Zerteilen, um zu herrschen

Schmutziger Machtkampf gefährdet Bitcoin-Cash-Guthaben

Die Kryptowährung Bitcoin Cash hat einen weiteren Hard Fork durchgeführt. Doch diesmal konnten sich die Entwickler auf gar nichts einigen, dringend notwendige Schutzmaßnahmen blieben auf der Strecke. Deshalb müssen die Nutzer selbst aktiv werden, um ihr Geld zu schützen.

Von Mirko Dölle

Ein Showdown wie im wilden Westen ist wahrscheinlich die beste Analogie, mit der sich der Streit und Machtkampf unter den Bitcoin-Cash-Entwicklern vergleichen lässt. Am Ende bekämpften sich die Kontrahenten bis aufs Blut. Dabei hatte man sich gerade ein Jahr zuvor zusammengerauft.

Es geraten auch Unbeteiligte in Gefahr, nämlich die Bitcoin-Cash-Besitzer: Da keine Seite der anderen entgegengekommen ist, fehlen die sonst bei Hard Forks üblichen Schutzmaßnahmen. Diese verhindern normalerweise, dass Transaktionen doppelt ausgeführt werden können. Bitcoin-Cash-Besitzer müssen deshalb ihr Geld zunächst in Sicherheit bringen, bevor sie die Kryptowährung wieder nutzen können (Details dazu im Kasten „Schutzmaßnahmen“).

Im Grunde geht es um einen Streit zwischen zwei Entwicklergruppen, die mit aller Macht und ohne Rücksicht auf Verluste jeweils ihre eigenen Ideen durchsetzen wollen und die des anderen Lagers vollumfänglich ablehnen. Dabei wären die Neuerungen sogar weitestgehend miteinander kompatibel, könnten also gleichzeitig umgesetzt werden.

Anlass für den Streit ist der am 15. November durchgeführte Hard Fork von Bitcoin Cash, mit dem die Spielregeln der Kryptowährung erneut verändert werden. Diese Änderungen sind so grundlegend, dass ältere Bitcoin-Cash-Clients und -Miner die neuen Blöcke der Blockchain ablehnen würden, weil sie gegen das alte Bitcoin-Cash-Protokoll verstoßen.

In Fachkreisen werden solche Änderungen, die zu früheren Protokollen inkompatibel sind und bei der sämtliche Teilnehmer die Software ihrer Clients, der Knoten und der Miner austauschen müssen, als Hard Fork bezeichnet. Die Entwickler nutzen Hard Forks dazu, um teils radikale Neuerungen in eine bestehende Kryptowährung einzufügen.

Abgespalten

Genau auf diese Weise entstand am 1. August 2017 Bitcoin Cash aus Bitcoin. Bereits im November 2017 sowie im Mai 2018 erfolgten die nächsten Hard Forks von Bitcoin Cash. Auch hierbei entstanden im Prinzip neue Kryptowährungen. Weil sich Entwickler und Miner einig waren und alle auf die neuen Regeln umstiegen, gab es einen nahtlosen Übergang, weshalb man den Namen der Kryptowährung beibehalten konnte.

Bei dem Hard Fork am 15. November 2018 konnte man sich jedoch nicht einigen: Während die Entwickler von Bitcoin ABC (abgekürzt BCHABC) die Kryptowährung für Smart Contracts weiter öffnen wollen, verfechten die Widersacher vorgeblich die Visionen des mutmaßlichen Bitcoin-Erfinders Satoshi Nakamoto – und nennen ihre Initiative Bitcoin SV („Satoshi’s Vision“, kurz BCHSV). Tatsächlich behauptet einer der Bitcoin-SV-Entwickler sogar, der geheimnisvolle Satoshi zu sein.

Die Rede ist von Craig Wright, dem Chef-Entwickler des Blockchain-Unternehmens nChain. Dieser hatte bereits im Mai 2016 behauptet, unter dem Pseudonym Satoshi Nakamoto die heute bekannteste Kryptowährung entwickelt zu haben. Einen Beweis dafür blieb er bislang schuldig, allerdings war eine Mobilfunknummer, die in einer angeblich von Satoshi stammenden E-Mail auftauchte, auf Wright gemeldet.

Wright hat sich zum Verfechter von Satoshis Idee ernannt und will mit Bitcoin Cash den wahren Bitcoin wiederauferstehen lassen. Dazu hat er bereits im Mai-Fork etliche mathematische Operationen (OP-Codes) wieder eingeführt, die bei Bitcoin im Rahmen von abwärtskompatiblen Soft

Forks vor Jahren abgeschaltet wurden. Mit dem Hard Fork vom 15. November wurden weitere OP-Codes der frühen Bitcoin-Protokolle bei Bitcoin SV wiederbelebt.

Dem Ansinnen der ABC-Entwickler, Bitcoin Cash durch Einführung eines neuen OP-Codes um externe Smart Contracts zu erweitern und künftig eine andere Reihenfolge der Transaktionen in den Blöcken zu verwenden, erteilte Wright eine drastische Absage: „They are not adding this to BCH." Er beschuldigte die ABC-Entwickler sowie den Kryptowährungsexperten und -Mining-Pool-Besitzer Roger Ver von Bitcoin.com sogar, mit ihrem Vorschlag Kinderpornografie und Drogenhandel zu unterstützen: „If (...) devs want to make permissionless kiddie porn sites and Silk Road Version 2.0 they can piss off to Dash (...) This is the only real use case they have."

»Du bist mein Feind. Ich bin Satoshi. Du wirst jetzt erleben, wie es ist, wenn ich angepisst bin.«

Craig Wright

Roger Ver veröffentlichte außerdem eine E-Mail, die er von Wright erhalten haben will, in der dieser ihn und die ABC-Gemeinde als seine Feinde bezeichnet – und unverhohlen damit drohte, dass er Satoshi sei und sie nun erleben würden, was es bedeutet, wenn er angepisst sei: „Side with ABC, you hate Bitcoin, you are my enemy. You have fucking no idea what that means. You will. I am Satoshi (...) You will now discover me when pissed off."

Wright drohte außerdem damit, den Handel mit Bitcoin Cash für Jahre vollständig lahmzulegen: „If you want a war ... I will do 2 years of no trade. Nothing. In the war, no coin can trade."

Angriff auf ABC

Dazu wollte Wright große Mining-Pools leere Blöcke ohne Transaktionen erzeugen lassen und so den Handel mit Bitcoin ABC torpedieren. Das war keineswegs eine leere Drohung, denn mit den Mining-Pools Bitcoin-SV und Coingeek gehörten knapp 60 Prozent der gesamten Hash-Leistung des Bitcoin-Cash-Netzes vor dem Fork dem SV-Lager an, und Craig soll Insidern zufolge weitere Kapazitäten angemietet haben. Auch erhielten etliche Mining-Pool-Betreiber in aller Welt Besuch von nChain – um über die Vorzüge des Wechsels in das SV-Lager informiert zu werden.

Bekanntermaßen genügen bereits 51 Prozent Hash-Leistung, um die Kryptowährung nach Belieben zu kontrollieren [1]. Sollte das SV-Lager schneller eine Kette leerer Blöcke auf der ABC-Blockchain erzeugen können als der Rest der ABC-Miner Blöcke mit Transaktionen, würden immer wieder die mit Transaktionen bestückten Blöcke absterben – und die Transaktionen wären nie geschehen.

Trotz der vermeintlichen Übermacht der SV-Fraktion scheint aber das ABC-Lager als Sieger aus dem Streit hervorzugehen, zu dessen prominenten Mitgliedern neben Mining-Pool-Betreiber Bitcoin.com auch der Miner-Hersteller Bitmain zählt. Insider berichten, dass Bitmain einen Pool von 90.000 AntMiner S9 in der Hinterhand hält, die jederzeit Bitcoin Cash minen könnten, um dem ABC-Lager notfalls die Mehrheit der Hash-Leistung zu sichern.

Der Fork von Bitcoin ABC und Bitcoin SV fand nach Block Nummer 556766 statt; es war Bitcoin.com aus dem ABC-Lager, das den Block des neuen ABC-Zweigs fand. Kurze Zeit später fand Mempool den ersten Block des SV-Zweigs, womit beide Währungen ihren Fork erfolgreich abschlossen. Seitdem ist Bitcoin SV im Rückstand, bei Redaktionsschluss knapp 24 Stunden nach dem Fork war die Bitcoin-ABC-Blockchain rund 50 Blöcke länger als die Bitcoin-SV-Blockchain.

Bitcoin ABC zum Sieger und neuen Bitcoin Cash zu erklären wäre aber verfrüht: Die SV-Miner könnten eine mit leeren Blöcken ausgestattete Blockchain noch nach Tagen und Wochen veröffentlichen und so den bisher gültigen Zweig der ABC-Blockchain absterben lassen. Doch je länger dies nicht passiert, desto unwahrscheinlicher wird dieses Szenario. Schließlich kostet der Betrieb eines Schatten-Miner-Netzes, das heimlich eine leere Blockchain erzeugt, viel Geld.

(mid@ct.de) c't

Literatur

[1] Mirko Dölle, Kettenreaktion, Wie 51-Prozent-Angriffe Bitcoin & Co. bedrohen, c't 14/2018, S. 26

Schutzmaßnahmen

Durch den am 15. November erfolgten Fork erhielt jeder, ähnlich wie bei einem Aktiensplit, für seine Bitcoin Cash (BCH) den gleichen Betrag Bitcoin ABC (BCHABC) sowie zusätzlich den gleichen Betrag Bitcoin SV (BCHSV). Da es keinen Replay-Schutz zwischen den beiden neuen Bitcoin-Cash-Varianten gibt, kann eine mit Bitcoin ABC ausgeführte Überweisung von jedermann dupliziert und mit Bitcoin SV wiederholt werden.

So könnte sich ein Empfänger ungerechtfertigt bereichern, indem er nicht nur die vereinbarten Bitcoin ABC für eine Leistung erhält, sondern sich zusätzlich die Bitcoin SV unter den Nagel reißt. Damit das nicht passieren kann, muss man sein Bitcoin-Cash-Vermögen auf zwei neue Wallets aufteilen, bevor man Bitcoin Cash an jemand anderen transferiert.

Wer bisher den von Bitcoin Core abgeleiteten offiziellen Bitcoin-Cash-Client verwendet hat, installiert zunächst die beiden Client-Programme von bitcoinabc.org respektive github.com/bitcoin-sv und erzeugt in den Programmen jeweils ein neues Wallet – eins für Bitcoin ABC und eins für Bitcoin SV. Öffnen Sie dann eine Kopie Ihres alten Wallets in den beiden Clients und überweisen Sie das gesamte Guthaben mit dem ABC-Client an eine Adresse des neuen ABC-Wallets. Danach überweisen Sie das gesamte Guthaben Ihres alten Wallets mit dem SV-Client an eine Adresse des neuen SV-Wallets. Ist das Guthaben nach einigen Tagen noch immer auf den beiden Wallets verbucht, ist Ihr Geld sicher vor Replay-Angriffen. Bewahren Sie ihr altes Wallet dennoch gut auf – für den Fall, dass es einen größeren Rollback in der Blockchain geben sollte.

Nutzer von Electron Cash benötigen die Coin-Splitter-Version des Clients von Mark Blundberg, die auf electoncash.org verlinkt ist. Die Anleitung, wie Sie Ihre Coins sichern, finden Sie auf der Download-Seite bei GitHub verlinkt.