CATENA
for a smarter blockchain

C_Chain – Frequently Asked Questions

C_Chain kann als Blockchain-Basistechnologie in beliebige Software eingebunden werden und bietet so eine flexible Einsetzbarkeit in verschiedensten Anwendungsfällen. Diese werden so leichter zu verwalten und nachhaltig abgesichert. Auf eher technischer Ebene zeichnet sich C_Chain durch eine übersichtliche und einzigartige Architektur aus. Im Folgenden soll auf die häufigsten Fragen zur Architektur des C_Chain Ökosystems eingegangen werden, um Zweifel aus dem Weg zu räumen und die Vorteile von C_Chain im Vergleich zu klassischen Blockchain-Lösungen herauszustellen.

Inhalt

CATENA
for a smarter blockchain

Zentralisierte Architektur

Entsteht durch die Zentralisierung des CCM ein „Single Point of Failure"?

Nein. Ketten können in C_Chain beliebig oft repliziert, also von verschiedenen Nutzern lokal gesichert werden. Auch wenn die Buchung einzelner Blöcke von einer zentralen Stelle aus durchgeführt wird, erfolgt die Überprüfung verteilt durch mehrere Agenten. Jeder Teilnehmer des Systems hat grundsätzlich jederzeit die Möglichkeit die Korrektheit einzelner Blöcke nachzuprüfen. Ein Datenverlust im Falle eines ausgefallenen CCM wird durch Backups sowie durch die Möglichkeit einer lokalen Replizierung von Blöcken und Ketten bei den Nutzern vermieden. Durch eine geplante, neue Speicherarchitektur, die eine globale Verteilung und Sicherung der Daten sicherstellt, kann Datenverlust nahezu komplett ausgeschlossen werden.

Erhält der CCM durch die Zentralisierung die absolute Datenhoheit und kann so Kontrolle über die Daten nach Belieben ausüben?

Nein. Die Daten sind jederzeit doppelt signiert, einmal vom Sender und vom CCM, was Betrugsversuche unmöglich macht. Inhalte einzelner Buchungen können Ende-Zu-Ende verschlüsselt werden. Das ist optional und bietet Nutzern eine weitere Möglichkeit, die volle Kontrolle über die Daten sicherzustellen. Durch die Nutzung der Verschlüsselung können nur noch betroffene Parteien auf die geschützten Daten zugreifen. Nicht mal der CCM kann also an Details der ausgetauschten Daten gelangen. Dadurch und durch die doppelten Signaturen hat der CCM keine Möglichkeit zu betrügen oder Daten zu fälschen.

C_Chain folgt dem Schema „Security by Design" und garantiert standardmäßig die absolute Sicherheit der Daten. Durch verschiedene Konfigurationsmöglichkeiten können Rechte vergeben und die Sichtbarkeit der einzelnen Ketten individuell eingestellt werden.

Die Datenhoheit wird durch die Umsetzung der DSGVO-Konformität in einem späteren Update garantiert (siehe DSGVO Konzept).

Verursacht die Zentralisierung des CCM nicht einen großen, auf den CCM fokussierten Angriffsvektor und damit ein hohes Risiko?

Nein. Um die Integrität der Daten zu brechen, müssten die verwendeten Schlüssel erlangt werden. Die Schlüssel des CCM sind im Microsoft Key-Vault gesichert und die Datensicherheit wird durch Microsoft auf Basis von TPM garantiert. Verschiedene Key-

Rotationen reduzieren außerdem die Angreifbarkeit. So existiert beispielsweise kein „Masterkey“, der das gesamte System zu Fall bringen könnte. Auf Ebene der Ketten und der einzelnen Blöcke werden zusätzliche Sicherheitsmaßnahmen umgesetzt. Wie bei anderen Blockchain-Lösungen auch, hält sich C_Chain hierbei an die gängigen Standards.

Würde ein Ausfallen des CCM, zum Beispiel durch außer Betrieb nehmen des zugehörigen Servers, das gesamte System lahmgelegen?

Nein. Der CCM läuft in Kubernetes Clustern verteilt auf mehreren Rechenzentren und besteht damit bereits aus vielen Servern und nicht nur einem einzigen. Diese Cluster werden in Microsoft Azure betrieben und können optional gleichzeitig auch zusätzlich bei anderen Cloud-Anbietern gehostet werden. Um die Sicherheit der Daten zusätzlich zu gewährleisten, sollen diese in Zukunft global repliziert und gesichert werden.
Noch ist das System nicht live. Sobald es live geschaltet wird, erfolgt zunächst der Einsatz der Kubernetes Cluster, danach wird ein Modell zur globalen Replizierung der Daten umgesetzt.

Verwendung mehrerer paralleler Ketten

Sind die verschiedene Ketten zur zusätzlichen Absicherung miteinander verknüpft?

Nein. Das würde dem Kerngedanken der C_Chain aus verschiedenen Gründen widersprechen. Eine Verknüpfung der Ketten würde die Performanz deutlich verschlechtern und die Anfälligkeit des ganzen Systems erhöhen (siehe nächster Punkt). Einer der Kernargumente für C_Chain und gegen klassische Blockchains ist die Möglichkeit beliebig viele Ketten in Abhängig von den Anforderungen einer Anwendung einsetzen zu können. Das steigert nicht nur die Performanz und Effizienz des Systems, sondern garantiert auch eine perfekte Skalierbarkeit.

Wie wird die Datenintegrität sichergestellt, obwohl nicht alle Daten in einer zentralen Kette kryptografisch miteinander verknüpft ist?

Alle Regeln bezüglich der Sicherheit und Integrität, die für Ketten in beliebigen Blockchain-Lösungen mit einer einzigen Kette gelten, gelten auch für ein System aus mehreren Ketten. Ein Vorteil mehrerer Ketten ist, dass im unwahrscheinlichen Fall, einer Kompromittierung einzelner Ketten, niemals das gesamte System betroffen ist.
Es gibt auch klassische Blockchains, wie zum Beispiel Ethereum, die mehrere Ketten verwenden. Seit einem Angriff unbekannter Hacker im Jahr 2016, die es schafften

mehrere Millionen Dollar in Form von Token zu stehlen, spaltete Ethereum die bis dahin einzige Kette in zwei auf (Ethereum – DAO Event).

Was passiert, wenn eine Kette im System gelöscht werden soll?

Da das Löschen von Ketten den allgemeinen Blockchain-prinzipien widerspricht, gibt es bei C_Chain bisher keine Möglichkeit, dies zu tun. Eine Löschungsstrategie zum Zwecke der DSGVO-Konformität wird aber bereits erarbeitet und folgt in einem späteren Update (siehe DSGVO Konzept).

Sonstige Fragen

Ist C_Chain nur eine verschlüsselte Datenbank?

Nein. Wie weiter oben bei den Fragen zur Zentralisierung und der Nutzung von Kettenstrukturen in der Buchung des Systems zu sehen ist, handelt es sich bei C_Chain um eine Blockchain-Lösung und nicht um eine klassische Datenbank. Eine Datenbank kann durch Administratoren beliebig manipuliert werden. Bei C_Chain ist durch Anwendung der sogenannten Immutability-Eigenschaft sichergestellt, dass Daten nicht im Nachhinein verändert werden können.

Warum verwendet C_Chain zur Identifizierung eine CryptID anstelle einfacher Public-Keys?

Die CryptID enthält als zusätzliche Sicherheitsmaßnahme noch die Signatur des Public-Keys durch den Besitzer des Schlüsselpaares mit dem zugehörigen Private-Key. Dadurch wird gewährleistet, dass es sich um einen validen Schlüssel handelt, zu dem ein tatsächlicher Nutzer existiert. Es handelt sich hierbei um eine Art selbstsigniertes Zertifikat, das in späteren Versionen durch ein qualifiziertes Zertifikat ersetzt wird.

Was sind die Vorteile von C_Chain?

C_Chain besticht im Vergleich zu anderen Blockchain-Lösungen durch seine Schnelligkeit, Effizienz und beliebige Skalierbarkeit. Durch seine effiziente Arbeitsweise und einen geringen Bedarf an Rechenleistung, und damit Strom, sind die Kosten für den Betrieb sehr niedrig. C_Chain sorgt außerdem durch seine leichte Infrastruktur für eine einfache Einsetzbarkeit bei verschiedensten Anwendungsfällen. Im Software Development Kit von C_Chain sind Libraries für alle allgemeinen Aufgaben wie Verschlüsselung, Signaturen, etc. enthalten, so dass sich Entwickler voll auf die Anwendung konzentrieren und diese in sehr kurzer Zeit umsetzen können.

Was passiert, wenn der Schlüssel des CCM kompromittiert werden würde?

Sollte der unwahrscheinliche Fall eintreten und der Schlüssel des CCM kompromittiert werden, wird dieser sofort entwertet. Der CCM erzeugt dann einen neuen Schlüssel mit welchem alle Blöcke, die noch auf dem kompromittierten Schlüssel basieren, neu signiert werden. Das alte Schlüsselpaar wird in keinem Zusammenhang mehr verwendet und Signaturen mit diesem Schlüssel werden nicht mehr akzeptiert.