Harald Bögeholz, Fabian A. Scherschel

Währung im Kollektiv

So funktioniert die Kryptowährung Bitcoin

Bitcoin ist dezentral und frei von der Kontrolle durch Regierungen, Banken und Konzerne. Es wird deshalb von Freidenkern und Hackern als Währung der Zukunft gehandelt. Abgesichert sind die Vermögenswerte dabei durch die stringente Anwendung von Kryptografie.

Die virtuelle Währung Bitcoin arbeitet wie ein kollektives Buchführungssystem. Eine Art weltweites Rechnungsbuch vermerkt jede Transaktion und den Verbleib jeder virtuellen Münze. Zwar existiert eine Bitcoin (BTC) nur im Computer, doch das System sorgt dafür, dass die Gesamtzahl der Münzen begrenzt wird und niemand sie fälschen oder gar zweimal ausgeben kann. Dadurch schützt sich das Kollektiv der Nutzer gegen einzelne, böswillige Individuen: Solange die Mehrzahl der Teilhaber an der Verlässlichkeit der Währung interessiert ist, kann niemand die Buchführung manipulieren.

Bitcoins tauchen in diesem globalen Buchführungssystem nur als Teil von Transaktionen auf. Eine Transaktion ist im Kontext der Peer-to-Peer-Währung eine Nachricht an alle anderen Clients im Netzwerk, welche die Absicht ausdrückt, Geld von einer Bitcoin-Adresse an eine andere zu senden. Jeder Nutzer kann beliebig viele solcher Adressen erschaffen und Beträ-

ge zwischen ihnen hin- und herbuchen. Welche Adresse über wie viele Bitcoins verfügen kann, geht dabei aus der öffentlichen Transaktionshistorie hervor, die von jedem Teilnehmer im Netz geprüft werden kann. Hier steht genau, welche Bitcoin seit ihrer Entstehung wohin geflossen ist, und daraus folgt, über wie viele Bitcoins jede Adresse verfügen kann.

Bezahlen mit Bitcoins

Angenommen, Stefan möchte von Mary einen Webserver mieten. Da Mary ihre Hosting-Firma in den USA betreibt und Stefan in Deutschland lebt, ist Bitcoin eine attraktive Alternative zur Kreditkarte oder einem Online-Bezahldienst. Stefan kann Bitcoins relativ schnell und problemlos überweisen – und im Moment muss er dafür nicht mal Transaktionsgebühren bezahlen.

Als Erstes brauchen Stefan und Mary jeweils eine Bitcoin-Adresse. Um eine Adresse anzulegen, erzeugt Stefan ein Schlüsselpaar aus öffentlichem und privatem Schlüssel. Den privaten Schlüssel benötigt er, um seine Transaktionen mit dem Elliptic Curve Digital Signature Algorithm (ECDSA) kryptografisch sicher zu unterschreiben und allen anderen Teilnehmern im Netz zu bestätigen, dass er auch wirklich mit seiner Adresse diese Transaktion ausführen will. Ein Hash des öffentlichen Schlüssels ergibt die Bitcoin-Adresse. Das Ganze ist quasi ein öffentliches Konto: Alle Bitcoin-Nutzer wissen, wie viel Geld mit der Adresse verknüpft ist, aber niemand weiß, dass es Stefan gehört. Und niemand außer Stefan kommt an das Geld heran – jedenfalls, solange Stefan den geheimen Schlüssel nicht aus der Hand gibt. Jeder kann allerdings Geld an die Adresse überweisen und muss dafür nur die Adresse kennen.

Um seine erste Transaktion tätigen zu können, braucht Stefan erst einmal Bitcoins. Er kann zum Beispiel bei einem Anbieter im Netz Euros gegen Bitcoins tauschen: Er überweist dem Händler das Geld in Euro und der Händler schickt den entsprechenden Gegenwert in Bitcoins an die von Stefan angegebene Adresse. Oder Stefan könnte sich unter die Goldgräber begeben und seine Bitcoins selbst schürfen.

Angenommen, er hat vom Händler 5 Bitcoins (BTC) gekauft. Für den von ihm anvisierten Mietserver veranschlagt Marys Firma 0,2 BTC im Monat – also nach aktuellem Wechselkurs etwa 40 US-Dollar. Um Mary 0,2 BTC zu überweisen, generiert Stefans Bitcoin-Client eine Transaktion. Hier vermerkt er die Transaktion, mit der der Händler ihm die 5 BTC geschickt hat, als sogenannten Input. Die 0,2 BTC an Marys Bitcoin-Adresse sind der erste Output. Der zweite Output sendet die restlichen 4,8 BTC an Stefans eigene Adresse zurück. Das ist wichtig, denn man darf jeden Output nur einmal als Input einer Folgetransaktion verwenden. Der Restbetrag muss also einen eigenen Output bekommen.

Digitale Unterschrift

Stefan unterschreibt diese Transaktion mit seinem geheimen Schlüssel. Dann schickt sein Client sie an das Peer-to-Peer-Netz. Marys Client erfährt auf diesem Wege davon und sieht, dass 0,2 BTC an eine ihrer Adressen geschickt wurden. Mary kann dann mit Stefans öffentlichem Schlüssel die Signatur der Transaktion überprüfen. Ihre 0,2 BTC kann Mary jetzt in einer weiteren Transaktion verwenden.

Die digitalen Signaturen gewährleisten, dass nur der Empfänger eines Bitcoin-Betrags diesen wieder ausgeben kann. Jetzt muss nur noch sichergestellt werden, dass er dies nicht mehrfach tut. Dafür gibt es eine einfache Regel: Sollten mehrere Transaktionen mit demselben Input auftauchen, gilt nur die erste. Das durchzusetzen erfordert einen Zeitstempel für alle Transaktionen.

Es wäre ein Leichtes, wenn es eine zentrale Instanz gäbe, die alle Transaktionen nach Eingangsreihenfolge beglaubigt. In einem Peer-to-Peer-Netz, in dem alle gleichberechtigt sind und in dem man nicht weiß, wem man vertrauen kann, ist das etwas kniffliger. Im Bitcoin-System kann sich jeder Teilnehmer, der möchte, als Miner betätigen und an der Beglaubigung von Transaktionen mitarbeiten.

Mining

Ein Miner prüft alle eingehenden Transaktionen auf Gültigkeit (Signaturen stimmen, Ausgangssumme nicht größer als Eingangssumme, kein Output mehrfach als Input verwendet) und verwirft ungültige. Die gültigen sammelt er zu einem Block. Dazu packt er noch einen Zeitstempel und den Hash des vorangehenden Blocks sowie eine Zahl, die sogenannte Nonce. Über das Ganze bildet er einen Hash, indem er zweimal den SHA-256-Algorithmus anwendet. Das Bitcoin-System verlangt nun, dass dieser Hash kleiner als ein vorgegebener Zielwert sein muss.

Dadurch wird die Aufgabe, einen gültigen Hash zu finden, schwierig: Kryptografische Hash-Funktionen wie SHA-256 haben die Eigenschaft, dass sie nicht umkehrbar sind. Man kann also leicht zu einem Datenblock einen Hash finden, aber der umgekehrte Weg von einem vorgegebenen Hash zu einem Datenblock ist praktisch unmöglich. Die Hash-Funktion verhält sich fast wie ein Zufallsgenerator: Ändert man an den Eingabedaten auch nur ein Bit, kommt ein völlig anderes Ergebnis heraus.

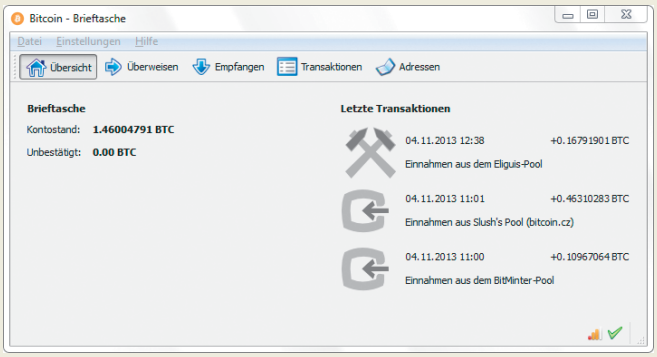
Wenn der errechnete Hash nicht kleiner als der geforderte Zielwert ist, bleibt dem Miner nichts anderes, als die Nonce eins hochzuzählen und den Block erneut zu hashen. Er tut dies so lange, bis der Hash zufällig einmal klein genug ist. Die Wahrscheinlichkeit, mit der das passiert, ergibt sich direkt aus dem Zielwert: Je kleiner die Zielvorgabe, desto geringer die Wahrscheinlichkeit, desto schwieriger also die Rechenaufgabe, einen geeigneten Hash zu finden.

Alle Miner arbeiten gleichzeitig an dieser Aufgabe, aber

Bitcoin-Wallets

Das Wallet eines Bitcoin-Clients ist eher ein Schlüsselbund als eine Geldbörse. Hier sichert man seine diversen Bitcoin-Adressen und kann nach Belieben neue anlegen. Die Adressen bestehen immer aus einem Paar von Schlüsseln, die mit dem ECDSA-Algorithmus erstellt wurden. Der öffentliche Schlüssel identifiziert die Adresse, der geheime erlaubt es dem Nutzer, an die mit der Adresse verknüpften Bitcoins zu kommen.

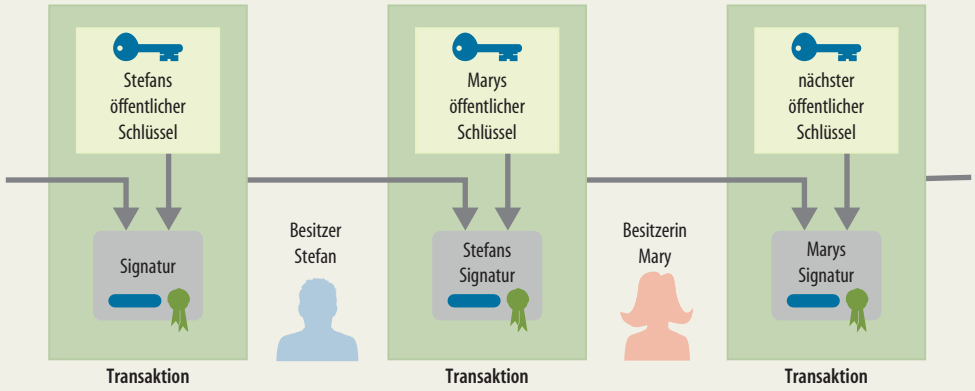
Die in dem Wallet gespeicherten Informationen sind alles, was man braucht, um über die virtuelle Währung verfügen zu können. Dementsprechend sollte es abgesichert werden. Backups sind hier unverzichtbar – stirbt die Festplatte, auf der das Wallet gespeichert ist, sind die Bitcoins weg. Auch sollte man darüber nachdenken, das Wallet eventuell zu verschlüsseln oder wenigstens mit einem guten Passwort abzusichern. Schon längst gibt es Trojaner, die beim Infizieren eines Rechners Bitcoin-Wallets abgreifen. Durch die hohe Anonymität bei der Benutzung der virtuellen Währung ist es so gut wie unmöglich, solchen Dieben auf die Schliche zu kommen.



Ein Wallet verwaltet beliebig viele Bitcoin-Adressen. Die Adressen sind Paare von öffentlichen und geheimen Schlüsseln, die zum Unterzeichnen von Transaktionen verwendet werden.

Das Bitcoin-Prinzip

Vereinfacht dargestellt ist eine elektronische Münze eine Kette digitaler Signaturen mit dem Besitzer am Ende. Der Besitzer gibt die Münze weiter, indem er ans Ende der Kette eine Transaktion anfügt und mit seinem geheimen Schlüssel unterschreibt. Mit dem öffentlichen Schlüssel lässt sie sich überprüfen.

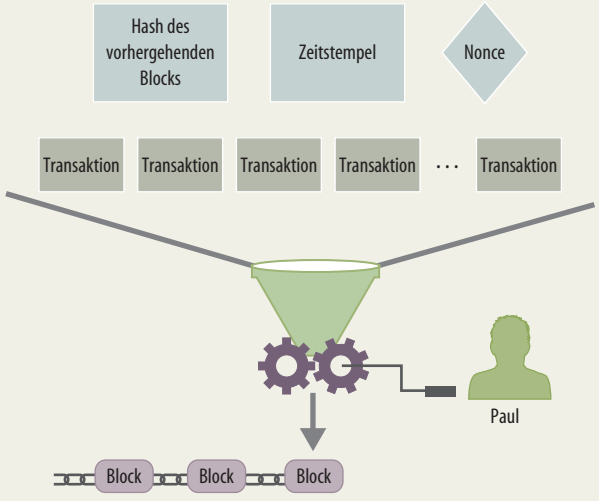


nicht exakt an derselben. Jeder Miner fügt nämlich in seinen Block eine spezielle Transaktion ein, die ihm den Lohn für seine Mühe in Form neuer Bitcoins überweist. Diese sogenannte Coinbase-Transaktion sammelt außerdem alle Transaktionsgebühren ein, die in den anderen Transaktionen in Form nicht ausgegebener Teilbeträge enthalten sind.

Der Miner, der als Erster einen gültigen Hash findet, hat das große Los gezogen und veröffentlicht seinen Block im Netz. Da der Block den Hash des vorigen Blocks enthält, sind die Blöcke miteinander verkettet zur sogenannten Blockchain. Einen gültigen Hash zu finden, ist wie gesagt sehr schwierig, ihn zu überprüfen aber leicht. Dazu muss man den Block nur einmal hashen und sich überzeugen, dass das Ergebnis mit dem veröffentlichten Hash übereinstimmt.

Beglaubigung durch Mining

Bitcoinminer Paul sammelt Transaktionen und überprüft sie. Er beglaubigt einen Block von Transaktionen, indem er einen Hash bildet. Das System verlangt, dass dieser kleiner als ein vorgegebener Zielwert ist. Paul muss daher die Nonce variieren und es immer wieder probieren. Findet er einen gültigen Hash, erhält er Bitcoins als Lohn.



Ewiges Rechnungsbuch

Die Blockchain ist das ewige Rechnungsbuch der Bitcoin-Währung. Nur Transaktionen, die darin enthalten und durch die fortlaufende Kette von Hashes wieder und wieder beglaubigt werden, sind gültig. Für den Fall, dass es einmal Verzweigungen in der Blockchain gibt, sind die Bitcoin-Clients so programmiert, dass sie beim Minen immer die längste Kette fortsetzen.

Dadurch ist das System robust gegen Störungen, etwa wenn das Netz vorübergehend in mehrere Teile zerfällt oder wenn zufällig zwei Miner gleichzeitig jeweils ihren gelösten Block veröffentlichen. Vor allem aber schützt das rechenintensive Mining vor Manipulationen. Ein Angreifer, der das System manipulieren wollte, müsste mehr Rechenleistung aufbringen als alle ehrlichen Teilnehmer des Systems zusammen.

Manipulationen sind ja vor allem für die Vergangenheit interessant, indem man nämlich zunächst jemandem Geld überweist und die entsprechende Transaktion dann – nachdem man den Gegenwert erhalten hat – wieder verschwinden lässt. Um einen alten Block zu manipulieren, müsste man aber eine gültige Kette von Blöcken errechnen, die länger als die ehrliche Kette wird. Das ist umso aussichtsloser, je länger der zu manipulierende Block zurückliegt. Wer so viel Rechenleistung unter seiner Kontrolle hat, betätigt sich besser als Miner und schürft so auf ganz legalem Wege Bitcoins. Damit trägt er zur Stabilität der Währung bei, was ja in seinem eigenen Interesse ist.

Steigende Schwierigkeit

Das Bitcoin-System passt die Schwierigkeit der Rechenaufgabe so an, dass im Schnitt alle zehn Minuten ein Block erzeugt wird. Dazu justiert es nach jeweils 2016 Blöcken die Zielvorgabe für die Hash-Funktion. Diese Anzahl Blöcke sollte 14 Tage gebraucht haben, sechs Blöcke pro Stunde. Ging es schneller, wird die Schwierigkeit erhöht, hat es länger gedauert, wird sie reduziert.

So sollte eine neue Transaktion nach ungefähr zehn Minuten in der Blockchain auftauchen. Wenn Händler und Kunden sicher sein wollen, dass wirklich Geld geflossen ist, warten sie bis dahin oder noch ein wenig länger: Je mehr Blöcke hinter einer Transaktion in der Blockchain hängen, desto unwahrscheinlicher ist es, dass diese Kette noch von einer längeren – mit einer anderen Version der Wahrheit – abgelöst wird.

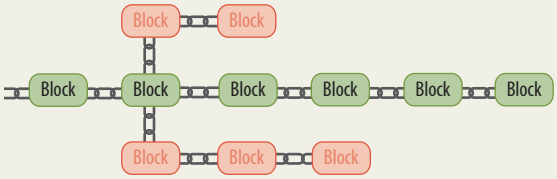
Zwar wurde die Schwierigkeit seit Bestehen der virtuellen Währung ein paar Mal nach unten angepasst, generell steigt sie aber – besonders seit Anfang 2013, als ASIC-basierte Spezialhardware für das Mining aufkam und so die Rechenleistung explodierte.

Deflation

Das Protokoll begrenzt die Anzahl an Bitcoins auf insgesamt 21 Millionen und garantiert somit eine Deflation der Währung [1]. Das Kollektiv halbiert dazu die Zahl der mit der Coinbase-Transaktion generierten Bitcoins ungefähr alle vier Jahre. Im Augenblick beträgt der Lohn für einen Block noch 25 BTC. Aber selbst wenn alle Bitcoins geschürft sind, beim aktuellen Tempo etwa um das Jahr 2140 herum, muss die Erzeugung von Blöcken weitergehen, da der Prozess des Bitcoin-Minings eben auch die Buchführung des Systems am

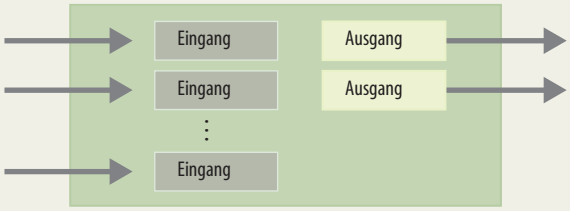
Die einzig wahre Blockchain

Die von den Minern errechneten Blöcke bilden eine Kette, die Blockchain. Sollte sie sich einmal verzweigen, betrachten Bitcoin-Clients immer die längste Kette als die echte. Kürzere Zweige werden verworfen. Ein Angreifer müsste mehr Rechenleistung als alle ehrlichen Clients zusammen haben, um mit einer manipulierten Kette die echte zu überholen.



Verschmelzen und teilen

Transaktionen haben mehrere Ein- und Ausgänge. Die Summe der Eingangsbeträge wird auf die Ausgänge verteilt. Eine eventuelle Differenz zwischen Eingangssumme und Ausgangssumme erhält der Miner als Transaktionsgebühr.

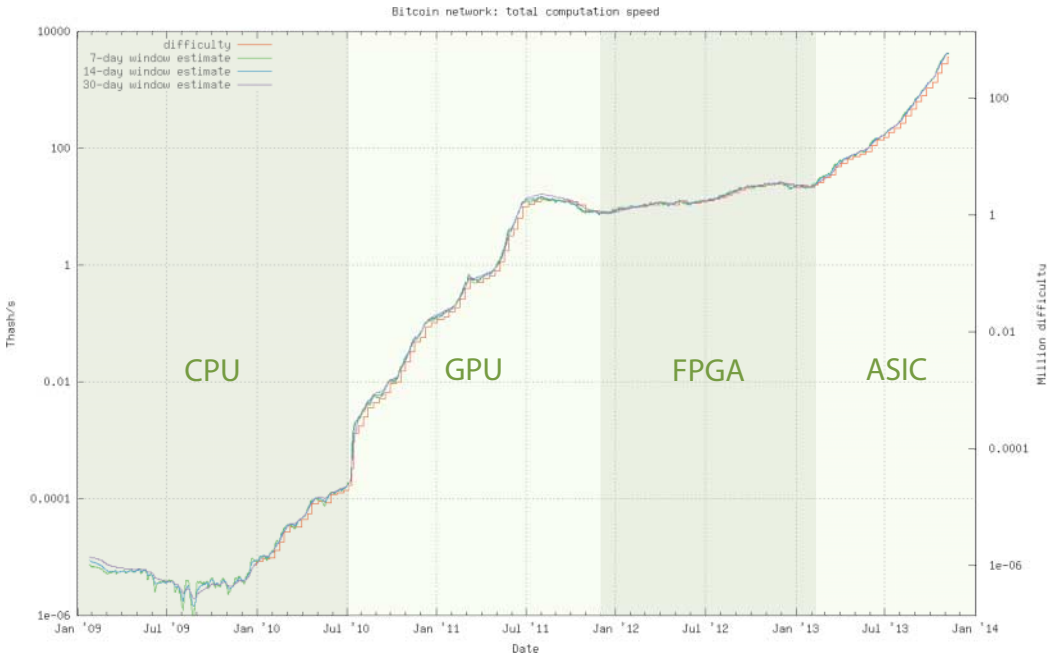


Laufen hält. Ohne ihn würden die Transaktionen nicht zu Blöcken verarbeitet und Nutzer des Systems könnten sich nicht sicher sein, dass mit der kollektiven Buchführung alles seine Richtigkeit hat.

Nach der Vorstellung der Erfinder sollen nach und nach die Transaktionsgebühren den Anreiz für das Mining bilden. Ein Miner könnte einfach nur solche Transaktionen in seine Blöcke aufnehmen, die ihn in angemessenem Umfang beteiligen. Transaktionen ganz ohne Spende würde er einfach unter den Tisch fallen lassen.

Momentan reicht die Rechenkraft im Netzwerk locker, um die anfallenden Transaktionen effektiv abzuarbeiten. Was aber passiert, wenn der Goldrausch vorbei ist und die zur Verfügung stehende Rechenkraft drastisch fällt, weil sich das Minen nicht mehr lohnt? Oder gar alle Bitcoins verteilt sind? Wenn Bitcoin als Währung zusätzlich den Durchbruch in den Mainstream schafft, wäre außerdem eine dramatische Erhöhung der Transaktionsdichte zu erwarten. So verarbeitet die Kreditkartenfirma Visa in der Weihnachtszeit über zehntausend Transaktionen pro Sekunde. Und Bitcoin soll ja irgendwann sogar Bargeld ersetzen können, also sind noch mehr Transaktionen zu erwarten.

Das Protokoll kann im Moment maximal sieben Transaktionen pro Sekunde verarbeiten. Für den Bitcoin-Kietz in Berlin [2] mag das reichen, nicht aber für den weltweiten Ersatz von Bargeld, von dem die Verfechter der virtuellen Währung träumen. Diese Grenze ist künstlich festgelegt und soll verhindern, dass die Blockchain zu schnell wächst. Immerhin muss sie von jedem Client heruntergeladen werden, um die komplette Transaktionshistorie überprüfen zu können, und hat vor Kurzem die Größe von 10 GByte überschritten. Allerdings ist das Bitcoin-Protokoll ähnlich wie andere technische Spezifikationen nicht in Stein gemeißelt, sondern kann im Konsens der Entwickler mit den teilnehmenden Nutzern modifiziert werden, um auf aktuelle Entwicklungen zu reagieren.



Die Schwierigkeit der zu lösenden Hashes steigt seit Einführung der virtuellen Währung. Gut zu erkennen sind die rapiden Anstiege, wenn bei der Blockerzeugung neue Technologien zum Einsatz kommen. So wurde zuerst mit der CPU und später der GPU von Desktop-Rechnern geschürft, mittlerweile kommt spezialisierte Hardware wie FPGAs und ASICs zum Einsatz.

Nach dem Goldrausch

Konzeptionell sollen professionelle Bezahldienstleister irgendwann die Goldrausch-Miner ablösen. Transaktionen würden dann auf großen, wahrscheinlich mit ASICs bestückten, Server-Racks mit Backbone-Anbindung abgewickelt werden. Diese Dienstleister würden dann mit den im Protokoll vorgesehenen Spenden bezahlt. Die Bitcoin-Community ist momentan recht zuversichtlich, dass diese spezialisierten Server auch ein Transaktionsvolumen von der Größenordnung des Visa-Systems bewältigen könnten.

Ob das wirklich stimmt, wird sich zeigen. Bis dahin ist denkbar, dass der Goldrausch noch eine Weile weitergehen wird, denn immer, wenn genug Miner aus dem System aussteigen, weil sich das Schürfen nicht mehr lohnt, fällt die Schwierigkeit. Und das ruft neue Goldgräber auf den Plan. (bo/fab)

Literatur

[1] Florian Hofmann, Jörn Loviscach, Virtuelles Vermögen, Die digitale Währung Bitcoin, c't 17/11, S. 74

[2] Axel Kannenberg, Coins für alle Fälle, Wie sich die Kryptowährung Bitcoin langsam etabliert, c't 19/13, S. 78