C-chain Highlights

Prof. Rudolf Bayer, TU München, Januar 2020

Zusammenfassung

Dieses Papier ist eine Zusammenfassung der wichtigsten Eigenschaften von C-chain auf sehr allgemeiner Ebene. Details der involvierten Kryptografie und Formeln sind ausgespart, sie sind in [2] genau beschrieben. C-chain löst ein ähnliche Probleme wie Blockchain Varianten, nämlich die Führung eines öffentlichen Hauptbuches (public ledger) für die sichere und unverfälschbare Buchung von Transaktionen, die einen Geschäftsprozess ausmachen, ist aber wesentlich effizienter, sicherer, einfacher und sehr leicht zu installieren und zu benutzen.

Öffentliche Schlüsselpaare (public key pairs)

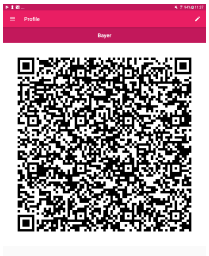
C-chain stützt sich sehr stark auf Kryptografie und relationale Datenbanken ab. Deshalb hat jeder Nutzer ein Schlüsselpaar **[π, σ]** bestehend aus dem öffentlichen Schlüssel π und dem privaten, geheimen **σ. π** dient als digitale Identität eines Nutzers U und gleichzeitig zum Verschlüsseln geheimer Nachrichten an einen Empfänger V. σ dient zur Leistung digitaler Unterschriften mit kryptografischer Absicherung.

cryptID

Sie besteht aus π und einer digitalen Signatur für **π** mit Hilfe von σ. So wird sichergestellt, dass π nicht irgendeine Zahl ist, sondern der erste Teil eines Schlüsselpaares, das einem (unbekannten) Nutzer O gehört. π ist vergleichbar mit einer E-Mail Adresse E. E braucht aber gar nicht zu existieren oder gehört gar nicht dem Nutzer, der sie eingibt. E muss deshalb in vielen Anwendungen erst durch eine sog. Zweifaktor Methode verifiziert werden. Eine cryptID dagegen ist immer kryptografisch abgesichert und gehört garantiert dem Nutzer O. Aber O braucht seine cryptID nicht zu merken oder jemals einzugeben. Die cryptID ist vergleichbar mit einer digitalen DNA, die von dem (unbekannten) Nutzer O stammt. Wie die DNA ist die cryptID kein Geheimnis, sondern steht in der öffentlichen Datenbank UDB (User Data Base).

Login und Passwort (PWD)

Beide entfallen bei C-chain für den Nutzer ersatzlos. Herkömmliche login Verfahren benutzen einen login Namen sowie ein geheimes PWD. Bei C-chain dient als login Name die per SW erzeugte cryptID. Als Ersatz für das PWD dient eine zufällige Zahl r, die mit σ signiert ist. Der Nutzer braucht sich nichts zu merken oder einzugeben. So sieht meine cryptID (ohneSignatur) aus:



Auf diese Weise wird in C-chain jedes konventionelle und meinst mühsame login Verfahren vollständig ersetzt. Die Client-SW auf einem Smartphone oder sonstigen Rechner macht das login sofort beim Einschalten automatisch, ohne dass der Nutzer davon etwas bemerkt.

Infrastruktur

C-chain benötigt zum login keine Infrastruktur mehr, keine chip Karte, kein Lesegerät, keinen chip/TAN Generator und keine Nutzer Eingaben, alles wird durch die Client SW durch dieses kryptografisch absolut sichere Verfahren ersetzt, das wesentlich bequemer und sogar wesentlich sicherer ist als herkömmliche Verfahren.

Universelle Kryptografische Sicherung

ALLE Verfahren und Objekte in C-chain sind grundsätzlich kryptografisch abgesichert, sie können so weder verstümmelt noch verfälscht oder verleugnet werden, da sie öffentlich sichtbar sind und von vielen Nutzern kopiert und verifiziert werden können (auch als *public ledger* bekannt). Auch alle in Datenbanken gespeicherten Objekte sind kryptografisch abgesichert. Bei jedem Versuch, ein signiertes Objekt zu manipulieren oder zu ändern zerplatzt es wie bei einer Seifenblase.

Transaktionen

Sie sind digitale Verträge zwischen zwei Nutzern U und V und haben die einfache Struktur T = [U, V, p]. U ist der Urheber von T, der Empfänger ist V und p ist die Payload einer Transaktion und beschreibt den Inhalt des digitalen Vertrages, im einfachsten Fall ein Text. p kann aber auch beliebig strukturiert sein. In der technischen Umsetzung von T stehen U und V für ihre cryptIDs. p kann öffentlich oder geheim sein, ist aber auf jeden Fall vom Urheber U digital unterschrieben (signiert) und somit absolut sicher und kann von niemandem mehr manipuliert werden. Digitale Signaturen sind grundsätzlich unwiderrufbar, unveränderbar, und sogar unzerstörbar, da sie sofort beliebig oft im Netz kopiert werden können.

Transaktionsketten

Transaktionen, die zu einem Geschäftsprozess gehören, werden zu Ketten zusammen gefasst. Auch diese Ketten müssen sicher, also zuverlässig, unverfälschbar und unzerstörbar gebucht werden. Dieser Buchungsprozess ist das Kernstück von blockchain und C-chain. Bei blockchain erfolgt die Absicherung der Buchungen durch den sog. PoW (Proof of Work), das sind extrem aufwendige und verschwenderische Rechenprozesse, die nur durch hochspezialisierte Superrechner erbracht werden können, siehe [3], [4]. Bei C-chain werden die Buchungen durch kryptografische Verfahren von dem C-Chain Manager (CCM) System technisch umgesetzt und abgesichert. Dadurch ist C-chain im Gegensatz zu blockchain hocheffizient, perfekt skalierbar und zudem wesentlich sicherer und einfacher zu benutzen. Da gebuchte Transaktionen grundsätzlich erst durch U und dann durch den CCM selbst signiert sind, können sie auch nicht mehr verändert werden, weder durch U noch durch en CCM oder gar durch Dritte. Die Buchung im CCM garantiert sofortiges ***final settlement*** einer Business Transaktion. Dieses final settlement ist für viele besonders interessante Anwendungen (z.B. IoT) unerlässlich, fehlt aber bei fast allen konventionellen Blockchain Varianten, die Transaktionen nur mit einer gewissen Wahrscheinlichkeit, aber nicht endgültig buchen können. Erstaunlicherweise wird dieses Defizit fast immer ausgeblendet.

Verteilte Transaktionsketten

Bei blockchain gibt es nur eine zentrale Kette, in der alle Transaktionen verbucht werden, obwohl zwischen den meisten Transaktionen gar keine Beziehung besteht. Diese Kette wird deshalb sehr groß (bei Bitcoin > 400 GB) und muss von allen Nutzern kopiert und lokal gespeichert werden. Deshalb wird oft behauptet, dass blockchain eine verteilte Datenbank sei, was nur für die Lesbarkeit stimmt, für den Buchungsprozess ist das falsch.

Bei C-chain dagegen werden die Transaktionen nach sinngemäß zusammengehörigen Ketten zusammengefasst und verwaltet. Eine Kette ist nur für die daran beteiligten Agenten interessant und wird meistens auch nur von ihnen lokal repliziert und auf ihrem Smartphone oder Computer sogar mehrfach gespeichert. Dadurch bleiben diese Ketten sehr klein, in praktischen Anwendungen nur wenige MB pro Jahr. Sie werden bei einer in der CCM neu gespeicherten Transaktion sofort mit den beteiligten Agenten und ihren devices synchronisiert.

Durch diese Replizierung und sofortige Verteilung der Transaktions Ketten bei mindestens 3 unabhängigen Agenten (U, V, CCM) - optional sogar bei beliebig vielen weiteren - sind die gebuchten Transaktionen absolut sicher und außerdem sofort *finally settled*, ein enormer Vorteil gegenüber blockchain. Außerdem würde jede Fehlfunktion sofort entdeckt, da die Synchronisation zwischen den Agenten automatisch im Rahmen einer Buchung in weniger als 1 Sekunde erfolgt.

Ein typisches Beispiel sind Wartungsketten von PKWs: In Deutschland gibt es ca 50 Mio zugelassene PKWs. Es macht absolut keinen Sinn, sämtliche Wartungsvorgänge für alle PKWs in einer einzigen riesigen Blockchain zu buchen. Im Gegensatz dazu verwendet eine C-chain Lösung dieses Problems genau eine Transaktionskette pro PKW, also 50 Mio individuelle Ketten, und skaliert dadurch sogar perfekt.

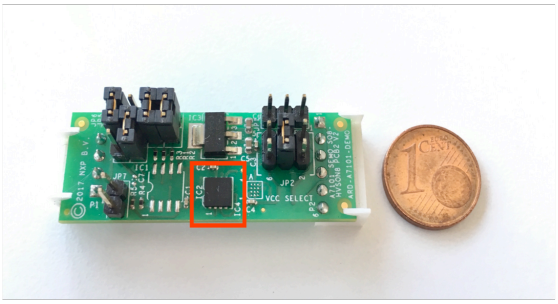
Identität und Authentizität

Diese beiden Begriffe werden in der IT oft völlig falsch verwendet. Die cryptID ist die eindeutige und unverfälschbare Identität eines Nutzers. Die Authentizität ist derjenige Nutzer, zu dem diese Identität gehört, und ist viel schwerer festzustellen und zu beweisen. Ein Haar, das an einem Tatort gefunden wird, determiniert den zu diesem Haar gehörigen Menschen eindeutig, das ist schnell erledigt. Die Feststellung der Authentizität dieses Menschen nimmt aber den gesamten restlichen Krimi in Anspruch. In der IT wird Authentizität durch verschiedene Verfahren angestrebt, eine Authentifizierung ist aber nie ein Beweis, sondern immer nur eine Behauptung über die Identität, z.B. den Besitzer einer gültigen E-Mail Adresse. Selbst die üblichen Zertifikate stellen sich bei genauer Betrachtung nur als simple und oft völlig wertlose Behauptungen heraus. Bei C-chain, genauer in der UDB, erfolgt die Authentifizierung überwiegend durch ein Video Selfie des Nutzers, in dem er einen Teil seines eigenen öffentlichen Schlüssels vorliest. Ein solches Video ist als Nachweis der Authentizität viel sicherer als jedes Zertifikat.

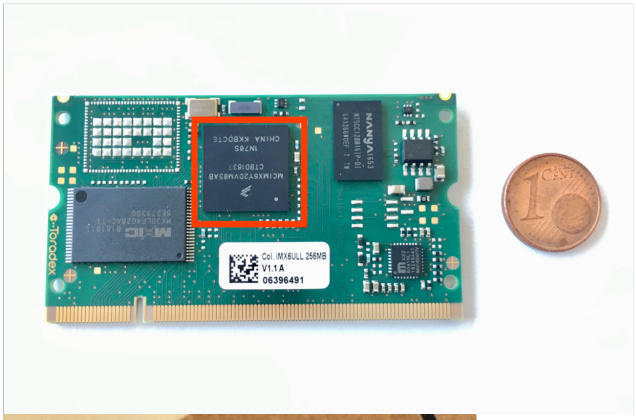
Darüber hinaus ist Authentifizierung natürlich auch über klassische Zertifikate oder persönliches Treffen oder über unabhängige Kommunikationskanäle wie Telefon und PIN Briefe möglich.

C-chain für IoT

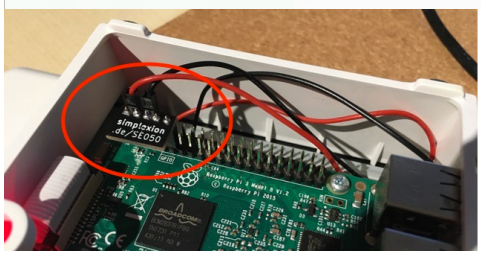
Aufgrund seiner schlanken Infrastruktur konnte das gesamte C-chain System einschließlich des CCM auf Edge Rechner und sogar auf Mikrokontroller portiert werden. Dabei verwendet diese C-chain Lösung sogar Hardware Sicherheits Module (HSM) als kryptografische Koprozessoren, um extrem hohe Performanz und gesteigerte Sicherheit zu erreichen.



A71CH or SE050 of NXP on Board: Coprocessor for RSA and ECC Cryptography



iMX6ULL on Board: System on Module Computer with Linux etc.



HSM SE050 in red circle on a Raspberry Pi

Dadurch ermöglicht C-Chain völlig neue Anwendungen für die Blockchain Technologie vor allem im zukünftigen Marksegment IoT, denn hier werden hocheffiziente Lösungen mit sehr hohen Transaktionsraten gefordert.

Referenzen, auf https://db.in.tum.de/research/projects/C-chain/?lang=en

1. https://blockchain.info
2. R. Bayer: C-chain
3. https://en.wikipedia.org/wiki/Satoshi_Nakamoto
4. http://www.euroforum.de/best-of-blockchain/#
5. Manifesto