserem Zentanode-Algorithmus verwendet zu werden, und stellen die beste Option für die

AES-Verschlüsselung dar. Aufgrund der Leistungsfähigkeit von Quantencomputern müssen sie jedoch in Zukunft möglicherweise aufgerüstet werden, und auch hier müssen die Bits ausreichend leistungsfähig sein.

16. Kryptoanalyse

Die Kryptoanalyse ist ein Prozess, der darin besteht, Methoden zu untersuchen, um die Bedeutung verschlüsselter Informationen zu erhalten, im Allgemeinen ohne Zugang zu geheimen Informationen. Typischerweise geht es darum, herauszufinden, wie das System funktioniert und einen geheimen Schlüssel zu finden. Die Kryptoanalyse wird auch als "Entschlüsselung" oder "Knacken" des Codes bezeichnet. (Brute-Force) Das Kryptogramm ist normalerweise der am einfachsten zu erhaltende Teil eines Kryptosystems und daher ein wichtiger Teil der Kryptoanalyse. Je nach den verfügbaren Informationen und der Art der analysierten Chiffre können Kryptoanalytiker einem oder mehreren Angriffsmustern folgen, um eine Chiffre zu knacken. Eine kryptographische Lösung muss auch dann sicher sein, wenn der Angreifer oder ein Drittbenutzer alle Details des kryptographischen Systems mit Ausnahme des Schlüssels kennt. Insbesondere muss das Verfahren auch dann sicher sein, wenn der Angreifer den Ver- und Entschlüsselungsalgorithmus kennt, und der Algorithmus muss auch gegen analytische Angriffe geschützt sein. Ein Angreifer wird immer die schwächste Stelle eines Verschlüsselungsverfahrens ausnutzen. Eine Verschlüsselung mit einem großen Schlüssel reicht nicht aus, um zu garantieren, dass die Verschlüsselung ausreichend sicher ist. Sie kann zum Beispiel mathematische Schwächen haben.



- **Klassischer Angriff**

Bei der klassischen Kryptoanalyse gibt es verschiedene Ziele, die ein Hacker verfolgen kann. Die beiden häufigsten Situationen sind, wenn der Angreifer entweder den Klartext x oder den Schlüssel k für eine gegebene Verschlüsselungsrate y berechnen will. Bei der Suche nach dem vollständigen Schlüssel wird die Verschlüsselung als Black Box betrachtet, während bei analytischen Angriffen die interne Struktur des Verschlüsselungsverfahrens ausgenutzt wird.

- **Angriff mit roher Gewalt**

Bei Force-Brute-Angriffen wird der Verschlüsselungsalgorithmus für alle möglichen Schlüsselfälle ausgeführt, bis eine Übereinstimmung gefunden wird.

- **Analytischer Angriff**

Analytische Angriffe sind solche, die darauf abzielen, das kryptographische System zu knacken, indem die interne Struktur des Verschlüsselungsalgorithmus analysiert wird.

- **Angriff auf Social Engineering**

Social-Engineering-Angriff ist Manipulation - zwischenmenschliche Einflüsse (wie gefälschte Konten) werden ausgenutzt, um an die Krypto-Schlüssel zu gelangen. Phishing-Angriffe sind die bekanntesten Vertreter des Social Engineering-Angriffs.

Beispiel: "Guten Morgen, ich bin X aus der IT-Abteilung. Wir benötigen Ihr Passwort für ein dringendes Sicherheits-Update."
Ein Angreifer sucht nach dem schwächsten Glied in der Kette, um das Kryptosystem zu überwinden. Daher reichen leistungsfähige kryptographische Algorithmen, die der klassischen Kryptoanalyse allein widerstehen, nicht aus, und Social-Engineering- und Anwendungsangriffe sollten
verhindert werden.

- **Angriff auf die Umsetzung**

Implementierungsangriffe wie die Subkanalanalyse können zur Erlangung eines geheimen Schlüssels verwendet werden. Sie sind in Fällen relevant, in denen sich der Angreifer physisch Zugang zum Kryptosystem verschaffen kann.

Wie viele Bits Schlüsselgröße brauchen wir?

Die Schlüssellängen für symmetrische und asymmetrische Verfahren unterscheiden sich erheblich. Beispielsweise bietet ein symmetrischer Algorithmus mit einem 128-Bit-Schlüssel ungefähr die gleiche Sicherheit wie RSA mit 3072 Bit (RSA ist eines der beliebtesten asymmetrischen Verfahren).

Angriffszeiten mit vollständiger Schlüsselsuche für symmetrische Algorithmen:

- Es dauert ein paar Stunden oder Tage, um die 64-Bit-Schwelle zu überschreiten.
- 128 Bit Langfristig: es ist möglich, sie mit einem Quantencomputer zu brechen.
- 256 Bit Langfristig: Mit Quantencomputern ist es nicht zerbrechlich.

Was brauchen wir für sichere Systeme?

Ein Sicherheitssystem schützt Vermögenswerte wie Daten, Geld oder Gebäude. Kryptografische Algorithmen spielen bei der Sicherung digitaler Systeme oft eine zentrale und dezentrale Rolle.

Regeln eines sicheren Systems & Schlüssellängen von symmetrischen Algorithmen:

1. Der Bruch wird teurer sein als der zu schützende Wert.
2. Die Schutzwerte und Sicherheitsziele sollten zunächst definiert werden.
3. Verwenden Sie nur Kryptoalgorithmen (d.h. symmetrische und asymmetrische Chiffren und Hash-Funktionen) oder Protokolle, die seit langem öffentlich bekannt sind und umfassend analysiert wurden.

4. Es dauert viele Jahre, 128 Bit zu knacken, es sei denn, der Hacker verfügt über Quantencomputer.
5. 256 Bit: Schutz vor Hackern mit Quantencomputern.
6. Die Schlüssellängen der 128-, 192- und 256-Bit-AES-Verschlüsselung sind seit mehreren Jahrzehnten gegen Brute-Force-Angriffe geschützt.
7. Wir brauchen RSA oder das DHKE-Protokoll ist ein Muss für den Austausch von Schlüsseln in einer ungesicherten Kanalverbindung. Sobald der symmetrische Schlüssel entschlüsselt ist, können beide Parteien (A) und (B) ihn für die symmetrische Ver- und Entschlüsselung von Nachrichten verwenden.

8. Verschlüsseln Sie die Daten mit symmetrischen oder asymmetrischen Algorithmen wie RSA, El-Gamal oder 3DES.

17. Das Zentamesh-Netzwerk und die Zentanodes

Die Knoten verstehen
Mit der Übernahme der Paketvermittlungstheorie und dem Konzept der verteilten Netzwerke wurden Knotenideen populär. In diesem Zusammenhang waren Knotenpunkte Gateways, die Informationen über verschiedene Pfade in einem verteilten Netzwerk empfangen, speichern und senden konnten. Jeder Knoten hatte eine gleichberechtigte Position im Netzwerk, was bedeutet, dass der Verlust eines Knotens dem Netzwerk keinen Schaden zufügte.

Warum ist Zentameshnet besser?

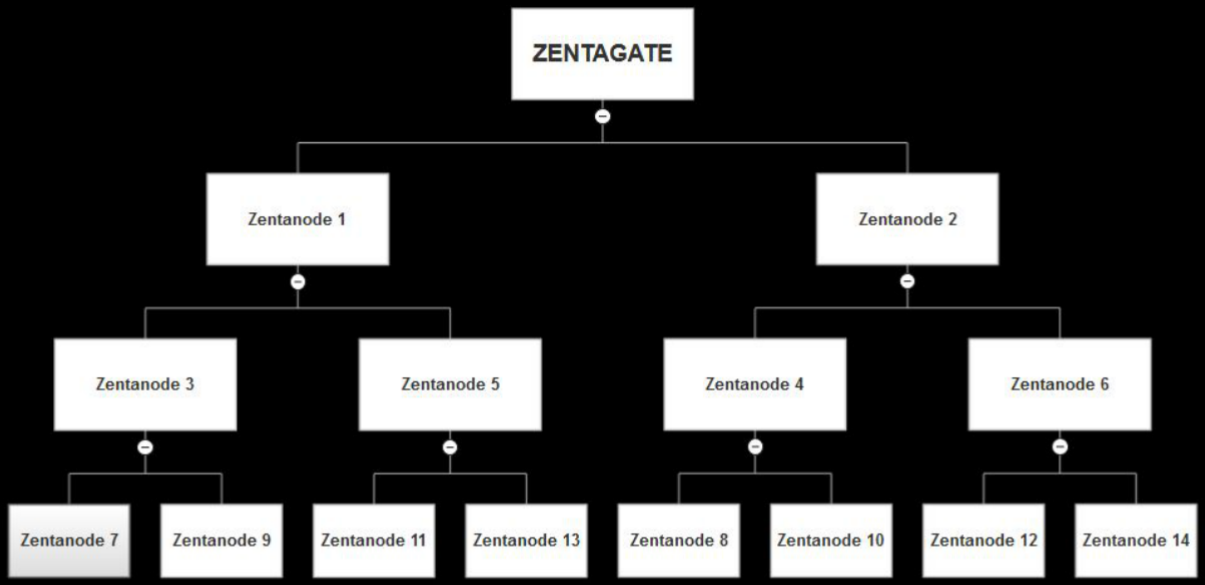
Zentameshnet hat selbstreparierende Eigenschaften, die zu seiner Fähigkeit beitragen, der Zensur zu widerstehen. Selbstreparatur bedeutet, dass, wenn die Verbindung eines Knotens blockiert oder deaktiviert ist, das Maschennetz sich selbst reparieren und um den verlorenen Knoten herum umgeleitet werden kann. Die Daten werden umgeleitet, und das Netzwerk ist immer noch funktionsfähig. Vermaschte Netzwerke können sowohl auf drahtgebundene als auch auf drahtlose Netzwerke angewendet werden, und Zentalk wird ein vermaschtes drahtloses lokales Netzwerk (WLAN) einrichten. Dieses drahtlose LAN kann mit einem Zentanode Mesh WLAN realisiert werden. Dieses Netzwerk wird für die Offline-Kommunikation über Zentalk benötigt.

Das bedeutet, dass ein Zentanode-Besitzer eine Internetverbindung herstellen und mit anderen teilen kann und auch mit Geräten kommunizieren kann, die keinen Zugang zum Internet haben (Offline-Offline). Dies kann auch dann geschehen, wenn es nur wenig oder gar keine Infrastruktur gibt. Die Besitzer von Zentanode werden von Zenta belohnt. Knoten sind aktive Netzwerkkomponenten wie Mobiltelefone, Router, Switches, Brücken und Gateways.

Jede Zentanode in einem Netzwerk ist ein Verbindungspunkt. Es kann entweder ein Umverteilungspunkt oder ein Endpunkt bei der Datenübertragung sein. Es wird verwendet, um Übertragungen zu entdecken, zu verarbeiten und an andere Knoten im Netzwerk zu übertragen. Ein Netzwerkknoten hat mindestens zwei, in der Regel mehr Verbindungen zu anderen Netzwerkelementen.

Jedes Zentameshnet Zentanode kann auch als Gateway zur Erweiterung des Zentamesh Netzwerks dienen. Der Benutzer muss auch in der Lage sein, sein Netzwerk mit einem Pincode zu schließen, um sich nur mit seinen Zentanodes zu verbinden. Jede Zentanode wird ihre eigene Kennung haben.

Die Rolle einer Zentanode wird mit einem Gerät verbunden sein, das die Zentalk-Messenger-Anwendung auf einem Mobiltelefon, Tablet oder Computer ausführt.



11 Gründe für den Einsatz der Zentamesh-Technologie:

1. Stabilität des Netzwerks

Die Daten im (drahtlosen) Mesh-Netzwerk können über andere Zentanodes übertragen werden, selbst wenn einer oder einige der Zentanodes fehlerhaft oder defekt sind und die Daten durch andere Zentanodes im Ökosystem geleitet werden.

2. Hohe Bandbreite.

Zentamesh-Netzwerke sind so konzipiert, dass sie den optimalsten (dynamischen) Routen folgen und eine höhere Bandbreite ermöglichen. Mit der Zunahme der Anzahl der Knoten und der Anzahl der möglichen Pfade wird die Gesamtbandbreite stark erhöht.

3. Sicherheit und Gefahrenabwehr

Verglichen mit dem Single-Hop-Mechanismus von WLAN bestimmt der Multi-Hop-Mechanismus des Zentamesh-Netzwerks, dass die Benutzerkommunikation über mehrere Zentanodes laufen muss.

4. Reichweite der Zentanodes

- Je mehr Zentanode-Benutzer, desto größer und schneller wird Ihr drahtloses Zentamesh-Netzwerk.

- Die Reichweite einer einzelnen Zentanode beträgt derzeit ohne Internetzugang bis zu 25-50 km (mehr Knoten = mehr Reichweite).
- Benutzer der Zentanode können die Zentanode dort auch als eigenes Benutzer-Gateway betreiben.

- Ohne Zentanode beträgt die Reichweite über Wi-Fi-Verbindung etwa 100 Meter.

5. Datenübertragung über Zentameshnet

- Im Zentameshnet-Netz wird es zunächst nur möglich sein, Daten und Dateien von maximal 15 Mb über die Wifi & BLE-Verbindung zu übertragen.
- Mit einer Internetverbindung von bis zu 150 Mb wird die Download-Geschwindigkeit 17,88/ Sekunde betragen.

6. Zentanode Hash(H) & Verschlüsselung(E)

- AES(E), RSA(E), Hybrid(E)
- Zentanode Hash-Algorithmen: SHA-256
- SLL

7. Betriebsfrequenzen:

- Europe - 868MHz
- USA, Kanada und Mexiko- 902MHz
- Lateinamerika & SE-Asien- 922MHz

8. Verfügbare Netzwerke:

- IEEE 802.11,(Wifi) Bluetooth, LTE, 4G, 5G

9. Die Wifi-Verbindung

- Sie stützen sich auf die gleichen WiFi-Standards (802.11a, b und g), die bereits für die meisten drahtlosen Netzwerke gelten.
- Tiefer Schlaf: Ja

10. Bluetooth

- Niedrige Energie

11. Zentagateway

- AES 128

18. Zentavault

Zentavault ist die zweite dApp, die aus der Zentachain-Anwendungspipeline freigegeben wurde. Zentavault ist eine dApp mit hohem Durchsatz, die als hoch verschlüsselter und verteilter Speicherdienst konzipiert ist. Dieser Dienst wird auf der Zentachain-Plattform gehostet. Die dApps von ZentaChain werden niemals auf zentralisierte Systeme angewiesen sein und werden absolut keine Backup-Datenbanken für die Metadaten der Benutzer haben. Auf diese Weise wird Zentavault den Datenschutz, die Anonymität und die kommerzielle Leistung auf einem hohen Niveau halten.

Zentavault erhebt keine monatliche Nutzungsgebühr, sondern nur eine geringe Transaktionsgebühr für das Herunterladen von Daten. Zentavault ist ein Werkzeug zur Verschlüsselung und Dateiverteilung. Die Benutzer haben die volle Kontrolle über Verschlüsselung, Speicherung und gemeinsame Nutzung von Inhalten in der von ihnen gewählten Art und Weise. Mit Zentavault können Sie sicherstellen, dass Ihre Daten verschlüsselt und dauerhaft in das Interplanetare Dateisystem, auch IPFS genannt, eingebettet sind. Hierbei handelt es sich um ein kundenspezifisches Netzwerk, das es Ihnen ermöglicht, Inhalte mit Hilfe einer assoziativen Speicherstrategie zu integrieren und gemeinsam zu nutzen. Wenn sich Inhalte auf dem IPFS befinden, wird ihnen eine eindeutige Kennung zugewiesen, die als kryptografischer Hash oder Id-Hash bezeichnet wird. Dies kann verwendet werden, um die Daten des Benutzers ausfindig zu machen oder sie zwischen zwei Parteien auszutauschen. Sobald sich Ihr Inhalt auf dem IPFS befindet, wird der Datei ein Id-Hash zugewiesen, der verwendet werden kann, um den Inhalt zu finden oder mit anderen zu teilen. Durch die Verwendung von Peer-to-Peer-Hypermedia-Protokolltechnologien wie IPFS ist Zentavault in der Lage, einen schnelleren, sichereren und leichter zugänglichen Dienst zur Speicherung und Übertragung von Dateien anzubieten.

IPFS (InterPlanetary File System)

Das moderne Internet, obwohl eine der führenden Technologien unserer Zeit, hat seit seiner Entstehung in den 1990er Jahren seine Grenzen gezeigt. Im Zuge des technologischen Fortschritts müssen immer mehr Technologien aufgerüstet oder sogar völlig neu konzipiert werden. Dies ist der Fall beim HTTP-Protokoll.

In letzter Zeit haben wir eine erhöhte Nachfrage nach Lösungen für Fragen des Datenschutzes, der Sicherheit und der Geschwindigkeit festgestellt - Bereiche, in denen HTTP sich sozusagen nicht als "up to speed" erwiesen hat. Glücklicherweise wurde das IPFS als eine Idee vorgestellt, die Lösungen für diese Probleme bietet.

Wie funktioniert das?

Wir können es in den Begriffen eines BitTorrent-Schwarms betrachten, aber mit der Fähigkeit, Dateiversionen über die Zeit zu speichern und zu verfolgen. Im Gegensatz zu HTTP, bei dem die Ressourcen über standortbasierte IP-Adressen abgebildet werden, verwendet IPFS ein inhaltsadressiertes System. Dieses dezentralisierte System speichert Dateien über Peers hinweg und ermöglicht den Zugriff auf sie über einen kryptographischen Hash auf eine Datei, die als Adresse verwendet wird. Das bedeutet, dass der Benutzer gleichzeitig zum Client und zum Host wird.

Dies wird durch die Merkle DAG (Directed Acyclic Graphs)-Datenarchitektur ermöglicht und gewährleistet Unveränderbarkeit und Inhaltsversionierung auf IPFS. Aufgrund ihrer ähnlichen Strukturen eignen sich IPFS perfekt für die Blockkettenintegration. Es geht jedoch noch etwas weiter, indem es das leidige Problem der Datenspeicherung von Blockchain löst und zusammen mit Blockchain eine Lösung für die Speicherung, Verschlüsselung und gemeinsame Nutzung großer Daten und Dateien schafft. Obwohl das IPFS noch in den Kinderschuhen steckt, verfügt es über alle Werkzeuge, um der Nachfolger von HTTP zu werden und eine neue Ära des weltweiten Wir einzuleitenb

IPFS-Identitäten

Knoten werden durch eine NodeId identifiziert, dem kryptografischen Hash3 eines öffentlichen Schlüssels, der mit S/Kademlias statischem Kryptopuzzle erstellt wurde. Die Knoten speichern ihre öffentlichen und privaten Schlüssel (verschlüsselt mit einer Passphrase). Es steht den Benutzern frei, bei jedem Start eine "neue" Knoten-ID zu initiieren, wobei sie jedoch einige der erworbenen Netzwerkvorteile verlieren; es wird empfohlen, dass die Knoten gleich bleiben.

IPFS-Netzwerk

IPFS-Knotenpunkte kommunizieren regelmäßig mit Hunderten von anderen Knotenpunkten im Netzwerk über das breite Internet. Die Merkmale des IPFS-Netzwerkstapels:

- Verkehr: IPFS kann jedes Transportprotokoll verwenden und eignet sich am besten für WebRTC-Datenkanäle (für Browser-Konnektivität) oder uTP(LEDBAT).
- Zuverlässigkeit: IPFS kann Zuverlässigkeit bieten, wenn die zugrundeliegenden Netzwerke dies nicht bieten, indem uTP (LEDBAT) oder SCTP verwendet wird.
- Konnektivität: IPFS verwendet auch ICE NAT-Traversal-Techniken.
- Integrität: prüft optional die Integrität von Nachrichten unter Verwendung einer Hash-Prüfsumme.
- Authentizität: prüft optional die Authentizität von Nachrichten unter Verwendung von HMAC mit dem öffentlichen Schlüssel des Absenders.

IPFS-Routing

Für das Routing verwendet der IPFS verteilte Hash-Tabellen auf der Basis von S/Kademlia und Coral. Sein Zweck ist es, ::

1. Daten ankündigen, die zu den Knoten hinzugefügt werden

2. Lokalisieren der von bestimmten Knoten angeforderten Daten

Daten mit einer Größe von weniger als 1 KB werden direkt auf dem DHT gespeichert. Für Daten, die größer als 1 KB sind, speichert das DHT Referenzen, die die NoodeIds der Peers sind, die den Block bedienen können.

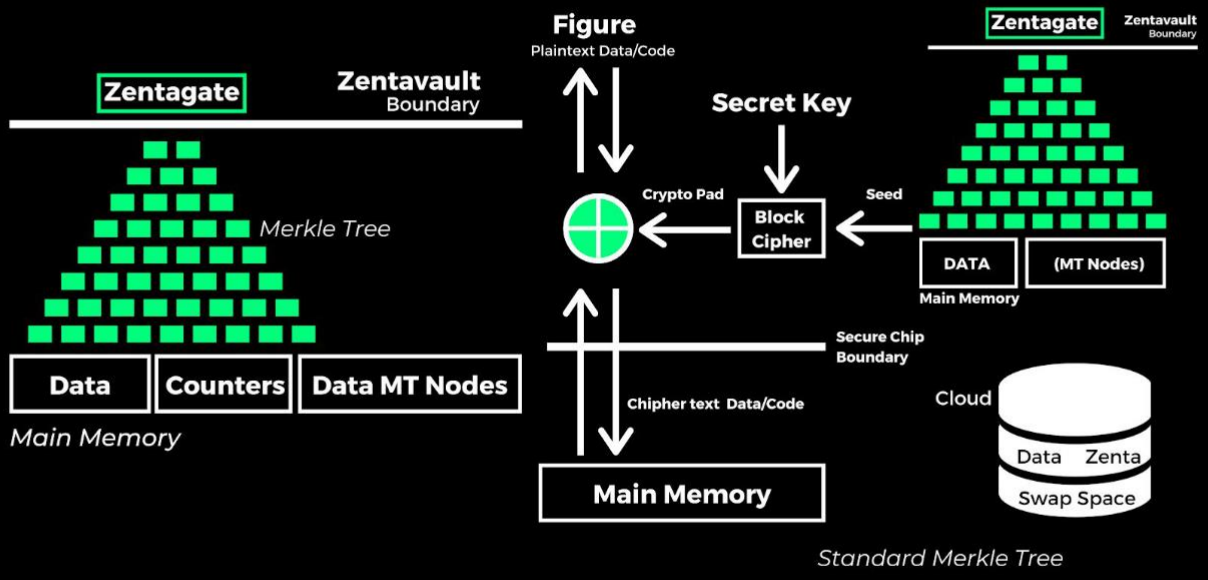
Objekte Merkle DAG

Merkle DAG (Merkle Directed Acyclic Graph) wird verwendet, um die Reihenfolge der Objektdateien im InterPlanetary File System beizubehalten. Mit Merkle DAG können Dateien durch ihren einzigartigen kryptographischen Hash, der als HashId bezeichnet wird, miteinander verknüpft werden. Die HashId (Objekt) umfasst alle HashId-Objektverknüpfungen. Merkle DAG verleiht IPFS nützliche Eigenschaften wie:

- Schutz des Inhalts: Merkle DAG versichert die Sicherheit, den Schutz und die Integrität aller Inhalte auf dem IPFS Wenn ein Objekt, das auf dem IPFS gespeichert oder gehostet wird, manipuliert oder anderweitig beschädigt wurde, ändert Merkle DAG automatisch den Root-Hash. Dies zeigt die an der Datei vorgenommenen Änderungen an.
- Anti-Duplikation aus Effizienzgründen (Es werden nicht dieselben Daten doppelt gespeichert): Alle Objekte, die Inhalte auf IPFS enthalten, werden durchsortiert, duplizierte Objekte werden erkannt und dann gelöscht. Dadurch wird sichergestellt, dass Inhalte nicht mehrfach auf dem IPFS gespeichert werden.

- Adressierung von Inhalten: Alle Inhalte können durch Identifizierung der eindeutigen HashId oder Multi-Hash einschließlich Links lokalisiert werden.

19. ZENTAGATE



Verwendung der adressunabhängigen Seed-Verschlüsselung

Der Zweck der Speicherverschlüsselung besteht darin, sicherzustellen, dass alle Daten und Codes, die außerhalb der Grenzen des sicheren Prozessors gespeichert werden, in einer unverständlichen Form vorliegen, die nichts über die tatsächlich gespeicherten Werte verrät. Die Abbildung veranschaulicht, wie dies bei der Verschlüsselung im Gegenmodus erreicht wird. Wenn ein Block in den Speicher zurückgeschrieben wird, wird ein Seed mit einer Blockchiffre (z.B. AES) und einem geheimen Schlüssel, der nur dem Prozessor bekannt ist, verschlüsselt.

Die verschlüsselte Sequenz wird als "kryptographischer Block" bezeichnet, und dieser Block wird durch eine XOR-Operation auf Bit-Ebene mit dem Klartextblock kombiniert, um den Chiffretext des Blocks zu erzeugen, bevor er in den Speicher geschrieben werden kann. In ähnlicher Weise wird bei der Extraktion eines Blocks von Chiffriertext aus dem Speicher derselbe Seed verschlüsselt, um denselben Block zu erzeugen, der zur Verschlüsselung des Blocks verwendet wurde. Wenn der Block auf dem Chip ankommt, wird der Block durch eine weitere bitweise XOR-Verknüpfung mit dem Block wieder in seine ursprüngliche Klartextform gebracht. Mathematisch gesehen, wenn P der Klartext, C der Chiffretext, E die Blockchiffrierfunktion und K der geheime Schlüssel ist, führt die Chiffre C = P EK(Seed) aus. Indem auf beiden Seiten ein XOR mit EK(Seed) gebildet wird, ergibt die Entschlüsselung den Klartext P = C EK(Seed)).

IPFS-Dateien

IPFS definiert auch einen Satz von Objekten zur Modellierung eines versionierten Dateisystems auf der Merkle DAG. Dieses Objektmodell ist ähnlich wie das von Git:

1. lock: ein Datenblock variabler Größe.
2. list: eine Sammlung von Blöcken oder andere List.
3. tree: eine Sammlung von Blöcken, List oder tree.
4. commit: eine Momentaufnahme in der Versionsgeschichte eines tree.

Warum brauchen wir IPFS?

- **Bandbreite**

Es kann Nachteile haben, nur von einer zentralen Stelle aus auf Daten zugreifen zu können. Stellen Sie sich vor, Sie möchten eine Akte mit einem Raum voller Menschen teilen. Sie würden diese Datei dann auf einen zentralen Server hochladen, der wahrscheinlich weit von Ihnen entfernt ist (das Rückgrat des Internets) und auf dem Weg dorthin auf mehrere Server umgeleitet wird. Andere Personen würden dann auf diese Datei zugreifen, indem sie sich erneut mit diesem entfernten Server verbinden und die Datei abrufen.

Insbesondere bei großen Dateien wie Fotos und Videos kann dies dazu führen, dass eine große Menge an Bandbreite verwendet wird, um diese Datei mit einem Raum voller Menschen zu teilen, die wahrscheinlich alle an dasselbe lokale Netzwerk angeschlossen sind wie Sie. Mit IPFS kann diese Datei von allen Rechnern im Raum, die über die Datei verfügen, direkt über das lokale Netzwerk bedient werden und benötigt daher viel weniger Bandbreite, da der Umweg über den zentralen Server entfällt. Dies wird besonders wichtig, wenn man die Kosten der Verbindungsgeschwindigkeit berücksichtigt, die viel langsamer sinken als die Kosten der Speicherung. Wenn sich dieser Trend fortsetzt, werden die Benutzer in der Lage sein, viel mehr Daten zu speichern und damit ihre Netzwerknutzung zu erhöhen. Da sich die Bandbreite jedoch nicht im gleichen Maße verbessert, wird die Verbindungsgeschwindigkeit anscheinend immer langsamer und langsamer. Auch die Sicherheit nimmt zu - DDoS-Angriffe zum Beispiel würden nicht funktionieren, weil sie auf den Angriff auf ein zentrales Verteilungssystem angewiesen sind, über das der IPFS nicht verfügt. Geschwindigkeit ist ein weiterer

Faktor, der immer mehr zunimmt. In einem verteilten Netzwerk fragt jeder Knotenpunkt, der nach etwas fragt, an dem ihm am nächsten gelegenen Knotenpunkt danach, und nicht an einem einzigen zentralen Ort.

- **Latenzzeit**

Ein damit zusammenhängendes Problem ist die Latenz. Da die Lichtgeschwindigkeit konstant ist und nicht verändert werden kann, besteht die einzige Möglichkeit, die Latenz zu verringern, darin, die Daten von einem Punkt aus zu bedienen, der näher am Benutzer liegt. Aus diesem Grund haben die großen Anbieter von Cloud-Diensten jetzt damit begonnen, Speicherorte nach Regionen anzubieten. IPFS versucht, die Entfernung zu dem Computer, der die angeforderten Daten bereitstellt, wenn möglich zu verringern.

- **Offline sein**

Viele der Dienste, die wir tagtäglich in Anspruch nehmen, stützen sich ausschließlich auf die Arbeiten, die wir online erledigen. Wenn Sie gemeinsam mit anderen Personen im gleichen Raum an einem Dokument arbeiten oder Daten von Ihrem Telefon auf Ihren Laptop übertragen wollen, können Sie dies meist nur tun, wenn Sie mit den zentralen Servern des Backbones des Internets verbunden sind. Wenn es Bandbreiten- oder Infrastrukturprobleme wie Überlastung, ISP-Ausfall oder Rechenzentrumsprobleme gibt, können Sie diese Dienste nicht mehr nutzen. IPFS hofft, dies zu ändern, indem es Ihnen erlaubt, sich direkt mit anderen Peers zu verbinden, ohne dass Sie sich mit diesen zentralen Servern verbinden müssen.

- **Zensur**

Der Zugang zu Daten oder Dienstleistungen kann viel einfacher zensiert oder eingeschränkt werden, wenn alles auf zentralen Servern gespeichert ist und auf diesen läuft, als in einem P2P-Netzwerk. Ein Beispiel dafür ist die Tatsache, dass die ägyptische Regierung während des arabischen Frühlings 2011 jeglichen Zugang zum Internet unterbrach, um die Organisation der Protestierenden zu verhindern und die Kommunikation zwischen ihnen einzuschränken. Durch die Anbindung von P2P hofft das IPFS, diese Form der Zensur unmöglich zu machen.

- **Dauerhaftigkeit**

Jeder ist schon einmal auf einen Fehler 404 gestoßen. Dies bedeutet, dass der benötigte Inhalt nicht gefunden werden konnte, weil er gelöscht oder verschoben wurde. Dies kann ein großes Problem darstellen, wenn Sie auf diesen Inhalt verlinken möchten, z.B. weil er für den Inhalt, den Sie bereitstellen, unerlässlich ist. Im Allgemeinen wäre es für die Gesellschaft von Vorteil, wenn das meiste Wissen, das sich im Web angesammelt hat, zugänglich bliebe und nicht gelöscht würde, weil jemand absichtlich oder versehentlich einige Websites geschlossen hat. Mit dem IPFS sind Sie in der Lage, eine Version des verlinkten Inhalts selbst zu speichern und zu hosten, und auf diese Weise wird sichergestellt, dass dieser Inhalt den Benutzern immer zur Verfügung steht, auch wenn die ursprünglichen Hosts ihn nicht mehr hosten. Die Idee besteht darin, ein dauerhaftes Netzwerk zu schaffen, in dem kein Inhalt verloren geht, weil alle Inhalte von vielen Leuten gehostet werden.

- **Sicherheit**

Wie die zahlreichen Hacks in den letzten Jahren gezeigt haben, reicht es nicht aus, nur an die Sicherheit in der Kommunikation zwischen Servern und Clients zu denken. IPFS zielt darauf ab, die Daten selbst durch verbesserte Methoden der Authentifizierung und Verschlüsselung zu schützen.

- **Selbst-zertifizierte Dateisysteme - SFS**

Kein sicheres Netzwerk-Dateisystem hat sich jemals über das Internet ausgebreitet. Allen bestehenden Systemen fehlt ein adäquates Schlüsselmanagement für Sicherheit im globalen Maßstab. Angesichts der Vielfalt des Internets wird ein bestimmter Mechanismus, den ein Dateisystem zur Verwaltung von Schlüsseln einsetzt, viele Arten der Nutzung nicht unterstützen. Wir schlagen vor, die Schlüsselverwaltung von der Sicherheit des Dateisystems zu trennen und der Welt ein einziges globales Dateisystem zur Verfügung zu stellen, unabhängig davon, wie einzelne Personen Schlüssel verwalten. Wir stellen SFS vor, ein sicheres Dateisystem, das die interne Schlüsselverwaltung vermeidet. WÃ?hrend andere Dateisysteme eine SchlÃ?sselverwaltung benÃ¶tigen, um Dateinamen VerschlÃ?sselungsschlÃ?sseln zuzuordnen, enthalten SFS-Dateinamen effektiv Ã¶ffentliche SchlÃ?ssel, was sie zu selbstzertifizierenden Pfadnamen macht. Die Schlüsselverwaltung in SFS erfolgt außerhalb des

Dateisystems, unabhängig davon, welches Verfahren die Benutzer zur Generierung von Dateinamen wählen. Das selbstzertifizierende Dateisystem (SFS) befasst sich mit dem Problem der Schlüsselverwaltung in kryptographischen Dateisystemen und schlägt vor, die Schlüsselverwaltung von der Sicherheit des Dateisystems zu trennen.

Server haben einen öffentlichen Schlüssel, und Clients verwenden den öffentlichen Schlüssel des Servers, um den Server zu authentifizieren und einen sicheren Kommunikationskanal aufzubauen. Damit Clients Server an Ort und Stelle authentifizieren können, ohne vorher von ihnen gehört zu haben, führt SFS das Konzept eines "selbstzertifizierenden Pfadnamens" ein."

Ein selbstzertifizierender Pfadname enthält den Hash des öffentlichen Schlüssels des Servers, so dass der Client überprüfen kann, ob er tatsächlich mit dem legitimen Server spricht. Sobald der Client den Server verifiziert hat, wird ein sicherer Kanal eingerichtet und der eigentliche Dateizugriff erfolgt. Der Zugriff auf entfernte SFS-Dateisysteme erfolgt über den Einhängepunkt /sfs. Ein SFS-Pfadname gehorcht der folgenden Syntax: /sfs/ location:hostid/real/pathname, wobei ``` location" der Name (IP-Adresse oder DNS-Name) des Servers ist, der das Dateisystem exportiert, und ``` hostid" der Hash einer Zeichenkette ist, die den öffentlichen Schlüssel des Servers und einige andere Informationen enthält. SFS kümmert sich nicht darum, wie der Pfadname vom Benutzer erhalten wurde; ein Benutzer kann schließlich unter Verwendung einer vorhandenen PKI (Public Key Infrastructure) Host-ID's erhalten. Auf der anderen Seite müssen sich Benutzer, sobald sie einen selbstzertifizierenden Pfadnamen für die Dateien, an denen sie interessiert sind, erhalten haben, keinen Schlüssel mehr merken.

Dies wird verwendet, um das IPNS-Namensystem für IPFS zu implementieren. Es erlaubt uns, eine Adresse für ein entferntes Dateisystem zu generieren, wo der Benutzer die Gültigkeit der Adresse überprüfen kann. SFS führte eine Technik zum Aufbau selbst-zertifizierter Dateisysteme ein: die Adressierung entfernter Dateisysteme nach folgendem Schema:

/sfs/<Location>:<HostID>

Wo ist die Netzwerkadresse des Servers, und:

HostID = hash(public_key || Location)

So zertifiziert der Name eines SFS-Dateisystems seinen Server.

Es ist so konzipiert, dass es so funktioniert, wie es das Web bereits tut, wie Sie oben lesen können. Anstelle eines speziellen Links, den nur bestimmte Programme verstehen, oder einer Datei zum Herunterladen anderer Dateien, ist der IPFS so konzipiert, dass er mit allgemeinen Links arbeitet, die im Browser funktionieren, und Sie brauchen keine spezielle Software zu installieren. IPFS kann jede Netzwerkarchitektur verwenden, und jeder Dateityp kann als DAG verwendet werden. Diese Funktion wird IPLD (InterPlanetary Linked Data) genannt.

Zentachain geht davon aus, dass alles, was im Whitepaper steht, auf Zentachain-Wissen basiert und dass es niemandem erlaubt ist, Texte oder Bilder zu kopieren und zu manipulieren und dann falsche Informationen über Zentachain zu verbreiten. Zentachain erlaubt die Verbreitung nur in Form einer Originaldatei mit dem ursprünglichen Text, Bildern und Inhalt. Die Verantwortung für das Weißbuch liegt bei Zentachain.io. Als Zentachain behalten wir uns das Recht vor, das Zentachain Lab ständig zu aktualisieren, um mit den schnellen technologischen Veränderungen Schritt zu halten.

REFERENZEN

Adnan Abdul-Aziz Gutub, Farhan Abdul-Aziz Khan, Hybrid Crypto Hardware Utilizing Symmetric-Key & Public-Key Cryptosystems, 2012 International Conference on Advanced Computer Science.

Shankar Dhakar, Ravi & Kumar Gupta, Amit & Sharma, Prashant, Modified RSA Encryption Algorithm (MREA), 2012 2nd International Conference on Advanced Computing and Communication Technologies(ACCT), pp. 426-429, 2012.

Nishtha Mathur and Rajesh Bansode, AES Based Text Encryption Using 12 Rounds with Dynamic Key Selection, Procedia Computer Science 79, pp. 1036 – 1043, Elsevier, 2016.

Koorosh Goodarzi, Abbas Karimi, Cloud Computing Security by Integrating Classical Encryption, Procedia Computer Science 42, pp. 320 – 326, Elsevier, 2014.

Shilpi Gupta and Jaya Sharma, A Hybrid Encryption Algorithm based on RSA and Diffie-Hellman, 2012 International Conference on Computational Intelligence and Computing Research, IEEE, 2012.

R. Rizk, Y. Alkady, Two-phase hybrid cryptography algorithm for wireless sensor networks, Journal of Electrical Systems and Information Technology Vol 2, Issue 3, pp. 296-313, 2015.

Koorosh Goodarzi, Abbas Karimi, Cloud Computing Security by Integrating Classical Encryption, Procedia Computer Science 42, pp. 320 – 326, Elsevier, 2014.

M. Indra Sena Reddy and A.P. Siva Kumar, Secured Data Transmission Using Wavelet Based Steganography and Cryptography by Using AES Algorithm, Procedia Computer Science 85, pp. 62-69, Elsevier, 2016.

Wang Rui; Chen Ju; Duan Guangwen, 'A k-RSA algorithm,' Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on , vol., no., pp.21,24, 27-29 May 2011.

Liang Wang, Yonggui Zhang, A New Personal Information Protection Approach Based on RSA Cryptography, IEEE, 2011.

Christof Paar, Jan Pelzl, "Understanding Cryptography", SpringerVerlag Berlin Heidelberg, pp. 3-9, 30-31, 2010.

Assad Ibraheem Khyoon," Modification on the Algorithm of RSA Cryptography System" 2006.

Laiphrakpam Dolendro Singh and Khumanthem Manglem Singh, Implementation of Text Encryption using Elliptic Curve Cryptography, Procedia Computer Science 54, pp. 73-82, Elsevier, 2015.

Diffie: Whitfield Diffie and Martin Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, Nov 1976.

Vitalik Buterin. Ethereum 2.0 mauve paper. 2016

Polkadot:
https://polkadot.network/PolkaDotPaper.pdf

Cosmos:
https://cosmos.network/cosmos-whitepaper.pdf

ABCI:
https://github.com/tendermint/abci

Bitcoin:
https://bitcoin.org/bitcoin.pdf

BitShares:

https://bitshares.org/technology/delegated-proof-of-stake-consensus

Computer Networks:
https://digitalescobar.wpcomstaging.com/wp-content/uploads/2018/12/DigitalEscobar.com-Computer-Networks-A-Systems-Approach-by-Larry-L.-Peterson-Bruce-S.-Davie-.pdf

AES Encryption:
https://townsendsecurity.com/sites/default/files/AES_Introduction.pdf

Blake2:
https://blake2.net/

Hybrid Encryption Algorithm:
https://pdfs.semanticscholar.org/d518/9533fd596a5cbc39864d21a5ef4e0156359d.pdf

A hybrid encryption algorithm based on RSA and Diffie-Hellman:
https://ieeexplore.ieee.org/document/6510190

IPFS:
https://ipfs.io/ipfs/QmR7GSQM93Cx5eAg6a6yRzNde1FQv7uL6X1o4k7zrJa3LX/ipfs.draft3.pdf

A Review on Hybrid Encryption in Cloud Computing:

https://www.semanticscholar.org/paper/A-Review-on-Hybrid-Encryption-in-Cloud -Computing-Kumar-Badal/ad6ba7c05455b4b1416e19b52aa42ec050a5dd74

Ietf.org:
https://en.wikipedia.org/wiki/History_of_cryptography

Diffie–Hellman:

https://www.math.brown.edu/~jhs/MathCrypto/SampleSections.pdf

Crypho Security Whitepaper:
https://www.crypho.com/downloads/crypho_security_whitepaper.pdf

On the Security of ElGamal Based Encryption:

https://www.researchgate.net/publication/221010812_On_the_Security_of_ElGamal _Based_Encryption

Descriptions of SHA-256, SHA-384, and SHA-512:
http://www.iwar.org.uk/comsec/resources/cipher/sha256-384-512.pdf