BIP 361 - "alte" Bitcoins markieren

Erfasst am : 23. April 2026 10:17 | Erfasst von : Martin
Verknüpfte Kategorie(n): Beobachtungen, Bitcoin

Derzeit macht das BIP (Bitcoin Improvement Proposal) 361 die Runde. Darin geht es darum, was man im Advent des Quantencomputers (QC) an Vorsichtsmassnahmen treffen solle für all die nicht ausgegebenen Bitcoins (UTXOs), die für ewig in der Blockchain mit ihrem Public Key drin stehen.

Die Gefahr besteht, dass die QCs diese Paarung von zwei zusammengehörenden Dingern wie eben Public und Private Keys aufgrund der bipolaren Struktur unseres Universums gerade mit Hilfe der Bausteine dieses Universums, der Quanten, einander zugeordnet werden können in der Zukunft.

Denn es ist einfach ein bisher algorithmisch unlösbares (oder seeeeehr schwieriges) Problem, das die Mathematik uns stellt. Es ist ja keine Hexerei, die Publik Key Verschlüsselungen, es ist nur mathematisch schwierig, einen Rückweg zu finden.

Ich habe darüber schon oft geschrieben. Und daher verlinke ich auch wieder gern auf den Florian Bruce, der diese Meldungen bezüglich Googles QCs Hack sehr gut einordnete.

Zur möglichen Fähigkeit der QCs dieses Video von Veritasium. Alles nur einfache Mathe :-)

Also, nun zum BIP 361. Die Grundidee ist, dass man "alte" und bisher nicht bewegte Bitcoins irgendwie speziell behandeln soll.

WIESO?

Wir erklären und predigen seit Jahren, dass Bitcoin die höchste Anforderung an die eigene Verantwortung darstellt: Not your keys, not your coins. Also: Sicherung des Seeds, Selbstverwahrung, Vererbung etc. KEINER kann irgendeinem Bitcoin-Holder dreinreden. Wie auch, denn nur derjenige, der den Private Key hat, kann sich gegenüber dem Bitcoin-Protokoll als Handlungsberechtigter ausweisen. Weil er den zum Public Key gehörenden Private Key einsetzen kann.

Wo ist das Problem?

Es gibt im Bitcoin Protokoll halt verschiedene Adressformate, die in einer Transaktion ja sichtbar sein müssen, damit jeder Knoten im Bitcoin-Netzwerk die Gültigkeit einer Transaktion unabhängig validieren kann.

Über die Zeit hinweg haben sich da einige Versionen etabliert, darunter eine, die den Public Key im Klartext in der Transaktion festhält (Abkürzung P2PK = Pay To Public Key). Also für ewig. Solange dieser Bitcoin nicht bewegt wird, kann ihn eigentlich jeder abstauben, der den Private Key findet, der zum veröffentlichten Public Key passt. Und das ist nun das "Problem". Leute mit einem künftigen QC können sich eventuell diese Bitcoins abholen, weil der QC den Private Key errechnen kann aus dem Public Key.

Deshalb nennt man sie "alte" Adressen, weil man sie schon seit über 10 Jahren

nicht mehr braucht. Es gibt Adressformate, die bei einem UTXO den Public Keys nicht in der Blockchain verewigen. Dass ein Public Key in einer Transaktion aber bei dessen Ausgeben veröffentlicht wird, ist klar, denn jeder Bitcoin-Teilnehmer muss ja völlig autonom die Gültigkeit der Transaktion validieren können.

Gibt also jemand seinen BTC aus, kommt der Public Key spätestens dann in die Blockchain. Für wie lange hätte ein QC-Owner nun die Chance, diese Transaktion zu behändigen, manipulieren, sich zuzuschanzen? Tja, bis der nächste Block gefunden wird, also die bekannten ca. 10 Minuten.

IN DER ZEIT SIND ALLE TRANSAKTIONEN VERLETZLICH! Die Sicherungen sind seit jeher nur: Mathematik und Zeit.

Wer Public Key Verschlüsselung nachhaltig schneller als in 10 Minuten knacken kann, hat Bitcoin gekillt - und wohl Hunderttausende von anderen Systemen, inkl. HTTPS etc. auch.

Wem das unklar ist: Eine Verschlüsselung hat nur die Aufgabe, Information nur demjenigen zu enthüllen, der den passenden Schlüssel hat. Für alle anderen soll der Aufwand und die Zeit so gross sein, dass es sich weder ökonomisch noch zeitlich lohnt, die Verschlüsselung zu knacken. Wenn nach 10 Milliarden Universumsaltern etwas endlich geknackt werden könnte, ist das wohl für den Verschlüsseler wie den Cracker irrelevant ...

Und bei Bitcoin wird es noch schwieriger: Sobald die erste Bestätigung da ist, muss der Cracker auch noch schneller minen als all die anderen, damit sein Hack nicht erkannt, beanstandet würde.

Also an sich wirklich kein Problem. Sicher nicht für Bitcoin, das Protokoll. Für wenn denn sonst? Klar, die 1 Millionen Bitcoins, die Nakamoto zugeordnet sind, wären ein lukratives Ziel für QC-Besitzer. Aber das sind sie schon immer gewesen, denn man kann ja mit Brute Force probieren, alle möglichen Private Keys auszuprobieren. Allerdings ist das - bis auf den sprichwörtlichen Glückstreffer - ein (fast) absolut sinnloses Unterfangen (etwas Rechnerei dazu).

Gegeben, dass die QCs nun also einen realistisch ausreichend schnellen Weg finden, Bitcoins zu rauben. Was soll dann mit den 1 MBTC passieren? Tja, dann werden sie halt geraubt, verkauft, verhökert, verbrannt.

Das stört das Bitcoin-Protokoll überhaupt nicht. Es stört nur diejenigen, die das FIAT-Spiel machen, NGU (Numbers Go Up), weil das Angebot zu erhöhen in Bitcoin würde temporär dessen FIAT Aufwiegung etwas drücken - sprich, er wird billiger. Was sonst noch? Na, der, dem sie bisher gehörten, sind sie halt gestohlen - er hat sie nicht mehr. Das ist alles. Es gilt immer noch 1 BTC = 1 BTC.

Was bedeutete es jedoch, wenn wir solche BTCs anders behandeln? Und mit welcher Rechtfertigung? Weil wir nicht wissen, ob der Inhaber jener Coins noch am Leben ist und seinen Private Key einsetzen könnte? Na, von denen gibt es auch ohne Nakamoto eh schon genug. All die, die ihr Wallet respektive Seed verloren, geschrottet, gelöscht, vergessen haben. Alle diese spendeten ihre BTCs dem Netzwerk bzw. belasten es, weil diese Transaktionen immer mitgetragen werden müssen, da sie zur Validierung ja nötig sind (dazu gibt es auch Optimierungen).

Also, wenn Nakamoto noch lebt (ist ja erst 17 Jahre her, das mit Bitcoins

Geburt), was ist denn schlimm, denn dem die BTC geklaut werden? Wer denn besser als genau er weiss, dass er diese BTC in näherer Zukunft mal bewegen müsste, auf eine QC-sichere Adresse?

Und wenn er/sie/es das nicht macht, wieso sollen andere sich darum kümmern? Wir wollen ja gerade die absolute Selbstverantwortung. Bisher sind diese BTCs eben unbewegt, aber beobachtet. Das Signal einer Bewegung dieser BTCs wäre nur, er/sie/es lebt oder hat seinen/ihren Private Key weitergegeben - oder eben, sie sind gestolen.

Wen also bitte soll das interessieren? Wenn das Bitcoin-Protokoll nur einen einzigen Pfifferling wert sein soll, dann darf diese Bewegung nichts aussergewöhnliches veranstalten.

Anders gesagt: Es ist scheissegal, ob diese BTCs geklaut werden. Denn: Wenn er/sie/es sich um die Sicherheit jener BTCs kümmen will, können diese BTCs in 10 Minuten auf ein neue, QC-sicheres Adressformat transferiert werden. Punkt.

Jegliches Blockieren, Timeboxen, Verlangsamen, Deckeln, Verbrennen, Ossifizieren einer Transaktion ... durch Fremdeinfluss(!) ... gehört nicht ins Mindset eines Bitcoiners.

Wer Nakamoto ist, bleibt auch dann ein Geheimnis, wenn seine BTCs verschoben werden. Die Welt weiss dann nur: Hoppla, Nakamoto lebt noch. Nett. Zurück zum Bau (Business as usual).

Also: Nein zum BIP 361.