Ungleiche Brüder

Wie viel Bitcoin in Facebooks Libra steckt

Der langersehnte Durchbruch der Kryptowährungen, die Revolution der Zahlungssysteme weltweit – an Vorschusslorbeeren wurde für Facebooks Entwurf der neuen digitalen Währung Libra nicht gespart. Wir zeigen, wo die Gemeinsamkeiten und Unterschiede zu Bitcoin liegen und was das für Nutzer bedeutet.

Von Mirko Dölle

Zusammen mit dem Like kommt das Geld: So könnte die Zukunft aussehen, wenn Facebooks Plan aufgeht, Libra als weltweit einheitliche digitale Währung einzuführen. Außer in China, wo Facebooks Dienste seit langem gesperrt sind. Allerdings ist es nicht Facebook allein, das hinter der neuen Währung steht, der Internet-Riese ist nur eins von knapp 30 Unternehmen [1].

Neben dem Libra-Projekt kündigte Facebook auch an, mit dem Tochterunternehmen Calibra ein eigenes Wallet für Libra zu entwickeln. Es soll in Facebooks Dienste wie Facebook Messenger und WhatsApp eingebunden werden. So werden die über zwei Milliarden Facebook-Nutzer zu potenziellen Nutzern des Libra.

Die Ankündigung einer eigenen digitalen Währung schlug hohe Wellen – sowohl in der Welt der Kryptowährungen als auch bei Regulatoren. Denn mit einer so gigantischen Nutzerbasis ist Libra ab Tag eins ein Konkurrent zu Bitcoin. Allerdings gibt es große Unterschiede zwischen Bitcoin und Libra.

Exclusiv-Club

Das fängt bei der Organisation an: Hinter Libra soll die Libra Association stehen, eine unabhängige gemeinnützige Organisation mit Sitz in Genf, an der neben Facebook auch MasterCard, Visa, PayPal, Spotify und Uber beteiligt sind. Am Ende sollen es bis zu 100 Firmen sein, die die Geschicke des Libra lenken – die Eintrittskarte für diesen exklusiven Club kostet 10 Millionen US-Dollar. Bitcoin hingegen ist lediglich ein Protokoll, Computer-Code, der von einem Unbekannten unter dem Pseudonym Satoshi Nakamoto geschrieben und veröffentlicht wurde.

Das Bitcoin-Protokoll ist öffentlich, jeder kann Bitcoin-Wallets implementieren, Nodes zur Validierung der Blockchain betreiben oder mit einem Miner Transaktionen verarbeiten. Es kann auch jeder Änderungen an Bitcoin vorschlagen oder kurzerhand selbst implementieren – übernimmt die Mehrheit der anderen sie, ist sie eingeführt.

Kurz gesagt ist Bitcoin ein offenes, weltumspannendes Netzwerk, an dem sich jeder beteiligen kann. Es gibt keine Zentrale und keinen Herrscher, Bitcoin ist ein dezentrales Netzwerk, das nicht abgeschaltet werden kann. Zwar gibt es Unternehmen, die ihr Geschäftsmodell in irgendeiner Art und Weise auf Bitcoin aufbauen oder daran anlehnen, etwa Exchanges oder Mining-Unternehmen, allerdings hängt die Existenz des Bitcoins nicht von irgendwelchen Unternehmen ab.

Bei Libra sieht die Sache etwas anders aus: Das Netzwerk steht ausschließlich den Mitgliedsunternehmen der Libra Association offen, nur sie validieren neue Transaktionen. Darüber hinaus sind die Mitglieder der Organisation bekannt. Diese Zentralisierung um die Association bringt Angriffspunkte mit sich. Regulatoren könnten Druck ausüben, gewisse Transaktionen zu zensieren, rückabzuwickeln, Konten einzufrieren oder gewisse Individuen gänzlich aus dem Netzwerk auszuschließen. Das ist bei dem dezen-

tralen Peer-to-Peer-Netzwerk von Bitcoin schlicht nicht möglich.

Ausgegrenzt

Durch die Aufnahmegebühr von 10 Millionen US-Dollar werden private Nutzer von vornherein davon ausgeschlossen, an der Entwicklung von Libra mitzuarbeiten. Das wirft auch einen Schlagschatten auf die Ankündigung, den Code von Libra unter einer Open-Source-Lizenz veröffentlichen zu wollen: Änderungen werden nur übernommen, wenn sie von den Mitgliedern der Libra Association eingereicht und verabschiedet werden. Immerhin sehen Facebooks Pläne vor, das Netzwerk nach etwa fünf Jahren komplett zu öffnen.

Der Unterschied zwischen einem offenen und einem geschlossenen Netzwerk hat weitreichende Konsequenzen für die Sicherheit und Verlässlichkeit von Transaktionen. Da Bitcoin offen ist und jeder mitmischen kann, muss das Protokoll auch berücksichtigen, dass sich Teilnehmer untereinander nicht vertrauen oder gar gegeneinander arbeiten. Satoshi Nakamoto löste das Problem unter anderem durch die Einführung eines dynamischen Proof-of-Work-Algorithmus, der seit nunmehr zehn Jahren dafür sorgt, dass niemand abgeschlossene Transaktionen manipulieren kann.

Im Bitcoin-Netzwerk arbeiten Clients, Nodes und Miner zusammen: Die Clients schicken Transaktionen an die Miner, die diese zunächst im Memory Pool (kurz: Mempool) sammeln und nach und nach zu Blöcken verarbeiten. Die Schwierigkeit besteht darin, die Daten des Blocks so anzuordnen, dass sein Hash-Wert einen sich verändernden Schwierigkeitsgrad erfüllt – die sogenannte Difficulty. Da sich Hash-Werte nicht vorhersagen lassen, muss der Miner die Daten des Blocks auf gut Glück neu anordnen und erneut den Hash berechnen – so lange, bis der Block die Anforderungen erfüllt. Dabei wird der Schwierigkeitsgrad alle zwei Wochen so angepasst, dass statistisch gesehen weltweit nur alle 10 Minuten jemand das Glück hat, einen neuen Block zu finden.

Wenn ein Miner einen gültigen Hash für seinen Block gefunden hat, sendet er ihn an einen oder mehrere Nodes. Ergibt die Prüfung des Nodes, dass der Block tatsächlich gültig ist, verteilt er ihn an andere Nodes und schließlich an die Clients weiter – die Blockchain ist um einen Block gewachsen und die Suche nach dem nächsten Block beginnt von Neuem. Wichtig hierbei ist, dass die einzelnen Miner und Nodes niemand anderem im Netzwerk vertrauen, sondern stets selbst verifizieren, dass nur gültige Blöcke an die Blockchain angehängt werden.

Proof of Stake

Im Gegensatz dazu steht das Modell von Libra. Der hier eingesetzte Konsens-Algorithmus heißt LibraBFT und ist eine Variation des Proof of Stake. Beim Proof of Stake muss keine Energie für das Errechnen gültiger Hashes aufgewendet werden. Stattdessen setzen die Validatoren ihre Beteiligung an der Digitalwährung als Garantie für die Gültigkeit der bestätigten Transaktionen ein.

Der Unterschied im Konsensmechanismus führt auch zu unterschiedlichen Datenstrukturen. Mit der von Bitcoin bekannten Blockchain, die lediglich Transaktionen enthält, hat die im Libra-Protokoll beschriebene Datenstruktur nichts zu tun: Libra nutzt sogenannte States, die den aktuellen Kontostand des Netzwerks wiedergeben. Transaktionen hingegen werden in einem separaten Archiv gespeichert. Die Mitglieder der Libra Association wechseln sich gegenseitig mit dem Validieren von Transaktionen ab, sie verlassen sich aufeinander und stehen nicht im Wettbewerb.

Das Libra-Modell der States, also quasi der Kontostände, steht in deutlichem Kontrast zum UTXO-Modell (Unspent Transaction Outputs) von Bitcoin. Ein Unspent Transaction Output ist, wie der Name andeutet, das Ergebnis einer Transaktion, das noch nicht erneut ausgegeben wurde. Zudem wird eine Bitcoin-Adresse üblicherweise nur für eine einzige Transaktion genutzt, und da die Adressen keine Informationen über den Besitzer enthalten, kann ein Außenstehender nicht ohne Weiteres feststellen, wie viel Geld jemand besitzt oder wofür er es ausgegeben hat.

Dieser Unterschied hat auch Auswirkungen auf die Wallet-Anwendungen. Während ein Libra-Wallet lediglich den aktuellsten Datenblock mit den Kontoständen benötigt, muss ein Bitcoin-Wallet erst die komplette Blockchain von Anbeginn an durchforsten, um festzustellen, wie viel Geld auf den unterschiedlichen Adressen eines Wallets lagert.

Anonym wird Libra nicht sein: Die Wallet-Anwendung Calibra, die die gleichnamige Facebook-Tochter entwickelt, soll einen KYC-Prozess („Know Your Customer“) enthalten. Das bedeutet, dass sich Nutzer mit ihrem amtlichen Ausweis identifizieren müssen, bevor sie das Wallet nutzen können. Eines der Ziele der Libra Association ist außerdem, „einen offenen Identitätsstandard zu entwickeln“, denn „eine dezentralisierte und portable digitale Identität“ sei eine Grundvoraussetzung für finanzielle Inklusion und Wettbewerb.

Das bedeutet jedoch, dass sich sämtliche Transaktionen den daran beteiligten Personen zuordnen lassen, weltweit – der Libra-Nutzer wird also gläsern. Ob es eine gute Idee ist, einer Facebook-Tochter wie Calibra derart intime Daten anzuvertrauen und „nach Zustimmung“ an Dritte weitergeben zu lassen, darf man angesichts Facebooks Umgang mit vertraulichen Benutzerdaten in der Vergangenheit bezweifeln. Immerhin soll Facebook keinen Zugriff auf Transaktionsdaten und umgekehrt Calibra keinen Zugriff auf Facebook-Nutzerdaten haben.

Vielversprechend

Trotz allem hat Libra das Zeug, um künftig Bitcoin als wichtigste digitale Währung abzulösen. Mit Facebook und den Kreditkartenunternehmen im Rücken ist Libra quasi zum Erfolg verdammt. Libra wird Bitcoin wohl aber nicht ersetzen, mit Identifizierungszwang und leicht regulierbarer Struktur hat Libra nichts von der freien, unabhängigen, unregulierbaren Währung, die Satoshi Nakamoto bei der Entwicklung von Bitcoin vorschwebte. *(mid@ct.de)* c't

Literatur

[1] Hartmut Giesen, Schöne neue Weltwährung, Was Facebooks Kryptogeld Libra für Banken und Milliarden Nutzer bedeutet, c't 15/2019, S. 32