RUBIKON

Mittwoch, 01. Juni 2022, 16:00 Uhr
~8 Minuten Lesezeit

Die Krypto-Falle

Anonymität und monetäre Freiheit erhoffen sich viele Menschen von Kryptowährungen, doch die NSA forschte bereits vor Jahrzehnten zu dieser Technik.

von Birgit Naujeck
Foto: Maksim Shmeljov/Shutterstock.com

Entspricht es der Realität, dass der Bitcoin beziehungsweise die zugrundeliegende Blockchain-Technologie von dem Pseudonym Satoshi Nakamoto (Satoshi bedeutet unter anderem erleuchtet, weise oder intelligent; Nakamoto kann man mit Mitte, Basis, Wurzel oder zentral übersetzen; übersetzt als "Zentrale Intelligenz" Englisch: Central Intelligence) entwickelt wurde? Ja, wenn wir davon absehen, dass es sich um keinen Menschen, sondern eine Organisation handelt! Ist es richtig, dass die durch eine Geheimdienstorganisation entwickelte Technologie dann an Gavin (Bell) Andresen übergeben, gar

verschenkt wurde? Ja! Er ist nunmehr das öffentliche Gesicht hinter Bitcoin. Manche haben im Laufe der Zeit die Frage gestellt, warum Bitcoin die SHA-256 Hash Function benutzt, die von der NSA entwickelt und vom National Institute for Standards and Technology (NIST) veröffentlicht wurde. Falls — und wir können davon ausgehen, dass — SHA-256 versteckte Hintertüren enthält, wäre jegliche Anonymität und vor allem die Sicherheit von Bitcoin-Zahlungen dahin.

Während einige sagen werden, dass der folgende Artikel etwas spekulativ ist — wie spekulativ ist Bitcoin selbst, wenn Leute ihre Häuser verpfänden, um es zu kaufen? Wenn viele Menschen im Zeitalter der orchestrierten Entdollarisierung den sicher geglaubten Anlage-Hafen Kryptowährung, insbesondere Bitcoin, ansteuern, um vielleicht in naher Zukunft feststellen zu müssen, dass die Technologie durch die Central Bank Digital Currency (CBDC) unter Leitung der Bank für Internationalen Zahlungsausgleich (BIZ) komplett ausgeschaltet wird.

Vor mehr als 25 Jahren hat die National Security Agency (NSA, Nachrichtendienst der Vereinigten Staaten) ein wichtiges Dokument über Kryptowährungen verfasst — allein das ist Alarm genug, dass die Dinge nicht so sind, wie sie scheinen.

Davon ausgehend, dass das Darknet, die Blockchain-Technologie, der Bitcoin nicht durch weltverbessernde Nerds erfunden, entwickelt, programmiert wurden und außerhalb der Reichweite des Tiefen Staates ihr Eigenleben führen, sondern dass es sich hierbei um ein Projekt, ein Experiment, durchgeführt vom Tiefen

Staat, handelt, können wir heute sagen:

> ***Es geht beim Bitcoin darum, die Öffentlichkeit mit der digitalen Währung vertraut zu machen.***

Sobald diese etabliert ist, werden die Fiat-Währungen der Welt in einem künstlich herbeigeführten Schuldenkollaps ausgelöscht und dann durch eine von der Regierung genehmigte Kryptowährung ersetzt, wobei alle Transaktionen und digitalen Geldbörsen von den westlichen Regierungen der Welt verfolgt werden.

1996 — die Basis für die Bitcoin-Erschaffung wird veröffentlicht

Welche Beweise gibt es für diese Vorstellung? Werfen wir zunächst einen Blick auf dieses **Dokument** (https://groups.csail.mit.edu/mac/classes/6.805/articles/money/nsamint/nsamint.htm) mit dem Titel „How to Make a Mint: The Cryptography of Anonymous Electronic Cash“. Dieses Dokument, das vor mehr als fünfundzwanzig Jahren veröffentlicht wurde, beschreibt die allgemeine Struktur und Funktion der Kryptowährung Bitcoin. Wie wir der Schlussfolgerung (conclusion) entnehmen können, ist bereits 1996 von einem verschlüsselten Mechanismus der Rückverfolgbarkeit die Rede. Aber auch:

„Weil es so einfach ist, die exakte Kopie einer elektronischen Münze anzufertigen, muss ein sicheres elektronisches Cash-System die Fähigkeit besitzen, das mehrfache Bezahlen mit ein und derselben Münze zu verhindern. Wenn das System online implementiert ist, dann kann das mehrfache Bezahlen verhindert werden, indem eine Datenbank mit bereits gezahlten Münzen gepflegt wird und indem diese Liste mit jeder Zahlung abgeglichen wird.Die Anzahl an Transfers pro Münze muss begrenzt werden. Münzen können teilbar

gemacht werden, ohne dass dabei irgendwelche Sicherheits- oder Anonymitäts-Features eingebüßt werden. Dies geht aber zu Lasten von Speicherkapazität und Transaktionsdauern.“

> ***Mit anderen Worten, die NSA hat in ihrem Dokument Schlüsselelemente von Bitcoin beschrieben, lange bevor Bitcoin überhaupt existierte.***

Ein Großteil des Bitcoin-Protokolls wird in diesem Dokument detailliert beschrieben, einschließlich der Techniken zur Authentifizierung von Unterschriften, der Eliminierung von Krypto-Coin-Fälschungen durch Transaktionsauthentifizierung und mehrerer Funktionen, die die Anonymität und Unverfolgbarkeit von Transaktionen unterstützen. In dem Dokument wird sogar auf das erhöhte Risiko der Geldwäsche hingewiesen, das mit Kryptowährungen leicht zu bewältigen ist. Es beschreibt auch „sicheres Hashing“ als „einseitig und kollisionsfrei“.

Obwohl Bitcoin diese Struktur um Mining und ein gemeinsames Peer-to-Peer-Blockchain-Transaktionsauthentifizierungssystem erweitert, ist es klar, dass die NSA Kryptowährungen erforschte, lange bevor gewöhnliche Nutzer jemals von diesem Begriff gehört hatten.

Die NSA schrieb auch den Krypto-Hash, der von Bitcoin zur Sicherung aller Transaktionen verwendet wird: **SHA-256-Hash** (https://de.bitcoinwiki.org/wiki/SHA-256), von dem jede Bitcoin-Transaktion auf der Welt abhängt.

Wie *The Hacker News* (THN) **erklärt** (https://thehackernews.com/2013/09/NSA-backdoor-bitcoin-encryption-sha256-snowden.html):

„*Die Integrität von Bitcoin hängt von einer Hash-Funktion namens SHA-256 ab, die von der NSA entwickelt und vom National Institute*

for Standards and Technology (NIST) veröffentlicht wurde.“

THN fügt außerdem hinzu: „Wenn man davon ausgeht, dass die NSA etwas mit SHA-256 gemacht hat, was noch kein Forscher von außen entdeckt hat, dann wäre sie in der Lage, mit glaubwürdigen und nachweisbaren Maßnahmen Transaktionen zu fälschen. Die wirklich beängstigende Sache ist, dass jemand einen Weg findet, Kollisionen in SHA-256 wirklich schnell zu finden, ohne es zu erzwingen oder viel Hardware zu verwenden, und dann die Kontrolle über das Netzwerk zu übernehmen“, sagte der Kryptografieforscher Matthew D. Green von der Johns Hopkins University.

Mit anderen Worten, wenn der SHA-256-Hash, der von der NSA entwickelt wurde, tatsächlich eine Hintertür zum Knacken der Verschlüsselung hat, würde das bedeuten, dass die NSA die Bitcoins von allen stehlen könnte, wann immer sie will. Oder wurde der Bitcoin von Anfang an als Werkzeug entwickelt, um die Kontrolle über die Geldversorgung der Welt zu behalten, also die Kontrolle über die weltweite Geldmenge zu erlangen, während unser bekanntes Fiat-Währungssystem zusammenbricht und durch eine von den Eliten kontrollierte digitale Währung ersetzt wird?

> ***Wer glaubt heute noch, dass Kryptografie kugelsicher ist?***

Dazu THN in dem **Artikel** (https://thehackernews.com/2017/07/gnupg-libgcrypt-rsa-encryption.html) „Researchers Crack 1024-bit RSA Encryption in GnuPG Crypto Library“:

„Der Angriff ermöglicht es einem Angreifer, den geheimen Krypto-Schlüssel aus einem System zu extrahieren, indem er das Muster der Speichernutzung oder die elektromagnetischen Ausgaben des Geräts analysiert, die während des Entschlüsselungsprozesses abgegeben werden.“

Wichtig ist, dass es sich um ein 1024-Bit-Verschlüsselungssystem handelt. Die gleiche Technik soll auch in der Lage sein, eine 2048-Bit-Verschlüsselung zu knacken. In der Tat werden Verschlüsselungsschichten täglich von cleveren Hackern geknackt. Einige dieser Verschlüsselungsschichten werden derzeit für verschiedene Kryptowährungen verwendet. Solange man kein hochqualifizierter Mathematiker ist, kann man nicht mit Sicherheit sagen, ob eine Kryptowährung wirklich nicht gehackt werden kann.

Tatsächlich wird jede Kryptowährung mit der Erfindung von Quantencomputern im großen Maßstab obsolet. Sobald es einem Land, einer Organisation oder einem Menschen gelingt, einen funktionierenden 256-Bit-Quantencomputer zu bauen, können sie effektiv alle Bitcoins der Welt und darüber hinaus die meisten Staatsgeheimnisse stehlen und andere globale Gräueltaten nach Belieben begehen.

Ein möglicher Plan der Mächtigen, die totale Kontrolle über die Geldmenge, die Ersparnisse, die Besteuerung und die Finanztransaktionen der Welt zu übernehmen und die Menschheit somit zu steuern, steht meines Erachtens bereits vor der Vollendung:

1. den von der NSA geschaffenen Bitcoin auf den Markt bringen, um die Öffentlichkeit für eine digitale Währung zu begeistern;
2. in aller Stille eine von den Globalisten kontrollierte Kryptowährung vorbereiten, die dessen Platz einnehmen soll — die Bank für Internationalen Zahlungsausgleich ist maßgeblich verantwortlich;
3. Initiieren einer massiven weltweiten Operation unter falscher Flagge — Pandemie, Krieg, Energiekrise —, die die globalen Schuldenmärkte zum Absturz bringt und Fiat-Währungen in Flammen aufgehen lässt;
4. einen Schuldigen finden, der politisch akzeptabel ist wie die Russen, Nordkorea;
5. anhaltender Zusammenbruch der Schuldenpyramide der Fiat-Währung, bis die Schafe so verzweifelt sind, dass sie selbst vor dem

Gedanken, Abfall zu essen, nicht zurückschrecken;

6. mit großem Tamtam eine staatlich unterstützte Kryptowährung als Ersatz für alle Fiat-Währungen ankündigen und die Weltregierung als Retter der Menschheit darstellen;
7. Bargeld zu verbieten und den Privatbesitz von Gold und Silber durch Bürger zu kriminalisieren, das natürlich im Namen der „Sicherheit“;
8. Kriminalisierung aller nichtoffiziellen Kryptowährungen wie Bitcoin, sodass ihr Wert praktisch über Nacht abstürzt und alle in die Kryptowährung der Weltregierung einfließen, in der die NSA die Blockchain kontrolliert;
9. digitale ID oder biometrische Identifikatoren für alle Transaktionen als Voraussetzung zu definieren, um die Aktivitäten der digitalen Kryptowährung der einen Welt zu authentifizieren. Niemand darf mehr essen, reisen oder ein Gehalt verdienen, ohne mittels QR-Code auf ein Objekt reduziert zu sein;
10. Sobald die absolute Kontrolle über die neue digitale Eine-Welt-Währung erreicht ist, wird die von der Regierung verfolgte Blockchain als Waffe eingesetzt, um alle Transaktionen, Investitionen und kommerziellen Aktivitäten zu verfolgen. Social Scoring (Sozialkreditsystem) wird eingesetzt, um den vorauseilende Gehorsam eines jeden Einzelnen zu gewährleisten.

2022 — die Regulierung beziehungsweise Abschaffung privater Kryptowährungen

Die Präsidentin der Europäischen Zentralbank, Christine Lagarde, hat die existierenden Kryptowährungen ins Visier genommen und sich in einem **Interview** (https://www.politico.eu/article/crypto-assets-worth-nothing-ecb-christine-lagarde/) besorgt gezeigt, dass Menschen sich der Risiken nicht bewusst sind, dass sie alles verlieren und schrecklich enttäuscht sein könnten, und dass sie deshalb für eine Regulierung der privaten Kryptowährungen plädiert.

Bereits im Januar 2021 forderte Lagarde eine globale Regulierung von Bitcoin. In einem **Interview** (https://www.reuters.com/technology/reuters-next-ecbs-lagarde-calls-regulating-bitcoins-funny-business-2021-01-13/) mit der Nachrichtenagentur *Reuters* sagte sie seinerzeit, dass die digitale Währung zur Geldwäsche benutzt worden sei, und plädierte für Regeln, die entsprechende Schlupflöcher schließen würden.

Lagarde ging zwar nicht näher auf die Besonderheiten der Geldwäsche im Zusammenhang mit Kryptowährungen ein, sprach sich aber für eine Regulierung aus, die auf globaler Ebene vereinbart und angewandt werden sollte, „denn wenn es einen Ausweg gibt, wird dieser Ausweg genutzt werden", und bezog sich dabei auf Regulierungslücken.

Der spektakuläre Kurssturz des UST (UST ist ein algorithmischer Stablecoin, der nicht eins zu eins mit Dollar gedeckt ist) veranlasste den Vorsitzenden der Börsenaufsichtsbehörde, Gary Gensler, vor wenigen Tagen zu der **Aussage** (https://news.bitcoin.com/sec-chair-gensler-warns-a-lot-of-crypto-tokens-will-fail-luna-ust-collapse/), dass er ebenso wie Lagarde befürchtet, dass die Anleger auf den Kryptomärkten Schaden nehmen werden.

„Ich denke, dass viele dieser Token scheitern werden", sagte Gensler Reportern nach einer Anhörung des House Appropriations Committee am 18. Mai 2022.

„Ich befürchte, dass bei Kryptowährungen (...) viele Menschen zu Schaden kommen werden, und das wird das Vertrauen in die Märkte und das Vertrauen in die Märkte im Allgemeinen untergraben."

Neben den Regulierungsbehörden und anderen Beamten, die ihre Krypto-Kritik verstärken, haben auch prominente Persönlichkeiten Vorbehalte gegenüber der Anlageklasse geäußert.
Bill Gates **sagte** (https://www.gatesnotes.com/About-Bill-

Gates/2022-Reddit-AMA?WT.tsrc=BGTW) während einer „Reddit Ask Me Anything"-Sitzung am 19. Mai, dass er nicht in Kryptowährungen investiert habe, weil sie „keinen Beitrag zur Gesellschaft leisten".

„Ich besitze keine", schrieb Gates. „Ich investiere gerne in Dinge, die einen wertvollen Output haben. Der Wert von Unternehmen basiert darauf, wie sie großartige Produkte herstellen. Der Wert von Kryptowährungen ist nur das, was eine andere Person entscheidet, dass jemand anderes dafür bezahlen wird, also kein Beitrag zur Gesellschaft wie andere Investitionen."

Elon Musk gab Anfang 2021 bekannt, privat als auch mit seinen Unternehmen Tesla und Neuralink in den Bitcoin zu investieren und Zahlungen in Bitcoin zuzulassen. Monate später stoppte Musk Zahlungen in Bitcoin und stieg aus der Kryptowährung aus. Warum wohl?

> ***Der Startschuss zur Abschaffung des Bitcoin beziehungsweise zu einem Hinübergleiten in eine von Zentralbanken gesteuerte Kryptowährung ist bereits gefallen.***

Wie denken Sie jetzt über Ihren Bitcoin?

Birgit Naujeck, Jahrgang 1963, ist nicht in der DDR aufgewachsen, aber wurde durch die DDR sozialisiert. Sie hat lange Jahre in unterschiedlichen Ländern als Projektmanagerin in der Informationstechnologie gearbeitet. Die Natur- und Umweltschützerin lebt derzeit

am Rhein, arbeitet aber bereits an der Umsetzung ihres Kindheitstraums: ein Leben in der Natur mit Tier und Mensch. Aus ihrer Opposition zur Technokratie wendet sie sich deutlich gegen 5G, Transhumanismus, jegliche Eugenik und die Entkörperung unserer Sprache, die dazu führt, dass Geschichte und Geschlecht umgeschrieben werden.