MONTHLY SECURITY SUMMARY

)SCIP(

AUSGABE DEZEMBER 2022
FLIPPER ZERO UND BITCOIN LIGHTNING NETWORK

UMGANG MIT FLIPPER ZERO ALS TOOL

Flipper Zero wurde über eine Kickstarter Kampagne mit über 4.8 Millionen finanziert. Er unterstützt eine Vielzahl an drahtlosen Funkstandards und Protokollen, auf die wir in unserem Beitrag eingehen.

ZUKUNFT DES BITCOIN LIGHTNING NETWORK

Das Lightning-Netzwerk als Lösung des Trilemma-Problems Skalierbarkeit, Dezentralisierung und Sicherheit. Wir zeigen im Artikel, wie es aufgebaut ist und funktioniert.

Dezember 2022: Grüsse aus China

Im Rahmen unserer Tätigkeiten im *Cyber Threat Intelligence*-Bereich analysieren wir ein Mehr an Daten aus *China*. Unter anderem monitoren wir öffentliche Git-Repositories von chinesischen Software-Lösungen. Das Überwinden der sprachlichen und kulturellen Barrieren ist nicht einfach, vermag sich aber beständig als lohnenswert herauszustellen.

Dabei gibt es Eigenheiten, die man sich im Kontext der Schweiz von sich aus nicht vorstellen kann. Zum Beispiel fällt auf, dass Kommentare in Issues, Pull-Requests und Commits eher kurz angebunden, ja schon fast ruppig sind. Es scheint, als hätte man wenig oder gar keine Zeit für Formalitäten. In der Schweiz wäre man davon betüncht, würde es als Unhöflichkeit auslegen.

Ob es sich hier nun wirklich um eine kulturelle Eigenheit handelt. Oder ob halt einfach die Nuancen im Rahmen der Übersetzung verloren gegangen sind, lässt sich nicht immer mit Bestimmtheit sagen. Für die Open-Source-Community in China scheint das jedenfalls so zu funktionieren.

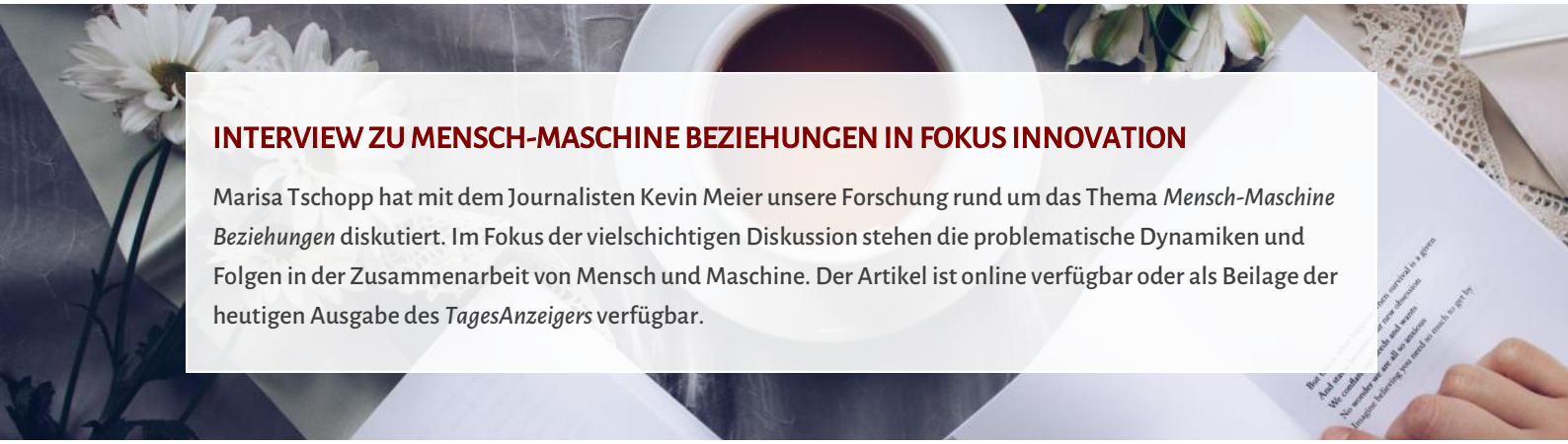
Marc Ruef
Head of Research

NEWS

WAS IST BEI UNS PASSIERT?

GASTVORTRAG AN UNIVERSITÄT ZÜRICH

Der Weiterbildungskurs *Ethik, Digitalisierung und Innovation* an der *Universität Zürich* vermittelt einen konzentrierten Einblick in die Methoden und Positionen der angewandten Ethik im Kontext von Digitalisierung und Innovation. Marisa Tschopp hat am Samstag, den 19.11.2022 einen Einblick in die Forschung und Praxis der scip AG geben.



INTERVIEW ZU MENSCH-MASCHINE BEZIEHUNGEN IN FOKUS INNOVATION

Marisa Tschopp hat mit dem Journalisten Kevin Meier unsere Forschung rund um das Thema *Mensch-Maschine Beziehungen* diskutiert. Im Fokus der vielschichtigen Diskussion stehen die problematische Dynamiken und Folgen in der Zusammenarbeit von Mensch und Maschine. Der Artikel ist online verfügbar oder als Beilage der heutigen Ausgabe des *TagesAnzeigers* verfügbar.

INTERVIEW ZU LENSA AI AUF SRF NEWS PLUS

Marisa Tschopp war zu Gast beim Newspodcast *News Plus* des *SRF* zum Thema *Hype um die App "Lensa" und Kritik an Künstlicher Intelligenz*. Zusammen mit Marc Bravin, wissenschaftlicher Mitarbeiter der der Hochschule Luzern, diskutieren sie, was die *Lensa AI App* kann und warum sie auch umstritten ist. Marisa Tschopp geht insbesondere auf die psychologische Perspektive ein und welche Gefahren in der Künstlichen Intelligenz liegen.

Weitere News zu unserem Unternehmen finden Sie auf unserer Webseite.

SCIP BUCHREIHE

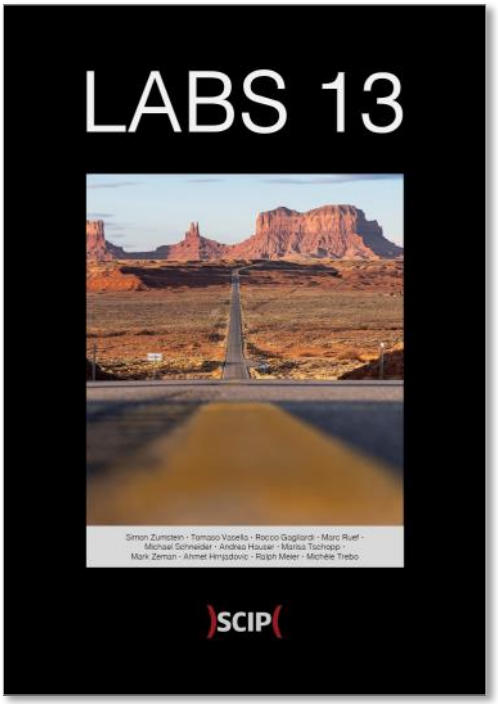
UNSER NEUES JAHRBUCH

Erneut veröffentlichen wir die aktuelle Ausgabe unseres Jahrbuchs. Bereits zum 13ten Mal fassen wir in diesem die Fachbeiträge von einem Jahr Forschung im Bereich Cybersecurity zusammen.

Das Buch ist wiederum sowohl in deutscher (ISBN 978-3-907109-30-4) als auch in englischer Sprache (ISBN 978-3-907109-31-1) verfügbar. Das Vorwort wurde von Dr. iur. David Vasella verfasst und setzt sich mit den rechtlichen Rahmenbedingungen der Informationssicherheit auseinander.

In unserem Katalog finden sich ebenfalls themenspezifische Bücher zu Künstlicher Intelligenz (ISBN 978-3-907109-14-4) und Sicherheit in der Hotellerie (978-3-907109-16-8).

Weitere Informationen auf unserer Webseite.



ISBN 978-3-907109-30-4 [de]
ISBN 978-3-907109-31-1 [en]

STÄRKE KANN AUS RUHE ERWACHSEN

Bildquelle: https://pixabay.com/images/id-7623362/

RALPH MEIER

FLIPPER ZERO
WAS KANN DAS HACKING TOOL

Beim Flipper Zero handelt es sich um ein Multi-Tool für Penetration Tester und Hardware Geeks, welches im Juli 2020 als Kickstarter Projekt initiiert wurde. Nach nur 8 Minuten war das Finanzierungsziel der Kampagne bereits erreicht. Insgesamt wurde eine Finanzierung von 4.8 Millionen US-Dollar erreicht. Durch die Corona-Pandemie und die daraus resultierende Chipknappheit mussten einige Komponenten ersetzt werden, was wiederum zu Anpassungen an Hardware und Software führte. Anfangs 2022 konnten die ersten Flipper Zeros die Produktion verlassen und an ihre Unterstützer versendet werden.

Zurzeit dieses Artikels gilt der Flipper Zero als Schweizer Taschenmesser im Bereich der kleinen portablen Hacking-Tools. Er bringt eine Menge an Module für das Senden und Empfangen von verschiedenen Frequenzen und Protokollen mit und kann zusätzlich noch über GPIO-Pins erweitert werden. Die Firmware und Software rund um den Flipper Zero sowie die elektronischen Schaltpläne sind Open Source unter der General Public License (GNU) v3.0.

INFRAROT SENDEEMPFÄNGER

Infrarot wird oft in Fernbedienungen für Fernseher, Klimaanlagen, Musikanlagen oder auch in Dusch-WCs eingesetzt. Der Flipper Zero kommt mit einer grossen Bibliothek an Infrarot-Sequenzen von den bekanntesten Fernseh- und Klimagerätehersteller, welche die gängigen Funktionen umfasst. Damit lässt es sich mit einem Knopfdruck sämtliche Ein-/Ausschaltbefehle für Fernsehgeräte versenden, um zum Beispiel das gewünschte Fernsehgerät auszuschalten. Dadurch, dass der Flipper Zero selbst auch Infrarotsignale empfangen kann, ist es möglich neue Fernbedienungen aufzuzeichnen und wiederzugeben. Quasi die Universalfernbedienung im Delphinkostüm.

SUB-1 GHZ SENDEEMPFÄNGER

Der Flipper Zero verfügt über ein Sub-1 GHz Modul, dieses befindet sich links vom Display und kann folgende Frequenzen empfangen und versenden: 300-348 MHz, 387-464 MHz, und 779-928 MHz. Es muss hier jedoch gesagt sein, dass je nach Region auf gewissen Frequenzbändern in der offiziellen Firmware nicht gesendet werden kann, dies aufgrund gesetzli-

cher Vorlagen. So kann in der Schweiz beispielsweise nicht auf 310 MHz gesendet werden, obwohl das Aufzeichnen solcher Signale möglich ist. Mit dem Sub-1 GHz Modul lassen sich unteranderem Funksteckdosen schalten, Garagentore bedienen und auch die Klappe des Ladeanschlusses von Tesla Fahrzeugen öffnen. Viele Autoschlüssel funken auch in diesem Bereich, diese verwenden aber oftmals einen Rolling-Code.

125KHZ RADIO-FREQUENCY IDENTIFICATION (RFID)

Am Boden des Flipper Zeros befindet sich eine 125kHz Antenne, welche das Lesen und Emulieren von RFID-Karten und Chips ermöglicht. Genauer gesagt können EM-4100 und HID Proximity Karten ausgelesen werden, da diese lediglich eine N-Byte ID enthalten und über keinen Authentifizierungsmechanismus verfügen. Eine ID kann auch manuell in den Flipper Zero hinzugefügt werden.

Durch ein Update der Firmware ist nun das Auslesen von Microchips für Haustiere wie Hunde und Katzen ebenfalls möglich. Wobei zum Zeitpunkt dieses Labs unklar ist, ob sämtliche Microchips, welche auf der Welt für Haustiere eingesetzt werden, ausgelesen werde können.

NEAR-FIELD COMMUNICATION (NFC)

Der Flipper Zero kann ebenfalls verschiedene Typen von NFC-Karten und Module auslesen und selbst emulieren. NFC ist eine Sammlung von Kommunikationsprotokollen, funktioniert zwischen zwei elektronischen Geräten auf eine Distanz von weniger als 4 Zentimeter und auf einer Frequenz von 13.56MHz. NFC begegnet einem in vielen Karten und Anwendungsbereiche im Alltag; kontaktloses Bezahlen mit Debit-/Kreditkarten oder Apple Pay funktioniert über NFC, der SwissPass besitzt einen NFC-Chip, welcher bei Kontrollen ausgelesen und damit werden vorhandene Tickets von den Servern der SBB geladen aber auch für das Hinterlegen und Verwenden anderer Tickets wie Skitickets verwendet werden kann. NFC ermöglicht einfaches Koppeln von Lautsprechern mit einem Smartphone oder das schnelle Verbinden in einem WLAN-Netzwerk. Ebenfalls wird NFC in Smartcards, anderen Zugangskarten und Chips anstelle von 125kHz RFID eingesetzt. Anders als RFID kann NFC in beide Wege kommunizieren und je nach Konfiguration können die

Daten auf dem NFC-Chip überschrieben werden. Der Flipper Zero unterstützt zum Zeitpunkt des Artikels verschiedene NFC Typ A Karten, welche kompatibel mit ISO 14'443 sind

Neben NFC Typ A Karten gibt es noch Typ B, Typ F und Typ V, bei welchen der Flipper Zero die UID lesen aber nicht speichern kann.

Zu Beginn der Kommunikation zwischen Lesegerät und NFC-Modul wird die genaue Technologie kommuniziert, damit beide das gleiche Protokoll verwenden. Je nach Typ wird ein anderes Encoding und andere Amplitudenmodulation verwendet. NFC Typ F ist sehr populär in Japan und wird dort unteranderem für bargeldlose Zahlungen, Tickets oder ÖV-Zugang sowie Personenidentifikation eingesetzt. Typ V bietet einen einzigen Kommunikationsmodus, welcher mit existierenden Speichertags nach ISO 15'693 kompatibel ist.

BLUETOOTH

Das Bluetooth Low Energy Modul im Flipper Zero ermöglicht die Kommunikation mit Apps auf dem Smartphone. Der Flipper Zero kann über die Flipper App gesteuert werden und so zum Beispiel Sub-GHz Kommandos abgeschickt werden. Auch hier gibt es eine Open Source Bibliothek, welche in selbst gemachte Apps eingebunden und verwendet werden kann.

GPIO-PINS

Durch die verbauten GPIO-Pins auf der Oberseite des Flipper Zeros kann das Multi-Tool erweitert werden mit zum Beispieleinem Developer Board, welches Debugging Funktionalität und 2.4GHz WLAN-Konnektivität mit sich bringt. Es können auch andere Chips sowie leere Prototyping Boards auf einfache Weise verbunden werden und eigene Erweiterungen geschaffen werden. Durch den vorhanden USB-Port und die GPIO-Pins kann der Flipper Zero auch als UART-, SPI- und I2C-Konverter eingesetzt werden.

IBUTTON

Flipper Zero verfügt ebenfalls über ein 1-Wire Connector, welcher es ihm ermöglicht, iButtons zu lesen, abzuspeichern, leere sogenannte Schlüssel zu beschreiben und den Schlüssel selbst zu emulieren. Die dafür notwendigen Pins sitzen auf der Hintersei-

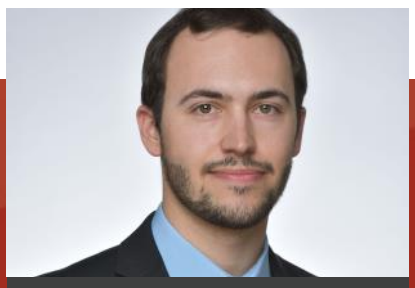
te des Flipper Zeros. Das 1-Wire Protokoll besitzt keine Authentifizierung. iButton wird zum Beispiel bei Kassensystemen in Restaurants eingesetzt, jeder Kellner hat seinen eigenen iButton Magnet-Kellnerschlüssel, welcher Zugriff auf das Kassen- und Bestellsystem in seinem Kontext ermöglicht.

USB-INTERFACE

Einerseits kann das Aktualisieren der Firmware über das USB-Interface via der qFlipper Desktopapplikation getätigt werden, was jedoch auch über die Flipper Smartphone App möglich ist, andererseits bringt das USB-Interface die Möglichkeit den Flipper Zero als BadUSB oder als Universal 2nd Factor (U2F) Security Token zu verwenden. Jedoch wird empfohlen für sicherheitssensitive Webseiten/Applikationen zertifizierte U2F Security Keys zu verwenden.

FAZIT

Flipper Zero vereint eine Vielzahl von Frequenzen und Protokollen in einem Formfaktor, welcher ohne Probleme in den Hosensack passt. Durch die vorhandenen GPIO-Pins, das USB-Interface und die Open Source Software sind Erweiterung in alle Richtungen möglich. Weitere technische Details und einen guten Einstiegspunkt befinden sich in der online Dokumentation von Flipper Zero selbst. Wir sind gespannt, wohin uns die Reise mit dem Flipper Zero noch führen wird. Ah und natürlich läuft auch Doom auf dem Flipper Zero.



Ralph Meier

Sie brauchen Unterstützung?

Niemand kann sich entziehen. Jede Firma ist betroffen und muss eine ihren Bedürfnissen gerechte Cybersecurity Strategie umsetzen und leben. Kommunikation, Anwendungen, Prozesse, verarbeitete Informationen, Partner. Sichern Sie sich mit uns erfolgreich.

SCIP

https://www.scip.ch

MICHÈLE TREBO

FUNKTIONSWEISE DES BITCOIN LIGHTNING NETWORK

Das Lightning-Netzwerk wird im Dokument The Bitcoin Lightning Network als dezentrales System beschrieben, bei dem Transaktionen über ein Netzwerk von Mikrozahlungskanälen gesendet werden, deren Wertübertragung ausserhalb der Blockchain und somit off-chain erfolgt. Damit wir verstehen, was das bedeutet, müssen wir zuerst wissen, wie Kryptowährungen funktionieren und was für Probleme bei Transaktionen mit Kryptowährung auftreten.

KRYPTOWÄHRUNGEN

Eine Kryptowährung ist eine digitale oder virtuelle Währung, die Transaktionen mittels Kryptografie, genauer Blockchain oder anderen digitalen Signaturen sichert. Da der Markt ständigen Schwankungen unterliegt, sind auch die Kurse der Kryptowährungen unbeständig. Dies ist auch der Grund, warum viele Händler Kryptowährungen nicht als Zahlungsmittel anerkennen. Der Markt ist ihnen zu unsicher. Inzwischen haben sich dieser Marktnische diverse Dienstleister angenommen. Diese übernehmen die Zahlungsabwicklung mit Kryptowährungen und bieten den Händlern einen zu diesem Zeitpunkt aktuellen Wechselkurs. Damit wird das Risiko der Kursschwankung reduziert. Der Hauptunterschied zu normalem Geld ist, dass keine Ausgabe- oder Regulierungsbehörde existiert. Die Regierung und finanzielle Institutionen haben keinen Einfluss. Eine Kryptozahlung geht also nicht über ein zentrales Computersystem, sondern über ein dezentrales System, das für die Verifikation von Transaktionen nicht auf Banken angewiesen ist.

Blockchain

Eine Blockchain ist eine verteilte, öffentliche Datenbank. Im Kontext von Bitcoin oder anderen Kryptowährungen wird diese Technologie in Form einer dezentralen Datenbank eingesetzt, um Vermögenstransaktionen zu verwalten. Dadurch reduzieren sich die Risiken und Kosten für alle Beteiligten deutlich. Blockchain ist von grosser Bedeutung. Je schneller Informationen übermittelt werden können und je präziser sie sind, desto besser. Blockchain liefert Informationen sofort gemeinsam für die Teilnehmer eines Netzwerkes nutzbar und transparent. Da alle Nutzer wahrheitsgetreue Details einer Transaktion durchgängig abrufen können, ist das Vertrauen grösser, die Effizienz steigt und es eröffnen sich neue Möglichkeiten. Eine gewöhnliche Bankzahlung wird meistens über ein zentrales Computersystem abge-

wickelt. In diesem Fall muss man dem Anbieter dieses Systems seine sensiblen Daten anvertrauen. Bei einer Blockchain hingegen tritt man bei einer Transaktion nicht mit seinem Namen, sondern mit dem sogenannten Public Key oder auf Deutsch öffentlichen Schlüssel auf, der aus einer langen Abfolge von Buchstaben und Zahlen besteht. Eine Transaktion wird, anders als bei einer gewöhnlichen Bankzahlung über die Computer aller Blockchain-Teilnehmer synchronisiert. Bevor eine Transaktion abgeschlossen wird, muss sie für alle Mitglieder sichtbar in einem Block abgelegt werden. Dies geschieht je nach Art der Blockchain anders.

Bitcoin

Bitcoin gehört zu den bekanntesten Kryptowährungen weltweit und basiert auf der Bitcoin-Blockchain. Im Bitcoin-Netzwerk kann das Erzeugen eines Blocks grundsätzlich von jedem Blockchain-Nutzer, der in diesem Fall als Miner bezeichnet wird, ausgeführt werden. Dabei werden mithilfe einer mathematischen Funktion aufgelaufene Transaktionen zu einem Block berechnet. Der Miner, der den Block als Erstes berechnet, erhält einen sogenannten Mining-Reward in Form einer vordefinierten Anzahl Bitcoins. Dadurch entsteht zwischen den Minern ein Wettbewerb. Ist der Block berechnet, wird er unveränderbar auf verschiedenen Computern abgelegt. Die Berechnung dieser Blöcke benötigt eine hohe Rechenleistung, viel Strom und ist damit nicht besonders ökologisch. Eine weitere Problematik besteht darin, dass pro Block nur ein gewisser Speicherplatz für Transaktionen zur Verfügung steht und per Definition ca. alle 10 Minuten ein Block geschaffen wird. Damit finden je nach Auslastung nicht alle Transaktionen im nächsten Block Platz. Dies führt dazu, dass es zu Verzögerungen im Zahlungsprozess kommt. Obwohl Bitcoin als anonym gilt, ist es möglich, anhand des Public Keys Rückschlüsse auf die Identität einer Person zu ziehen. Der Public Key lässt sich nicht eindeutig einem konkreten Nutzer zuordnen. Zudem besteht kein zentrales Register, welches Auskunft über den Inhaber eines Public Keys gibt. Anders bei der Kryptowährung Monero, die ihre Transaktionen zusätzlich verschlüsselt und damit die Transaktionsdetails nicht eingesehen werden können. Dadurch wird ein höherer Grad an Anonymisierung erreicht.

Problem

Im Kontext von Kryptowährungen und damit auch Bitcoin wird oft das sogenannte Blockchain-Trilemma referenziert. Die drei konkurrierenden Bereiche sind Skalierbarkeit, Dezentralisierung und Sicherheit. Da es sich um Gegensätze handelt, stehen diese in dauernder Konkurrenz, was dazu führt, dass die Erhöhung eines Bereiches zwangsweise auf Kosten der anderen geht. Am Beispiel Bitcoin ist eine hohe Dezentralisierung und eine hohe Sicherheit implementiert – allerdings leidet die Skalierbarkeit darunter. Will man die Skalierbarkeit erhöhen, müssen Abstriche im Bereich Sicherheit oder eine grössere Zentralisierung gemacht werden. Das Trilemma Skalierbarkeit, Dezentralisierung und SicherheitSo kann Bitcoin ein zensurresistentes Netzwerk mit unveränderlichen Regeln und den geringstmöglichen Angriffsvektoren gewährleisten. Das Problem der Skalierbarkeit muss allerdings vernachlässigt werden. Das Bitcoin-Netzwerk bewältigt pro Sekunde lediglich sieben Transaktionen. Liegt eine höhere Nutzung vor, so steigen auch die Gebühren. Da bei hoher Auslastung nicht alle Transaktionen in einem Block Platz finden, kommt es zu einem Konkurrenzkampf, welcher über die Höhe der Gebühr ausgetragen wird. Das macht kleinere Zahlungen oder Micropayments unwirtschaftlich. Wenn jeder Knoten im Netzwerk über jede stattfindende Transaktion Bescheid wissen muss, kann dies die Fähigkeit des Netzwerkes, alle globalen Finanztransaktionen zu erfassen, erheblich verlangsamen. Transaktionen sollen so erfasst werden können, dass Dezentralisierung und Sicherheit nicht beeinträchtigt werden. Um die Problematik der beschränkten Anzahl Transaktionen und den damit verbundenen steigenden Transaktionsgebühren zu lösen, ohne auf Sicherheit und Dezentralisierung zu verzichten, wurde das Bitcoin-Lightning-Netzwerk entwickelt.

THE BITCOIN LIGHTNING NETWORK

Ein Lightning-Netzwerk erhöht den Transaktionsdurchsatz pro Sekunde. Die Idee von Lightning-Netzwerken ist es, dass, wenn sich zwei Mitglieder für eine Transaktion interessieren, alle anderen Knoten nichts davon wissen müssen. Das Lightning-Netzwerk ermöglicht Peer-to-Peer-Zahlungen, die ausserhalb der Bitcoin-Blockchain über Zahlungskanäle zwischen Einzelpersonen erfolgen. Sobald die Beteiligten ihre Kanäle schliessen, erfolgt eine Abrechnung, um zu klären, wem was gehört. Das Light-

ning-Netzwerk kann so Millionen von Transaktionen pro Sekunde ausführen und ist nahezu gebührenfrei. Dieses Netzwerk ist ein Peer-to-Peer-Mesh-Network, indem jeder Knoten gleichgestellt ist (ohne zentrale Instanz), das Bitcoin-Konsensregeln verwendet, um Transaktionen abzuschliessen. Im Dokument The Bitcoin Lightning Network wird die Grundidee wie folgt erklärt. Wenn niemand das Fallen eines Baumes hört, spielt es keine Rolle, ob das Fallen ein Geräusch verursacht oder nicht. Ähnlich funktioniert es bei der Blockchain. Wenn sich nur zwei Nutzer für eine wiederkehrende Transaktion interessieren, müssen nicht alle anderen Knoten im Bitcoin-Netzwerk davon wissen. Besser ist es, wenn nur das absolute Minimum an Informationen in der Blockchain sind. Indem es aufgeschoben wird, die ganze Welt über jede Transaktion zu informieren, ermöglicht man den Nutzern, viele Transaktionen durchzuführen, ohne die Blockchain aufzublähen oder Vertrauen in eine zentralisierte Gegenpartei zu schaffen.

Transaktionen über das Bitcoin-Lightning-Netzwerk

Damit über das Bitcoin-Lightning-Netzwerk eine Transaktion ausgeführt werden kann, muss zuerst ein Zahlungskanal zwischen dem Sender und Empfänger eröffnet werden. Dieser Zahlungskanal ist eine Multisignaturadresse, die vom Bitcoin-Netzwerk verwendet wird. Sowohl der Sender als auch der Empfänger muss signieren, wenn eine Transaktion von der Multisignaturadresse gesendet werden soll. Zur Eröffnung eines Zahlungskanals wird eine Finanzierungstransaktion genauer eine reguläre Transaktion auf der Blockchain hinzugefügt. Dabei muss angegeben werden, wie viele Satoshis im Zahlungskanal sein sollen. Mit den Satoshis kann man so viele Transaktionen hin und her schicken, wie man möchte, solange sich noch Satoshis im Kanal befinden. Der Zahlungskanal hält den Überblick über die Kontostände der Nutzer. Das Erstellen einer Transaktion hat dabei immer zwei Ausgänge. Wenn man 100'000 Satoshis im Kanal hat und dem Empfänger 10'000 Satoshis senden möchte, werden einem selbst 90'000 Satoshis und dem Empfänger die 10'000 Satoshis verbucht. Erst wenn beide die Transaktion bestätigt haben, werden die Kontostände angepasst. Ausser den Beteiligten selbst kann niemand diese Peer-to-Peer-Transaktion zuordnen. Erst wenn der Kanal geschlossen wird, werden die finalen Kontostände öffentlich auf die Bitcoin-Blockchain zurückgeschrieben.

Netzwerkeffekte

Was, wenn eine Transaktion an einen Empfänger gehen soll, mit dem kein Zahlungskanal aufgebaut wurde? Allenfalls hat jemand, mit dem ein Kanal besteht, einen Zahlungskanal mit dem ersuchten Empfänger. So kann man seinem Kanalpartner den gewünschten Betrag innerhalb des aufgebauten Zahlungskanals senden und er leitet den Betrag an den gewünschten Endempfänger weiter. Das Netzwerk wird polynomial nützlicher, je mehr Knotenpunkte beteiligt sind. Damit sich der Aufwand für die Mittelsperson auszahlt, kann sie eine Gebühr, die sogenannte Routing Fee erheben. Dank des Hash-Time-Lock-Contracts, der die Durchführung zeitgebundener Transaktionen ermöglicht, kann das Gegenparteirisiko eliminiert werden. Das bedeutet, dass der Empfänger einer Transaktion die Zahlung innerhalb eines bestimmten Zeitrahmens durch einen kryptografischen Beweis bestätigen muss, damit die Transaktion zustande kommt. Wessen Kanäle genau benutzt werden, ist unbekannt. Denn es wird alles über Onion- und Host-Privacy-Technologien abgewickelt.

Wachstum

Alle relevanten Zahlen wie Knotenpunkte, Kanäle und die Kapazität steigen stetig. Das Lightning-Netzwerk ist nicht mehr Zukunft, sondern bestimmt bereits die Gegenwart. Dies zeigt auch die Visualisierung der Knotenpunkte und Kanäle auf LnRouter. Immer mehr Unternehmen beginnen, Bitcoin zu akzeptieren, wobei die vom Lightning-Netzwerk bereitgestellte Infrastruktur entscheidend dazu beiträgt. Das Lightning-Netzwerk kann ausserdem auch auf anderen Kryptowährungen implementiert werden. Die einzigen Bedingungen sind Multisignatur-Funktion und Hash-Time-Lock-Contracts. Das Lightning-Netzwerk ermöglicht Währungsumtausch in Echtzeit ohne Gebühren und innerhalb einer Sekunde. Über Sphinx, einem Echtzeit-Chat, können dank der Lightning-Technologie nicht nur Nachrichten für Aussenstehende komplett unsichtbar und dezentral versendet, sondern auch Zahlungen sofort getätigt werden. Das Lightning-Netzwerk revolutioniert auch andere Bereiche wie Twitter, Geschenkgutscheine (Bitrefill und Fold) oder Zahlungen über Geräte, die Visa-Debitkarten akzeptieren (Moon). Etwas, was mit dem Banksystem aktuell nicht möglich ist, ist das Geld-Streaming. Damit kann sekündlich eine

Zahlung ausgeführt werden, was Möglichkeiten für künftige Business-Modelle eröffnet. Diese Liste ist nicht abschliessend und wird immer länger.

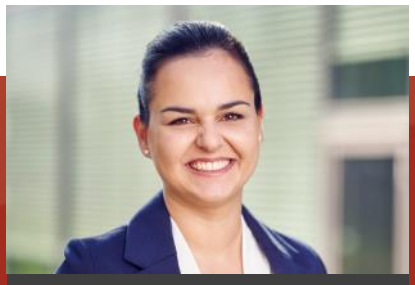
Probleme

Das Lightning-Netzwerk ist nicht frei von Problemen. Diese sind technisch herausfordernd, aber nicht unlösbar. Ein Problem ist die Liquidität der Kanäle und die damit verbundenen Grenzen. Es ist nicht intuitiv, dass zuerst ein Zahlungskanal mit Liquidität gefüllt werden muss, bevor eine Transaktion überhaupt möglich ist. Nur wenn genügend Knoten vorhanden sind, die genügend Liquidität haben, kann das System funktionieren. Weitere Risiken sind sogenannte Superknoten oder Hubs, die wie Banken agieren können und so die Dezentralisierung gefährden. Eine potenzielle Gefahr stellen ausserdem die fast gebührenfreien Transaktionen dar, die dazu führen, dass Miner weniger verdienen und damit die Basis (darunterliegende Bitcoin-Blockchain) gefährdet ist. Das bedeutet, dass der Markt ein Gleichgewicht finden muss, was über das Lightning-Netzwerk und was über die Blockchain abgerechnet wird. Weiter kann es schwierig sein, eine passende Route zu finden. Je mehr Knotenpunkte und Liquidität vorliegen, desto geringer die Gefahr, dass ein Routing scheitert. Das Braess-Paradoxon sagt im weiteren Sinne hingegen aus, dass je mehr Knoten hinzugefügt werden, desto langsamer der Fluss durch das Netz. Weiter müssen Lightning-Knoten (fast) immer online sein. Ausserdem sind Angreifer schwierig zu identifizieren, da nicht bekannt ist, wer wem Geld schickt. Es sind verschiedenste Angriffe auf das Netzwerk möglich, was sich auf die Sicherheit auswirkt. Viele Probleme sind aktuell noch gar nicht bekannt, diese werden erst im Laufe der Zeit zum Vorschein kommen. Allerdings kann man zuversichtlich sein, dass Lösungen gefunden werden, da sich täglich Fachspezialisten damit auseinandersetzen.

ZUSAMMENFASSUNG

Kryptowährungen sind digitale oder virtuelle Währungen und basieren auf der Blockchain-Technologie, so auch eine der bekanntesten Kryptowährungen Bitcoin. Weil eine Transaktion mit allen sich im Netzwerk befindenden Nutzern geteilt wird und eine hohe Rechenleistung braucht, nur ca. alle 10 Minuten ein Block erstellt wird und die Anzahl Transaktionen pro Block limitiert ist, dauert es lange,

bis eine Transaktion abgeschlossen ist. Dadurch steigen die Gebühren. Weil alle Nutzer die Transaktionsdetails in der Blockchain einsehen können, kann Zahlungsströmen gefolgt und auf Beteiligte zurück geschlossen werden. The Bitcoin Lightning Network löst insbesondere die genannten Schwächen von klassischen Bitcoin-Zahlungen wie die lange Wartezeit und hohe Gebühren. Dazu werden sogenannte Zahlungskanäle zwischen zwei Parteien eröffnet und alle weiteren Zahlungen off-chain auf einem neuen Netzwerk (dem Lightning-Netzwerk) durchgeführt. Erst wenn die Parteien den Kanal schliessen, werden die finalen Kontostände wieder mit einer Transaktion auf der Bitcoin-Blockchain synchronisiert. The Bitcoin Lightning Network ist noch in einer experimentellen Phase und weisst einige Probleme sowie Angriffsmöglichkeiten auf. Diese sind allerdings nicht unlösbar. Fachspezialisten setzen sich täglich mit deren Lösung auseinander. Das Netzwerk ist nicht nur auf Bitcoin anwendbar, sondern auch auf andere Kryptowährungen, welche die Multisignatur-Funktion und Hash-Time-Lock-Contracts besitzen. In einigen Jahren ist es durchaus denkbar, dass das Lightning-Netzwerk als weltweites Hauptzahlungsmittel fungiert.



Michèle Trebo

MANCHMAL HILFT ABWARTEN BEIM LÖSEN VON PROBLEMEN

Bildquelle:https://pixabay.com/images/id-7601873/

SCIP MONTHLY SECURITY SUMMARY

IMPRESSUM

ÜBER DEN SMSS

Das *scip Monthly Security Summary* erscheint monatlich und ist kostenlos.

Anmeldung: smss-subscribe@scip.ch
Abmeldung: smss-unsubscribe@scip.ch

Informationen zum Datenschutz.

Verantwortlich für diese Ausgabe:
Marc Ruef

ÜBER SCIP AG

Wir überzeugen durch unsere Leistungen. Die scip AG wurde im Jahr 2002 gegründet. Innovation, Nachhaltigkeit, Transparenz und Freude am Themengebiet sind unsere treibenden Faktoren. Dank der vollständigen Eigenfinanzierung sehen wir uns in der sehr komfortablen Lage, vollumfänglich herstellerunabhängig und neutral agieren zu können und setzen dies auch gewissenhaft um. Durch die Fokussierung auf den Bereich Information Security und die stetige Weiterbildung vermögen unsere Mitarbeiter mit hochspezialisiertem Expertenwissen aufzuwarten.

scip AG
Badenerstrasse 623
8048 Zürich
Schweiz

+41 44 404 13 13
www.scip.ch