# (Fast) 10 Jahre Bitcoin – eine Würdigung

**Als 2008 in einem Whitepaper unter dem Pseudonym Satoshi Nakamoto Bitcoin der Öffentlichkeit vorgestellt worden ist, fand die Idee kaum Beachtung. Heute sind digitale Währungen omnipräsent. Nach zehn Jahren bietet es sich nun an, den Erfolg von Bitcoin anhand der ursprünglichen Ziele zu überprüfen.**

**DER AUTOR**

**Walter Dettling**
Mathematiker und Dozent für Finanzmathematik und Wirtschaftsinformatik an der Hochschule für Wirtschaft FHNW

Wenn es in der breiten Öffentlichkeit um Bitcoin geht, steht meistens die Bedeutung und zukünftige Rolle von Bitcoin in der Finanz- und Wirtschaftswelt zur Diskussion. Anlässlich des bald zehnjährigen Jubiläums von Bitcoin wollen wir für einmal in die Vergangenheit blicken und die Frage stellen: Mit welchen Ideen und Zielen ist Bitcoin angetreten und wie weit wurden diese erreicht? Könnte es sein, dass der «Erfolg» von Bitcoin von den wahren Qualitäten dieser Idee ablenkt? Für alle, die sich nicht so genau erinnern können oder das Thema gar nie so genau verfolgt haben, zunächst ein kurzer Rückblick.

### Die Entstehung von Bitcoin während der Finanzkrise 2008

Am 31.Oktober 2008 wurde ein Whitepaper mit dem Titel «Bitcoin: A Peer-to-Peer Electronic Cash System» unter dem Pseudonym Satoshi Nakamoto veröffentlicht. Auf neun Seiten werden die Anwendungsmöglichkeiten und die grundlegenden Mechanismen von Bitcoin beschrieben. Im Zentrum steht dabei die digitale Überweisung von Zahlungen ohne den Einbezug einer zentralen Stelle, die als Vertrauensinstanz bei Onlinezahlungen bisher immer nötig war. Diese Idee fand damals nur bei einem sehr kleinen Kreis Beachtung. Andere Vorkommnisse beanspruchten die Aufmerksamkeit der Weltöffentlichkeit: Am 15. September 2008 gelangten mit dem Zusammenbruch der Investmentbank «Lehmann Brothers» die jahrelangen Auswüchse der Finanzbranche an die Öffentlichkeit. Auch die Schweiz war davon betroffen.

> Die voranschreitende Digitalisierung verlangt nach effizienten digitalen Zahlungssystemen.

Am 16. Oktober 2008 kündigten die Schweizer Nationalbank und der Bundesrat an, die UBS mit über 60 Milliarden Franken vor einem sofortigen Zusammenbruch zu retten. Diese war mit dem vierfachen Wert des gesamten schweizerischen Bruttoinlandproduktes (über 2000 Milliarden Franken) in Finanzspekulationen am US-Hypothekenmarkt verwickelt. Das war der damalige Preis, eine der grössten Investmentbanken der Welt zu sein!

Wiederum ohne Aufsehen wurde am 3. Januar 2009 die Bitcoin-Software zum ersten Mal produktiv eingesetzt. Einen Monat später bot Satoshi Nakamoto die Software in einem Blog als Open-Source-Anwendung zum Herunterladen an: «Ich habe ein neues Open-Source-P2P-E-Cash-System, kurz Bitcoin, entwickelt. Es ist komplett dezentral, es hat keinen zentralen Server und benötigt keine Vertrauensinstanz. Alles basiert auf kryptografischer Kontrolle anstelle von Vertrauen.»

> Wir können Bitcoin attestieren, die gesteckten Ziele weitgehend erfüllt und damit sehr viel erreicht zu haben.

Er präzisierte: «Das Hauptproblem zentraler Währungen ist das Ausmass an Vertrauen, das nötig ist, damit sie funktionieren. Den Zentralbanken muss vertraut werden, dass sie die Währungen nicht entwerten, den Banken, dass sie sorgfältig und vertrauensvoll mit unserem Geld und unseren Identitäten umgehen.» Dieses politische Anliegen unterstreicht folgendes Zitat, das im ersten Block der Bitcoin-Blockchain abgespeichert ist: «The Times 03/Jan/2009 Chancellor on brink of second bailout of banks.»

Das Besondere an Bitcoin ist die Verknüpfung von politischen, ökonomischen, gesellschaftlichen, wissenschaftlichen und technologischen Prinzipien. Auf zwei Wörter reduziert, kann man dieses Bauprinzip als «intelligente Dezentralisierung» bezeichnen.

### 2008 – 2018: Das Pflichtenheft von Bitcoin und seine Beurteilung

Die Sachlichkeit des Whitepapers und der politischen Aussagen von Satoshi Nakamato erlauben es, die mit Bitcoin verbundenen Absichten in einem Pflichtenheft zusammenzufassen. Mit der Bekanntgabe der Anforderungen vor dem Produktivstart hat Bitcoin die Voraussetzung geschaffen, den Erfolg an den ursprünglichen Zielen zu messen. Wir beziehen uns dabei auf das «Original», das aktuell mit der Bezeichnung Bitcoin Core Release 0.16.0 verwendet wird. Es gibt ausser Bitcoin zahlreiche Kopien, die unter ähnlichem oder völlig anderem Namen und mit den unterschiedlichsten Anpassungen ebenfalls elektronische


Bitcoin verbindet Gesellschaft, Politik, Wirtschaft und Handel, Kryptografie, Computer und Netzwerke in einem System.

Bilder: fox17 / Fotolia.com; Walter Dettling, 2018

Zahlungssysteme betreiben. Sie sind nicht Gegenstand dieses Artikels. Gehen wir die einzelnen Anforderungen durch, kommen wir zu folgenden Erkenntnissen:

- Ein elektronisches Zahlungssystem, das rund um die Uhr, auf der ganzen Welt und für jede und jeden zugänglich ist. **Teilweise erfüllt:** Bitcoin ist im Prinzip 24/7 auf der ganzen Welt verfügbar. Aus verschiedensten Gründen ist die Zugänglichkeit aber nicht für jedermann gewährleistet. Insbesondere die Benutzerfreundlichkeit ist für viele ein Hindernis.

- Das mehrfache (unrechtmässige) Ausgeben derselben Münze (Double Spending) ist nicht möglich. **Erfüllt:** Es gab bisher keinen dokumentierten Fall von echtem Double Spending.

- Der Schutz der Besitzerinnen und Besitzer vor Diebstahl und Betrug (vor allem durch die Banken mittels Abwertung!). **Teilweise erfüllt:** Diebstähle bei den direkten Anwendern und Anwenderinnen sind noch nie aufgetreten. Es gibt aber eine ganze Industrie von Bitcoin-Dienstleistern, bei denen immer wieder Betrügereien auftreten. Die Wertschwankungen beruhen nicht auf Veränderungen der Anzahl von Bitcoins, sondern werden vor allem durch Spekulationen im Sekundärmarkt ausgelöst.

- Schnelle, kostengünstige Mikrotransaktionen (Ausführung binnen Sekunden, definitive Bestätigung binnen einer Stunde). **Nicht erfüllt:** Es kann nur Sekunden dauern, manchmal aber auch Minuten oder Stunden, bis eine Transaktion ausgeführt wird. Die aktuellen Durchschnittskosten pro Transaktion betragen etwa 0.0001 Bitcoin, beim aktuellen «Marktpreis» von Bitcoin also etwa 0.70 Franken. Diese zeitlichen und wertmässigen Schwankungsbreiten sind für Mikrotransaktionen zu gross, weshalb wir diese Anforderung als nicht erfüllt bezeichnen.

- Vollständige Transparenz über erfolgte Zahlungen. **Erfüllt:** Jede Bitcoin-Transaktion ist vollständig transparent und kann jederzeit und von jedermann nachgeprüft werden. Der Ursprung und der gesamte Transaktionsweg aller Bitcoins sind vollständig dokumentiert.

- Unumkehrbarkeit von Zahlungen. **Erfüllt:** Nachdem eine Transaktion mit Bitcoin bestätigt wurde, kann diese von niemandem rückgängig gemacht werden.

- Zensurfreie Überweisungen. **Erfüllt:** Alle Transaktionen werden völlig anonym und ohne Rücksicht auf die Transaktionshöhe (die Kosten hängen nicht vom Betrag ab) gleichbehandelt.

Im zehnten «Lebensjahr» können wir Bitcoin attestieren, die gesteckten Ziele weitgehend erfüllt und damit sehr viel erreicht zu haben. Bitcoin ist das erste digitale Zahlungsmittel, das global und vollständig dezentral funktioniert. Bewunderung verdienen die Skalierbarkeit, die in den Bitcoin-Code eingebaut wurde, und die Tatsache, dass die Core-Entwickler diese Linie bisher nicht verlassen haben. Nicht vorhersehbar war, dass Bitcoin als Wertanlage und Spekulationsobjekt Marktmechanismen ausgesetzt ist, die seine Funktion als «technisches» Zahlungsmittel zurzeit massiv einschränken.

Die voranschreitende Digitalisierung verlangt nach effizienten digitalen Zahlungssystemen. Bitcoin hat gezeigt, dass es möglich ist, ein solches System sicher zu betreiben. Die Grundidee von Bitcoin, die digitale Version von Bargeld (E-Cash) zu sein, stösst aber noch auf viel Widerstand oder Unverständnis. Ein Grund dafür ist die dezentrale Struktur, die keiner Institution und keinem Land die Kontrolle über dieses Zahlungssystem erlaubt. Der Blick auf die Finanzmärkte heute zeigt, dass Zentralisierung und komplexe Regelwerke an Grenzen stossen. Wir können nicht darauf hoffen, dass die Lösung für ein globales, digitales und effizientes Zahlungssystem aus dem Kreis der Banken oder deren Regulierungsbehörden kommen wird. Das Internet lässt sich nicht mit territorialen beziehungsweise multilateralen Regeln wirksam und schon gar nicht entwicklungsfähig kontrollieren. Zehn Jahre nach dem Start von Bitcoin liegt uns ein Proof of Concept vor. Damit wir nicht noch zehn weitere Jahre auf eine Umsetzung warten müssen, braucht es jetzt den Willen, die Zukunft zu gestalten, statt nur darüber zu reden.