Lightning-Network: Blitzschnelle Bitcoins für den Alltag

Leichtes Netz

Oliver Gugger, Daniel Kobras

Das Lightning-Network erweitert die herkömmliche Bitcoin-Infrastruktur um neue Transaktionskanäle, die besonders schnell und leichtgewichtig sind. Die Autoren haben das in einem konkreten Projekt ausprobiert.

Mal futuristisch, mal zwielichtig: Wann immer Einsatzszenarien für Kryptowährungen zur Sprache kommen, sind sie eines ganz bestimmt nicht: alltäglich. Das mag einerseits daran liegen, dass Pommesbude oder Billig-Discounter der rechte Glanz fehlt für strahlende Zukunftsvisionen, hat andererseits aber ganz konkrete technische Gründe.

Die Blockchain à la Bitcoin stößt bei steigender Nutzung prinzipbedingt rasch an ihre Kapazitätsgrenze – sie skaliert schlecht und ist daher ungeeignet für Anwendungsfälle, die Klein- und Kleinsttransaktionen in hoher Zahl verarbeiten müssen. Mehr Kapazität für zusätzliche Transaktionen ließe sich nur zulasten von Speicherbedarf und Netzbandbreite jedes einzelnen Bitcoin-Knotens schaffen. Ganz abgesehen von der Frage, ob tatsächlich der Erwerb jeder Currywurst nachvollziehbar und revisionssicher in einer universellen Blockchain-Infrastruktur beglaubigt werden muss. Genau hier setzen Lösungen an, die das Skalierungsproblem beheben: Statt die Transaktionsgeschwindigkeit der Blockchain zu erhöhen, soll sie von unnötigen Transaktionen entlastet werden.

Dieser Grundidee folgt das erstmals 2015 vorgeschlagene Lightning-Network. Die Bitcoin-Blockchain dient hier nur noch als Unterbau für Vertrauensstellungen und Zahlungsmittel, während das Gros der Zahlungen selbst in eigenen Kanälen stattfindet. Die arbeiten ressourcenschonend und nahezu ohne

iX-TRACT

- Hohe Gebühren und lange Wartezeiten machen herkömmliche Bitcoin-Transaktionen ungeeignet für Zahlungen kleiner Geldbeträge.
- Lightning setzt ein eigenes, leichtgewichtiges Netzwerk schneller Zahlungskanäle auf die Bitcoin-Blockchain auf.
- Trotz relativ kurzer Entwicklungszeit setzen erste kommerzielle Pilotprojekte das Zahlungssystem bereits erfolgreich ein.
- Bislang gibt es noch wenig Auswahl an vollwertigen Lightning-Wallets.

Zeitverzögerung, sodass Lightning eine ernst zu nehmende, unabhängige Alternative zu den mobilen Bezahlsystemen kommerzieller Anbieter darstellt.

Gleichzeitig erbt Lightning aber auch die bedeutendsten Eigenschaften des 2008 als Reaktion auf die Finanzkrise und die Furcht vor politisch getriebener Geldentwertung ins Leben gerufenen Bitcoin – zuvorderst Unabhängigkeit von Zentralbanken und staatlicher Regulierung. Dazu kommen der Schutz der Privatsphäre durch Pseudonyme, offener, dezentraler Aufbau und die einfache Integration in Onlinezahlungsprozesse, aber auch einige der Schattenseiten: etwa die historisch hohe Schwankungsbreite des Wechselkurses im Vergleich zu herkömmlichen Währungen und der hohe Ressourcenverbrauch für den Proof-of-Work-Algorithmus, mit dem Bitcoin sich die Unabhängigkeit von zentralen Strukturen erkauft.

Zahlen in eine Richtung

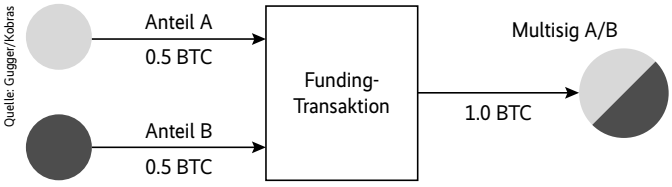
Die grundlegende Debatte darüber, ob die Unabhängigkeit von staatlichen Institutionen den Ressourcenbedarf rechtfertigt oder nicht, wird auch Lightning nicht lösen können. Aber es zeigt einen Weg auf, das schwere Gerät Bitcoin-Blockchain gezielt nur an den Stellen einzusetzen, wo seine Eigenschaften tatsächlich Vorteile bringen (on-chain), überall sonst jedoch leichtgewichtigeres Werkzeug zu verwenden (off-chain).

Um Lightning verstehen zu können, muss man zuerst Zahlungskanäle verstehen. Das Konzept der Zahlungskanäle wurde schon sehr früh in der Geschichte von Bitcoin vorgeschlagen. In ihrer einfachsten Variante funktionieren diese so: Sollen mehrere Zahlungen in die gleiche Richtung fließen, öffnet ein Käufer einen Zahlungskanal zu einem Verkäufer und befüllt den Kanal mit einem Teil seines verfügbaren Bitcoin-Vermögens. Dabei fließt noch kein Geld, der Vorgang wird aber als Smart Contract in der Bitcoin-Blockchain hinterlegt, die so die Vertrauensstellung zwischen beiden Parteien herstellt und die Zahlungsfähigkeit des Käufers verbürgt.

Mit dieser sogenannten Funding-Transaktion ist der On-Chain-Teil zunächst beendet. Der eigentliche Kaufvorgang findet off-chain statt. Der Käufer sendet dem Verkäufer über einen privaten Kommunikationskanal dazu eine signierte Transaktion über den geforderten Betrag. Der Verkäufer kann die Zahlung unmittelbar selbst validieren und hat nun die Wahl, ob er die Transaktion sofort einlöst oder den Kanal offen hält, um weitere Zahlungen entgegenzunehmen.

Im zweiten Fall sendet der Käufer über den Kanal eine weitere Transaktion, die den neuen Gesamtbetrag enthält. Eine „Vergiftung“, wie sie beim später vorgestellten bidirektionalen Zahlungskanal eingesetzt wird, ist hier nicht nötig. Denn der Verkäufer hat automatisch den Anreiz, nur die aktuellste Transaktion einzulösen, denn die enthält für ihn den höheren Betrag.

Auf diese Weise macht der unidirektionale Zahlungskanal die zuvor übermittelten Transaktionen zwar nicht formal, aber praktisch ungültig. Wartezeiten und Gebühren fallen erst beim Einlösen und Schließen des Zahlungskanals an. Das findet wieder on-chain statt. Öffentlich sichtbar wird dadurch nur die Summe aller



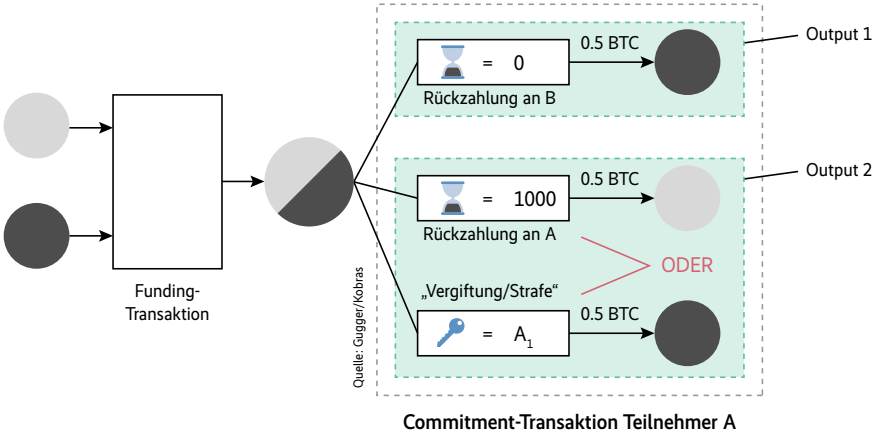
Zahlungspartner A und B zahlen in den Zahlungskanal ein (Abb. 1).

Zahlungen, nicht jede einzelne Transaktion selbst. So kann man beispielsweise aus allen Käufen eines Monats jeweils die Zahlungen summieren, und nur diese Summe wird on-chain sichtbar.

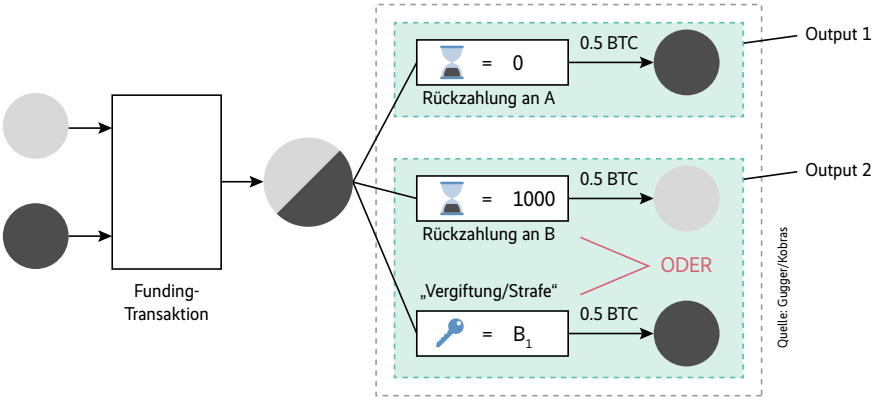
Bidirektionales Zahlen

Ein genauerer Blick auf die einzelnen Datenpakete macht klar, wie Lightning auch dann noch funktioniert, wenn innerhalb eines Zahlungskanals Geld in beide Richtungen fließen soll. Die Funding-Transaktion für einen Kanal erstellt eine neue Bitcoin-Adresse (Multisig Account), die von beiden Zahlungspartnern signiert ist und den Gesamtbetrag ihrer eingesetzten Bitcoins enthält (siehe Abbildung 1). Den zur Signatur gehörenden privaten Schlüssel behält jeder Zahlungspartner für sich. In diesem Zustand können beide Partner somit nur einvernehmlich über das Vermögen im Lightning-Kanal verfügen. Zusätzlich erstellen beide deshalb noch je eine Transaktion, die dem jeweiligen Partner die eingesetzte Summe aus dem Kanal wieder zurücküberweist (siehe Abbildung 2 und 3). Dazu muss jeder Zahlungspartner nur den eigenen privaten Schlüssel vorweisen.

Für den Restbetrag des Gegenübers stecken in der Transaktion jeweils zwei vorbereitete Alternativen: Der rechtmäßige Eigentümer erhält den Betrag entweder nach einer gewissen Wartezeit von beispielsweise 1000 Bitcoin-Blöcken (10 000 Minuten) zurück, oder der Zahlungspartner erhält sie mit dem privaten Schlüssel des ursprünglichen Eigentümers – den er zu diesem Zeitpunkt noch nicht kennt. Beide Parteien tauschen die entsprechend vorbereiteten Transaktionen aus und speichern sie bei sich ab. Der hier als Beispiel genannte Wert von 1000 Blöcken wird in der Praxis an die Größe des Betrags im Zahlungskanal angepasst. Je größer der Betrag, desto länger die Wartezeit.



Die gegensignierte Absicherungstransaktion, wie sie Teilnehmer A hält. Wird ein neuer Zustand ausgehandelt, übergibt Teilnehmer A seinen Schlüssel A1 an B, was ihn für den gesamten Betrag ermächtigt, sollte diese alte Transaktion jemals veröffentlicht werden (Abb. 2).



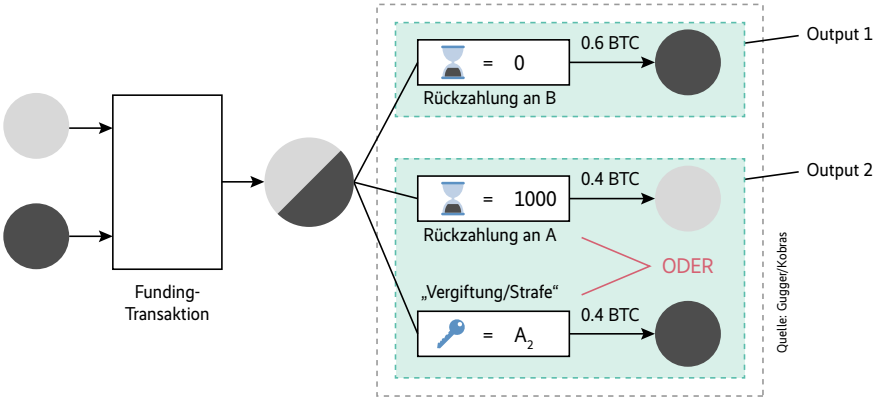
Commitment-Transaktion Teilnehmer B

Das symmetrische Gegenstück zur Transaktion aus Abbildung 2. Teilnehmer B hält diese Transaktion bei sich. Gibt es einen neuen Zustand, händigt Teilnehmer B seinen Schlüssel B1 aus und invalidiert somit diese Transaktion (Abb. 3).

Bei allen folgenden Zahlungsvorgängen geht es nun darum sicherzustellen, dass jede Partei im eigenen Interesse keine früheren Transaktionen veröffentlicht. Mit jeder neuen Transaktion erzeugen beide Partner dazu ein neues Schlüsselpaar, bauen damit wie oben beschrieben je eine Transaktion mit der aktuellen Zahlungsbilanz auf, tauschen sie aus und senden zusätzlich den privaten Schlüssel der vorherigen Transaktion an ihr Gegenüber (Abbildung 2, 3, 4). Das aktiviert die „Vergiftung“: Denn veröffentlicht eine Seite nun eine ältere Transaktion in der Blockchain, kennt nun auch die Gegenseite den passenden privaten Schlüssel und hat 1000 Blöcke Zeit, sich den gesamten im Kanal gespeicherten Betrag einzuverleiben. Das funktioniert in beide Richtungen. Egal wie sich die Balance im Lightning-Kanal im Verlauf der Zeit auch verschiebt, stets werden beide Seiten jeweils nur den letzten Zahlungsstand einlösen. Zudem hat jeder Partner jederzeit die Möglichkeit, den Kanal aufzulösen und damit den aktuellen Geldbetrag zurück ins reguläre Bitcoin-Netz zu überführen.

Passiert das einvernehmlich, erstellen die Parteien gemeinsam eine entsprechende Transaktion, die sich unmittelbar anwenden lässt. Löst ein Partner den Kanal einseitig, muss er hingegen die 1000 Blöcke Karenzzeit der „Vergiftung“ abwarten, um an sein frisch erworbenes Geld zu kommen.

Die gezeigten Kanäle erleichtern zwar wiederkehrende Zahlungen zwischen denselben Partnern, doch der Vorteil allein dadurch wäre stark begrenzt.



Commitment-Transaktion Teilnehmer A: Version 2

Neuer Zustand der Absicherungstransaktion von Teilnehmer A nach der Überweisung von 0.1 BTC an Teilnehmer B (Abb. 4)

Der eigentliche Clou von Lightning steckt darin, dass es als Netzwerk funktioniert. Zahlungen lassen sich nicht nur über direkte Kanäle zwischen Käufer und Verkäufer ausführen, sondern auch indirekt über mehrere Mittelsmänner, bezeichnet als Hubs oder Router. Die Zahlung läuft dann schrittweise vom Sender zum Empfänger. Jeder Hub leitet die Zahlung weiter im Austausch gegen einen vom Empfänger erzeugten geheimen Schlüssel, mit dem der Hub ein zusätzliches Feld der passenden eingehenden Transaktion entsperren und so seine eigene Zahlungsbilanz wieder ausgleichen kann. Auch hier müssen sich die Beteiligten in der Zahlungskette nicht vertrauen, denn die Transaktionen sind so aufgebaut und passend „vergiftet“, dass im Zweifel jeder beteiligte Knoten die erhaltene Transaktion in der Bitcoin-Blockchain veröffentlichen kann, um an das ihm zustehende Geld zu kommen. In einem zweiten Schritt können die einzelnen direkten Kommunikationspartner eine Multi-Hop-Transaktion dann jeweils zu den oben beschriebenen normalen Transaktionen vereinfachen. Das erleichtert nachfolgende Lightning-Transaktionen und begrenzt das Risiko, eine Transaktion einseitig on-chain veröffentlichen zu müssen.

Zahlen wird billiger

Für seine Dienste kann jeder Lightning-Hub Gebühren erheben, pro Transaktion (Base Fee) und anteilig an der weitergeleiteten Geldsumme (Fee Rate). Weil Lightning erheblich weniger Ressourcen verschlingt als das Mining von Bitcoin-Blöcken, fallen in der Praxis auch die Gebühren deutlich geringer aus. Dadurch eignet sich Lightning auch zum Zahlen von Kleinstbeträgen, den viel beschworenen Micropayments. Zahlungen innerhalb des Lightning-Netzwerks bleiben vertraulich. Über die Bitcoin-Blockchain öffentlich einsehbar ist letztlich nur die Zahlungsbilanz beim Schließen eines Kanals.

Bei diesen Eigenschaften wundert es wenig, dass neben Geeks und Pizzaläden auch die schattigeren Bereiche des Internets aus Online-Casinos und Versendern von „Erwachsenenbedarf“ zu den Early Adopters der Lightning-Technologie zählen – ein Umstand, der keineswegs von Dauer sein muss, denn vertrauliche und günstige Micropayments sind selbstredend auch für seriöse Geschäfte von Interesse. Alle nötigen Softwarekomponenten, um am Lightning-Netzwerk teilzunehmen, sind frei und quelloffen verfügbar, die Hardwareanforderungen so gering, dass selbst der eigene Point of Sale im Hobbykeller keine große Anstrengung erfordert (siehe Kasten „Bockbier aus der Blockchain“).

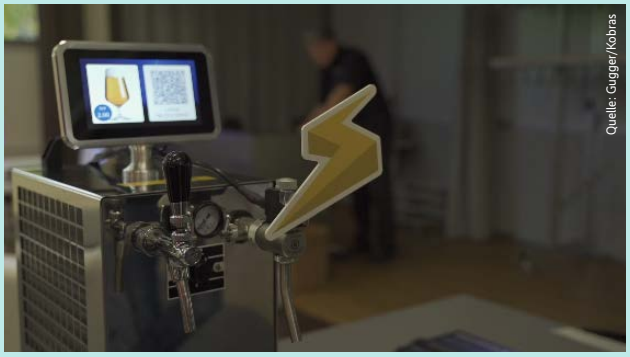
Für den Weg ins Lightning-Netzwerk steht Verkäufern bereits eine ansehnliche Palette an Zahlungssoftware zur Wahl – auch wenn die meisten Projekte noch ein „Beta“ in ihrer Versionsbezeichnung tragen. Den im Folgenden vorgestellten Softwarestack aus `bitcoind`, `lnd` und Zeus setzt die Schweizer Softwarefirma Puzzle

Bockbier aus der Blockchain

Wer auf GitHub im Projekt `puzzle/lightning-beer-tap` den Quellcode des Lightning-betriebenen Zapfhahns studiert, muss schon etwas genauer hinschauen. Schließlich stellt der Proof of Concept unter Beweis, wie wenig eigener Aufwand nötig ist, um aufbauend auf den im Hauptartikel beschriebenen Komponenten `bitcoind`, `lnd` und Zeus einen eigenen Point of Sale (PoS) einzurichten (Abbildung 5). Eine in Java geschriebene Applikation, die `websocket_bridge`, stellt die Webverbindung her zur generischen Selbstbedienungssoftware Zeus. Das Frontend für den Käufer präsentiert ein im Kioskmodus laufender Chromium-Browser (Abbildung 6). Ein kurzes Python-Skript steuert GPIO-Pins für die Warenausgabe an.

Auch die Liste der benötigten Hardware bleibt überschaubar: ein Raspberry Pi samt Display- und Steuerrechner sowie etwas Elektronik zur Hardwareansteuerung. Aufwendigste Komponente ist ein per Magnetventil regelbarer Zapfhahn aus dem Schankanlagenfachhandel, über den sich die Getränkeausgabe automatisieren lässt. Das genügt für den eigenen Automaten, der gegen Bitcoin Biergläser füllt.

Natürlich taugt das einfache Grundprinzip auch für viele andere Produkte. Doch die gewählte Variante bringt die Vorzüge des Lightning-Networks besonders zur Geltung: Schließlich wollen durstige Kehlen ihr Bier, bevor es schal wird.



Ein mit Lightning betriebener Bierzapfhahn (Abb. 5)

Display des Lightning-Bierzapfhahns (Abb. 6)

ITC, der Brötchengeber der Autoren, sowohl intern als auch in Kundenprojekten ein.

Drei Softwarekomponenten

`bitcoind` (auch „Bitcoin Core“ genannt, siehe ix.de/ix1913132) bildet die Basis und das Bindeglied zur Bitcoin-Blockchain. Für den Einsatz von Lightning ist aktuell der Betrieb eines vollwertigen Bitcoin-Knotens notwendig, der neben der kompletten Blockchain einen Index über alle darin enthaltenen Transaktionen mitführt. Der Dienst benötigt dazu beim Start die Kommandozeilenoption `-txindex`. Das führt zu spürbaren Auswirkungen, denn die Blockchain, zusammen mit dem Index, verschlingt momentan rund 250 GByte an Speicherplatz auf der Festplatte. Entsprechend großzügig sollte auch die Netzanbindung ausgelegt sein. Immerhin: Der Dienst muss zwar permanent Transaktionen überprüfen, aktiv am Bitcoin-Minining beteiligt er sich aber nicht, sodass zumindest die Ressourcen von CPU und GPU geschont bleiben. In der Test- und Entwicklungsphase empfiehlt es sich, `bitcoind` zusätzlich mit der Option `-testnet` zu starten.

Der Dienst verwendet dann speziell gekennzeichnete Bitcoins ohne realen Gegenwert – Spielgeld sozusagen, das sogenannte Faucets für das Testnetz frei zur Verfügung stellen. Ohne die Option läuft der Dienst im Bitcoin `mainnet`, arbeitet also mit „echtem“ Geld.

Als `lnd` oder Lightning Network Daemon firmiert die in Go geschriebene Implementierung des Lightning-Netzwerk-Protokolls. Der Dienst ist zuständig für den Aufbau und Betrieb der Zahlungskanäle sowie die Abwicklung der effektiven Off-Chain-Zahlungen. Diese Funktionen werden entweder über die Kommandozeile oder eine als gRPC-API implementierte Standardschnittstelle angeboten.

Für die grafische Interaktion mit Lightning ist eine weitere Komponente erforderlich, die von den konkreten Anforderungen des jeweiligen Point of Sale abhängt. Puzzle ITC hat hierzu die eigene Lösung Zeus mit Java und Angular gebaut und frei veröffentlicht. Sie stellt eine Weboberfläche als Schnittstelle zum Lightning-Netzwerk bereit. Derzeit erlaubt sie zwei Formen des Zugriffs: als klassischer Webshop mit Warenkorb und anschließender Lightning-Bezahlung oder als Selbstbedienungsbildschirm, bei dem das Bezahlen eines angezeigten Codes direkt die Bestellung eines Produktes auslöst. Zur Buchführung über die Bestellungen benötigt Zeus zusätzlich eine klassische, SQL-fähige Datenbank wie PostgreSQL. Neben Zeus stehen Entwicklern zahlreiche alternative Möglichkeiten zur Verfügung, um Lightning als Bezahlsystem in die eigenen Angebote zu integrieren, vom Stand-alone-System über eher kuriose Anwendungen wie den Slack-Tipbot bis hin zum Plug-in für WooCommerce-Shops.

Auf der Benutzer- beziehungsweise Kundenseite ist auch heute noch die größte Herausforderung, eine Smartphone-App zu finden, die alle nötigen Komponenten einer Lightning-Geldbörse (Wallet) beinhaltet, ohne dafür auf Ressourcen Dritter oder einen eigenen Bitcoin-Knoten zurückzugreifen (Übersicht siehe ix.de/ix1913132). Für Apples iOS gibt es bis heute im App Store zwar einige der abhängigen Varianten, aber noch keine völlig eigenständige Lightning-Wallet für das produktive Bitcoin-Mainnet. Die für Android-Betriebssysteme erhältliche App Eclair ist derzeit die verbreitetste Lösung, um rasch mit dem Smartphone über das Lightning-Netzwerk bezahlen zu können. Wie ein Blick in die Entwicklerszene zeigt, wird bereits Ende 2019 die Situation jedoch voraussichtlich ganz anders aussehen, sodass sowohl für iOS als auch für Android mehrere Apps in den entsprechenden Stores verfügbar sein werden. Wer lediglich im Testnet experimentieren möchte, kann bereits heute

Quelle: Gugger/Kobras

Selbstbedienungsbildschirm bei Energy Kitchen in Bern (Abb. 7)

auf den großen Mobilplattformen zwischen mehreren Alternativen wählen.

Erfahrungen beim Betrieb eines Lightning-Point-of-Sale

Möglichst einfach transportable Wallets für das Smartphone sind deshalb entscheidend, weil Lightning-Zahlungen sich nicht auf Online-Stores beschränken, sondern auch als Alternative für herkömmliche Geschäfte in Betracht kommen. Um schon früh Erfahrungen mit der Technik zu sammeln, hat Puzzle ITC zusammen mit dem Gastronomie-Unternehmen Energy Kitchen im September 2018 in Bern ein Pilotprojekt gestartet. Bitcoin- und Lightning-Enthusiasten können die beliebtesten Produkte von Energy Kitchen wie Cappuccino oder Sandwiches direkt über das Lightning-Netzwerk bezahlen. Bestellt wird entweder über einen klassischen Webshop oder über den weltweit ersten Selbstbedienungsbildschirm, der direkt bei der Kaffeebar im traditionsreichen Berner Warenhaus Loeb aufgestellt ist (siehe Abbildung 7).

Das neuartige Bedienkonzept des Bildschirms ist nur dank der synchronen Abwicklung und Rückmeldung von Lightning-Zahlungen möglich. Ein Kunde scannt dazu den angezeigten, einmalig gültigen QR-Zahlungscode mit der Lightning-Wallet-App ein und bezahlt damit direkt das gewählte Produkt. Erkennt die Applikation die erfolgreich abgeschlossene Bezahlung, gibt sie dem Kunden ein zufällig generiertes Wortpaar auf dem Bildschirm aus. Mit diesem „Einmalkennwort" weist sich der Kunde dann in der Kaffeebar an der Theke aus und erhält daraufhin das bestellte Produkt. Die gesamte Transaktion läuft ohne Interaktion oder Berührung am Bildschirm und kann so anonym wie mit Bargeld durchgeführt werden.

Bei der Umsetzung des Projekts hatten interessanterweise die größten technischen Herausforderungen keinen direkten Zusammenhang mit dem Lightning-Netzwerk. Die größte Ausfall- und Fehlerquelle war bislang die kabellose Internetverbindung des Mini-Computers im Schaukasten sowie die des Druckers, der hinter der Theke die Bestellungen für das Barpersonal ausdruckt. Die effektive Abwicklung der Zahlungen über das Lightning-Netzwerk hingegen funktioniert in der Praxis reibungslos, sofern die verwendete Wallet auf dem Smartphone bereits einen Lightning-Zahlungskanal eingerichtet hat. Jedenfalls berichten Touristen aus aller Welt via Twitter über ihre erfolgreiche Benutzung des „World's first Self Order Point powered by the Bitcoin Lightning Network".

Im Backend ereignete sich der einzige nennenswerte Zwischenfall mit der `bitcoind`- und `lnd`-Software ganz zu Beginn des Projekts. Ein eigens eingerichteter nächtlicher Backup-Auftrag hat den Lightning-Knoten genau zum falschen Zeitpunkt gestoppt und damit beim Gegenüber eine einseitige Schließung des Zahlungskanals ausgelöst. Was es bedeutet, 1600 Blöcke (umgerechnet rund zwei Wochen) auf sein Bitcoin-Guthaben zu warten, konnte das Team so hautnah miterleben. Und hat seine Lehren daraus gezogen: Seither stoppt das nächtliche Backup die Software nicht mehr, sondern kopiert im laufenden Betrieb die Daten weg. Der Fehler in der `lnd`-Software, der überhaupt erst zu der unglücklichen Situation beim Stoppen der Applikation geführt hat, ist mittlerweile auch behoben.

Fazit

Etwas mehr als ein Jahr nach der ersten Lightning-Zahlung mit „echten" Mainnet-Bitcoins steckt die Technologie nicht mehr in den Kinderschuhen, ist aber auch noch nicht bereit für den Massenmarkt. Gerade in den letzten Monaten ist jedoch ein großes Wachstum erkennbar, getrieben durch neue Möglichkeiten, die sich durch echte Mikrozahlungen eröffnen, die synchron und innerhalb von Millisekunden durchgeführt werden können. Das Lightning-Netzwerk hat durchaus das Potenzial, aus Bitcoin die native Internetwährung zu machen, die sie aus Sicht vieler schon lange sein sollte. (js@ix.de)

Quellen

Softwarekomponenten für Lightning: ix.de/ix1913132

Oliver Gugger

ist Senior Software Engineer im Lightning-Team des Schweizer IT-Dienstleisters Puzzle ITC und aktiver Contributor im Lightning-Projekt.

Daniel Kobras

ist Principal Architect bei Puzzle ITC Deutschland.