finalix.
business consulting

Bitcoins – Boom or Bust?

Roland Renggli, Yavor Vassilev, Christian Ullrich

Roland Renggli (Senior Consultant) studierte Experimentalphysik an der Universität Zürich und vertiefte sich im Gebiet Supraleitung. Als Consultant begleitete er während vier Jahren mehrere IT Beratungsprojekte bei Accenture. Nach seiner dreijährigen Auszeit als Linienpilot wurde Roland Renggli im März 2008 Teil des Finalix Teams. Roland Renggli ist ISTQB-zertifizierter Tester.

Yavor Vassilev (Senior Consultant) absolvierte sein Studium der Politikwissenschaften an der Universität Bern. Danach arbeitete er während einigen Jahren in Grossprojekten bei Swiss Life Asset Management als Business Process Engineer. Beratungserfahrung sammelte er bei CSC Switzerland, wo er auf Projekten im Versicherungsumfeld und im öffentlichen Verkehr seine Kenntnisse im Projektmanagement und in der Business-Analyse vertiefte. Er ist seit 2013 im Team von Finalix.

Christian Ullrich (Consultant) studierte Betriebswirtschaftslehre an der Universität Augsburg und in den USA. Nach der Durchführung und Leitung von Beratungsprojekten und abgeschlossener Promotion am Kernkompetenzzentrum Finanz- & Informationsmanagement in Augsburg stiess er Anfang 2014 zum Finalix Team.

1 Einleitung

Bitcoins sind in aller Munde. Virtuelle Internetwährungen faszinieren, verwirren aber auch durch die Komplexität der zugrundeliegenden Mechanismen. Ist die Bitcoin-Technologie der Anfang einer gesellschaftlichen Revolution, vergleichbar mit der Erfindung des E-Mails vor 20 Jahren, oder handelt es sich eher um ein dubioses Netzwerk von Cyber-Kriminellen, die sich primär am Geld von schlecht informierten Investoren bereichern wollen? In den Medien wird aktuell beiden Ansichten viel Platz eingeräumt.

Boom?

Auf der *Boom*-Seite liest man von eindrücklichen Erfolgsgeschichten. Es ist die Rede von astronomischen Kurszielen. Bis zu 10'000 US-Dollar pro Bitcoin werden geboten. Gleichzeitig ist von einer rasant zunehmenden Akzeptanz von Bitcoin als Zahlungsmittel zu hören. Erstaunt nehmen wir zur Kenntnis, dass die ersten Bitcoin-basierten ETFs unterwegs Richtung Börse sind.

Fakt ist, dass Bitcoins Stand Ende 2014 durchaus einen Achtungserfolg verbuchen können. Der aktuelle Marktwert beträgt CHF 4.4 Milliarden. Pro Tag finden im Schnitt rund 80‘000 Transaktionen statt. Weltweit gibt es etwa 3.2 Millionen Bitcoin-Wallets mit rund 500‘000 aktiven Benutzern. Mit 13.3 Millionen Bitcoins sind etwas mehr als die Hälfte aller vorgesehenen Bitcoins bereits im Umlauf.

Bust?

Umgekehrt thematisieren die Medien mit gleicher Regelmässigkeit auch die *Bust*-Seite der Internetwährungen. Die extreme Volatilität des Bitcoin-Preises sowie Hinweise auf kriminelle Machenschaften und regulatorische Unsicherheiten dominieren die Berichterstattung. Es gibt nicht wenige Stimmen, die hinter den Bitcoins nicht mehr als ein weiteres Schneeballsystem vermuten.

Zielsetzung

Vor dem Hintergrund der doch sehr kontrovers geführten Diskussion scheint eine eigene Meinungsbildung zu Relevanz und Zukunft des Phänomens schwierig. Im Sinne eines konstruktiven Beitrags wird deshalb im Folgenden:

1. Die Begriffswelt der Bitcoins erläutert
2. Die Funktionsweise des Bitcoin-Protokolls erklärt
3. Eine Einordnung im Vergleich mit anderen Währungen vorgenommen

2 Eigenschaften der Bitcoin-Technologie

Die Bitcoin-Technologie zeichnet sich im Kern durch drei Eigenschaften aus:

1. Öffentliche Transparenz
2. Dezentrale Verarbeitung
3. Kryptographische Verschlüsselung

Öffentliche Transparenz

Blockkette

Grundlage der öffentlichen Transparenz bildet die sogenannte *Blockkette* (Block Chain). Dabei handelt es sich um eine Art frei verfügbares Journal sämtlicher bisher getätigter Bitcoin-Transaktionen. Tatsächlich reicht die Historie bis zur ersten Bitcoin-Zahlung im Jahre 2009 zurück. Die Blockkette ist für alle Teilnehmer im Netzwerk problemlos einsehbar. Man kann sich die Blockkette als eine sehr grosse Textdatei vorstellen, die im Internet frei verfügbar und lokal auf allen Rechnern im Bitcoin-Netzwerk gespeichert ist.

Public Key

Mit der Blockkette kann für jedes Bitcoin für jeden Zeitpunkt seit seiner Entstehung nachvollzogen werden, wer der jeweilige Besitzer war. Die Blockkette stellt also quasi das kollektive Gedächtnis zu den Besitzverhältnissen jedes einzelnen Bitcoins oder jedes Bitcoin-Bruchteils dar. Dabei wird der Besitzer durch den *Public Key*, eine öffentliche Adresse, repräsentiert. Weder Sender noch Empfänger werden namentlich erwähnt. In diesem Sinne sind die Transaktionen zwar öffentlich einsehbar, bleiben aber anonym.

Dezentrale Verarbeitung

Peer-to-Peer

Bitcoins werden in einem *Peer-to-Peer-Netzwerk* erzeugt und ausgetauscht. Vereinfacht gesagt wird virtuelles Geld ähnlich wie ein E-Mail von einem Marktteilnehmer zum anderen geschickt. Es braucht weder eine Bank noch eine anderweitige Zwischenstelle, um eine Überweisung zu tätigen.

Mining

Darüber hinaus erfolgt auch die Erzeugung von Bitcoins dezentral durch einzelne Marktteilnehmer. Man spricht in diesem Zusammenhang vom *Mining* von Bitcoins.

Kryptographische Verschlüsselung

Die Bitcoin-Technologie basiert in wesentlichen Teilen auf mathematischen Erkenntnissen aus dem Bereich der Kryptographie.

Private Key

Eine entscheidende Rolle spielt dabei das asymmetrische Dual-Key-Verfahren. Dabei wird der *Private Key* eines Benutzers mit seinem Public Key kombiniert, um eine Bitcoin-Transaktion zu signieren.

Hash-Funktion

Ebenfalls auf kryptographischen Grundlagen basiert die sogenannte Hash-Funktion. Damit können beispielsweise IDs für einzelne Transaktionen generiert oder mehrere IDs von Transaktionen zu einem neuen eindeutigen Wert „verhashed“ werden.

Proof-of-Work

Daneben wird die Hash-Funktion auch bei der Verifikation von Bitcoin-Transaktionen angewendet. Die Hash-Funktion wird benutzt, um einen sogenannten *Proof-of-Work* zu erbringen.

3 Einrichten eines Bitcoin-Wallet

Was wird nun in der Praxis benötigt, um am Bitcoin Zahlungssystem teilnehmen zu können? Ein normales Bitcoin-Starter-Kit umfasst drei Komponenten:

1. Wallet
2. Private Key
3. Public Key

Wallet

Das *Wallet* ist die elektronische Geldbörse, in welcher die eigenen Bitcoins liegen. Es gibt grundsätzlich vier verschiedene Arten von Wallets: Online, Mobile, Desktop und Hardware/Paper. Ein typisches Online-Wallet kann innerhalb von wenigen Minuten angelegt werden. Es lässt sich aus Benutzersicht gut mit einem e-Banking Zugang vergleichen.[1]

Private Key

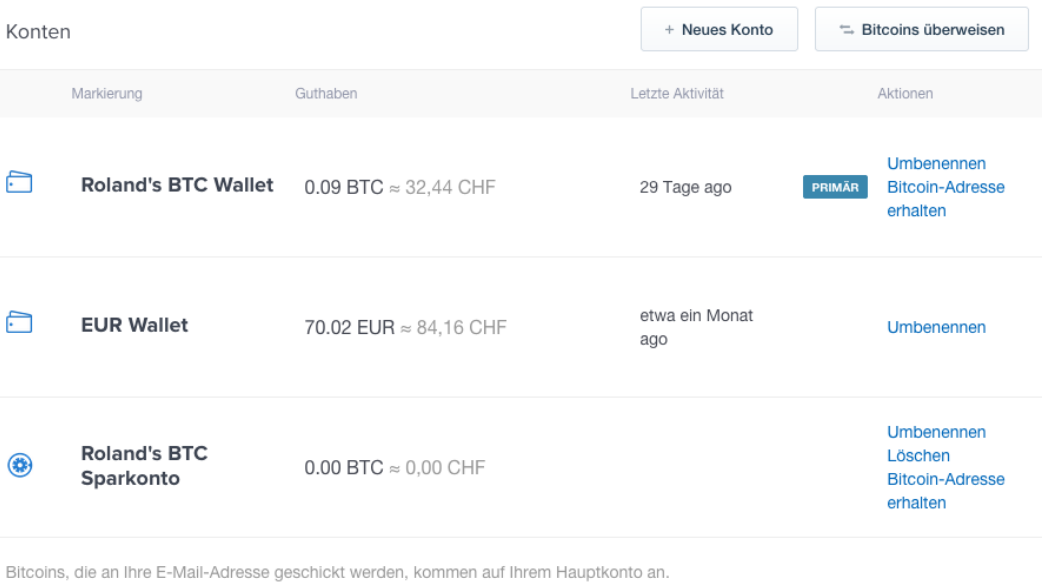
Der *Private Key* ist fest verbunden mit dem Wallet. Der Zugriff auf das Wallet und die sich darin befindlichen Bitcoins ist ausschliesslich mit diesem Schlüssel möglich. Ohne den Private Key können keine Transaktionen signiert werden. Wer ihn verliert, verliert alle Bitcoins im Wallet.

Public Key

Der *Public Key* ist die öffentlich bekannte Adresse, die zum Senden und Empfangen von Bitcoins benötigt wird. In Analogie zu herkömmlichen Bankkonten könnte dieser Schlüssel auch als IBAN des Wallets bezeichnet werden. Es ist möglich, für verschiedene Zwecke beliebig viele Public Keys anzulegen. Zur Verifikation von Transaktionen wird jeweils derjenige Public Key benötigt, von dem die Überweisung ausgegangen ist.

Die Abbildung unten zeigt die Benutzeroberfläche eines Bitcoin-Wallets. Im Beispiel handelt es sich um ein Online-Wallet des Anbieters *coinbase.com*.

Benutzer-Oberfläche eines Bitcoin-Wallets



[1] *siehe beispielsweise http://blockchain.info*

4 Überweisen von Bitcoins

Mit diesem Starter-Kit können unmittelbar nach dem Einrichten bereits eingehende Bitcoin-Transaktionen empfangen werden. Zu Beginn sind auf den Public Keys im Wallet keine Bitcoin-Guthaben vorhanden. Deshalb muss in einem ersten Schritt - in der Regel über eine normale Bank-Transaktion - Geld auf ein Konto bei der Partner-Bank des Wallet-Anbieters überwiesen werden. Der dorthin transferierte Betrag wird dann auf das Wallet übertragen. Im Falle des im obigen Beispiel gewählten Wallet-Anbieters coinbase.com dauert das ein bis zwei Arbeitstage. Danach können auch ausgehende Zahlungen getätigt werden.

Zahlung erfassen

Um eine Bitcoin-Transaktion zu tätigen, müssen auf der Wallet-Maske lediglich die Ziel-Adresse des Empfängers und der zu transferierende Betrag erfasst werden. Die Ziel-Adresse des Empfängers kann in Form des Public Keys oder als E-Mail-Adresse eingegeben werden. Noch einfacher kann eine Zahlung via Scannen eines QR Codes erfasst werden, welcher sowohl den Public Key als auch den Betrag bereits enthält.

Transaktion signieren

Beim Abschicken der Transaktion wird die sogenannte Transaktionsmessage erzeugt und mit dem privaten Schlüssel des Absenders signiert. Danach wird die Transaktionsmessage an das gesamte Bitcoin-Netzwerk versendet.

Bitcoins schürfen

Im Netzwerk wird die Transkation von den sogenannten *Minern* registriert. Die Bezeichnung Miner (oder deutsch *Mineur*) kann in Analogie zum Schürfen von „digitalem Gold“ interpretiert werden. Miner übernehmen im Netzwerk bestimmte Aufgaben und werden dafür mit neu erzeugten Bitcoins belohnt.

Auch das Schürfen von echtem Gold ist aufwändig und benötigt spezielles Werkzeug. Das ist bei Bitcoins nicht anders. Die Miner im Bitcoin-Netzwerk benötigen dazu eigens optimierte Hochleistungsrechner. Ihre Arbeit lässt sich vereinfacht auf zwei Kernaufgaben reduzieren:

1. Validieren von neuen Bitcoin-Transaktionen
2. Sequenzieren von neuen Bitcoin-Transaktionen

Validieren von Transaktionen

Die vollständige Validierung einer neuen Transaktion umfasst 18 technische Einzelprüfungen, im Zentrum steht jedoch die Prüfung von Signatur und Saldo.

Prüfen der Signatur

Die Prüfung der Signatur basiert auf dem speziellen Verhältnis von Private und Public Key. Um eine Transaktion zu signieren, wird der Private Key benötigt. Um die Korrektheit der Signatur zu prüfen, genügt hingegen der Public Key. Miner können also mit öffentlich verfügbaren Informationen verifizieren, ob die Transaktion tatsächlich vom angeblichen Sender ausgelöst wurde. Gleichzeitig kann nur der Sender mit seinem Private Key eigene Transkationen signieren.

Saldo-Prüfung

Bitcoin-Konten können grundsätzlich nicht überzogen werden. Entsprechend muss bei jeder Transaktion geprüft werden, ob der Sender über den notwendigen Bitcoin-Betrag auf seinem Public Key verfügt. Um diese Prüfung zu ermöglichen, werden jeder Zahlung die historischen Transaktionen mitgegeben, welche den Kontosaldo begründen. Die Struktur einer Bitcoin-Transaktion umfasst entsprechend einen Input- und einen Output-Bereich. Vereinfacht gesagt wird mit jeder Transaktion ein Kontoauszug des Senders mitgeschickt. Das erleichtert dem Miner die Prüfung des zur Verfügung stehenden Netto-Saldos. Die untenstehende Abbildung zeigt den Aufbau einer Transaktionsmessage mit Hash-Wert, Inputs (Eingaben) und Outputs (Ausgaben).

Erhalten	Betrag	Bestätigungen
ca4e822ad6bab84e75fa3772c65c9122b50bfda3ab98a5eb03f73d8df795ad69	24,62210000	0

ca4e822ad6bab84e75fa3772c65c9122b50bfda3ab98a5eb03f73d8df795ad69 — **0 confirmations**

Eingaben (mit Unterschrift)	Index / CB	→ Eingang	Ausgaben (Mit öffentlichem Schlüssel)		
1H6H15GrErtieRLe2VBeYKjT4v3…	10 / No	1,05983536 unconf	1,20888890	spent
1AyhaE9SB9NaiwUQk6cuQ6pFa…	10 / No	0,60220000 unconf	164hLn5bfYDJMrFiCPXy6uZQ6…	0,00960900	
1MpgHVLDjKm6AUrys8cywXZzx…	12 / No	1,05058494 unconf	1S4z6D7rmrRocUBTwhsz3ydTx…	1,19210000	
184j1TkGrDz4hDfR7mMz7Q2P4…	2 / No	1,01956166 unconf	1NYP8sRhSXEEdjwjZe7XpjnfuQ…	1,10197100	
1MMG9N7WEKT39bzPVCxFYe…	14 / No	1,30900000 unconf	1BXUaDNM8zMnwcp2REoif6xb…	1,21740000	
1PyFeNN6zTvmXqrEVsompsY46…	5 / No	6,21610000 unconf	1K85Eni2ayq2DrNwbhbt2unr1Xd…	1,26663000	
1tbFVRHHz9CL26c4XVbGmraqj…	11 / No	0,60100000 unconf	17j5xSbjc3QCuPKU7PpyixuZZd…	1,28390000	
13qALdQQJibLWTtQVSSN2oZb…	9 / No	0,96910048 unconf	18Y2TzwvUrh5AVDMp3ym4fzcj1…	1,19739684	spent
1PXRcd37NUwcQSv9dzM1tMQ…	11 / No	0,09670000 unconf	1ExpufpK8BqbxEjvNsUuT17yori…	1,09100000	
17zZKrbsLt7enPS4tCev6nJ9GNj…	24 / No	0,07200000 unconf	12xFkGyDb4DBY5ZXPjrsGikWiL…	1,15949839	spent
13i7PRFryAQRUJE2RRHTxYp6Y…	13 / No	1,04921086 unconf	1Cozu426obexyEL3tJg9EKkpcU…	1,26100000	
1Kqp8X9UnM7DjjDd4piN185iU…	15 / No	1,00207164 unconf	1AGUZzZdqGY2XLkJgqsinsRW…	1,08106000	
1GiqhJrMkZPhLrU1Sodn1CCPA…	7 / No	1,01760499 unconf	1AcWFgDkN9tuxeQcXn3kmFX7f…	1,16452410	spent
1KtX6qg8LARRg6McjJZwsDUsJ…	17 / No	1,31480000 unconf	12ZDdMUmxD4r2uLsvMBhEEg…	1,08300000	
12GdLwbugEGRMBebz43eBnM…	21 / No	1,03653007 unconf	1vtPWWA9kxtaTkeBSCGMmN1i…	1,18371374	spent
1BY7iwRoyhTPc9j3zBHHc2zdjy…	8 / No	6,20620000 unconf	1A5DAw6gwzY7hkZiYcwKtAT8H…	1,13538604	spent
			1Bbi3mhmmsRTvg2HoHkyqsSjP…	1,22020000	
			1DXsVBXnGuij7kP3Fvguxns8sU…	1,20213000	
			1JHfbrcmtQBMXDnUY2UTnMgb…	1,16740000	
			18c2xiyy8K8ug6MaVJ99Dtd95h…	1,15200000	
			1KwmK9EPK53BnbsGW8NZHN…	1,15459199	spent
			1JrKzFkVAi4Ca3Eoy8VWAznki6…	1,08870000	
			1NmV9szb116vYpQVKTJ78QdS…		

In Blöcken? Not yet **Zuerst gesehen:** November 11, 2014 07:35 (eine Minute ago) **Version:** 1 **Sperrzeit** 0 **Größe** 3 KB **Pool** tx pool **Gebühr:** 0.0004

Sequenzieren von Transaktionen

Sobald eine Transaktion die Validierung bestanden hat, wird sie von den Minern einem noch unbestätigten Block zugewiesen. Die nächste und deutlich schwierigere Aufgabe besteht nun darin, den unbestätigten Block zu bestätigen und der Blockkette hinzuzufügen.

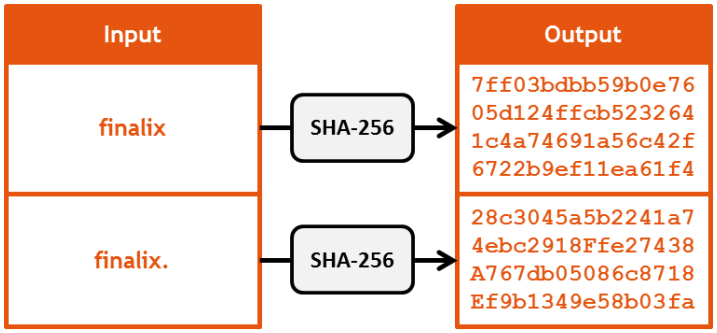
Double-Spending-Problem

Das Einhalten der korrekten Transaktionssequenz ist dabei von elementarer Wichtigkeit. Mit dem Bestätigungsprozess wird verhindert, dass der gleiche Bitcoin trotz verteilter Führung der Blockkette mehrfach ausgegeben werden kann (*Double-Spending-Problem*).

Grundlage für den Bestätigungsprozess ist die erwähnte Hash-Funktion. Konkret verwendet das Bitcoin-Protokoll den Algorithmus SHA-256[2]. Diese Funktion nimmt beliebige Input-Werte (z.B. einen Text) entgegen und gibt einen komplett zufälligen, alphanumerischen String von 64 Zeichen Länge zurück. Für die Sicherheit von Bitcoin-Transaktionen sind dabei zwei Eigenschaften entscheidend:

1. Unumkehrbarkeit
   Mit der Funktion SHA-256 kann ein Hash-Wert zwar sehr einfach erzeugt werden, es ist aber praktisch unmöglich, aus einem gegebenen Hash-Wert auf den Input zurückzuschliessen.
2. Lawineneffekt
   Bereits eine minimale Änderung des Input-Werts führt zu einem völlig anderen Hash-Wert.

Die untenstehende Abbildung zeigt exemplarisch, wie aus zwei fast identischen Text-Strings zwei komplett unterschiedliche Hash-Werte entstehen.[3]



Root-Hash

Um neue Transaktionen zu sequenzieren, kombinieren die Miner nun alle Transaktionen in einem unbestätigten Pool jeweils paarweise zu einem neuen Input für die Hash-Funktion. Damit werden die IDs der unbestätigten Transaktionen Schritt-für-Schritt verhashed. Am Ende der Aggregation steht ein eindeutiger Hash-Wert für den ganzen unbestätigten Block, ein sogenannter *Root-Hash*.

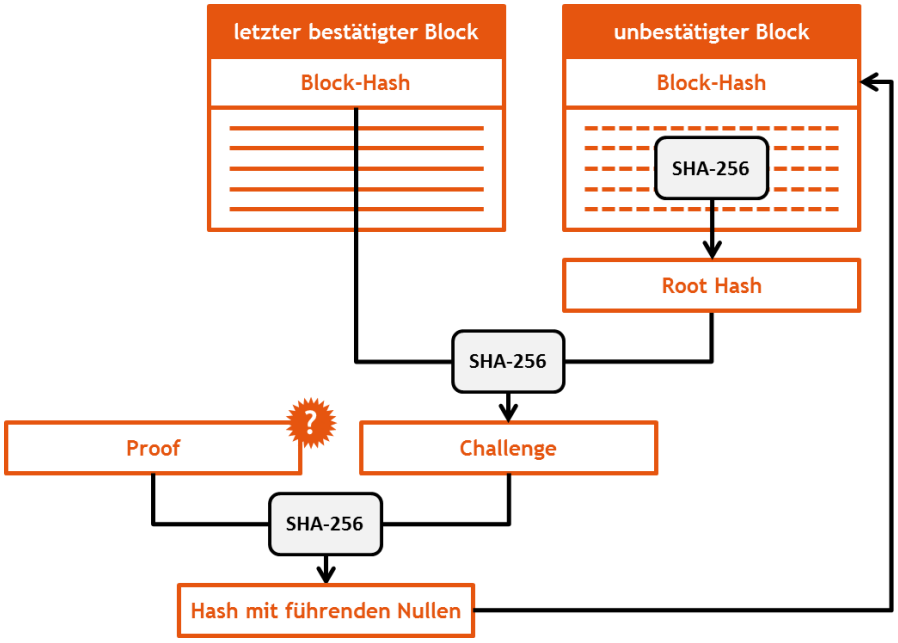
Challenge

Der Root-Hash wird nun wiederum mit dem Block-Hash des letzten bestätigten Blockes in der Kette verhashed. Der entstehende Hash-Wert wird als *Challenge* bezeichnet.

Proof-of-Work

Der Challenge bildet die Basis für den Arbeitsnachweis, den sogenannten *Proof-of-Work* der Miner. Das Werkzeug dafür ist wiederum die Hash-Funktion. Die Miner beginnen mit dem „Schürfen“ von neuen Bitcoins, sobald der Challenge vorliegt. Dabei suchen sie einen Input-Wert, den sogenannten *Proof*, der in Kombination mit dem Challenge einen Output-Wert mit einer festgelegten Anzahl führender Nullen ergibt. Der gesuchte Output-Wert wird später zum Block-Hash des neu bestätigten Blocks. Die untenstehende Abbildung gibt einen Überblick über den Ablauf des Proof-of-Work.

[2] *SHA steht für Secure Hash Algorithm, die Zahl 256 für die Länge des resultierenden Hash-Werts in Bits.*
[3] *Unter https://brainwallet.github.io können versuchsweise selbst Hash-Werte erzeugt werden.*



Lösung des Problems

Der Proof-of-Work wird umso schwieriger, je mehr führende Nullen verlangt werden. Die Anzahl der führenden Nullen wird schrittweise erhöht. Zurzeit dauert die Sequenzierung neuer Transaktionen im Bitcoin-Netzwerk rund 10 Minuten. Dazu müssen Milliarden verschiedener Kombinationen durchprobiert werden. Die Leistungsfähigkeit von Mining-Rechnern wird entsprechend in *Giga-Hash pro Sekunde* (GH/s) gemessen.

Bestätigung der Gültigkeit

Die Gültigkeit einer Lösung muss von mindestens sechs anderen Minern bestätigt werden. Sobald diese Bestätigungen vorliegen, wird der Hash mit den führenden Nullen als Block-Hash auf dem neuen Block eingetragen. Damit wird der Block bestätigt und in die Blockkette aufgenommen.

Die nachfolgende Abbildung zeigt die Stammdaten eines typischen Bitcoin-Blockes. Im Header sind die führenden Nullen im Hash-Wert ersichtlich. Zur Verankerung des Blocks in der Blockkette wird im Header auch die Referenz auf den Vorgänger-Block eingetragen.

Hash	00000000000000000139f9c7aa7920ecce658ba0e8e349e3187ac8a947ca6ce86
Vorheriger Block	00000000000000000073107dac8486a2bdfc2796c8b00a44432366c3f5c71a698
Nächster Block	00000000000000000a87983be97cfa04fce3cb7ff12c97f701590e8d5f73d080
Root-Hash	d663548df0cb60919de2390367099d94dd515cbb9569ca274970d84bf906d835
Höhe	329533
Transaktionen	641
Zeitstempel	2014-11-11 02:15:52
Bits	404472624
Nonce	317974384
Version	2
Zweig	main
Belohnung	25.00
Gebühren	0.08994003

Belohnung des Miners

Der schnellste Miner erhält als Gegenleistung für seine Arbeit neue Bitcoins. Derzeit werden mit jedem neuen Block 25 Bitcoins (also rund CHF 9‘000) liberiert.

Update der Blockkette

Der neue Block wird nun in den lokalen Kopien der Blockkette im Netzwerk nachgezogen. Damit werden die im Block enthaltenen Transaktionen quasi dezentral verbucht.

5 Zahlungsmittel im Vergleich

Herkömmliche Überweisungen

Wie unterscheidet sich nun eine Bitcoin-Transaktion von einer Transaktion mit traditionellen Zahlungsmitteln? Bei einer herkömmlichen Überweisung besitzen Sender und Empfänger je ein Konto bei einer Bank. Die Banken (oder die Post) bieten mit ihren Zahlungsverkehrsdienstleistungen die notwendige Drehscheibe für die Übertragung des Geldes vom Sender an den Empfänger. Validierung, Sequenzierung und Verbuchung von Transaktionen sind damit sichergestellt. Die Benutzer erlangen Sicherheit, weil Banken vom Staat reguliert werden und sowohl Organisation als auch Infrastruktur einer professionellen Governance unterliegen.

Bitcoin Zahlungen

Bei Zahlungen mit Bitcoins fehlen die Vorzüge institutionalisierter Sicherheit. An die Stelle der Banken tritt das Bitcoin-Netzwerk, welches die für einen funktionierenden Zahlungsverkehr benötigten Services erbringt.

Vergleich

Vor diesem Hintergrund stellt sich die Frage nach den Beweggründen für Einführung und Nutzung einer virtuellen Währung. Die untenstehende Abbildung zeigt die Eigenschaften von traditionellen Währungen, von Gold und von Bitcoins im Vergleich.

	Knapp	Beständig	Beweglich	Lagerfähig	Teilbar	Fungibel	Fälschungs-sicher	Geschützt	Akzeptiert
	+/-	+/-	+/-	+/-	+	+	+/-	+	+
	+	+	-	-	-	+/-	+	+	-
	+	+	+	+	+	+	+	+/-	-

Einschätzung

Bereits die Übersicht zeigt, dass virtuelle Währungen durchaus ihre Berechtigung haben. Im Detail dazu die folgende Einschätzung:

- Knappheit
  Bitcoins sind per Definition ein knappes Gut. Es wird nie mehr als 21 Millionen Bitcoins geben.
- Beständigkeit
  Da die Währung rein virtuell existiert, ist sie faktisch unzerstörbar (zumindest, solange das Internet existiert).
- Beweglichkeit
  Die Transaktionskosten von Bitcoin-Überweisungen sind vernachlässigbar.
- Lagerfähigkeit
  Bitcoins können kostenlos gelagert werden, z.B. in einem Online- oder Paper Wallet.
- Teilbarkeit
  Ein Bitcoin kann 10-Millionen-fach geteilt werden. Die kleinste Einheit wird als Satoshi bezeichnet.
- Fungibilität
  Bitcoins sind absolut homogen und daher austauschbar. Unterschiede wie beispielsweise bei den verschiedenen Qualitäten von Gold gibt es nicht.
- Fälschungssicherheit
  Bitcoins können aufgrund der kryptographischen Verschlüsselung und dem Mechanismus, wie die Blockkette konstruiert wird, nicht gefälscht werden.

- Sicherheit/Schutz
  Die Sicherheit ist massgeblich von der Vorsicht abhängig, mit welcher der Private Key gehandhabt wird. Unprofessionelle Services bei der Verwahrung dieser Schlüssel haben unter anderem zum Debakel um die Mt. Gox Börse geführt.

- Akzeptanz
  Aktuell liegt in diesem Bereich wohl noch der grösste Nachteil von Bitcoins als Währung. Der aktuelle Trend ist aber durchaus vielversprechend.

Fazit

Für eine abschliessende Beurteilung der Zukunftsaussichten von Bitcoins ist es noch zu früh. Ob es der Währung gelingen wird, die Akzeptanzschwelle zu überwinden und sich im Zahlungsverkehr zu etablieren, ist nicht zuletzt vom Verlauf der öffentlichen Meinungsfindung abhängig. Aktuell wechselt die Berichterstattung in den Medien mehr oder weniger täglich zwischen Boom und Bust. Entsprechend gleicht auch der Bitcoin-Kurs einem Wechselbad der Gefühle: An zehn Prozent der Tage schwankt der Wechselkurs von Bitcoins intraday um mehr als 10 Prozent! Umso erstaunlicher erscheint es, dass die grosse Mehrheit der Bitcoins eher als Wertaufbewahrungs- denn als Zahlungsmittel gehalten werden. Rund 80% der Bitcoins werden kaum je bewegt. Rein technisch hat das Bitcoin-Protokoll aber durchaus das Zeug zur ersten virtuellen Internet-Währung.