

# NSA und MIT haben wahrscheinlich Bitcoin erfunden

- [Drucken](#)
- [E-Mail](#)



## TEST FÜR DIGITALE WELTWÄHRUNG?

Sind Bitcoin und die Blockchain-Technologie wirklich von einem anonymen Robin Hood geschaffen

und an die Bevölkerung verschenkt worden, um eine Revolution anzuzetteln gegen die Zentralbanken und Geschäftsbanken?

Oder war das Ganze nur ein Freiluft-Experiment der Eliten? Damit nach einer wilden Phase an Bitcoin-Skandalen über Kursmanipulationen und Diebstähle die Zentralbanken und großen Privatbanken ihre eigenen Digi-Währungen verbreiten können?

Die [NSA und die Universität MIT](#) hatten 1996, also rund 12 Jahre vor dem Auftauchen von Bitcoin, ein [White Paper veröffentlicht](#) über anonyme kryptographische Währungen, die (zunächst) am gegenwärtigen Geldsystem vorbei operieren könnten.

*“Weil es so einfach ist, eine 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.”*

Die Wissenschaftler hatten natürlich auch bereits Probleme wie Geldwäsche und Ähnliches vorhergesehen. Das amerikanische Finanzamt IRS hat nun [neue Analyse-Werkzeuge](#) parat, um die neuen digitalen Geldströme zu verfolgen.

12 Jahre später hat dann „jemand“ die Blockchain und Bitcoin erschaffen und unter dem Namen Satoshi weitergegeben an einen Programmierer, der mit der CIA zusammenarbeiten und sich überhaupt nicht mit dem Establishment anlegen wollte. Mit der Blockchain und dem Fiat-Geld Bitcoin kann das Establishment [uns auch überwachen](#) in einer bargeldlosen Zukunft. [JP Morgan](#) und die [Federal Reserve](#) basteln schon fleißig mit an digitalem Fiat-Geld der Zukunft.

Bitcoin-Chefentwickler Gavin Andresen erzählte in einem Interview über seinen Vortrag im CIA-Hauptquartier 2011:

*“Insgesamt war die Reaktion recht positiv, auch wenn das keine besonders gesprächigen Leute sind. Einer der Teilnehmer war ein Wirtschaftswissenschaftler von der Federal Reserve, und ich war überrascht, wie aufgeschlossen er der Idee von Bitcoin gegenüberstand. Aus seinem Vortrag habe ich gelernt, dass die Zentralbanken überall auf der Welt an Macht über das Geldvolumen verlieren, weil eine Reihe von Geldersatzprodukten – wie die Finanzderivate des Schattenbankensystems – immer einflussreicher werden.”*

Andresen studierte an der elitären Princeton University (1988 Bachelor’s degree in Computer Science). Die geheimdienstliche Venture Capital Arm In-Q-Tel der CIA sucht nach Start Up-Firmen die im Interesse der nationalen Sicherheit liegen.

Er wollte Schwankungen und hohe Bitcoin-Wechselkurse eigentlich vermeiden:

*“Ich glaube, die wichtigste Herausforderung in naher und mittlerer Zukunft ist es, Bitcoin wirklich stabil zu machen. Nur eine stabile Währung ist eine gute Währung. Unser Geld soll langweilig und vorhersehbar sein.”*

Die einzigen, die Bitcoin tatsächlich als Währung gebrauchen, sind einerseits Fans der Technologie und andererseits Kriminelle. Deshalb sehen wir nun auch immer neue Gesetze weltweit zur Regulierung und Überwachung von Bitcoin-Strömen. Hauptsächlich sind Kryptowährungen inzwischen Spekulations-Objekte, deren Kurs von Insidern hoch- und runtergetrieben wird.

### **Wilder Westen und das “Experiment”**

Der Bitcoin-Kurs steigt zwar munter, aber dieses Geld-Experiment ist [in heftigen Schwierigkeiten](#). Es sind gierige, schlecht ausgesuchte Leute im diktatorischen Führungskader, aber auch gierige chinesische Miner, die das Projekt in den Untergang treiben. Die begrenzte Blockchain-Size verstopft seit geraumer Zeit alles, treibt Gebühren in die Höhe und macht Bitcoin als praktisches Zahlungsmittel fast nutzlos mit Wartezeiten von bis zu mehreren Tagen pro Transaktion. Ausgerechnet [China dominiert das Trading](#). [Neue Angriffsmöglichkeiten](#) werden auch regelmäßig entdeckt.

Die Insider wollen weiter prächtig abkassieren und die Kontrolle behalten und weigern sich, die Blockchain-Size zu vergrößern und [injizieren fragwürdige Sachen in den Code](#). Schon bei Karpeles‘ Wechselstube Mt. Gox wurden per Bots und Luftbuchungen die Kurse künstlich in die Höhe getrieben. Diejenigen, die das Projekt weiterentwickeln und damit retten wollten, wurden per irrsinnig hohen DDoS-Attacken angegriffen. Wer ein bisschen Geld zum Verzocken hat, mag sich ein paar Coins kaufen. Aber die existenziellen Probleme bei Bitcoin sind nicht lösbar. Die falschen Leute kontrollieren den Code.

Die Insider wollen so lange abkassieren wie möglich, bevor das dicke Ende kommt. Natürlich gibt es vielleicht irgendwann immer mehr Forks (neue Variationen) von Bitcoin, aber hier werden sich meistens die gleichen „people problems“ einstellen wie bei dem Bitcoin Core. Investoren zittern natürlich, dass dann die tollen Kurse vom Original-Bitcoin zusammenbrechen werden und die Märkte und Investoren verunsichert sein werden.

Bitcoin ist keine Geldrevolte gegen das Establishment. Bitcoin sind digitale [Tulpenzwiebeln](#), kultiviert von einer zwielichtigen Gruppe an Individuen.

### **Brock Pierce**

Er ist ein neuer Vorsitzender der Bitcoin-Stiftung. Seine Ernennung führte zu einigem erstaunten Raunen und manchen Rücktritten aus Protest. Vor 15 Jahren war er Mitbegründer einer Internetfirma mit zwei weiteren Unternehmern. Es wurden 60 Millionen Dollar verblasen ohne dass signifikante Einnahmen generiert wurden und man erklärte schließlich Insolvenz. Alle drei wurden in Anklageschriften genannt im Bezug auf sexuellen Missbrauch von Minderjährigen, Vergewaltigung und Morddrohungen. Bei manchen Angestellten der Firma, die so etwas wie Youtube hätte werden können, soll es sich um Minderjährige gehandelt haben. Auch Pierce selbst war erst 17 Jahre alt, als er in das Haus des 23 Jahre älteren Collins-Rector zog und prompt ein Gehalt von 250.000\$ kassierte. Zuvor war Pierce als Kinderstar in Disney-Produktionen zu sehen.

Alle drei flüchteten zunächst jedoch nach Spanien, weil weitere Zeugen ihnen Missbrauch vorwarfen. Pierce, Rector und Shackley ignorierten die Anklagen. 2002 folgte die Verhaftung der Männer nach einer Razzia durch Interpol. Bei der Hausdurchsuchung sollen Waffen, Juwelen und Kinderpornografie [gefunden worden sein](#).

Collins-Rector wurde schließlich verurteilt. Es existierten mehrere Verfahren und es kommen sogar heute noch Ankläger dazu, allerdings existieren nach so langer Zeit jedoch oft nur noch Aussagen.

Ein wahrer Pädö-Ring um Collins-Rector soll jahrelang männliche Teenager missbraucht und mit Karrierechancen gelockt haben. Pierce wohnte sogar in dem Haus des Regisseurs der X-Men-Reihe, der kürzlich wegen angeblicher Pädoparties angeklagt wurde.

Pierce erklärte nach seinem Direktorenposten bei der Bitcoin Foundation, dass ihm Anklageschriften nicht zugestellt wurden und er erst später Wissen von jenen erlangt hatte. Letztendlich sei ihm nichts nachgewiesen worden. Dennoch schadet seine Ernennung laut anderen Mitgliedern der Bitcoin-Stiftung und Beobachtern dem Ruf der digitalen Währung. Außerdem einigte sich Pierce mit dem Mitbegründer eines Internet-Unternehmens auf eine unbekannte Summe nach einer Anklage wegen Betrugs.

Nun will die Firma Sunlot Holdings Limited von Pierce die Reste von Mt. Gox kaufen, der ehemals weltgrößten Bitcoin-Wechselstube die ausgerechnet von einem Bitcoin-Mitbegründer geschaffen und an die Wand gefahren wurde. Mehrere hundert Millionen Dollar an Kundengelder gelten als verloren bzw. gestohlen.

## **Mark Karpeles**

[Laut der japanischen Presse](#) sollen Ermittlungen der Polizei von Tokio ergeben haben, dass der ehemals größte Handelsplatz für die digitale Währung Bitcoin wahrscheinlich von Insidern leergeräumt worden sei, und nicht von Hackern. Mt. Gox vermittelte noch im August 2013 insgesamt 60 % des weltweiten Bitcoin-Handelsvolumens. Anfang 2014 erklärte der Betreiber Mark Karpeles, das Opfer eines Hacks geworden zu sein und dass die Gelder der Kunden von Unbekannt gestohlen worden wären. Am 28. Februar 2014 meldete das Unternehmen bei einem japanischen Bezirksgericht Insolvenz an. Karpeles schüttelte Wochen später noch überraschend 200.000 Bitcoins aus dem Ärmel, die er angeblich in alten Konten gefunden haben will. Das besänftigt aber nicht die Kunden; vor allem da immer noch hunderttausende Bitcoins fehlen und sich in der Vergangenheit bereits mehrere Betreiber von Bitcoin-Börsen als Betrüger herausgestellt hatten.

Der für den Betrieb von Mt. Gox verantwortliche Karpeles ist ausgerechnet ein Gründungsmitglied der Bitcoin-Stiftung.

Die Sichtung der der Geschäftsaktivitäten durch japanische Ermittler hätte ergeben, dass zwei Konten bei Mt. Gox immer höhere Guthaben anhäuferten ohne dass reguläre Transaktionen dahintersteckten. Gelder von Kunden seien so abgeschöpft und die Beute gegen Dollars und andere reguläre Währungen verhökert worden.

Die [britische Zeitung Guardian berichtete bereits im Mai 2014](#), dass Ende 2013 bei Mt. Gox zwei sogenannte „Bots“, also Computerprogramme mit Administratorfähigkeiten, die atemberaubende Zahl von 650.000 Bitcoins gekauft haben sollen, ohne wirklich echtes Geld ausgegeben zu haben. Dies entspräche einem Vermögen von mehreren hundert Millionen Dollars. Ein anonymen Bericht erklärte, dass vieles auf eine Urheberschaft von Insidern bei Mt. Gox hinweise. Auf diese Weise hätten die Bots den Bitcoin-Kurs mit Hilfe von manipulativen Luftbuchungen auf über 1000\$ getrieben, was einen Run von Investoren auslöste. Die ständige Propaganda tat ihr Übriges und verkündete ständig, dass der Kurs noch in fünfstelligen oder sechsstelligen Regionen gehen werde.

### **Charlie Shrem**

Mitbegründer des Vorstandes der Bitcoin-Stiftung. Leitete die Wechselstube BitInstant. Wurde verhaftet am JFK-Flughafen weil er geholfen haben soll, 1 Million \$ an Geld zu waschen für Geschäfte auf der inzwischen geschlossenen Handelswebseite für Drogen namens Silk Road. Er selbst will von keinen illegalen Verwendungen des Geldes gewusst haben und plädiert für den Prozess im September auf unschuldig. Er deutete an, verfolgt zu werden, weil Bitcoin angeblich die etablierten Währungen bedrohe.

### **Satoshi Nakamoto**

Der angebliche Schöpfer von Bitcoin. Existiert er überhaupt? Niemand hat ihn je gesehen, nicht einmal die anderen Leute bei Bitcoin. Nicht sehr vertrauenswürdig. Er soll sein Werk an zwei Hanswürste übergeben haben, die zuvor jahrelang Online-Poker spielten.

### **Gavin Andresen**

Bitcoin-Chefentwickler Gavin Andresen erzählte in einem Interview über seinen Vortrag im CIA-Hauptquartier 2011:

*„Insgesamt war die Reaktion recht positiv, auch wenn das keine besonders gesprächigen Leute sind. Einer der Teilnehmer war ein Wirtschaftswissenschaftler von der Federal Reserve, und ich war überrascht, wie aufgeschlossen er der Idee von Bitcoin gegenüberstand. Aus seinem Vortrag habe ich gelernt, dass die Zentralbanken überall auf der Welt an Macht über das Geldvolumen verlieren, weil eine Reihe von Geldersatzprodukten – wie die Finanzderivate des Schattenbankensystems – immer einflussreicher werden.“*

Andresen studierte an der elitären Princeton University (1988 Bachelor's degree in Computer Science). Die geheimdienstliche Venture Capital Arm In-Q-Tel der CIA sucht nach Start Up-Firmen die im Interesse der nationalen Sicherheit liegen. Außerdem machte er eine deutliche Absage an Spekulanten und ihre Träume von vier- oder fünfstelligen Dollarwechsellkursen pro Bitcoin:

*„Ich glaube, die wichtigste Herausforderung in naher und mittlerer Zukunft ist es, Bitcoin wirklich stabil zu machen. Nur eine stabile Wahrung ist eine gute Wahrung. Unser Geld soll langweilig und vorhersehbar sein.“*

## **Andreas Antonopoulos**

Der leitende Sicherheitschef von Bitcoin [verlie das Projekt wegen einem „volligen Mangel an Transparenz“](#). Dabei wird ja gerade geworben damit, dass Bitcoin so offen und transparent sei. Er sagte, er will nicht einmal mehr die „kleinstmogliche Verbindung“ zur Bitcoin-Stiftung haben. Steigt er rechtzeitig aus?

## **„Bitcoin kann gebrochen werden“**

Einer der wichtigsten Entwickler von Bitcoin, Jeff Garzik, erklarte zusammenfassend:

*„Bitcoin ist nur eine Maschine. Sie kann gekauft werden. Oder angegriffen. Oder gebrochen werden.“*

## **Die Haifisch-Truppe**

Ein realistischer Preis fur eine Einheit der digitalen Wahrung Bitcoin liegt laut Berechnungen bei gerade einmal 4 US-Dollar. Die sogenannte „Haifisch-Truppe“ sitzt auf fast allen bisher erzeugten Bitcoins, schlielich konnte man diese vor Jahren noch muhelos generieren. Adi Shamir analysierte die Masse an anonymisierten, bisher stattgefundenen Transaktionen und kam zu interessanten Ergebnissen: Alle groen Transaktionen stammen von einer einzigen Mega-Transaktion ab. Durch weitere Zersplitterung und Verschachtelung sollte womoglich verschleiert werden, dass es sich um Fake-Trading einer einzelnen Person oder einer kleinen Gruppe handelte. Nach hunderten Zwischenkonten wurden die Geldstrome wieder zu dem Ursprungsbetrag zusammengefugt. Eine einzige Person besa im Jahr 2012 zwischen 200.000 und 400.000 Bitcoin, eine weitere Person besa zwischen 100.000 und 200.000, funf Personen besaen zwischen 50.000 und 100.000.

97% aller Bitcoin-Besitzer hatten weniger als 10 Transaktionen, wahrend gerade einmal 75 Besitzer mit 5000 Transaktionen in Verbindung gebracht werden. Man geht von hunderttausenden Pseudo-Konten die eine Kursmanipulation verschleiern konnen.

Der Piraten-Grunder Falkvinge analysiert auf seiner Webseite seitsame Transaktionen: In Schritt 1 kauft die Haifisch-Truppe eine Menge Bitcoins, der Kurs schiet um 8% nach oben. Diejenigen Trader, die auf ein Fallen gesetzt haben, ziehen sich zuruck. Ein Mitglied der Haifisch-Truppe kauft einfach direkt oder getarnt uber Strohmännchen-Konten von einem anderen Insider.

In Schritt zwei senkt die Haifisch-Truppe den Kurs wieder stetig ab und sorgt fur Panikverkaufe von gewohnlichen Tradern. Automatisiert werden alle funf Sekunden exakt ein Bitcoin verkauft. Der Eindruck entsteht, viele Trader wurden aus Panik verkaufen. Dabei verkauft nur ein Mitglied der Haifisch-Truppe an ein anderes. Gewohnliche Trader furchten hohere Kurseinbruche und verkaufen ihre Bitcoins – an die Insider. Ein wenig Absprache und schon wissen die 100 Insider theoretisch, wie der Kurs nachste Woche aussehen wird. Die anderen Bitcoin-User mussen raten und werden abgezockt. Das Muster wiederholt sich:

Würden die Insider ihre Millionen Bitcoins zu schnell auf den Markt werfen und gegen Dollars oder Euros tauschen, fiel der Kurs ins Bodenlose und die Party wäre vorbei.

Von [Alex Benesch](#)

*(recontr)*

*Ein weiterer interessanter Beitrag zum Thema Urheber des Bitcoin und die möglichen, zukünftigen Folgen, findet sich auch [HIER...](#)*