

Bitcoin Whitepaper verständlich erklärt

SWISSRATION LEITFADEN
TEIL 2.

Bitcoin Whitepaper verständlich erklärt

1. Was ist das Bitcoin-Whitepaper?

Am 31. Oktober 2008 veröffentlichte eine Person oder Gruppe unter dem Namen Satoshi Nakamoto ein technisches Dokument mit dem englischen Titel «Bitcoin: A Peer-to-Peer Electronic Cash System». Der Titel beschreibt ein System, mit dem Menschen elektronische Zahlungen direkt untereinander ausführen können, ohne dass dafür zwingend eine Bank oder ein anderer zentraler Zahlungsdienstleister als Vermittler benötigt wird. Mit «Peer-to-Peer» ist gemeint, dass Teilnehmer direkt miteinander in Verbindung treten können, ohne für jede Übertragung eine zentrale Stelle einschalten zu müssen. Bitcoin besteht dabei nicht aus physischen Geldscheinen oder Münzen. Es handelt sich um ein digitales Zahlungssystem, dessen Regeln von einem weltweit verteilten Computernetzwerk überprüft werden. Das Dokument wird als Bitcoin-Whitepaper bezeichnet. Ein Whitepaper ist ein Fachpapier, in dem eine Idee, ein bestehendes Problem und ein möglicher Lösungsweg beschrieben werden. Satoshi Nakamoto erklärte darin, wie ein elektronisches Zahlungssystem funktionieren könnte, bei dem keine einzelne Institution die gesamte Buchhaltung kontrolliert. Die zentrale Frage lautete: Wie können Menschen digitale Geldbeträge zuverlässig untereinander übertragen, wenn keine Bank darüber entscheidet, welche Zahlungen gültig sind?

Was war die besondere Idee?

Digitale Informationen lassen sich normalerweise beliebig kopieren. Ein Foto, ein Dokument oder eine andere Computerdatei kann auf mehreren Geräten gleichzeitig gespeichert werden. Jede Kopie enthält grundsätzlich dieselben Informationen. Bei einem digitalen Geldsystem würde dies zu einem erheblichen Problem führen. Wenn jemand einen digitalen Geldbetrag einfach kopieren könnte, wäre es möglich, denselben Betrag mehrfach auszugeben. Genau das muss ein funktionierendes Zahlungssystem verhindern. Satoshi Nakamoto stellte deshalb ein Verfahren vor, bei dem viele unabhängige Computer gemeinsam nach festgelegten Regeln überprüfen können, welche Zahlungen gültig sind. Dafür kombinierte er verschiedene technische Verfahren, die teilweise bereits zuvor bekannt waren. Dazu gehören digitale Signaturen, kryptographische Berechnungen, ein gemeinsames öffentlich überprüfbares Transaktionsregister und ein Verfahren, das als Arbeitsnachweis bezeichnet wird. Im Englischen heisst dieser Arbeitsnachweis «Proof of Work». Das Besondere an Bitcoin war nicht, dass sämtliche verwendeten Technologien neu erfunden wurden. Die entscheidende Neuerung bestand darin, diese Verfahren so miteinander zu verbinden, dass digitale Zahlungen ohne eine zentrale Buchungsstelle zuverlässig überprüft werden können.

Was erklärt das ursprüngliche Whitepaper?

Das Bitcoin-Whitepaper besteht aus einer einleitenden Zusammenfassung und zwölf aufeinander aufbauenden Abschnitten. Darin erklärt Satoshi Nakamoto unter anderem, wie elektronische Zahlungen freigegeben werden, wie das Netzwerk verhindert, dass derselbe Betrag mehrfach ausgegeben wird, und weshalb die Reihenfolge der Zahlungen eine entscheidende Rolle spielt. Ausserdem beschreibt er, wie neue Transaktionen bestätigt werden, weshalb dafür Rechenleistung eingesetzt wird und wie sich das Netzwerk gegen bestimmte Manipulationsversuche schützen soll. Weitere Abschnitte beschäftigen sich mit den wirtschaftlichen Anreizen für die Netzwerkteilnehmer, dem benötigten Speicherplatz, der vereinfachten Überprüfung von Zahlungen und dem Datenschutz. Zum Schluss untersucht Satoshi Nakamoto anhand mathematischer Überlegungen, unter welchen Voraussetzungen das vorgeschlagene System gegenüber bestimmten Angriffen widerstandsfähig ist. Diese einzelnen Bestandteile ergeben zusammen die technische Grundlage von Bitcoin.

Was erwartet dich in diesem Leitfaden?

In diesem zweiten Swisstration-Leitfaden beschäftigen wir uns mit dem ursprünglichen Bitcoin-Whitepaper aus dem Jahr 2008. Wir folgen der Reihenfolge des Originaldokuments und erklären jeden Abschnitt in verständlicher deutscher Sprache. Dabei geht es nicht um eine wortwörtliche Übersetzung der englischen Fachsprache. Unser Ziel ist es, die technischen Zusammenhänge so zu erklären, dass du sie auch ohne besondere Computerkenntnisse nachvollziehen kannst. Dafür verwenden wir Beispiele aus dem Alltag und einfache bildliche Darstellungen. Wichtige technische Begriffe werden erklärt, bevor sie verwendet werden. Mathematische Zusammenhänge werden dort vereinfacht dargestellt, wo dies für das Verständnis notwendig und ohne fachliche Verfälschung möglich ist. Dabei unterscheiden wir zwischen dem ursprünglichen Konzept von Satoshi Nakamoto und technischen Entwicklungen, die erst später entstanden sind. Das ist wichtig, denn Bitcoin wurde seit seiner Einführung weiterentwickelt. Das Whitepaper beschreibt die grundlegende Konstruktion, aber nicht jede Funktion des heutigen Netzwerks. Nach der Lektüre sollst du verstehen, welches Problem Satoshi Nakamoto lösen wollte, wie die verschiedenen technischen Bestandteile zusammenarbeiten und weshalb daraus ein funktionsfähiges digitales Zahlungssystem entstehen konnte.

ZIEL DES LEITFADENS:

Wir erklären nicht einfach, was Bitcoin heute ist, sondern wie Satoshi Nakamoto die ursprüngliche technische Lösung entwickelt und beschrieben hat. Du sollst nachvollziehen können, weshalb die einzelnen Bestandteile notwendig sind und wie sie gemeinsam funktionieren.

1.1 Die grundlegende Idee von Bitcoin

Verständliche Erklärung der Originalzusammenfassung

Am Anfang seines Whitepapers fasst Satoshi Nakamoto die wichtigste Idee seines Systems zusammen. Menschen sollen elektronische Zahlungen direkt untereinander ausführen können, ohne dass dafür zwingend eine Bank oder eine andere zentrale Institution als Vermittler benötigt wird. Damit ein solches System zuverlässig funktioniert, muss jedoch eine entscheidende Voraussetzung erfüllt sein: Niemand darf denselben digitalen Geldbetrag mehrfach ausgeben können. Dieses Problem wird als Doppelausgabeproblem bezeichnet. Im englischen Original verwendet Satoshi Nakamoto dafür den Begriff «Double Spending». Um zu verstehen, weshalb dieses Problem so wichtig ist, hilft ein einfaches Beispiel.

Warum digitale Zahlungen besondere Regeln benötigen

Stell dir vor, du besitzt eine digitale Datei auf deinem Computer. Diese Datei kannst du kopieren und anschliessend an mehrere Personen verschicken. Dabei bleibt die ursprüngliche Datei auf deinem Computer bestehen. Bei gewöhnlichen Informationen ist das erwünscht. Bei digitalem Geld wäre es jedoch problematisch. Angenommen, du besitzt einen digitalen Geldbetrag im Wert von 100 Franken. Wenn du diesen Betrag einfach kopieren könntest, wäre es theoretisch möglich, zuerst einer Person 100 Franken zu senden und anschliessend denselben Betrag noch einmal an eine andere Person zu übertragen. Beide Empfänger würden möglicherweise glauben, dass sie den Betrag rechtmässig erhalten haben. Tatsächlich wäre dadurch aber Geld mehrfach ausgegeben worden, das ursprünglich nur einmal vorhanden war. Ein digitales Zahlungssystem muss deshalb sicherstellen, dass ein bereits ausgegebener Betrag nicht ein zweites Mal verwendet werden kann. Bei gewöhnlichen Banküberweisungen übernimmt die Bank diese Aufgabe. Sie führt die Konten und prüft, ob ein bestimmter Betrag noch verfügbar ist. Bitcoin benötigt dafür eine andere Lösung, weil keine zentrale Bank die verbindliche Buchhaltung führen soll.

BEISPIEL:

Du besitzt einen verfügbaren Bitcoin-Betrag. Du versuchst, diesen Betrag gleichzeitig an zwei verschiedene Personen zu senden. Beide Zahlungen greifen auf denselben ursprünglichen Betrag zurück. Das Bitcoin-Netzwerk muss deshalb feststellen, welche Zahlung in die gültige Transaktionshistorie aufgenommen wird. Sobald dieser Betrag dort ausgegeben wurde, darf er nicht nochmals verwendet werden. So wird verhindert, dass derselbe Bitcoin-Betrag in der gültigen Transaktionshistorie mehrfach ausgegeben wird.

Wie löst Bitcoin dieses Problem?

Satoshi Nakamoto schlug vor, dass nicht eine einzelne Institution über die Gültigkeit von Zahlungen entscheidet. Stattdessen sollen viele unabhängige Computer nach denselben öffentlich bekannten Regeln arbeiten. Diese Computer bilden gemeinsam das Bitcoin-Netzwerk. Die Transaktionen werden an das Netzwerk übermittelt und können von entsprechend ausgestatteten Teilnehmern unabhängig überprüft werden. Dabei wird unter anderem kontrolliert, ob die notwendigen digitalen Freigaben vorhanden sind und ob die verwendeten Beträge bereits ausgegeben wurden. Gültige Transaktionen können anschliessend in sogenannten Blöcken zusammengefasst werden. Ein Block enthält Informationen über mehrere Bitcoin-Transaktionen. Diese Blöcke werden miteinander verbunden und bilden eine fortlaufende Transaktionshistorie. Sie wird Blockchain genannt. Damit nicht jeder Teilnehmer nach Belieben eine andere Version dieser Transaktionshistorie durchsetzen kann, verwendet Bitcoin einen besonderen Sicherheitsmechanismus. Diesen Mechanismus bezeichnet Satoshi Nakamoto als Proof of Work, auf Deutsch Arbeitsnachweis.

Warum benötigt Bitcoin einen Arbeitsnachweis?

Ein Arbeitsnachweis bedeutet vereinfacht, dass ein Computer bestimmte kryptographische Berechnungen durchführen muss, um einen neuen gültigen Block zu finden. Diese Berechnungen erfordern sehr viele Versuche und damit Rechenleistung. Ein erfolgreicher Arbeitsnachweis lässt sich von anderen Computern vergleichsweise einfach überprüfen. Das ist eine wichtige Eigenschaft. Einen passenden Arbeitsnachweis zu finden, ist aufwendig. Zu kontrollieren, ob ein gefundener Arbeitsnachweis die Bedingungen erfüllt, ist dagegen wesentlich einfacher. Dadurch kann das Netzwerk neue Blöcke überprüfen, ohne dass sämtliche Teilnehmer selbst die gesamte Rechenarbeit wiederholen müssen. Der Arbeitsnachweis schützt ausserdem die bereits entstandene Transaktionshistorie. Wer ältere bestätigte Zahlungen nachträglich verändern möchte, müsste eine konkurrierende gültige Geschichte aufbauen und dafür erneut erhebliche Rechenarbeit leisten. Gleichzeitig arbeitet das übrige Netzwerk weiter und fügt neue Blöcke hinzu. Ein Angreifer müsste deshalb mit seiner konkurrierenden Geschichte aufholen und die vom Netzwerk akzeptierte Kette an gesamter nachgewiesener Rechenarbeit übertreffen.

Weshalb werden ältere Zahlungen zunehmend schwerer veränderbar?

Stell dir vor, eine Bitcoin-Zahlung wurde gerade in einen neuen Block aufgenommen. Anschliessend entstehen weitere gültige Blöcke, die auf diesem Block aufbauen. Mit jedem zusätzlichen Block wächst die gesamte Rechenarbeit, die hinter dieser Transaktionshistorie steht. Wer die ursprüngliche Zahlung nachträglich verändern möchte, müsste eine alternative gültige Kette erstellen, in der diese Zahlung anders behandelt wird. Dafür müsste der Angreifer nicht nur die notwendige Rechenarbeit für den betroffenen Block erneut leisten. Er müsste auch eine konkurrierende Fortsetzung dieser Kette erzeugen und die weiterlaufende Arbeit des übrigen Netzwerks aufholen. Unter den Sicherheitsannahmen des Whitepapers wird ein solcher Angriff mit zunehmender Zahl von Bestätigungen immer unwahrscheinlicher. Dabei ist wichtig, dass Satoshi Nakamoto keine absolute Sicherheit behauptet. Die Sicherheit hängt wesentlich davon ab, wie viel Rechenleistung die ehrlichen Netzwerkteilnehmer gemeinsam kontrollieren und wie viel einem möglichen Angreifer zur Verfügung steht.

Das ursprüngliche Whitepaper geht insbesondere davon aus, dass die ehrlich arbeitenden Teilnehmer zusammen über mehr Rechenleistung verfügen als eine zusammenarbeitende Gruppe von Angreifern.

Warum benötigt Bitcoin keinen zentralen Betreiber?

Ein weiterer wichtiger Gedanke des Whitepapers betrifft die Organisation des Netzwerks. Bei einem herkömmlichen zentralen Zahlungssystem betreibt eine bestimmte Institution die verbindliche Buchhaltung. Bei Bitcoin können viele unabhängige Teilnehmer diese Buchhaltung nach denselben Regeln überprüfen. Jeder entsprechend ausgestattete Teilnehmer kann selbst kontrollieren, ob die erhaltenen Transaktionen und Blöcke gültig sind. Dafür muss er nicht einfach den Angaben eines einzelnen Unternehmens vertrauen. Ausserdem müssen die Computer nicht dauerhaft mit dem Netzwerk verbunden bleiben. Ein Teilnehmer kann das Netzwerk verlassen und später wieder beitreten. Bei seiner Rückkehr kann er die zwischenzeitlich entstandenen Daten beziehen und anhand der gültigen Netzwerkregeln überprüfen. Das System ist deshalb nicht auf einen einzigen zentralen Server angewiesen. Diese dezentrale Organisation bedeutet allerdings nicht, dass sämtliche Risiken verschwinden. Auch Bitcoin benötigt funktionierende Technik und ausreichende Netzwerkteilnahme. Die Sicherheit des Systems hängt ausserdem von den beschriebenen technischen und wirtschaftlichen Voraussetzungen ab.

MERKSATZ:

Die grundlegende Idee des Bitcoin-Whitepapers besteht darin, digitale Zahlungen ohne zwingend notwendige zentrale Abrechnungsstelle zu ermöglichen. Viele unabhängige Computer überprüfen die Transaktionen nach gemeinsamen Regeln. Eine öffentlich nachvollziehbare Transaktionshistorie und der Arbeitsnachweis sorgen gemeinsam dafür, dass derselbe digitale Betrag nicht beliebig mehrfach ausgegeben werden kann.

1.2 Warum ein neues digitales Zahlungssystem?

Verständliche Erklärung des Originalabschnitts «Introduction»

Im ersten Abschnitt seines Whitepapers beschreibt Satoshi Nakamoto, weshalb er ein anderes Verfahren für elektronische Zahlungen entwickeln wollte. Der Ausgangspunkt ist das Vertrauen. Wenn Menschen elektronisch bezahlen, benötigen sie im klassischen Finanzsystem normalerweise eine Bank oder einen Zahlungsdienstleister. Diese Institutionen übernehmen die Buchhaltung, kontrollieren Zahlungen und kümmern sich um deren Abwicklung. Sie sorgen beispielsweise dafür, dass ein Betrag vom Konto des Zahlenden abgebucht und dem Empfänger gutgeschrieben wird. Im Alltag funktioniert dieses Verfahren meistens zuverlässig. Allerdings ist damit eine Abhängigkeit verbunden. Die beteiligten Personen müssen darauf vertrauen, dass die zuständigen Institutionen ihre Aufgaben korrekt erfüllen. Satoshi Nakamoto wollte untersuchen, ob elektronische Zahlungen auch ohne eine solche zwingend notwendige zentrale Vertrauensinstanz möglich sind.

Warum können elektronische Zahlungen rückgängig gemacht werden?

Bei bestimmten elektronischen Zahlungsverfahren besteht die Möglichkeit, eine Zahlung unter festgelegten Voraussetzungen rückgängig zu machen. Das kann beispielsweise geschehen, wenn eine Zahlung nicht autorisiert wurde oder wenn es einen berechtigten Streitfall zwischen Käufer und Verkäufer gibt. Solche Verfahren haben durchaus Vorteile. Sie können Kunden vor bestimmten Formen von Betrug und fehlerhaften Abbuchungen schützen. Gleichzeitig verursachen sie Aufwand. Eine Bank oder ein Zahlungsdienstleister muss den Streitfall prüfen, Informationen einholen und gegebenenfalls über eine Rückabwicklung entscheiden. Für Händler kann dadurch zusätzliche Unsicherheit entstehen. Satoshi Nakamoto bezeichnet diese Abhängigkeit von vermittelnden Institutionen als eine grundlegende Schwäche des herkömmlichen elektronischen Zahlungsmodells.

Warum entstehen dadurch zusätzliche Kosten?

Stell dir vor, du betreibst ein kleines Geschäft und verkaufst Waren über das Internet. Ein Kunde bestellt einen Artikel und bezahlt elektronisch. Du erhältst eine Zahlungsbestätigung und versendest die Ware. Später beanstandet der Kunde die Zahlung. Je nach Zahlungsmethode und den geltenden Bedingungen kann daraufhin ein Verfahren zur Überprüfung oder Rückabwicklung beginnen. Du musst möglicherweise Unterlagen einreichen, den Versand nachweisen oder weitere Informationen zur Verfügung stellen. Auch der Zahlungsdienstleister muss den Fall bearbeiten. Solche Prüfungen verursachen Kosten. Diese Kosten entstehen nicht bei jeder einzelnen Zahlung in gleicher Höhe. Das gesamte Zahlungssystem muss jedoch entsprechende Verfahren und Sicherheitsmassnahmen bereitstellen. Satoshi Nakamoto argumentiert im Whitepaper, dass dadurch auch gewöhnliche elektronische Zahlungen teurer werden können. Besonders bei sehr kleinen Beträgen kann der Aufwand im Verhältnis zum Zahlungsbetrag erheblich sein. Ein Zahlungssystem, bei dem die Bearbeitung mehr kostet als der eigentliche Zahlungsbetrag, ist für bestimmte kleine Zahlungen wenig geeignet.

Warum müssen Händler ihren Kunden vertrauen?

Das herkömmliche elektronische Zahlungsmodell kann auch dazu führen, dass Händler zusätzliche Informationen über ihre Kunden benötigen. Wenn eine Zahlung später beanstandet werden kann, möchte sich der Händler möglichst gut gegen Betrug absichern. Deshalb werden je nach Situation beispielsweise persönliche Angaben, Rechnungsadressen oder weitere Informationen verlangt. Satoshi Nakamoto weist darauf hin, dass dadurch zusätzliche Anforderungen an das gegenseitige Vertrauen entstehen. Der Händler muss sich vor betrügerischen Käufern schützen. Der Käufer wiederum muss darauf vertrauen, dass der Händler die vereinbarte Ware oder Dienstleistung tatsächlich liefert. Das Whitepaper stellt deshalb die Frage, ob sich zumindest die technische Abwicklung einer Zahlung anders organisieren lässt.

Welche Rolle spielt die direkte Übergabe?

Wenn zwei Menschen persönlich einen Wertgegenstand übergeben, können sie den Austausch unmittelbar miteinander durchführen. Bei einer physischen Übergabe ist nicht zwingend eine Bank erforderlich, die den Vorgang elektronisch bestätigt.

Bei Zahlungen über das Internet fehlt diese Möglichkeit. Die beteiligten Personen befinden sich möglicherweise an unterschiedlichen Orten oder sogar in verschiedenen Ländern. Sie können sich den betreffenden Gegenstand nicht einfach persönlich überreichen. Deshalb werden elektronische Zahlungen normalerweise über technische Systeme und vermittelnde Institutionen abgewickelt. Satoshi Nakamoto wollte ein Verfahren entwickeln, das direkte elektronische Zahlungen auch über grosse Entfernungen ermöglicht. Dabei sollte nicht eine zentrale Organisation die Gültigkeit jeder Zahlung verbindlich feststellen müssen. Stattdessen sollte das Netzwerk anhand gemeinsamer technischer Regeln überprüfen können, ob eine Zahlung gültig ist.

Welche Lösung schlägt Satoshi Nakamoto vor?

Die vorgeschlagene Lösung beruht auf kryptographischen Nachweisen. Kryptographie bezeichnet mathematische Verfahren, mit denen Informationen geschützt und bestimmte Eigenschaften überprüft werden können. Bei Bitcoin werden solche Verfahren unter anderem dazu verwendet, elektronische Zahlungen mit digitalen Signaturen freizugeben. Eine digitale Signatur ist eine mathematisch erzeugte Bestätigung. Sie ermöglicht es dem Netzwerk zu prüfen, ob die erforderlichen geheimen Schlüssel für die Freigabe einer Zahlung verwendet wurden. Dabei müssen die geheimen Schlüssel selbst nicht veröffentlicht werden. Digitale Signaturen lösen allerdings noch nicht das gesamte Problem. Sie können nachweisen, dass eine Zahlung mit einem bestimmten Schlüssel freigegeben wurde. Sie verhindern für sich allein aber nicht, dass jemand versucht, denselben verfügbaren Betrag mehrfach auszugeben. Genau deshalb benötigt Bitcoin zusätzlich ein gemeinsames Verfahren, mit dem die Reihenfolge gültiger Zahlungen festgelegt werden kann. Diese Aufgabe übernimmt die Kombination aus öffentlicher Transaktionshistorie, Arbeitsnachweis und unabhängiger Überprüfung durch das Netzwerk.

Was bedeutet das für Verkäufer?

Für Verkäufer bietet das vorgeschlagene System eine wichtige Eigenschaft. Eine ausreichend bestätigte Bitcoin-Zahlung kann nicht einfach von einer zentralen Zahlungsstelle rückgängig gemacht werden. Mit zusätzlichen Bestätigungen wird eine nachträgliche Veränderung unter den üblichen Sicherheitsannahmen zunehmend schwieriger. Das kann bestimmte Risiken reduzieren, die bei rückbuchbaren elektronischen Zahlungsverfahren bestehen. Allerdings bedeutet dies nicht, dass jede empfangene Bitcoin-Zahlung sofort endgültig ist. Unbestätigte Zahlungen können durch konkurrierende Transaktionen gefährdet sein. Auch bei bestätigten Zahlungen besteht keine mathematisch garantierte absolute Endgültigkeit. Wie dieses Restrisiko mit zusätzlichen Bestätigungen abnimmt, untersucht Satoshi Nakamoto später im Whitepaper.

Was bedeutet das für Käufer?

Für Käufer entsteht durch die erschwerte Rückabwicklung eine andere Situation. Wenn du Bitcoin an eine falsche Empfangsadresse sendest oder an einen betrügerischen Verkäufer bezahlst, gibt es keine zentrale Stelle im Bitcoin-Netzwerk, die den Betrag einfach zurückholen kann. Das Netzwerk überprüft, ob die Zahlung technisch gültig ist. Es kontrolliert aber nicht, ob der Verkäufer ehrlich handelt oder ob eine Bestellung tatsächlich geliefert wird. Deshalb erwähnt Satoshi Nakamoto im ersten Abschnitt ausdrücklich, dass zusätzliche Schutzmechanismen für Käufer möglich sein sollen. Dazu gehören beispielsweise Treuhandverfahren. Bei einem Treuhandverfahren wird eine Zahlung

unter vorher vereinbarten Bedingungen verwaltet oder freigegeben. Ein solcher zusätzlicher Schutz ist jedoch nicht automatisch Bestandteil jeder Bitcoin-Transaktion. Er muss durch geeignete technische oder vertragliche Verfahren umgesetzt werden.

Was wollte Satoshi Nakamoto erreichen?

Das Ziel des ursprünglichen Whitepapers bestand nicht darin, sämtliche Aufgaben von Banken abzuschaffen. Satoshi Nakamoto wollte vielmehr ein elektronisches Zahlungssystem beschreiben, bei dem die Gültigkeit von Zahlungen nicht zwingend vom Vertrauen in eine zentrale Abrechnungsstelle abhängt. An die Stelle einer zentralen Buchhaltung sollte ein öffentlich überprüfbares System treten. Dieses System sollte es ermöglichen, digitale Beträge direkt zwischen Teilnehmern zu übertragen und gleichzeitig doppelte Ausgaben zu verhindern. Dafür waren mehrere technische Bestandteile erforderlich. Digitale Signaturen sollten Zahlungen absichern. Eine gemeinsame Transaktionshistorie sollte die Reihenfolge der Zahlungen nachvollziehbar machen. Ein Arbeitsnachweis sollte diese Historie gegen nachträgliche Veränderungen schützen. Und ein weltweit verteiltes Netzwerk sollte die Einhaltung der Regeln unabhängig überprüfen können. Wie diese Bestandteile im Einzelnen funktionieren, erklärt Satoshi Nakamoto in den folgenden Abschnitten seines Whitepapers.

MERKSATZ:

Das ursprüngliche Ziel von Bitcoin war ein elektronisches Zahlungssystem, bei dem Menschen digitale Beträge direkt untereinander übertragen können. Die Gültigkeit der Zahlungen soll durch überprüfbare technische Regeln sichergestellt werden, ohne dass dafür zwingend eine Bank als zentrale Abrechnungsstelle benötigt wird. Damit dies funktioniert, muss Bitcoin insbesondere verhindern, dass derselbe digitale Betrag mehrfach ausgegeben werden kann.

Zwei Wege, elektronisch zu bezahlen



Bei einer herkömmlichen elektronischen Zahlung übernehmen Banken oder Zahlungsdienstleister wesentliche Aufgaben der Abwicklung.

Bei Bitcoin können unabhängige Netzwerkteilnehmer die Gültigkeit einer Zahlung anhand gemeinsamer Regeln überprüfen.

Der Zahlungsempfänger benötigt deshalb nicht zwingend eine Bank, die diese Zahlung als zentrale Abrechnungsstelle bestätigt.

2. Wie funktionieren Bitcoin-Transaktionen?

Verständliche Erklärung des Originalabschnitts «Transactions»

Im zweiten Abschnitt seines Whitepapers erklärt Satoshi Nakamoto, wie digitale Geldbeträge von einer Person an eine andere übertragen werden können. Dabei steht eine entscheidende Frage im Mittelpunkt: Wie lässt sich überprüfen, dass eine Zahlung tatsächlich mit dem erforderlichen geheimen Schlüssel freigegeben wurde? Bei einer herkömmlichen Banküberweisung übernimmt die Bank diese Prüfung.

Sie kontrolliert beispielsweise, ob jemand über das entsprechende Konto verfügen darf. Bitcoin verwendet dafür ein anderes Verfahren. Die Freigabe einer Zahlung wird durch eine digitale Signatur nachgewiesen. Eine digitale Signatur ist eine mathematisch erzeugte Bestätigung. Sie ermöglicht es anderen Teilnehmern, die technische Berechtigung für eine Zahlung zu überprüfen, ohne dass dafür eine Bank als zentrale Kontrollstelle benötigt wird. Damit dies funktioniert, verwendet Bitcoin sogenannte kryptographische Schlüssel.

Was sind private und öffentliche Schlüssel?

Um das Prinzip zu verstehen, hilft ein Vergleich mit einer gewöhnlichen Unterschrift. Wenn du ein Dokument unterschreibst, bestätigst du damit normalerweise, dass du dessen Inhalt anerkennt. Bei Bitcoin übernimmt eine digitale Signatur eine ähnliche Aufgabe. Der entscheidende Unterschied besteht darin, dass die Unterschrift nicht mit einem Stift, sondern durch eine mathematische Berechnung erzeugt wird. Dafür werden zwei zusammengehörende Schlüssel verwendet. Der erste ist der private Schlüssel. Er ist geheim und dient dazu, eine Zahlung digital zu unterschreiben. Der zweite ist der öffentliche Schlüssel. Mit seiner Hilfe können andere überprüfen, ob eine digitale Signatur gültig ist. Der öffentliche Schlüssel darf bekannt sein. Der private Schlüssel muss dagegen geheim bleiben. Stell dir vereinfacht vor, du besitzt einen persönlichen Stempel, dessen Abdruck jeder überprüfen kann. Andere Menschen können erkennen, ob ein bestimmter Abdruck zu deinem Stempel passt. Sie erhalten dadurch aber nicht automatisch die Möglichkeit, selbst gültige Abdrücke zu erzeugen. Dieser Vergleich erklärt das Grundprinzip, ist technisch jedoch nicht vollständig. Bei Bitcoin sorgt ein mathematisches Verfahren dafür, dass sich eine digitale Signatur mit dem öffentlichen Schlüssel überprüfen lässt, ohne den privaten Schlüssel offenzulegen.

MERKSATZ:

Der private Schlüssel dient dazu, Bitcoin-Zahlungen digital freizugeben. Der zugehörige öffentliche Schlüssel ermöglicht die Überprüfung dieser Freigabe. Aus dem öffentlichen Schlüssel lässt sich der private Schlüssel mit den heute verwendeten mathematischen Verfahren praktisch nicht zurückberechnen.

Wie beschreibt Satoshi Nakamoto eine Bitcoin-Übertragung?

Satoshi Nakamoto beschreibt eine elektronische Geldeinheit im Whitepaper vereinfacht als eine Kette digitaler Signaturen. Damit meint er, dass sich die Weitergabe eines digitalen Geldbetrags durch aufeinanderfolgende, miteinander verbundene Freigaben nachvollziehen lässt. Stell dir drei Personen vor. Anna besitzt einen verfügbaren Bitcoin-Betrag. Sie möchte diesen Betrag an Beat übertragen. Beat möchte den erhaltenen Betrag später an Carla weitergeben. Bei der ersten Übertragung erstellt Anna eine digitale Signatur. Diese Signatur verbindet die bisherige Transaktion mit dem öffentlichen Schlüssel des neuen Empfängers Beat. Beat kann überprüfen, ob die entsprechende Freigabe gültig ist. Wenn Beat den Betrag später an Carla weitergeben möchte, erstellt er seinerseits eine neue Transaktion und gibt sie mit seinem privaten Schlüssel frei. Auch diese Übertragung kann überprüft werden. So entsteht eine nachvollziehbare Folge von Transaktionen. Wichtig ist dabei, dass die heutigen Bitcoin-Bestände technisch nicht als einzelne, dauerhaft unveränderte digitale Münzen gespeichert werden. Bitcoin arbeitet mit verfügbaren Beträgen aus früheren Transaktionen, die bei neuen Zahlungen verwendet werden können.

Wie solche Beträge zusammengeführt und aufgeteilt werden, erklärt Satoshi Nakamoto später in Abschnitt 9 seines Whitepapers.

Was überprüft das Bitcoin-Netzwerk?

Bei einer Bitcoin-Zahlung müssen verschiedene technische Voraussetzungen erfüllt sein. Zunächst muss die Transaktion auf einen Betrag verweisen, der nach den geltenden Regeln ausgegeben werden darf. Ausserdem müssen die erforderlichen Freigaben vorhanden sein. Das Netzwerk überprüft deshalb unter anderem die digitalen Signaturen und die zugehörigen Ausgabebedingungen. Dabei ist eine wichtige Unterscheidung notwendig. Das Bitcoin-Netzwerk überprüft nicht, ob eine Person im rechtlichen Sinn tatsächlich Eigentümer eines bestimmten Vermögenswerts ist. Es überprüft, ob die technischen Voraussetzungen für die Ausgabe erfüllt sind. Wenn beispielsweise jemand einen privaten Schlüssel stiehlt, kann er damit unter Umständen eine technisch gültige Zahlung erstellen. Das Netzwerk erkennt nicht automatisch, dass dieser Schlüssel unrechtmässig verwendet wurde. Die technische Gültigkeit einer Zahlung ist deshalb nicht dasselbe wie ihre rechtliche Zulässigkeit. Für das Verständnis des Whitepapers ist diese Unterscheidung besonders wichtig.

Warum reicht eine digitale Signatur allein nicht aus?

Jetzt kommen wir zu einem entscheidenden Problem. Eine digitale Signatur kann nachweisen, dass eine Transaktion mit dem erforderlichen privaten Schlüssel freigegeben wurde. Sie kann aber für sich allein nicht beweisen, dass derselbe verfügbare Betrag nicht bereits in einer anderen Transaktion verwendet wurde. Stell dir vor, Anna verfügt über einen Bitcoin-Betrag. Sie erstellt eine Zahlung an Beat. Gleichzeitig erstellt sie eine zweite Zahlung an Carla. Beide Zahlungen verwenden denselben ursprünglichen Betrag. Anna könnte beide Transaktionen mit ihrem privaten Schlüssel gültig unterschreiben. Die digitalen Signaturen wären damit möglicherweise beide korrekt. Trotzdem dürfen nicht beide Zahlungen in derselben gültigen Transaktionshistorie ausgeführt werden. Denn Anna kann denselben verfügbaren Betrag nicht zweimal ausgeben. Genau hier zeigt sich die Grenze digitaler Signaturen. Sie sichern die Freigabe einer Transaktion ab. Sie lösen aber noch nicht das Problem, welche von zwei miteinander konkurrierenden Zahlungen gültig sein soll.

Weshalb benötigt Bitcoin eine gemeinsame Transaktionshistorie?

Satoshi Nakamoto erklärt deshalb, dass die Teilnehmer des Netzwerks eine gemeinsame Grundlage benötigen, um über die Reihenfolge von Zahlungen entscheiden zu können. Bei einer Bank ist das relativ einfach. Die Bank führt eine zentrale Buchhaltung. Sie kann feststellen, welche Zahlung bereits verbucht wurde und welcher Betrag danach noch verfügbar ist. Bei Bitcoin soll jedoch keine einzelne Bank diese Entscheidung treffen. Stattdessen müssen sich unabhängige Netzwerkteilnehmer anhand gemeinsamer Regeln auf eine gültige Transaktionshistorie verständigen können. Dazu werden Transaktionen öffentlich an das Netzwerk übermittelt. Öffentlich bedeutet in diesem Zusammenhang nicht, dass automatisch die Namen aller beteiligten Personen bekannt sind.

Es bedeutet, dass die technischen Informationen der Transaktionen für die Überprüfung verfügbar gemacht werden. Anschliessend benötigt das Netzwerk ein Verfahren, um diese Transaktionen in eine gemeinsame Reihenfolge einzuordnen. Dabei zählt nicht einfach, wer nach seiner eigenen Uhr zuerst auf eine Schaltfläche gedrückt hat.

Entscheidend ist, welche Ausgabe in der vom Netzwerk akzeptierten Transaktionshistorie enthalten ist. Wird ein verfügbarer Betrag dort ausgegeben, kann eine konkurrierende Zahlung denselben Betrag nicht zusätzlich verwenden. Wie Bitcoin diese gemeinsame Reihenfolge ohne zentrale Kontrollstelle organisiert, beschreibt Satoshi Nakamoto im nächsten Abschnitt.

BEISPIEL:

Anna besitzt einen verfügbaren Bitcoin-Betrag. Sie erstellt zwei unterschiedliche Zahlungen:

Zahlung A: Der Betrag soll an Beat gehen. Zahlung B: Derselbe Betrag soll an Carla gehen. Beide Zahlungen können eine gültige digitale Signatur besitzen. Trotzdem dürfen nicht beide ausgeführt werden. Das Netzwerk benötigt deshalb eine gemeinsame Transaktionshistorie, die festlegt, welche Ausgabe des Betrags gültig ist.

MERKSATZ:

Digitale Signaturen ermöglichen es, Bitcoin-Zahlungen ohne Offenlegung privater Schlüssel zu überprüfen. Sie allein verhindern jedoch nicht, dass jemand versucht, denselben Betrag mehrfach auszugeben. Dafür benötigt Bitcoin zusätzlich eine gemeinsam überprüfbare Transaktionshistorie.

GRAFIK 2

Von Anna über Beat zu Carla

So wird eine Bitcoin-Übertragung mit einem privaten Schlüssel freigegeben und mit einer digitalen Signatur überprüft.



Die digitalen Signaturen weisen die **technische Freigabe** nach. Ob ein Betrag bereits ausgegeben wurde, muss zusätzlich anhand der **gültigen Transaktionshistorie** geprüft werden.

Bei Bitcoin wird die Freigabe einer Zahlung durch eine digitale Signatur nachgewiesen. Der private Schlüssel muss dafür nicht an den Empfänger weitergegeben werden.

3. Wie entsteht eine überprüfbare zeitliche Reihenfolge?

Verständliche Erklärung des Originalabschnitts «Timestamp Server»

Im dritten Abschnitt seines Whitepapers beschreibt Satoshi Nakamoto, wie sich eine nachvollziehbare Reihenfolge von Transaktionen herstellen lässt.

Im englischen Original verwendet er dafür den Begriff «Timestamp Server». Sinngemäss lässt sich dieser Ausdruck als System zur zeitlichen Dokumentation von Daten verstehen. Die Grundidee besteht darin, digitale Informationen so miteinander zu verbinden, dass spätere Veränderungen erkennbar werden. Für Bitcoin ist das besonders wichtig. Denn das Netzwerk muss nachvollziehen können, welche Transaktionen bereits in die gültige Geschichte aufgenommen wurden. Nur so kann es verhindern, dass derselbe verfügbare Betrag mehrfach ausgegeben wird.

Warum ist die Reihenfolge entscheidend?

Stell dir vor, zwei Personen führen unabhängig voneinander ein Kassenbuch. Beide erhalten Informationen über dieselben Zahlungen. Allerdings treffen die Informationen nicht immer in derselben Reihenfolge ein. Die erste Person erfährt zuerst von einer Zahlung an Beat. Die zweite Person erfährt zuerst von einer konkurrierenden Zahlung an Carla. Wenn beide Zahlungen denselben ursprünglichen Betrag verwenden, entsteht ein Problem. Ohne gemeinsame Grundlage könnten die beiden Personen zu unterschiedlichen Ergebnissen kommen. Bei Bitcoin können Transaktionen ebenfalls zu unterschiedlichen Zeitpunkten bei verschiedenen Netzwerkteilnehmern eintreffen. Das liegt daran, dass Informationen über ein weltweit verteiltes Computernetzwerk übertragen werden. Die Teilnehmer benötigen deshalb ein Verfahren, mit dem eine gemeinsame Geschichte gültiger Zahlungen aufgebaut werden kann. Satoshi Nakamoto beginnt die Lösung dieses Problems mit einem Verfahren zur nachprüfaren Dokumentation von Daten.

Was ist ein digitaler Fingerabdruck?

Ein zentrales Hilfsmittel ist der sogenannte Hash. Ein Hash ist das Ergebnis einer mathematischen Berechnung. Ein Computer verarbeitet dabei bestimmte Daten und erzeugt daraus eine Zeichenfolge fester Länge. Diese Zeichenfolge kann man sich vereinfacht wie einen digitalen Fingerabdruck vorstellen. Der Fingerabdruck hängt von den ursprünglichen Daten ab. Werden die Daten verändert, entsteht mit überwältigender Wahrscheinlichkeit ein anderer Fingerabdruck. Stell dir vor, du schreibst einen Brief und lässt von einem Computer dessen digitalen Fingerabdruck berechnen. Anschliessend änderst du nur ein einziges Wort des Briefes. Wenn du den Fingerabdruck erneut berechnen lässt, erhältst du ein anderes Ergebnis. So kann überprüft werden, ob die vorliegenden Daten noch mit dem ursprünglichen Fingerabdruck übereinstimmen. Der Fingerabdruck verrät allerdings nicht den vollständigen Inhalt des Briefes. Aus ihm allein lässt sich der ursprüngliche Text nicht einfach wiederherstellen. Bei Bitcoin werden solche Fingerabdrücke verwendet, um Daten miteinander zu verbinden und Veränderungen erkennbar zu machen.

BEISPIEL:

Ein Verein veröffentlicht jeden Monat seinen Kassenbericht. Für jeden Bericht wird zusätzlich ein digitaler Fingerabdruck berechnet. Wenn später jemand einen Betrag im Kassenbericht verändert, passt der ursprüngliche Fingerabdruck nicht mehr zu den geänderten Daten. Dadurch kann eine nachträgliche Veränderung erkannt werden. Der Fingerabdruck verhindert die Veränderung nicht unmittelbar. Er macht sie jedoch überprüfbar.

Wie entsteht daraus ein zeitlicher Nachweis?

Satoshi Nakamoto beschreibt im Whitepaper ein einfaches Grundprinzip. Mehrere Informationen werden zu einem Datenpaket zusammengefasst. Anschliessend wird für dieses Datenpaket ein digitaler Fingerabdruck berechnet. Dieser Fingerabdruck wird öffentlich bekannt gemacht. Satoshi erwähnt dafür beispielsweise die Veröffentlichung in einer Zeitung oder in einem öffentlich zugänglichen Nachrichtensystem. Der Gedanke dahinter ist einfach. Wenn der Fingerabdruck eines bestimmten Datenpakets bereits zu einem früheren Zeitpunkt veröffentlicht wurde, lässt sich später überprüfen, ob das Datenpaket zu dieser Veröffentlichung passt. So entsteht ein Nachweis, dass die betreffenden Daten spätestens zum Zeitpunkt der Veröffentlichung vorhanden gewesen sein müssen. Dabei ist wichtig, dass ein solcher Nachweis nicht automatisch den exakten Entstehungszeitpunkt jeder einzelnen Information feststellt. Er dokumentiert vielmehr, dass bestimmte Daten bereits zu einem nachweisbaren Zeitpunkt existiert haben.

Warum werden mehrere Datenpakete miteinander verbunden?

Der nächste Schritt ist besonders wichtig. Satoshi Nakamoto schlägt vor, dass jedes neue Datenpaket zusätzlich den digitalen Fingerabdruck des vorherigen Datenpakets enthält. Dadurch entsteht eine fortlaufende Verbindung. Stell dir drei aufeinanderfolgende Blöcke vor. Block 1 enthält bestimmte Informationen. Aus diesen Informationen wird ein digitaler Fingerabdruck berechnet. Block 2 enthält neue Informationen und zusätzlich einen Verweis auf den Fingerabdruck von Block 1. Block 3 enthält wiederum neue Informationen und einen Verweis auf den Fingerabdruck von Block 2. Auf diese Weise hängen die drei Blöcke miteinander zusammen. Wenn jemand nachträglich den Inhalt von Block 1 verändert, entsteht für diesen Block ein anderer Fingerabdruck. Der bisherige Verweis in Block 2 passt dann nicht mehr. Damit die Verbindung wieder stimmen würde, müsste auch Block 2 entsprechend verändert werden. Dadurch würde sich wiederum sein Fingerabdruck ändern. Diese Veränderung hätte Auswirkungen auf Block 3. So setzt sich die Abhängigkeit entlang der gesamten Kette fort.

Warum ist diese Verkettung nützlich?

Die Verbindung der Blöcke macht nachträgliche Veränderungen erkennbar. Eine einzelne Information kann nicht einfach ausgetauscht werden, ohne dass dies Auswirkungen auf die nachfolgenden Verweise hat. Je mehr Blöcke auf einem früheren Block aufbauen, desto weiter reichen diese Auswirkungen. Damit entsteht eine nachvollziehbare Abfolge von Datenpaketen. Diese Konstruktion bildet einen wesentlichen Bestandteil der Blockchain. Der Begriff Blockchain bedeutet übersetzt Blockkette.

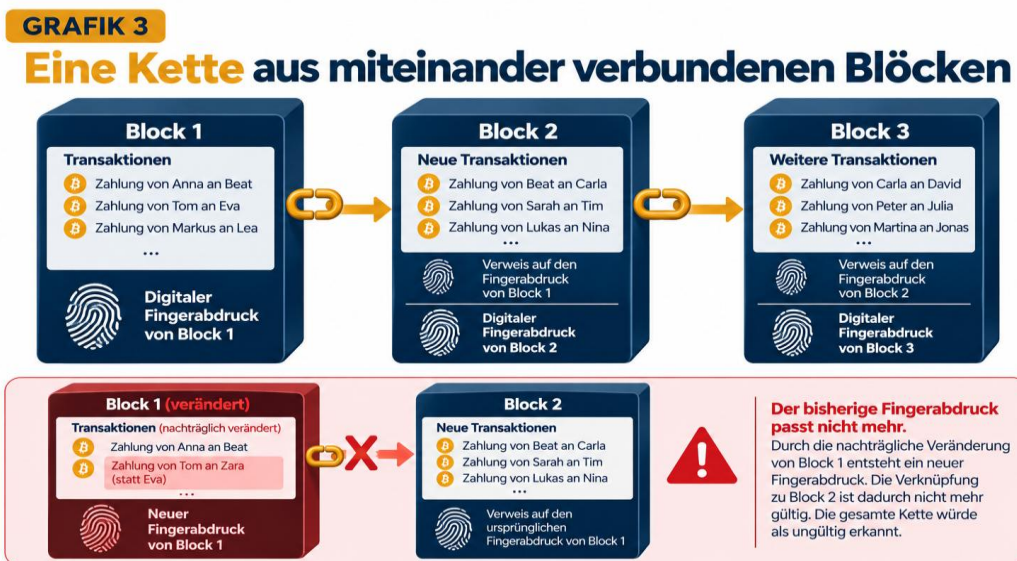
Er beschreibt, dass einzelne Datenblöcke mithilfe kryptographischer Verweise miteinander verbunden sind. Allerdings ist die Verkettung allein noch kein vollständiger Schutz gegen einen Angreifer. Jemand könnte theoretisch mehrere Blöcke verändern und anschliessend alle dazugehörigen Fingerabdrücke neu berechnen. Dafür benötigt Bitcoin einen zusätzlichen Schutzmechanismus. Genau diesen beschreibt Satoshi Nakamoto im folgenden Abschnitt seines Whitepapers.

Bedeutet ein Zeitstempel eine genaue Uhrzeit?

Der Begriff Zeitstempel kann leicht missverstanden werden. Er könnte den Eindruck erwecken, dass Bitcoin jede Zahlung mit einer amtlich bestätigten, sekundengenauen Uhrzeit versieht. Das ist nicht der Fall. Bitcoin-Blöcke enthalten zwar Zeitangaben. Diese werden jedoch nicht von einer zentralen, verbindlichen Uhr festgelegt. Ausserdem ist der Zeitpunkt, zu dem eine Transaktion erstellt oder an das Netzwerk gesendet wird, nicht zwangsläufig identisch mit dem Zeitpunkt ihrer Aufnahme in einen Block. Für die Sicherheit von Bitcoin ist vor allem die nachvollziehbare Abfolge der akzeptierten Blöcke entscheidend. Diese Abfolge zeigt, welche Transaktionen Teil der gemeinsamen Geschichte geworden sind. Eine exakte zeitliche Reihenfolge sämtlicher ursprünglich versendeter Transaktionsnachrichten lässt sich daraus dagegen nicht ableiten.

MERKSATZ:

Bitcoin verbindet Datenblöcke mithilfe digitaler Fingerabdrücke. Jeder neue Block verweist auf den vorherigen Block. Dadurch entsteht eine nachvollziehbare Kette, in der nachträgliche Veränderungen erkennbar werden. Damit ein Angreifer nicht einfach die gesamte Kette neu berechnen kann, benötigt Bitcoin zusätzlich einen Arbeitsnachweis.



Jeder Block enthält einen Verweis auf den vorherigen Block. Werden frühere Daten verändert, passen die bisherigen Verknüpfungen nicht mehr. Der zusätzliche Arbeitsnachweis erschwert es, eine veränderte Kette als gültige Geschichte durchzusetzen.

4. Proof of Work – warum Bitcoin Rechenarbeit benötigt

Verständliche Erklärung des Originalabschnitts «Proof-of-Work»

Im vierten Abschnitt seines Whitepapers beschreibt Satoshi Nakamoto den Sicherheitsmechanismus, der die miteinander verbundenen Blöcke gegen nachträgliche Veränderungen schützen soll. Dieser Mechanismus wird Proof of Work genannt. Auf Deutsch bedeutet das Arbeitsnachweis. Die Grundidee lautet: Wer einen neuen Block erstellen möchte, muss zuerst eine bestimmte Rechenaufgabe lösen. Diese Aufgabe ist so gestaltet, dass das Finden einer passenden Lösung viel Rechenarbeit erfordern kann. Andere Computer können anschliessend vergleichsweise einfach überprüfen, ob die gefundene Lösung gültig ist. Dadurch entsteht ein Unterschied zwischen dem Aufwand für die Erstellung eines Blocks und dem Aufwand für seine Überprüfung.

Warum reicht eine einfache Blockkette nicht aus?

Im vorherigen Kapitel haben wir gesehen, dass Bitcoin-Blöcke durch digitale Fingerabdrücke miteinander verbunden sind. Diese Verbindung macht Veränderungen erkennbar. Sie verhindert aber noch nicht, dass jemand eine vollständig neue Kette berechnet. Stell dir vor, ein Angreifer möchte eine frühere Zahlung nachträglich verändern. Er könnte theoretisch den betreffenden Block anpassen und anschliessend die digitalen Fingerabdrücke aller folgenden Blöcke neu berechnen. Wenn dafür nur gewöhnliche, schnell ausführbare Berechnungen notwendig wären, könnte der Angreifer relativ leicht eine veränderte Geschichte erstellen. Das Netzwerk müsste dann entscheiden, welche der unterschiedlichen Geschichten gültig sein soll. Bitcoin löst dieses Problem, indem die Erstellung eines neuen Blocks mit einem zusätzlichen Rechenaufwand verbunden wird. Eine gültige Blockkette kann deshalb nicht beliebig schnell neu erzeugt werden.

Wie funktioniert der Arbeitsnachweis?

Satoshi Nakamoto beschreibt dafür ein Verfahren, bei dem ein Computer sehr viele unterschiedliche Werte ausprobiert. Für jeden Versuch wird ein digitaler Fingerabdruck berechnet. Dieser Fingerabdruck muss eine bestimmte mathematische Bedingung erfüllen. Im Whitepaper beschreibt Satoshi diese Bedingung anhand einer vorgegebenen Anzahl von Nullen am Anfang des berechneten Ergebnisses. Die Berechnung verwendet ein kryptographisches Verfahren namens SHA-256. Du musst diese Bezeichnung nicht auswendig lernen. Entscheidend ist das Grundprinzip. Der Computer kann nicht einfach vorhersagen, welcher Versuch zum gewünschten Ergebnis führt. Er muss unterschiedliche Möglichkeiten ausprobieren. Erst wenn ein berechneter Fingerabdruck die vorgegebenen Anforderungen erfüllt, wurde ein gültiger Arbeitsnachweis gefunden. Der dafür verwendete Wert wird im Whitepaper als Nonce bezeichnet. Das ist ein veränderbarer Wert, mit dem der Computer unterschiedliche Berechnungsversuche durchführen kann. Wenn ein Versuch nicht erfolgreich ist, verändert der Computer diesen Wert und berechnet einen neuen Fingerabdruck. Heute können bei der Blocksuche zusätzlich weitere veränderbare Daten verwendet werden.

Das Grundprinzip bleibt jedoch gleich: Es müssen sehr viele Berechnungsversuche durchgeführt werden, bis ein gültiges Ergebnis gefunden wird.

Ein Vergleich mit einem Zahlenschloss

Stell dir ein Zahlenschloss mit sehr vielen möglichen Kombinationen vor. Du kennst die richtige Zahlenkombination nicht. Deshalb musst du unterschiedliche Kombinationen ausprobieren. Manchmal findest du die passende Kombination nach wenigen Versuchen. Manchmal benötigst du sehr viele Versuche. Sobald die richtige Kombination gefunden wurde, lässt sich dagegen schnell überprüfen, ob sie tatsächlich funktioniert. Beim Arbeitsnachweis von Bitcoin besteht ein ähnlicher Unterschied. Das Finden einer gültigen Lösung kann aufwendig sein. Die anschließende Überprüfung ist vergleichsweise einfach. Der Vergleich mit dem Zahlenschloss erklärt allerdings nur den Unterschied zwischen Suchen und Prüfen. Bei Bitcoin wird kein gewöhnliches Schloss geöffnet. Stattdessen muss das berechnete Ergebnis eine mathematisch festgelegte Bedingung erfüllen.

BEISPIEL:

Stell dir eine Aufgabe vor, bei der du eine bestimmte Zahlenkombination finden musst. Niemand kann dir die richtige Kombination im Voraus nennen. Du probierst deshalb unterschiedliche Möglichkeiten aus. Nach vielen Versuchen findest du eine passende Lösung. Nun zeigst du das Ergebnis einer anderen Person. Diese muss nicht sämtliche deiner bisherigen Versuche wiederholen. Sie muss nur überprüfen, ob deine gefundene Lösung die vorgegebenen Bedingungen erfüllt. Genau dieser Unterschied zwischen aufwendiger Suche und einfacher Kontrolle ist für den Arbeitsnachweis von Bitcoin entscheidend.

Wer führt diese Berechnungen durch?

Die Suche nach gültigen Arbeitsnachweisen wird als Mining bezeichnet. Die daran beteiligten Personen oder Unternehmen nennt man Miner. Sie betreiben Computer, die fortlaufend versuchen, einen neuen gültigen Block zu finden. Als Satoshi Nakamoto das Whitepaper veröffentlichte, waren gewöhnliche Computerprozessoren für solche Berechnungen vorgesehen. Deshalb spricht das Original teilweise von einer Stimme pro Computerprozessor. Heute wird Bitcoin-Mining dagegen überwiegend mit speziell dafür entwickelten Geräten betrieben. Diese Geräte sind wesentlich leistungsfähiger als gewöhnliche Computer. Sie werden als ASIC-Miner bezeichnet. Ein ASIC-Miner ist ein spezieller Computerchip, der für eine bestimmte Art von Berechnungen entwickelt wurde. Für das Verständnis des Whitepapers ist vor allem wichtig, dass das Erstellen neuer Blöcke tatsächliche Rechenleistung erfordert. Diese Rechenleistung verursacht Kosten. Dazu gehören insbesondere Anschaffung und Betrieb der Geräte sowie der benötigte Strom.

Warum können andere Teilnehmer die Arbeit einfach überprüfen?

Angenommen, ein Miner hat nach vielen Berechnungsversuchen einen gültigen Arbeitsnachweis gefunden. Er veröffentlicht den vorgeschlagenen Block zusammen mit den erforderlichen technischen Informationen.

Andere Computer im Bitcoin-Netzwerk können den Arbeitsnachweis selbst überprüfen. Sie berechnen dafür den digitalen Fingerabdruck des vorgeschlagenen Blocks und kontrollieren, ob er die geltenden Anforderungen erfüllt. Diese Überprüfung ist wesentlich weniger aufwendig als die vorangegangene Suche nach einer passenden Lösung. Allerdings reicht ein gültiger Arbeitsnachweis allein nicht aus. Der vorgeschlagene Block muss zusätzlich sämtliche übrigen Bitcoin-Regeln erfüllen. Beispielsweise dürfen seine Transaktionen keine bereits ausgegebenen Beträge erneut verwenden. Ein Miner kann deshalb nicht einfach einen Block mit beliebigen Zahlungen erstellen und erwarten, dass andere Teilnehmer ihn akzeptieren. Unabhängig prüfende Netzwerkteilnehmer weisen Blöcke zurück, die gegen die geltenden Regeln verstossen.

Warum lässt sich nicht einfach durch viele Computer abstimmen?

Satoshi Nakamoto beschreibt im Whitepaper ein weiteres Problem. Wie soll ein offenes Netzwerk entscheiden, welche Transaktionshistorie gültig ist? Eine einfache Abstimmung nach der Anzahl der Teilnehmer wäre problematisch. Stell dir vor, jede Computerverbindung erhielte genau eine Stimme. Ein Angreifer könnte versuchen, sehr viele Verbindungen oder technische Identitäten einzurichten. Dadurch würde es so aussehen, als würden besonders viele unabhängige Teilnehmer seine Version unterstützen. In Wirklichkeit könnten sämtliche Verbindungen von derselben Person kontrolliert werden. Satoshi Nakamoto wollte deshalb vermeiden, dass allein die Anzahl angemeldeter Teilnehmer entscheidend ist. Sein Lösungsansatz war, den Einfluss auf die Erstellung neuer Blöcke an tatsächlich geleistete Rechenarbeit zu binden. Im ursprünglichen Whitepaper beschreibt er das vereinfacht als eine Stimme pro Computerprozessor. Heute ist diese Formulierung technisch überholt, weil unterschiedliche Mining-Geräte sehr unterschiedliche Leistungen erbringen. Das zugrunde liegende Prinzip gilt jedoch weiterhin: Entscheidend ist nicht die Anzahl der Geräte oder Internetverbindungen, sondern die verfügbare Rechenleistung und die daraus nachgewiesene Arbeit.

Welche Blockkette wird vom Netzwerk bevorzugt?

Es kann vorkommen, dass unterschiedliche Miner ungefähr gleichzeitig einen gültigen Block finden. Dann existieren vorübergehend zwei verschiedene Fortsetzungen derselben bisherigen Blockchain. Beide Fortsetzungen können zunächst gültig sein. Das Netzwerk benötigt deshalb eine Regel, um zu entscheiden, welche Geschichte weitergeführt wird. Satoshi Nakamoto beschreibt hierfür die Bevorzugung derjenigen Kette, hinter der die grösste Rechenarbeit steht. Im Original verwendet er dafür den Begriff der längsten Kette. Für die heutige technische Beschreibung ist eine Präzisierung wichtig: Entscheidend ist die insgesamt nachgewiesene Rechenarbeit einer gültigen Kette. Es geht also nicht bloss darum, möglichst viele Blöcke zu zählen. Die Netzwerkteilnehmer prüfen weiterhin selbst, ob die einzelnen Blöcke gültig sind. Eine Kette mit ungültigen Transaktionen wird nicht allein dadurch akzeptiert, dass jemand viel Rechenleistung eingesetzt hat. Damit verbindet Bitcoin zwei Schutzmechanismen. Erstens müssen die geltenden Regeln eingehalten werden. Zweitens wird unter den gültigen konkurrierenden Ketten diejenige mit der grössten gesamten nachgewiesenen Rechenarbeit bevorzugt.

Warum schützt Proof of Work die Vergangenheit?

Stell dir vor, eine Bitcoin-Zahlung wurde in einen Block aufgenommen. Danach entstehen fünf weitere gültige Blöcke. Ein Angreifer möchte nun die ursprüngliche Zahlung rückgängig machen.

Dazu müsste er eine alternative gültige Transaktionshistorie aufbauen. Weil die Blöcke miteinander verbunden sind, müsste er für die veränderte Geschichte erneut gültige Arbeitsnachweise finden. Er müsste also nicht nur den betreffenden Block ersetzen. Er müsste auch eine konkurrierende Fortsetzung dieser Geschichte erzeugen. Gleichzeitig arbeitet das übrige Netzwerk weiter und findet neue Blöcke. Der Angreifer müsste deshalb mit seiner alternativen Kette die gesamte nachgewiesene Rechenarbeit der vom Netzwerk akzeptierten Kette aufholen und übertreffen. Wenn die ehrlich arbeitenden Miner gemeinsam über mehr Rechenleistung verfügen als der Angreifer, ist dieser langfristig im Nachteil. Mit zunehmendem Rückstand wird es unter diesen Voraussetzungen immer unwahrscheinlicher, dass er noch aufholen kann. Diesen Zusammenhang untersucht Satoshi Nakamoto später im elften Abschnitt des Whitepapers auch mathematisch.

Was geschieht bei einem Angreifer mit sehr viel Rechenleistung?

Der Schutz durch Proof of Work ist stark, aber nicht absolut. Ein Angreifer mit einem erheblichen Anteil der gesamten Rechenleistung könnte versuchen, eine konkurrierende Transaktionshistorie aufzubauen. Unter bestimmten Voraussetzungen könnte er damit eigene frühere Zahlungen rückgängig machen und denselben Betrag anders ausgeben. Er könnte ausserdem versuchen, die Aufnahme bestimmter Transaktionen zu behindern. Dabei ist jedoch eine wichtige Grenze zu beachten. Auch ein Angreifer mit sehr grosser Rechenleistung kann nicht einfach gültige digitale Signaturen für fremde private Schlüssel fälschen. Ebenso kann er einem unabhängig prüfenden Netzwerkteilnehmer nicht ohne Weiteres einen Block aufzwingen, der gegen dessen geltende Bitcoin-Regeln verstösst. Proof of Work entscheidet darüber, welche gültige Transaktionshistorie sich durchsetzt. Es ersetzt nicht die übrigen Regeln des Bitcoin-Netzwerks. Satoshi Nakamoto geht im Whitepaper davon aus, dass die ehrlich arbeitenden Teilnehmer gemeinsam über mehr Rechenleistung verfügen als eine zusammenarbeitende Gruppe von Angreifern. Diese Annahme ist eine wesentliche Grundlage seiner Sicherheitsüberlegungen.

Warum wird die Schwierigkeit angepasst?

Die Rechenleistung des Bitcoin-Netzwerks bleibt nicht immer gleich. Neue Miner können hinzukommen. Andere können ihre Geräte ausschalten. Ausserdem werden Computer und spezielle Mining-Geräte im Laufe der Zeit leistungsfähiger. Wenn die Anforderungen für einen gültigen Arbeitsnachweis unverändert blieben, könnten neue Blöcke bei steigender Rechenleistung immer schneller gefunden werden. Bei sinkender Rechenleistung würden sie dagegen langsamer entstehen. Deshalb sieht Bitcoin eine regelmässige Anpassung der Schwierigkeit vor. Im Whitepaper beschreibt Satoshi Nakamoto diesen Mechanismus bereits grundsätzlich. Die Schwierigkeit soll so angepasst werden, dass langfristig eine bestimmte durchschnittliche Anzahl neuer Blöcke entsteht. Im heutigen Bitcoin-Hauptnetz erfolgt diese Anpassung nach jeweils 2'016 Blöcken.

Das Ziel liegt bei durchschnittlich ungefähr zehn Minuten pro Block. Wenn die Blöcke im zurückliegenden Anpassungszeitraum insgesamt schneller als vorgesehen gefunden wurden, wird die Schwierigkeit grundsätzlich erhöht. Wenn sie langsamer gefunden wurden, wird sie grundsätzlich gesenkt. Diese Anpassung besitzt technische Grenzen, die hier für das Grundverständnis nicht entscheidend sind.

Wichtig ist vor allem: Die zehn Minuten sind ein langfristiger Durchschnitt und keine feste Wartezeit. Ein einzelner Block kann wesentlich schneller oder langsamer gefunden werden.

Weshalb benötigt Bitcoin dafür Energie?

Proof of Work beruht darauf, dass Miner tatsächlich Berechnungen durchführen. Dafür benötigen ihre Geräte elektrische Energie. Der Energieverbrauch ist deshalb kein zufälliger Nebeneffekt. Er hängt unmittelbar mit dem gewählten Sicherheitsverfahren zusammen. Die Rechenarbeit erschwert es, die Transaktionshistorie nachträglich zu verändern. Gleichzeitig entstehen dadurch reale Kosten. Wie hoch der Energieverbrauch insgesamt ausfällt, hängt unter anderem von der eingesetzten Hardware, der gesamten Rechenleistung und den Betriebsbedingungen ab. Die Auswirkungen auf die Umwelt hängen zusätzlich davon ab, wie der benötigte Strom erzeugt wird. Das Whitepaper beschreibt in diesem Abschnitt vor allem die technische Aufgabe des Arbeitsnachweises. Es enthält keine umfassende heutige Bewertung der ökologischen und wirtschaftlichen Folgen des weltweiten Bitcoin-Minings. Für das Verständnis ist deshalb wichtig, zwischen dem technischen Sicherheitsmechanismus und seiner wirtschaftlichen beziehungsweise ökologischen Beurteilung zu unterscheiden.

Warum ist Proof of Work ein zentraler Bestandteil von Bitcoin?

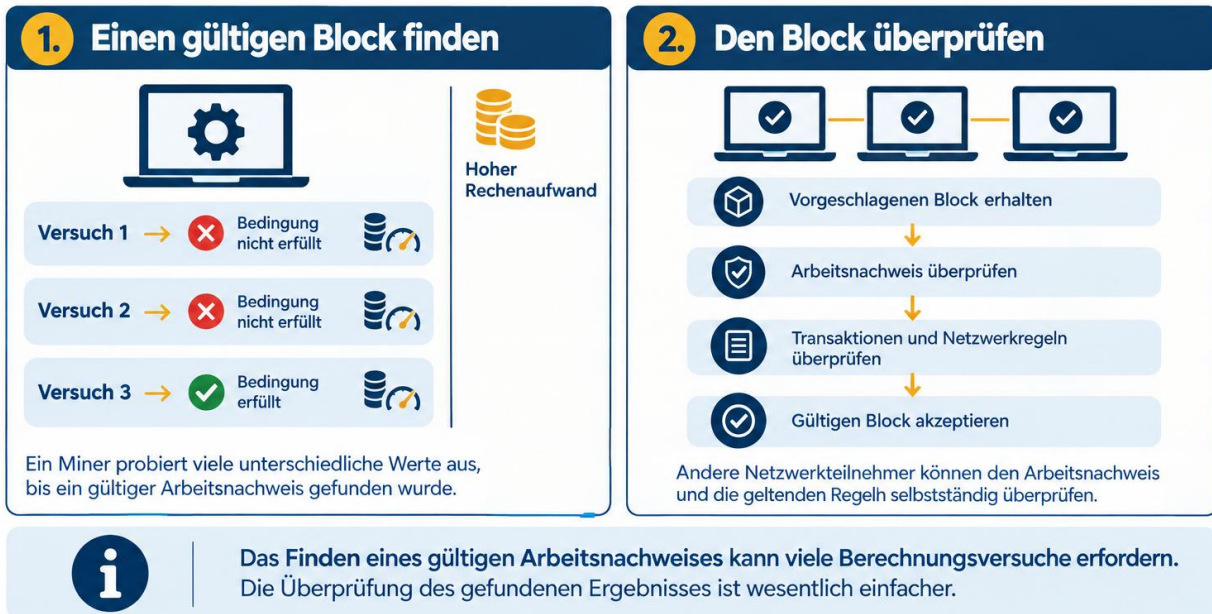
Satoshi Nakamoto verbindet mit Proof of Work mehrere wichtige Eigenschaften. Neue Blöcke können nicht einfach ohne entsprechenden Rechenaufwand erzeugt werden. Die Gültigkeit eines gefundenen Arbeitsnachweises lässt sich vergleichsweise einfach überprüfen. Nachträgliche Veränderungen einer bestätigten Transaktionshistorie erfordern zusätzliche Rechenarbeit. Und konkurrierende gültige Blockketten können anhand ihrer gesamten nachgewiesenen Rechenarbeit miteinander verglichen werden. Zusammen mit den unabhängig überprüfbaren Bitcoin-Regeln entsteht dadurch ein System, das keine zentrale Stelle benötigt, um die gültige Transaktionshistorie für alle verbindlich festzulegen. Allerdings funktioniert dieser Schutz nicht unabhängig von seinen Voraussetzungen. Die Verteilung der Rechenleistung, das Verhalten der Netzwerkteilnehmer und die Einhaltung der übrigen Regeln bleiben entscheidend. Proof of Work macht bestimmte Manipulationen aufwendig und bei ausreichend grossem Rückstand zunehmend unwahrscheinlich. Es macht sie nicht grundsätzlich unmöglich.

MERKSATZ:

Proof of Work bedeutet Arbeitsnachweis. Miner müssen Rechenleistung einsetzen, um neue gültige Blöcke zu finden. Andere Teilnehmer können den Arbeitsnachweis einfach überprüfen und kontrollieren zusätzlich, ob sämtliche Bitcoin-Regeln eingehalten wurden. Die dafür aufgewendete Rechenarbeit erschwert nachträgliche Veränderungen der Blockchain. Je mehr gültige Blöcke auf einer bestätigten Zahlung aufbauen, desto schwieriger wird es unter den üblichen Sicherheitsannahmen, eine konkurrierende Geschichte durchzusetzen.

GRAFIK 4

Proof of Work: **Aufwendig finden, einfach überprüfen**



Miner investieren Rechenleistung in die Suche nach einem gültigen Arbeitsnachweis. Andere Netzwerkteilnehmer können das Ergebnis mit wesentlich geringerem Aufwand überprüfen. Zusätzlich kontrollieren sie, ob der vorgeschlagene Block sämtliche geltenden Bitcoin-Regeln erfüllt.

5. Wie arbeitet das Bitcoin-Netzwerk zusammen?

Verständliche Erklärung des Originalabschnitts «Network»

Im fünften Abschnitt seines Whitepapers beschreibt Satoshi Nakamoto, wie die verschiedenen Teilnehmer des Bitcoin-Netzwerks zusammenarbeiten. In den bisherigen Kapiteln haben wir erfahren, dass Bitcoin digitale Signaturen, miteinander verbundene Datenblöcke und einen Arbeitsnachweis verwendet. Nun stellt sich eine weitere Frage: Wie können viele Computer auf der ganzen Welt gemeinsam ein Zahlungssystem betreiben, obwohl es keine zentrale Leitung gibt? Bei einer Bank ist die Zuständigkeit klar geregelt. Die Bank betreibt ihre eigenen Computersysteme und entscheidet anhand ihrer internen Verfahren, welche Buchungen ausgeführt werden. Bei Bitcoin gibt es dagegen keine einzelne Organisation, die sämtliche Transaktionen entgegennimmt, überprüft und für alle Teilnehmer verbindlich freigibt. Stattdessen arbeiten zahlreiche Computer nach denselben öffentlich bekannten Regeln. Satoshi Nakamoto beschreibt im Whitepaper sechs grundlegende Schritte, aus denen sich die Zusammenarbeit im Netzwerk zusammensetzt. Diese sechs Schritte bilden den Kern des folgenden Kapitels.

Schritt 1 – Eine neue Zahlung wird an das Netzwerk übermittelt

Stell dir vor, Anna möchte Beat einen Bitcoin-Betrag senden. Anna öffnet ihre digitale Geldbörse. Eine solche Geldbörse wird bei Bitcoin als Wallet bezeichnet. Sie gibt den gewünschten Betrag und die Empfangsadresse von Beat ein. Die Wallet erstellt daraus eine Bitcoin-Transaktion. Anschliessend gibt Anna die Zahlung mit den erforderlichen privaten Schlüsseln frei. Die fertige Transaktion wird an das Bitcoin-Netzwerk übermittelt. Dabei wird sie nicht an eine einzige zentrale Abrechnungsstelle geschickt. Stattdessen gelangt sie zunächst zu einem oder mehreren Computern, die mit dem Bitcoin-Netzwerk verbunden sind. Diese Computer können die Transaktion an weitere Teilnehmer weiterleiten. So verbreitet sich die Information über die neue Zahlung im Netzwerk. Diesen Vorgang kann man sich ähnlich wie die Weitergabe einer Nachricht vorstellen. Eine Person erhält die Nachricht und gibt sie an mehrere andere Personen weiter. Diese wiederum können die Nachricht an weitere Teilnehmer übermitteln. Nach kurzer Zeit kann die Information an vielen unterschiedlichen Orten bekannt sein. Dabei muss nicht jeder Computer die Nachricht im exakt gleichen Moment erhalten. Entscheidend ist, dass die Transaktion genügend Teilnehmer erreicht, damit sie überprüft und für die Aufnahme in einen Block berücksichtigt werden kann.

Schritt 2 – Die Transaktion wird überprüft

Wenn ein entsprechend ausgestatteter Computer eine neue Bitcoin-Transaktion erhält, kann er ihre Gültigkeit selbstständig überprüfen. Ein solcher Computer wird als Prüfknoten bezeichnet. Im Englischen spricht man von einem Node. Eine vollständige Prüfstelle, die die geltenden Netzwerkregeln selbst kontrolliert, wird Full Node genannt. Die Prüfknoten überprüfen unter anderem, ob die Transaktion korrekt aufgebaut ist.

Sie kontrollieren auch, ob die erforderlichen digitalen Signaturen gültig sind und ob die verwendeten Beträge nach den geltenden Regeln ausgegeben werden dürfen.

Wenn die Transaktion gegen diese Regeln verstösst, wird sie zurückgewiesen. Ist die Transaktion gültig, kann der Prüfknoten sie vorläufig speichern und an weitere Teilnehmer weiterleiten. Dieser vorläufige Speicher wird als Mempool bezeichnet. Du kannst dir darunter eine Art Warteliste für noch nicht bestätigte Zahlungen vorstellen. Dabei gibt es allerdings keine einzige zentrale Warteliste für das gesamte Bitcoin-Netzwerk. Jeder Prüfknoten verwaltet seinen eigenen vorläufigen Speicher. Deshalb können sich die gespeicherten Transaktionen von Computer zu Computer unterscheiden. Wichtig ist ausserdem: Eine Transaktion wird nicht allein dadurch endgültig, dass sie von einem Prüfknoten als gültig angesehen wird. Sie muss zunächst noch in einen gültigen Block aufgenommen werden.

Schritt 3 – Miner stellen einen neuen Block zusammen

Nun kommen die Miner ins Spiel. Miner sind Netzwerkteilnehmer, die mit spezieller Rechenleistung versuchen, neue Bitcoin-Blöcke zu finden. Sie wählen dafür Transaktionen aus, die nach den geltenden Regeln in einen Block aufgenommen werden können. Anschliessend stellen sie einen möglichen neuen Block zusammen. Dieser Block enthält unter anderem Informationen über die ausgewählten Transaktionen und einen Verweis auf den vorherigen Block. Danach beginnt die Suche nach einem gültigen Arbeitsnachweis. Dafür führen die Mining-Geräte sehr viele kryptographische Berechnungen durch.

Wie wir im vorherigen Kapitel gesehen haben, lässt sich das Ergebnis nicht einfach im Voraus bestimmen. Die Geräte müssen so lange unterschiedliche Werte ausprobieren, bis ein gültiger Arbeitsnachweis gefunden wurde. Im ursprünglichen Whitepaper beschreibt Satoshi Nakamoto diesen Vorgang noch so, dass die Netzwerkteilnehmer selbst neue Blöcke zusammenstellen und dafür Rechenarbeit leisten. Heute müssen wir genauer unterscheiden. Viele Computer überprüfen ausschliesslich die Bitcoin-Regeln. Andere Teilnehmer, insbesondere Miner und Mining-Pools, beteiligen sich an der Suche nach neuen Blöcken. Nicht jeder Prüfknoten betreibt also gleichzeitig Bitcoin-Mining. Diese Unterscheidung ist wichtig, weil das Überprüfen der Regeln und das Finden neuer Blöcke unterschiedliche Aufgaben sind.

Schritt 4 – Ein gefundener Block wird veröffentlicht

Angenommen, ein Miner findet einen gültigen Arbeitsnachweis. Dann kann er seinen vorgeschlagenen Block an das Bitcoin-Netzwerk übermitteln. Der Block wird zunächst an andere verbundene Computer gesendet. Diese können ihn wiederum an weitere Teilnehmer weitergeben. So verbreitet sich der neue Block über das Netzwerk. Damit ist der Block allerdings noch nicht automatisch von allen akzeptiert. Auch wenn ein Miner viel Rechenleistung eingesetzt hat, müssen die übrigen Teilnehmer ihm nicht einfach vertrauen. Die unabhängige Überprüfung ist ein entscheidender Bestandteil von Bitcoin.

Schritt 5 – Die Prüfknoten kontrollieren den neuen Block

Sobald ein Prüfknoten den vorgeschlagenen Block erhält, überprüft er dessen Gültigkeit. Dazu gehört zunächst die Kontrolle des Arbeitsnachweises. Der Computer prüft, ob das berechnete Ergebnis die geltenden Anforderungen erfüllt. Anschliessend kontrolliert er die übrigen Regeln. Beispielsweise darf der Block keine ungültigen Transaktionen enthalten.

Auch dürfen innerhalb der gültigen Transaktionshistorie keine bereits ausgegebenen Beträge ein zweites Mal verwendet werden. Ausserdem muss die Vergütung, die der Miner für den gefundenen Block beansprucht, den geltenden Regeln entsprechen. Wenn der Block alle Prüfungen besteht, kann er als gültige Erweiterung der bisherigen Blockchain akzeptiert werden. Wenn er gegen eine Regel verstösst, wird er zurückgewiesen. Das gilt selbst dann, wenn der Miner einen gültigen Arbeitsnachweis gefunden hat. Hier zeigt sich ein wichtiger Unterschied zwischen Mining und Regelprüfung. Miner schlagen neue Blöcke vor. Unabhängige Prüfknoten kontrollieren, ob diese Blöcke tatsächlich den geltenden Regeln entsprechen. Kein einzelner Miner kann deshalb beliebige neue Regeln für alle anderen Computer verbindlich machen.

BEISPIEL:

Stell dir einen Verein vor, dessen Mitglieder ein gemeinsames Kassenbuch führen. Ein Mitglied schlägt eine neue Seite mit mehreren Buchungen vor. Die anderen Mitglieder übernehmen diese Seite aber nicht einfach ungeprüft. Sie kontrollieren zunächst, ob sämtliche Buchungen den vereinbarten Regeln entsprechen. Ist alles korrekt, kann die neue Seite in das gemeinsame Kassenbuch aufgenommen werden. Enthält die Seite falsche Buchungen, wird sie zurückgewiesen. Der Vergleich zeigt den Unterschied zwischen dem Vorschlagen neuer Einträge und ihrer unabhängigen Überprüfung.

Schritt 6 – Das Netzwerk arbeitet am nächsten Block

Nachdem ein gültiger Block akzeptiert wurde, können die Miner auf dieser Grundlage den nächsten Block erstellen. Dafür übernehmen sie den digitalen Fingerabdruck des akzeptierten Blocks als Verweis in ihren neuen Block. Anschliessend suchen sie wieder nach einem gültigen Arbeitsnachweis. Wenn dieser gefunden wird, entsteht der nächste Block der Kette. So wächst die Blockchain Schritt für Schritt weiter. Im Whitepaper beschreibt Satoshi Nakamoto diesen Vorgang als eine Form der Zustimmung. Indem Teilnehmer auf einem akzeptierten Block weiterarbeiten, unterstützen sie die Fortsetzung dieser Transaktionshistorie. Dabei ist jedoch wichtig, die heutige technische Bedeutung richtig einzuordnen. Ein Prüfknoten kann einen gültigen Block akzeptieren, ohne selbst Mining zu betreiben. Die Miner wiederum dürfen nur auf Blöcken aufbauen, die nach den geltenden Regeln gültig sind, wenn ihre Arbeit von entsprechend prüfenden Teilnehmern anerkannt werden soll. Bitcoin verbindet damit zwei unterschiedliche Aufgaben: Die unabhängige Kontrolle der Regeln und die Rechenarbeit zur Fortsetzung der Blockchain.

Was geschieht, wenn zwei Miner gleichzeitig einen Block finden?

Bisher haben wir den Ablauf so betrachtet, als würde immer nur ein neuer Block gefunden. In der Praxis kann es jedoch vorkommen, dass zwei Miner fast gleichzeitig einen gültigen Block entdecken. Stell dir vor, der letzte allgemein bekannte Block trägt die Nummer 100. Miner A findet einen gültigen Block 101. Fast gleichzeitig findet Miner B ebenfalls einen gültigen Block 101. Beide Blöcke enthalten einen Verweis auf Block 100.

Sie können sich jedoch beispielsweise darin unterscheiden, welche Transaktionen sie enthalten. Nun verbreiten beide Miner ihre Blöcke im Netzwerk. Einige Computer erhalten zuerst den Block von Miner A. Andere erhalten zuerst den Block von Miner B. Dadurch entstehen vorübergehend zwei unterschiedliche Fortsetzungen derselben bisherigen Blockchain. Eine solche vorübergehende Aufspaltung wird als konkurrierender Zweig bezeichnet. Im Englischen wird dafür häufig der Begriff Fork verwendet. Hier ist allerdings nicht eine dauerhafte Änderung der Bitcoin-Regeln gemeint. Es geht lediglich darum, dass kurzfristig zwei gültige Blöcke um denselben Platz in der Transaktionshistorie konkurrieren.

Wie entscheidet das Netzwerk zwischen zwei gültigen Blöcken?

Satoshi Nakamoto beschreibt dafür eine einfache Grundregel. Die Teilnehmer orientieren sich an der gültigen Kette, hinter der insgesamt die grösste nachgewiesene Rechenarbeit steht. Im ursprünglichen Whitepaper spricht er vereinfacht von der längsten Kette. Die heutige präzisere Beschreibung lautet: Massgeblich ist die gesamte nachgewiesene Rechenarbeit einer gültigen Kette. Angenommen, ein Teil der Miner arbeitet zunächst auf dem Block von Miner A weiter. Ein anderer Teil arbeitet auf dem Block von Miner B. Findet nun ein Miner einen weiteren gültigen Block, kann eine der beiden Ketten einen Vorsprung erhalten. Die Netzwerkteilnehmer können dann erkennen, welche gültige Kette insgesamt die grössere nachgewiesene Rechenarbeit besitzt. Sie richten sich nach dieser Kette aus. Die andere Fortsetzung wird nicht mehr als Teil der aktuell bevorzugten Blockchain verwendet. Diesen Vorgang bezeichnet man als Kettenreorganisation. Er wird auch Blockchain-Reorganisation genannt. Die darin enthaltenen Transaktionen verschwinden allerdings nicht zwangsläufig vollständig.

Gültige Transaktionen aus einem nicht mehr bevorzugten Block können später erneut in einen anderen Block aufgenommen werden, sofern sie nicht mit der nun akzeptierten Geschichte in Konflikt stehen.

Weshalb sind Bestätigungen wichtig?

Wenn eine Bitcoin-Zahlung in einen gültigen Block aufgenommen wurde, besitzt sie ihre erste Bestätigung. Wenn danach ein weiterer Block auf diesem Block aufbaut, erhöht sich die Anzahl der Bestätigungen. Mit jeder weiteren Bestätigung wächst unter den üblichen Sicherheitsannahmen der Aufwand, der für eine erfolgreiche nachträgliche Veränderung erforderlich wäre. Deshalb warten Händler, Handelsplattformen oder andere Zahlungsempfänger je nach Situation auf mehrere Bestätigungen. Wie viele Bestätigungen angemessen sind, hängt unter anderem vom Betrag und vom jeweiligen Risiko ab. Eine feste Anzahl bedeutet jedoch keine absolute Sicherheitsgarantie. Das ursprüngliche Whitepaper erklärt später ausführlicher, weshalb das Risiko einer erfolgreichen nachträglichen Veränderung mit zunehmender Zahl von Bestätigungen abnimmt. Diesen Zusammenhang behandeln wir in Kapitel 11.

Müssen alle Computer jederzeit dieselben Informationen besitzen?

Nein. Das Bitcoin-Netzwerk ist bewusst so aufgebaut, dass nicht jeder Teilnehmer zu jedem Zeitpunkt sämtliche Nachrichten erhalten muss. Satoshi Nakamoto beschreibt diese Eigenschaft ausdrücklich im fünften Abschnitt seines Whitepapers. Eine neu übermittelte Transaktion muss nicht sofort jeden einzelnen Computer erreichen. Es genügt grundsätzlich, wenn sie sich ausreichend im Netzwerk verbreitet, damit sie von Minern berücksichtigt werden kann. Auch einzelne Blocknachrichten können unterwegs verloren gehen oder verspätet eintreffen. Ein Computer kann dann feststellen, dass ihm Informationen fehlen. Anschliessend kann er die fehlenden Daten von anderen Netzwerkteilnehmern anfordern. Das Netzwerk benötigt deshalb keine zentrale Stelle, die jede Nachricht gleichzeitig an sämtliche Teilnehmer verteilt. Diese Widerstandsfähigkeit ist eine wichtige Eigenschaft der dezentralen Organisation.

Was geschieht, wenn ein Computer ausfällt?

Stell dir vor, ein Betreiber eines Bitcoin-Prüfknotens schaltet seinen Computer für mehrere Tage aus. Während dieser Zeit arbeitet das übrige Bitcoin-Netzwerk weiter. Neue Transaktionen werden verarbeitet und weitere Blöcke entstehen. Wenn der Computer später wieder eingeschaltet wird, kann er erneut Verbindung zu anderen Netzwerkteilnehmern aufnehmen. Anschliessend bezieht er die Daten, die während seiner Abwesenheit entstanden sind. Ein vollständig prüfender Computer kann diese Daten anhand der geltenden Regeln selbst kontrollieren. Er muss deshalb nicht einfach darauf vertrauen, dass ein einzelner fremder Computer die richtige Geschichte übermittelt. Wie aufwendig das Nachholen der Daten ist, hängt unter anderem davon ab, wie lange der Computer ausgeschaltet war. Das grundlegende Prinzip bleibt aber gleich: Ein Teilnehmer kann das Netzwerk verlassen und später wieder beitreten. Das Bitcoin-Netzwerk ist nicht davon abhängig, dass jeder einzelne Computer dauerhaft eingeschaltet bleibt.

Warum ist diese Organisation so wichtig?

Die sechs Schritte zeigen, wie Bitcoin ohne zentrale Leitung eine gemeinsame Transaktionshistorie aufbauen kann. Neue Zahlungen werden im Netzwerk verbreitet. Unabhängige Teilnehmer überprüfen die Einhaltung der Regeln. Miner stellen mögliche neue Blöcke zusammen und suchen nach gültigen Arbeitsnachweisen. Gefundene Blöcke werden veröffentlicht und erneut überprüft. Anschliessend wird die gültige Blockchain fortgesetzt. Wenn kurzfristig unterschiedliche Fortsetzungen entstehen, richtet sich das Netzwerk nach der gültigen Kette mit der grössten gesamten nachgewiesenen Rechenarbeit. Dadurch können viele voneinander unabhängige Computer an einem gemeinsamen Zahlungssystem teilnehmen. Satoshi Nakamoto beschreibt damit keine zentral gesteuerte Organisation. Er beschreibt ein offenes Netzwerk, dessen Teilnehmer anhand gemeinsamer technischer Regeln zusammenarbeiten.

MERKSATZ:

Bitcoin benötigt keine zentrale Stelle, die jede einzelne Zahlung für alle Teilnehmer verbindlich bestätigt. Transaktionen und Blöcke werden im Netzwerk verbreitet und unabhängig überprüft. Miner schlagen neue Blöcke vor. Prüfknoten kontrollieren die Einhaltung der Regeln. Die gültige Blockchain wird anhand der insgesamt nachgewiesenen Rechenarbeit fortgesetzt.



BILDUNTERSCHRIFT: Eine Bitcoin-Zahlung wird im Netzwerk verbreitet und nach gemeinsamen Regeln überprüft. Miner können sie in einen neuen Block aufnehmen. Unabhängige Prüfknoten kontrollieren diesen Block, bevor sie ihn als gültige Erweiterung der Blockchain akzeptieren.

6. Warum unterstützen Miner das Bitcoin-Netzwerk?

Verständliche Erklärung des Originalabschnitts «Incentive»

Im sechsten Abschnitt seines Whitepapers beschäftigt sich Satoshi Nakamoto mit einer wirtschaftlichen Frage. Warum sollten Menschen überhaupt Computer betreiben und Rechenleistung zur Verfügung stellen, damit das Bitcoin-Netzwerk funktioniert? Schliesslich entstehen dadurch Kosten. Computer müssen angeschafft, betrieben und gewartet werden. Ausserdem benötigen die Geräte elektrische Energie. Ein Zahlungssystem, das auf freiwilliger Beteiligung beruht, benötigt deshalb einen Anreiz, damit genügend Teilnehmer bereit sind, diese Aufgaben zu übernehmen. Satoshi Nakamoto beschreibt dafür ein Vergütungssystem. Wer erfolgreich einen neuen gültigen Block findet, kann nach den geltenden Regeln eine Belohnung erhalten. Diese Belohnung besteht aus neu ausgegebenen Bitcoin und den Gebühren der im Block enthaltenen Transaktionen. Im englischen Original verwendet Satoshi Nakamoto für einen solchen wirtschaftlichen Anreiz den Begriff «Incentive».

Warum gibt es überhaupt eine Belohnung?

Stell dir vor, mehrere Menschen betreiben gemeinsam ein öffentliches Informationssystem. Damit es funktioniert, müssen Computer eingeschaltet bleiben und bestimmte Aufgaben ausführen. Der Betrieb verursacht Kosten. Wenn niemand einen Vorteil daraus ziehen kann, stellt sich die Frage, weshalb Menschen langfristig bereit sein sollten, diese Kosten zu tragen. Satoshi Nakamoto löste dieses Problem nicht durch einen zentralen Betreiber, der Rechnungen bezahlt und Mitarbeiter beschäftigt. Stattdessen entwarf er ein System, bei dem erfolgreiche Teilnehmer direkt nach festgelegten Regeln vergütet werden können. Bei Bitcoin erhalten Miner diese Vergütung nicht allein dafür, dass sie ihren Computer einschalten. Sie müssen einen gültigen Block finden, der von den unabhängig prüfenden Netzwerkteilnehmern akzeptiert wird. Der Arbeitsnachweis ist damit eine Voraussetzung dafür, dass ein Miner die vorgesehene Blockvergütung beanspruchen kann.

Wie entstehen neue Bitcoin?

Satoshi Nakamoto beschreibt im Whitepaper, dass die erste Transaktion eines neuen Blocks eine besondere Funktion besitzt. Sie kann neue Bitcoin erzeugen. Diese spezielle Transaktion wird heute als Coinbase-Transaktion bezeichnet. Der Begriff beschreibt hier eine technische Besonderheit im Bitcoin-Protokoll. Er hat nichts mit einem Handelsunternehmen gleichen Namens zu tun. Eine gewöhnliche Bitcoin-Transaktion verwendet bereits vorhandene Beträge aus früheren Transaktionen. Die besondere erste Transaktion eines Blocks funktioniert anders. Sie kann nach den geltenden Netzwerkregeln einen festgelegten Betrag neuer Bitcoin erzeugen und zusammen mit den Gebühren dem erfolgreichen Miner zuordnen. Dadurch gelangen neue Bitcoin erstmals in Umlauf. Für die Ausgabe dieser neuen Einheiten ist keine Zentralbank erforderlich. Sie erfolgt anhand der Regeln des Bitcoin-Netzwerks. Wichtig ist allerdings, dass Miner nicht selbst entscheiden dürfen, wie viele neue Bitcoin sie erzeugen. Der zulässige Betrag ist durch die Netzwerkregeln begrenzt. Ein Block, der eine zu hohe Vergütung beansprucht, wird von unabhängig prüfenden Teilnehmern zurückgewiesen.

Wie viele neue Bitcoin darf ein Miner erhalten?

Das Bitcoin-Netzwerk besitzt einen festgelegten Ausgabeplan. Nach diesem Plan wird die Menge neuer Bitcoin, die pro Block ausgegeben werden darf, in bestimmten Abständen reduziert. Im heutigen Bitcoin-Protokoll geschieht dies nach jeweils 210'000 Blöcken. Diese regelmässige Halbierung der neuen Blockvergütung wird als Halving bezeichnet. Am Anfang des Netzwerks betrug die Vergütung für einen gültigen Block 50 neue Bitcoin. Im Laufe der Zeit wurde dieser Betrag mehrfach halbiert. Dadurch sinkt die Geschwindigkeit, mit der neue Bitcoin entstehen. Nach den geltenden Regeln ist die gesamte vorgesehene Ausgabe auf knapp 21 Millionen Bitcoin begrenzt. Hier ist eine wichtige historische Unterscheidung notwendig. Satoshi Nakamoto beschreibt im Whitepaper bereits die Grundidee einer festgelegten Ausgabe und eines späteren Übergangs zur Finanzierung durch Transaktionsgebühren. Die konkrete Obergrenze von knapp 21 Millionen Bitcoin und die heutige Halbierungsregel werden im ursprünglichen Whitepaper jedoch nicht im Detail erläutert. Sie gehören zu den Regeln der später veröffentlichten Bitcoin-Software. Wir erwähnen sie hier, damit du die heutige Funktionsweise nachvollziehen kannst.

Weshalb vergleicht Satoshi Bitcoin-Mining mit der Goldförderung?

Im Whitepaper zieht Satoshi Nakamoto einen Vergleich zur Förderung von Gold. Gold kann nicht einfach nach Belieben hergestellt werden. Um neues Gold aus einer Lagerstätte zu gewinnen, müssen Unternehmen Ressourcen einsetzen. Sie benötigen beispielsweise Maschinen, Energie, Personal und Zeit. Auch die Förderung von Bitcoin ist mit einem Aufwand verbunden. Miner müssen spezielle Computer betreiben, die sehr viele Berechnungen durchführen. Dafür benötigen sie unter anderem elektrische Energie. Wenn ein Miner einen gültigen Block findet, kann er neue Bitcoin nach den festgelegten Regeln erhalten. Dieser Vergleich erklärt, weshalb Satoshi Nakamoto von Mining spricht. Das englische Wort bedeutet Bergbau oder Förderung. Allerdings bestehen wichtige Unterschiede. Bei Gold wird ein physisches Metall aus der Erde gewonnen. Bei Bitcoin wird kein physischer Rohstoff gefördert. Die neuen Einheiten entstehen nach den Regeln eines digitalen Netzwerks. Auch lässt sich die weltweite Goldförderung nicht durch ein einziges verbindliches Ausgabeprogramm festlegen. Bei Bitcoin ist die vorgesehene Ausgabe dagegen durch die geltenden Netzwerkregeln bestimmt. Der Vergleich mit Gold soll deshalb vor allem den notwendigen Ressourceneinsatz veranschaulichen. Er bedeutet nicht, dass Bitcoin und Gold technisch oder wirtschaftlich dasselbe sind.

Was sind Transaktionsgebühren?

Die zweite Einnahmequelle der Miner sind Transaktionsgebühren. Wenn du eine Bitcoin-Zahlung ausführst, kann dafür eine Gebühr anfallen. Diese Gebühr ist nicht mit einem festen Prozentsatz vergleichbar, den eine Bank für eine bestimmte Geldüberweisung verlangt. Bei Bitcoin ergibt sich die Gebühr technisch aus dem Unterschied zwischen den insgesamt verwendeten Transaktionsbeträgen und den neu zugeordneten Beträgen. Das klingt zunächst kompliziert. Ein einfaches Beispiel hilft beim Verständnis. Angenommen, Anna verfügt über einen verwendbaren Bitcoin-Betrag von 100'000 Satoshi. Ein Satoshi ist die kleinste Einheit eines Bitcoin auf der Blockchain. Anna möchte Beat 60'000 Satoshi senden. Die übrigen Satoshi sollen an Anna zurückgehen.

Wenn Anna 39'000 Satoshi als Restbetrag für sich selbst vorsieht, ergibt sich folgende Rechnung:
Verwendeter Betrag: 100'000 Satoshi Zahlung an Beat: 60'000 Satoshi Restbetrag für Anna: 39'000 Satoshi Unterschied: 1'000 Satoshi Die Differenz von 1'000 Satoshi bildet in diesem Beispiel die Transaktionsgebühr. Ein Miner, der die Transaktion in einen gültigen Block aufnimmt, kann diese Gebühr im Rahmen der Blockvergütung beanspruchen. Wichtig ist: Diese Zahlen dienen ausschliesslich der Erklärung. Sie stellen weder eine aktuelle Gebühr noch eine Empfehlung für eine bestimmte Zahlung dar.

Warum können Gebühren unterschiedlich hoch sein?

Nicht jede Bitcoin-Transaktion verursacht dieselbe Gebühr. Bei der Berechnung spielt insbesondere eine Rolle, wie viel Speicherplatz eine Transaktion innerhalb eines Blocks beansprucht. Ausserdem hängt die tatsächlich verlangte beziehungsweise bezahlte Gebühr von der Nachfrage nach dem begrenzten Platz in neuen Blöcken ab. Wenn viele Menschen gleichzeitig Bitcoin-Transaktionen ausführen möchten, können die angebotenen Gebühren steigen. Miner können bei der Auswahl gültiger Transaktionen berücksichtigen, welche Gebühren sie dadurch verdienen. Deshalb kann eine Transaktion mit einer höheren Gebühr unter vergleichbaren Bedingungen früher berücksichtigt werden als eine mit einer sehr niedrigen Gebühr. Eine hohe Gebühr garantiert allerdings keine Aufnahme in den nächsten Block. Ebenso bedeutet eine niedrige Gebühr nicht automatisch, dass eine Transaktion niemals bestätigt wird. Die tatsächliche Wartezeit hängt von mehreren Faktoren ab.

Was geschieht, wenn immer weniger neue Bitcoin entstehen?

Der Ausgabeplan von Bitcoin sieht vor, dass die Menge neu erzeugter Bitcoin pro Block langfristig immer kleiner wird. Damit verringert sich auch der Anteil neuer Bitcoin an der Vergütung der Miner. Satoshi Nakamoto beschreibt deshalb im Whitepaper die Möglichkeit, dass Transaktionsgebühren später die Finanzierung des Netzwerks übernehmen. Nach dem vorgesehenen Ausgabeplan wird die Neuausgabe neuer Bitcoin langfristig auslaufen. Miner könnten dann ihre Einnahmen ausschliesslich aus Transaktionsgebühren erzielen. Das ist ein wichtiger Bestandteil der wirtschaftlichen Konstruktion. Es bedeutet jedoch nicht, dass damit bereits garantiert wäre, dass zukünftige Gebühren immer ausreichen, um ein bestimmtes Sicherheitsniveau aufrechtzuerhalten. Die Höhe der Miner-Einnahmen hängt unter anderem davon ab, wie stark das Netzwerk genutzt wird und welche Gebühren Nutzer bereit sind zu bezahlen. Auch der Bitcoin-Marktpreis und die Betriebskosten der Miner spielen eine Rolle. Die langfristige Entwicklung dieser wirtschaftlichen Faktoren lässt sich nicht mit Sicherheit vorhersagen. Das Whitepaper beschreibt damit einen vorgesehenen Finanzierungsmechanismus, keine Garantie für dessen zukünftige wirtschaftliche Ergebnisse.

Warum sollen Miner die Regeln einhalten?

Satoshi Nakamoto beschäftigt sich anschliessend mit einer weiteren Frage. Was hält einen Miner davon ab, seine Rechenleistung für einen Angriff auf das Netzwerk einzusetzen? Sein Lösungsansatz beruht auf wirtschaftlichen Anreizen. Ein Miner, der einen gültigen Block findet und sich an die Regeln hält, kann eine Vergütung erhalten. Wer dagegen versucht, ungültige Blöcke durchzusetzen, riskiert, dass seine Arbeit von anderen Teilnehmern zurückgewiesen wird. Der entsprechende Aufwand könnte dann ohne die gewünschte Vergütung bleiben.

Satoshi Nakamoto geht ausserdem davon aus, dass es für einen sehr grossen Miner wirtschaftlich sinnvoller sein kann, das Netzwerk erfolgreich zu unterstützen, statt dessen Glaubwürdigkeit zu beschädigen. Denn wenn jemand einen grossen Anteil der Rechenleistung kontrolliert, könnte er bei regelkonformer Beteiligung auch einen entsprechend grossen Anteil der verfügbaren Mining-Vergütungen erzielen. Ein erfolgreicher Angriff könnte dagegen das Vertrauen in Bitcoin und damit möglicherweise auch den Wert der eigenen Einnahmen beeinträchtigen. Das ist die wirtschaftliche Überlegung hinter Satoshis Argument.

Bedeutet das, dass Miner niemals betrügen würden?

Nein. Wirtschaftliche Anreize können bestimmtes Verhalten begünstigen. Sie können aber nicht garantieren, dass sich sämtliche Teilnehmer immer ehrlich verhalten. Ein Miner oder eine Gruppe von Minern könnte unter bestimmten Umständen andere wirtschaftliche Ziele verfolgen. Denkbar sind beispielsweise Angriffe, bei denen eigene frühere Zahlungen nachträglich verändert werden sollen. Auch politische Interessen oder andere Motive könnten das Verhalten beeinflussen. Ausserdem hängt die wirtschaftliche Bewertung davon ab, welche Kosten ein Angreifer tatsächlich tragen müsste und welchen möglichen Vorteil er sich verspricht. Das Whitepaper liefert deshalb keine Garantie dafür, dass Mining-Unternehmen immer im Interesse sämtlicher Bitcoin-Nutzer handeln. Satoshi beschreibt vielmehr einen Mechanismus, der regelkonformes Verhalten wirtschaftlich attraktiv machen soll. Zusätzlich bleiben die unabhängigen Prüfungen der Netzwerkregeln notwendig. Auch ein wirtschaftlich mächtiger Miner kann einem unverändert prüfenden Computer nicht einfach einen ungültigen Block aufzwingen.

Warum ist das Vergütungssystem für Bitcoin entscheidend?

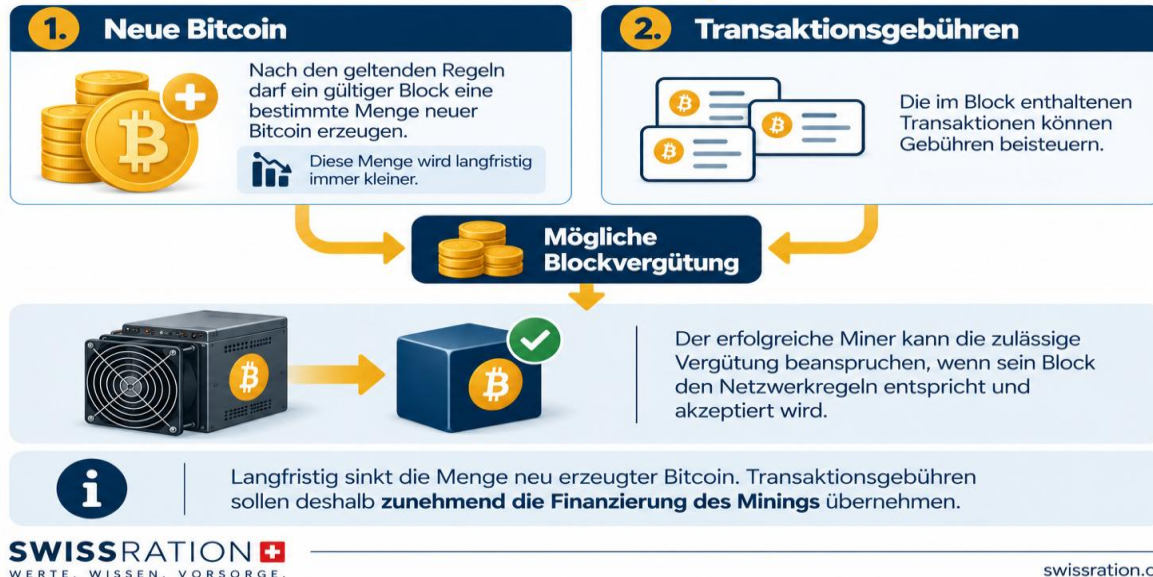
Bitcoin benötigt keine zentrale Stelle, die neue Einheiten nach eigenem Ermessen ausgibt. Die Ausgabe erfolgt nach vorher festgelegten Regeln. Gleichzeitig schafft die mögliche Blockvergütung einen Anreiz, Rechenleistung für das Netzwerk einzusetzen. Miner können Einnahmen erzielen, wenn sie gültige Blöcke finden. Diese Einnahmen bestehen aus der jeweils zulässigen Neuausgabe und den Gebühren der enthaltenen Transaktionen. Das System verbindet damit die Ausgabe neuer Bitcoin mit dem Aufbau und der Absicherung der gemeinsamen Transaktionshistorie. Die Idee dahinter ist, dass wirtschaftliches Eigeninteresse zur Unterstützung des Netzwerks beitragen kann. Ob dies langfristig unter allen Umständen ausreicht, bleibt jedoch eine wirtschaftliche Frage. Der zentrale Gedanke des Whitepapers lautet deshalb nicht, dass Miner aus reiner Hilfsbereitschaft handeln müssen. Vielmehr sollen die Regeln des Systems Anreize schaffen, damit sich die Teilnahme am Netzwerk für sie lohnen kann.

MERKSATZ:

Bitcoin-Miner setzen Rechenleistung ein, um neue gültige Blöcke zu finden. Dafür können sie eine Vergütung erhalten. Diese besteht aus neu ausgegebenen Bitcoin und den Gebühren der im Block enthaltenen Transaktionen. Die Neuausgabe folgt festen Regeln und nimmt langfristig ab. Satoshi Nakamoto entwarf diese Vergütung als wirtschaftlichen Anreiz, damit Teilnehmer das Netzwerk unterstützen und sich möglichst an seine Regeln halten.

GRAFIK 6

Woher stammt die Vergütung der Bitcoin-Miner?



Die Vergütung für einen gültigen Bitcoin-Block setzt sich aus der zulässigen Neuausgabe und den Gebühren der enthaltenen Transaktionen zusammen. Mit der langfristig sinkenden Neuausgabe sollen Gebühren eine zunehmend wichtige Rolle übernehmen.

7. Wie lässt sich der Speicherbedarf der Blockchain reduzieren?

Verständliche Erklärung des Originalabschnitts «Reclaiming Disk Space»

Im siebten Abschnitt seines Whitepapers beschäftigt sich Satoshi Nakamoto mit einem praktischen Problem. Wenn Bitcoin dauerhaft funktioniert, entstehen immer mehr Transaktionen. Diese Transaktionen werden in Blöcken gespeichert. Mit jedem neuen Block wächst die gesamte Transaktionshistorie. Daraus ergibt sich eine naheliegende Frage: Muss jeder Computer für alle Zeiten jede einzelne alte Transaktion vollständig speichern? Satoshi Nakamoto beschreibt deshalb ein Verfahren, mit dem sich bestimmte ältere Daten platzsparender aufbewahren lassen. Der englische Titel dieses Abschnitts lautet «Reclaiming Disk Space». Auf Deutsch bedeutet dies sinngemäss: Bereits belegten Speicherplatz wieder freigeben. Das Ziel besteht darin, den Speicherbedarf zu verringern, ohne die wichtigen kryptographischen Verbindungen innerhalb der Blockchain zu zerstören.

Warum benötigt die Blockchain Speicherplatz?

Bei jeder Bitcoin-Transaktion entstehen digitale Informationen. Dazu gehören beispielsweise Angaben über die verwendeten bisherigen Beträge, die neuen Empfängerbeträge und die erforderlichen digitalen Freigaben.

Diese Informationen müssen zunächst verarbeitet und überprüft werden. Wenn gültige Transaktionen in einen Block aufgenommen werden, werden sie Teil der Blockchain. Im Laufe der Zeit kommen immer mehr Blöcke hinzu. Dadurch wächst die Menge der gespeicherten Daten. Stell dir ein Geschäft vor, das jeden Tag zahlreiche Rechnungen ausstellt. Am Anfang genügt vielleicht ein einzelner Ordner. Nach einigen Jahren werden jedoch immer mehr Ordner benötigt. Das Geschäft muss sich deshalb überlegen, welche Unterlagen dauerhaft verfügbar bleiben sollen und welche Informationen platzsparender archiviert werden können. Bei Bitcoin stellt sich eine ähnliche Frage. Allerdings müssen dabei die technischen Sicherheitsanforderungen des Netzwerks berücksichtigt werden.

Warum kann man alte Transaktionen nicht einfach löschen?

Die Bitcoin-Blockchain besteht aus miteinander verbundenen Blöcken. Jeder Block enthält Informationen, die für die Überprüfung seiner Verbindung zum vorherigen Block wichtig sind. Ausserdem müssen die Transaktionen den geltenden Regeln entsprechen. Wenn man ältere Informationen einfach unkontrolliert löschen oder verändern würde, könnten notwendige Nachweise verloren gehen. Die Blockchain könnte dann nicht mehr auf dieselbe Weise überprüft werden. Satoshi Nakamoto benötigte deshalb ein Verfahren, das zwei Anforderungen miteinander verbindet. Einerseits sollen bestimmte ältere Daten entfernt werden können, um Speicherplatz zu sparen. Andererseits soll weiterhin überprüfbar bleiben, dass diese Daten ursprünglich zu einem bestimmten Block gehörten. Für dieses Problem verwendet Bitcoin eine besondere Anordnung digitaler Fingerabdrücke. Diese wird Merkle-Baum genannt.

Was ist ein Merkle-Baum?

Ein Merkle-Baum ist eine Methode, mit der sich viele digitale Informationen durch miteinander verbundene Fingerabdrücke zusammenfassen lassen. Der Begriff geht auf den Informatiker Ralph Merkle zurück. Im Englischen heisst diese Datenstruktur «Merkle Tree». Das Wort Tree bedeutet Baum. Der Name ergibt sich aus dem Aufbau. Viele einzelne Informationen bilden gewissermassen die untersten Äste eines Baumes. Diese Informationen werden schrittweise zusammengefasst. Am Ende bleibt ein einziger digitaler Fingerabdruck übrig, der sämtliche ursprünglichen Informationen miteinander verbindet. Um das zu verstehen, betrachten wir ein einfaches Beispiel mit vier Bitcoin-Transaktionen.

Ein Merkle-Baum mit vier Transaktionen

Stell dir vor, ein Bitcoin-Block enthält vier Transaktionen. Wir nennen sie Transaktion A, Transaktion B, Transaktion C und Transaktion D. Für jede dieser vier Transaktionen wird zunächst ein digitaler Fingerabdruck berechnet. Dadurch entstehen vier unterschiedliche Ergebnisse. Im nächsten Schritt werden die Fingerabdrücke von Transaktion A und Transaktion B miteinander verbunden. Aus dieser Verbindung wird ein neuer gemeinsamer Fingerabdruck berechnet. Dasselbe geschieht mit den Fingerabdrücken von Transaktion C und Transaktion D. Nun besitzen wir zwei zusammengefasste Fingerabdrücke. Diese beiden Ergebnisse werden wiederum miteinander verbunden. Anschliessend wird daraus ein letzter gemeinsamer Fingerabdruck berechnet. Dieser letzte Fingerabdruck steht an der Spitze des Merkle-Baumes. Man nennt ihn Merkle-Wurzel. Im Englischen lautet der Begriff «Merkle Root».

Der Begriff Wurzel kann zunächst verwirrend sein, weil wir sie uns bei einem gewöhnlichen Baum unten vorstellen. In einer technischen Darstellung befindet sich diese sogenannte Wurzel häufig ganz oben. Gemeint ist damit der abschliessende gemeinsame Fingerabdruck aller Transaktionen, die in diese Berechnung eingeflossen sind.

Warum ist die Merkle-Wurzel wichtig?

Die Merkle-Wurzel fasst die Transaktionen eines Blocks auf besondere Weise zusammen. Sie ist nicht einfach eine frei gewählte Nummer. Ihr Wert hängt von den digitalen Fingerabdrücken der enthaltenen Transaktionen ab. Wenn eine Transaktion verändert wird, verändert sich dadurch mit überwältigender Wahrscheinlichkeit auch ihr digitaler Fingerabdruck. Diese Veränderung wirkt sich auf die darüberliegenden Verbindungen aus. Am Ende entsteht dadurch eine andere Merkle-Wurzel. So kann überprüft werden, ob die vorhandenen Transaktionsdaten noch zu der ursprünglich berechneten Zusammenfassung passen. Der entscheidende Vorteil besteht darin, dass nicht sämtliche Transaktionen direkt in den digitalen Fingerabdruck des Blockkopfs aufgenommen werden müssen. Stattdessen enthält der Blockkopf die Merkle-Wurzel. Sie stellt die kryptographische Verbindung zu den Transaktionen her.

BEISPIEL:

Stell dir vier Dokumente vor. Für jedes Dokument wird ein eigener digitaler Fingerabdruck erstellt. Anschliessend werden jeweils zwei Fingerabdrücke zusammengefasst. Aus den beiden Ergebnissen wird wiederum ein gemeinsamer Fingerabdruck berechnet. Am Ende entsteht ein einziger Wert, der von allen vier Dokumenten abhängt. Wird später eines der Dokumente verändert, passt dieser abschliessende Fingerabdruck nicht mehr zu den veränderten Daten. So lassen sich viele Informationen miteinander verbinden, ohne ihren vollständigen Inhalt in einen einzigen langen Fingerabdruck schreiben zu müssen.

Was ist ein Blockkopf?

Im Whitepaper unterscheidet Satoshi Nakamoto zwischen einem vollständigen Block und dessen Kopf. Der Blockkopf enthält wichtige technische Angaben über den Block. Dazu gehören unter anderem der Verweis auf den vorherigen Block und die Merkle-Wurzel der enthaltenen Transaktionen. Ausserdem enthält er Informationen, die für den Arbeitsnachweis benötigt werden. Der Blockkopf ist wesentlich kleiner als der vollständige Block mit sämtlichen Transaktionsdaten. Du kannst dir diesen Unterschied wie bei einem umfangreichen Buch vorstellen. Das Buch enthält viele Seiten mit detaillierten Informationen. Auf dem Umschlag stehen dagegen nur wenige wichtige Angaben. Der Umschlag ersetzt nicht den gesamten Inhalt. Er ermöglicht aber eine kompakte Kennzeichnung des Buches. Beim Bitcoin-Blockkopf ist der Zusammenhang technisch strenger. Seine Angaben sind Bestandteil kryptographischer Berechnungen. Insbesondere verbindet die Merkle-Wurzel die Transaktionsdaten mit dem Blockkopf. Dadurch lässt sich nachweisen, dass bestimmte Transaktionen zu dem betreffenden Block gehören.

Wie können ältere Daten platzsparender gespeichert werden?

Satoshi Nakamoto beschreibt im Whitepaper, dass ältere, bereits ausgegebene Transaktionsdaten unter bestimmten Voraussetzungen entfernt werden können.

Dafür nutzt er den Aufbau des Merkle-Baumes. Nicht sämtliche ursprünglichen Informationen müssen in jeder Situation weiterhin vollständig gespeichert werden. Bestimmte Zweige des Baumes können entfernt werden. Die verbleibenden digitalen Fingerabdrücke können dabei weiterhin die notwendigen Verbindungen zur Merkle-Wurzel erhalten. Stell dir noch einmal unseren Baum aus vier Transaktionen vor. Die vier Transaktionen wurden zunächst zu zwei gemeinsamen Fingerabdrücken zusammengefasst. Aus diesen beiden Ergebnissen entstand die Merkle-Wurzel. Wenn später bestimmte ältere Transaktionsdaten nicht mehr vollständig benötigt werden, kann ein Teil der ursprünglichen Daten durch geeignete zusammenfassende Fingerabdrücke ersetzt werden. Dadurch wird weniger Speicherplatz benötigt. Die kryptographische Verbindung zur Merkle-Wurzel bleibt erhalten, soweit die dafür notwendigen Informationen aufbewahrt werden. Allerdings bedeutet dies nicht, dass die gelöschten Transaktionsdaten aus der Merkle-Wurzel wiederhergestellt werden könnten. Ein digitaler Fingerabdruck enthält nicht sämtliche ursprünglichen Daten in einer Form, aus der sich diese einfach zurückgewinnen lassen. Wer später den vollständigen Inhalt einer gelöschten Transaktion erneut untersuchen möchte, benötigt die entsprechenden Daten aus einer anderen Quelle.

Was bedeutet das für die Sicherheit?

Die Idee des Merkle-Baumes ist besonders wertvoll, weil sich damit Informationen kompakt zusammenfassen und kryptographisch miteinander verbinden lassen. Ein Computer kann anhand geeigneter Nachweise überprüfen, ob eine bestimmte Transaktion zu einem Block gehört. Dafür muss er nicht immer sämtliche anderen Transaktionen dieses Blocks zur Verfügung haben. Das ist eine wichtige Grundlage für platzsparende Prüfverfahren. Allerdings müssen wir zwischen unterschiedlichen Aufgaben unterscheiden. Es ist eine Sache, nachzuweisen, dass eine bestimmte Transaktion in einem Block enthalten ist. Es ist eine andere Sache, sämtliche Regeln aller historischen Transaktionen vollständig selbst zu überprüfen. Für eine vollständige Prüfung werden zusätzliche Informationen benötigt. Die Merkle-Wurzel allein reicht dafür nicht aus. Wenn ältere Daten entfernt wurden, kann man sie nicht allein aus den verbleibenden Fingerabdrücken rekonstruieren. Deshalb bedeutet eine platzsparende Speicherung nicht automatisch, dass sämtliche früheren Prüfungen jederzeit ohne weitere Daten wiederholt werden können.

Wie funktioniert die platzsparende Speicherung heute?

Das ursprüngliche Whitepaper beschreibt eine grundsätzliche technische Möglichkeit zur Verringerung des Speicherbedarfs. Seit 2008 wurde die Bitcoin-Software jedoch weiterentwickelt. Deshalb entspricht nicht jedes heute eingesetzte Speicherverfahren genau der im Whitepaper dargestellten Methode. Bitcoin Core, eine weitverbreitete Bitcoin-Software, unterstützt beispielsweise eine Funktion zur Begrenzung des dauerhaft gespeicherten Bestands älterer Blockdaten. Diese Funktion wird Pruning genannt. Auf Deutsch bedeutet das sinngemäss Zurückschneiden. Ein entsprechend eingerichteter Prüfknoten kann die historischen Blöcke zunächst herunterladen und überprüfen. Anschliessend kann er ältere Blockdateien entfernen, um Speicherplatz zu sparen. Dabei müssen die Informationen erhalten bleiben, die für seine weitere regelkonforme Arbeit erforderlich sind. Ein solcher Computer kann weiterhin selbstständig die Gültigkeit neuer Blöcke prüfen. Er bewahrt jedoch nicht mehr sämtliche älteren Blockdateien vollständig auf.

Wichtig ist:

Dieses heutige Verfahren ist nicht einfach identisch mit dem im Whitepaper gezeichneten Entfernen einzelner Zweige eines Merkle-Baumes. Beide Ansätze verfolgen zwar das Ziel, Speicherplatz zu sparen. Ihre konkrete technische Umsetzung unterscheidet sich jedoch. Für den Swissration-Leitfaden ist diese Unterscheidung wichtig, weil wir das ursprüngliche Konzept erklären möchten, ohne spätere Entwicklungen fälschlicherweise als Bestandteile des Whitepapers darzustellen.

Wie viel Speicherplatz benötigt ein Blockkopf?

Satoshi Nakamoto nennt im Whitepaper auch ein konkretes Rechenbeispiel. Ein Bitcoin-Blockkopf besitzt eine Grösse von ungefähr 80 Byte. Ein Byte ist eine kleine Einheit zur Messung digitaler Datenmengen. Zum Vergleich: Ein längeres Foto oder ein Video benötigt normalerweise wesentlich mehr Speicherplatz als 80 Byte. Satoshi geht in seiner Berechnung von durchschnittlich einem neuen Block alle zehn Minuten aus. Das entspricht ungefähr sechs neuen Blöcken pro Stunde. Für einen ganzen Tag ergibt das ungefähr 144 Blöcke. Über ein Jahr gerechnet sind es ungefähr 52'560 Blöcke. Wenn jeder Blockkopf 80 Byte benötigt, ergibt sich folgende Rechnung: $80 \text{ Byte} \times 6 \text{ Blöcke pro Stunde} \times 24 \text{ Stunden} \times 365 \text{ Tage}$. Das Ergebnis beträgt 4'204'800 Byte. Das entspricht ungefähr 4,2 Megabyte pro Jahr. Diese Berechnung zeigt, wie wenig Speicherplatz die reinen Blockköpfe im Vergleich zu vollständigen Blöcken beanspruchen. Die vollständigen Bitcoin-Blöcke enthalten zusätzlich sämtliche gespeicherten Transaktionsdaten. Sie benötigen deshalb wesentlich mehr Platz. Die Zahl von ungefähr 4,2 Megabyte pro Jahr bezieht sich ausdrücklich nur auf die Blockköpfe und nicht auf die vollständige Blockchain.

Warum war diese Berechnung im Jahr 2008 wichtig?

Als Satoshi Nakamoto sein Whitepaper veröffentlichte, waren die Speichermöglichkeiten gewöhnlicher Computer deutlich begrenzter als heute. Er wollte deshalb zeigen, dass zumindest die Speicherung der fortlaufenden Blockköpfe keinen besonders grossen Speicherbedarf verursachen müsste. Dazu verglich er seine Berechnung mit dem damals verfügbaren Arbeitsspeicher gewöhnlicher Computer. Aus seiner Sicht war die benötigte Datenmenge klein genug, um die langfristige Speicherung der Blockköpfe praktikabel erscheinen zu lassen. Dabei handelt es sich um eine technische Einschätzung aus dem Jahr 2008. Sie ist nicht mit einer Garantie gleichzusetzen, dass der gesamte Bitcoin-Datenbestand für alle Zeiten klein bleiben würde. Satoshi betrachtete in diesem Rechenbeispiel lediglich die Blockköpfe. Die vollständigen Transaktionsdaten benötigen zusätzlich Speicherplatz. Ausserdem haben sich die Anforderungen an die Bitcoin-Software und die Möglichkeiten der Computertechnik seitdem weiterentwickelt.

Warum ist diese Idee für Bitcoin wichtig?

Ein weltweit genutztes Zahlungssystem muss nicht nur sicher sein. Es muss auch über lange Zeiträume betrieben werden können. Wenn sämtliche Teilnehmer unbegrenzt grosse Datenmengen speichern müssten, könnte dies die Teilnahme am Netzwerk erschweren. Satoshi Nakamoto beschäftigte sich deshalb bereits im ursprünglichen Whitepaper mit der Frage, wie Daten effizient organisiert werden können. Der Merkle-Baum ist dafür ein wichtiger Bestandteil. Er ermöglicht es, viele Transaktionen durch miteinander verbundene digitale Fingerabdrücke zusammenzufassen. Dabei entsteht eine Merkle-Wurzel, die im Blockkopf gespeichert wird.

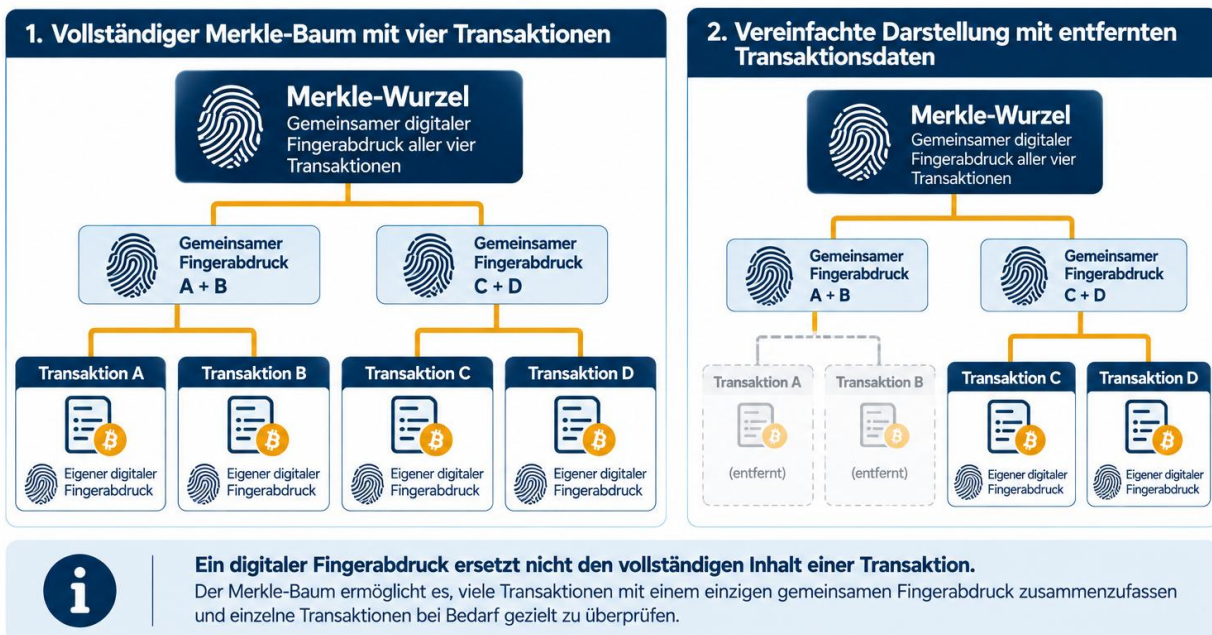
Diese Konstruktion erlaubt es, bestimmte Informationen platzsparend nachzuweisen. Sie ist ausserdem die technische Grundlage für eine weitere wichtige Idee des Whitepapers: Die vereinfachte Überprüfung von Bitcoin-Zahlungen. Genau damit beschäftigt sich Satoshi Nakamoto im nächsten Abschnitt.

MERKSATZ:

Die Bitcoin-Blockchain wächst mit jeder neuen Transaktion und jedem neuen Block. Satoshi Nakamoto beschreibt deshalb eine Methode, mit der bestimmte ältere Daten platzsparender gespeichert werden können. Dafür verwendet Bitcoin sogenannte Merkle-Bäume. Sie fassen viele Transaktionen mithilfe digitaler Fingerabdrücke zusammen. Die abschliessende Merkle-Wurzel wird im Blockkopf gespeichert und verbindet diesen kryptographisch mit den Transaktionsdaten. So lassen sich bestimmte Nachweise kompakt führen, ohne immer sämtliche Transaktionen gleichzeitig vorhalten zu müssen.

GRAFIK 7

Vier Transaktionen - ein gemeinsamer digitaler Fingerabdruck



Ein Merkle-Baum verbindet die digitalen Fingerabdrücke mehrerer Transaktionen zu einem einzigen gemeinsamen Ergebnis. Diese Merkle-Wurzel wird im Blockkopf gespeichert. Damit lassen sich Transaktionsdaten kryptographisch zusammenfassen und bestimmte Nachweise mit vergleichsweise wenig Speicherplatz führen.

8. Wie können Bitcoin-Zahlungen vereinfacht überprüft werden?

Verständliche Erklärung des Originalabschnitts «Simplified Payment Verification»

Im achten Abschnitt seines Whitepapers beschäftigt sich Satoshi Nakamoto mit einer wichtigen praktischen Frage. Muss jeder Mensch, der Bitcoin verwendet, die gesamte Blockchain auf seinem eigenen Computer speichern und sämtliche Transaktionen selbst überprüfen? Wenn das notwendig wäre, könnte die Nutzung von Bitcoin für viele Menschen aufwendig werden. Schliesslich wächst die Blockchain mit jedem neuen Block weiter. Satoshi Nakamoto beschreibt deshalb ein Verfahren, mit dem sich die Aufnahme einer Zahlung in die Blockchain überprüfen lässt, ohne einen vollständigen Bitcoin-Prüfknoten betreiben zu müssen. Dieses Verfahren nennt er «Simplified Payment Verification». Auf Deutsch bedeutet das vereinfachte Zahlungsprüfung. Die Idee besteht darin, nur bestimmte Informationen aus der Blockchain zu verwenden. Damit lässt sich nachvollziehen, ob eine bestimmte Transaktion in einem Block enthalten ist und wie viel nachgewiesene Rechenarbeit auf diesem Block aufbaut. Diese vereinfachte Methode ist allerdings nicht mit der vollständigen, unabhängigen Überprüfung sämtlicher Bitcoin-Regeln gleichzusetzen.

Was macht ein vollständiger Prüfknoten?

Um die vereinfachte Zahlungsprüfung zu verstehen, müssen wir zunächst betrachten, was ein vollständiger Bitcoin-Prüfknoten macht. Ein solcher Computer überprüft die Transaktionen und Blöcke anhand der geltenden Regeln des Bitcoin-Netzwerks. Er kontrolliert beispielsweise, ob die erforderlichen digitalen Signaturen gültig sind und ob die verwendeten Beträge tatsächlich noch ausgegeben werden dürfen. Ausserdem prüft er, ob neue Blöcke den vorgeschriebenen Arbeitsnachweis besitzen. Ein vollständiger Prüfknoten verlässt sich dabei nicht einfach auf die Aussage eines anderen Computers, dass eine Zahlung gültig sei. Er überprüft die notwendigen Informationen selbst. Das ist ein wichtiger Bestandteil der Dezentralität von Bitcoin. Allerdings benötigt diese vollständige Prüfung Computerleistung, Speicherplatz und eine Verbindung zum Netzwerk. Satoshi Nakamoto wollte deshalb auch eine einfachere Möglichkeit beschreiben, mit der Nutzer bestimmte Zahlungsnachweise kontrollieren können.

Welche Informationen werden für die vereinfachte Prüfung benötigt?

Satoshi Nakamoto beschreibt zwei wesentliche Bestandteile. Der erste Bestandteil ist die Kette der Blockköpfe. Der zweite Bestandteil ist ein Nachweis, dass die gesuchte Transaktion in einem bestimmten Block enthalten ist. Diesen Nachweis ermöglicht der Merkle-Baum, den wir im vorherigen Kapitel kennengelernt haben. Beide Informationen werden miteinander verbunden. Dadurch kann ein Nutzer überprüfen, ob eine bestimmte Transaktion in einem Block enthalten ist, der zu einer Kette mit nachgewiesener Rechenarbeit gehört. Je mehr weitere gültig erscheinende Blöcke darauf aufbauen, desto stärker wird dieser Nachweis unter den zugrunde liegenden Sicherheitsannahmen.

Was ist die Kette der Blockköpfe?

Ein Bitcoin-Block besteht aus einem Blockkopf und den zugehörigen Transaktionsdaten. Der Blockkopf enthält wichtige technische Informationen.

Dazu gehören der Verweis auf den vorherigen Block, die Merkle-Wurzel und die Angaben zum Arbeitsnachweis. Wie wir in Kapitel 7 gesehen haben, ist ein Blockkopf ungefähr 80 Byte gross. Das ist wesentlich weniger als die Datenmenge eines vollständigen Blocks. Wenn ein Computer nur die Blockköpfe speichert, benötigt er deshalb deutlich weniger Speicherplatz als für sämtliche vollständigen Blockdaten. Die Blockköpfe sind ausserdem miteinander verbunden. Jeder neue Blockkopf enthält einen Verweis auf den vorherigen Block. So entsteht eine eigene, zusammenhängende Kette der Blockköpfe. Anhand dieser Kette kann überprüft werden, welche Rechenarbeit nachgewiesen wurde. Ein Nutzer benötigt jedoch eine geeignete Verbindung zu anderen Netzwerkteilnehmern, um diese Informationen zu erhalten. Im Whitepaper beschreibt Satoshi Nakamoto, dass die Blockköpfe von verschiedenen Netzwerkteilnehmern angefordert werden können. Der Nutzer soll dadurch die Kette mit der grössten nachgewiesenen Rechenarbeit ermitteln können. Wichtig ist, dass eine solche Prüfung noch nicht bedeutet, dass der Nutzer sämtliche Transaktionen und Bitcoin-Regeln selbst überprüft hat.

Wie kann man eine einzelne Transaktion in einem Block nachweisen?

Stell dir vor, Beat erhält eine Bitcoin-Zahlung von Anna. Beat möchte überprüfen, ob diese Zahlung in einem bestimmten Block enthalten ist. Dafür müsste er theoretisch den vollständigen Block mit sämtlichen Transaktionen untersuchen. Satoshi Nakamoto beschreibt jedoch eine platzsparendere Möglichkeit. Sie verwendet den Merkle-Baum. Zur Erinnerung: Ein Merkle-Baum fasst die digitalen Fingerabdrücke vieler Transaktionen schrittweise zusammen. Am Ende entsteht ein einziger gemeinsamer Fingerabdruck. Dieser wird als Merkle-Wurzel bezeichnet. Die Merkle-Wurzel ist im Blockkopf enthalten. Um die Aufnahme einer bestimmten Transaktion nachzuweisen, müssen nicht sämtliche anderen Transaktionen des Blocks übertragen werden. Es genügt eine passende Auswahl digitaler Fingerabdrücke. Mit diesen Informationen lässt sich der Rechenweg bis zur Merkle-Wurzel nachvollziehen. Eine solche Auswahl nennt man Merkle-Nachweis. Im englischen Whitepaper wird dafür der Begriff «Merkle Branch» verwendet.

Ein einfaches Beispiel mit vier Transaktionen

Stell dir einen Bitcoin-Block mit vier Transaktionen vor. Wir nennen sie A, B, C und D. Für jede Transaktion wird ein eigener digitaler Fingerabdruck berechnet. Anschliessend werden die Fingerabdrücke von A und B miteinander verbunden. Dasselbe geschieht mit C und D. Die beiden Ergebnisse werden erneut miteinander verbunden. Daraus entsteht die Merkle-Wurzel. Nun möchte Beat überprüfen, ob Transaktion C in diesem Block enthalten ist. Dafür benötigt er nicht die vollständigen Daten von A, B und D. Er benötigt die Transaktion C und bestimmte zusätzliche Fingerabdrücke. Mit dem Fingerabdruck von D kann er zunächst den gemeinsamen Wert für C und D berechnen. Mit dem bereits zusammengefassten Fingerabdruck von A und B kann er anschliessend die Merkle-Wurzel berechnen. Stimmt das Ergebnis mit der Merkle-Wurzel im Blockkopf überein, besitzt Beat einen kryptographischen Nachweis dafür, dass Transaktion C in der betreffenden Zusammenfassung enthalten ist. Damit ist allerdings noch nicht vollständig bewiesen, dass die Transaktion nach sämtlichen Bitcoin-Regeln gültig ist. Der Merkle-Nachweis bestätigt zunächst die Zugehörigkeit der Transaktion zu einem bestimmten Block.

BEISPIEL:

Stell dir einen umfangreichen Aktenordner vor. Du möchtest nachweisen, dass ein bestimmtes Dokument zu diesem Ordner gehört. Anstatt dir sämtliche Dokumente des Ordners zu geben, erhältst du eine besondere Zusammenfassung und einige überprüfbare Verweise. Damit kannst du nachvollziehen, dass dein Dokument in die ursprüngliche Zusammenfassung eingeflossen ist. Bei Bitcoin übernehmen digitale Fingerabdrücke diese Aufgabe. Der Unterschied besteht darin, dass die Verbindung nicht auf einer einfachen schriftlichen Bestätigung beruht, sondern auf mathematisch überprüfbaren Berechnungen.

Warum sind zusätzliche Bestätigungen wichtig?

Wenn eine Transaktion in einem Block enthalten ist, kann der Nutzer überprüfen, wie viele weitere Blöcke auf diesem Block aufbauen. Jeder nachfolgende Block besitzt wiederum einen eigenen Arbeitsnachweis. Dadurch wächst die gesamte nachgewiesene Rechenarbeit der Kette. Unter den Sicherheitsannahmen des Whitepapers wird es damit zunehmend schwieriger, eine konkurrierende Geschichte durchzusetzen. Satoshi Nakamoto verbindet deshalb den Merkle-Nachweis mit der Kette der Blockköpfe. Der Merkle-Nachweis zeigt, dass eine bestimmte Transaktion in einem bestimmten Block enthalten ist. Die Kette der Blockköpfe zeigt, wie viel weitere nachgewiesene Rechenarbeit auf diesem Block aufbaut. Zusammen ermöglichen diese Informationen eine vereinfachte Einschätzung des Bestätigungsstatus. Allerdings bleibt ein Unterschied zur vollständigen Prüfung bestehen. Ein Nutzer mit dieser vereinfachten Methode überprüft nicht selbst sämtliche Regeln aller enthaltenen Transaktionen.

Wo liegen die Grenzen der vereinfachten Zahlungsprüfung?

Satoshi Nakamoto weist im Whitepaper ausdrücklich darauf hin, dass die vereinfachte Methode weniger unabhängig ist als die Prüfung durch einen vollständigen Netzwerkknoten. Der Grund ist einfach. Ein vollständiger Prüfknoten kann selbst kontrollieren, ob ein Block sämtliche geltenden Regeln erfüllt. Bei der vereinfachten Prüfung fehlen dem Nutzer dafür bestimmte Informationen. Er kann zwar den Arbeitsnachweis und die Zugehörigkeit einer Transaktion zu einem Block kontrollieren. Er kann aber nicht allein anhand dieser Angaben feststellen, ob jede Transaktion des Blocks gültig ist. Deshalb ist die vereinfachte Methode stärker auf die Zuverlässigkeit der übrigen Netzwerkteilnehmer angewiesen. Solange ehrliche Teilnehmer das Netzwerk ausreichend kontrollieren und korrekte Informationen verfügbar sind, kann die Methode nützliche Zahlungsnachweise liefern. Wenn ein Angreifer dagegen die zugänglichen Informationen manipuliert oder die Netzwerksituation beherrscht, kann die vereinfachte Prüfung in die Irre geführt werden. Das Whitepaper beschreibt deshalb keine vollständig gleichwertige Alternative zur unabhängigen Prüfung sämtlicher Regeln.

Wie könnte ein Angreifer die vereinfachte Prüfung täuschen?

Stell dir vor, ein Nutzer erhält seine Informationen ausschliesslich von Computern, die unter der Kontrolle eines Angreifers stehen. Der Angreifer könnte versuchen, dem Nutzer eine irreführende Sicht auf das Bitcoin-Netzwerk zu vermitteln. Wenn der Nutzer nicht selbst alle Regeln überprüft, kann er bestimmte Fehler oder ungültige Daten möglicherweise nicht erkennen.

Ein Merkle-Nachweis allein sagt beispielsweise nichts darüber aus, ob sämtliche übrigen Transaktionen des betreffenden Blocks gültig sind. Satoshi Nakamoto beschreibt deshalb im Whitepaper zusätzliche Schutzmöglichkeiten. Eine Idee besteht darin, Warnmeldungen von vollständigen Prüfknoten zu berücksichtigen. Wenn solche Prüfknoten einen ungültigen Block entdecken, könnten sie andere Teilnehmer darauf aufmerksam machen. Der betroffene Nutzer könnte daraufhin die vollständigen Daten anfordern und die Unstimmigkeit untersuchen. Wichtig ist jedoch: Das Whitepaper beschreibt hier einen möglichen Schutzmechanismus. Es bedeutet nicht, dass jedes heutige Bitcoin-Wallet automatisch über genau dieses Warnsystem verfügt.

Warum könnten Unternehmen vollständige Prüfknoten benötigen?

Satoshi Nakamoto weist darauf hin, dass Unternehmen mit vielen eingehenden Zahlungen ein besonderes Interesse an einer möglichst unabhängigen Überprüfung haben können. Stell dir ein Unternehmen vor, das täglich zahlreiche Bitcoin-Zahlungen entgegennimmt. Wenn es sich ausschliesslich auf fremde Informationen verlässt, entsteht eine zusätzliche Abhängigkeit. Ein eigener vollständiger Prüfknoten ermöglicht es dagegen, die geltenden Bitcoin-Regeln selbst zu überprüfen. Das kann die Unabhängigkeit und die Kontrolle über den Zahlungsablauf verbessern. Allerdings entstehen dadurch auch Anforderungen an die technische Einrichtung und den Betrieb. Für private Nutzer ohne entsprechende Kenntnisse kann eine vereinfachte Lösung praktischer sein. Welche Lösung geeignet ist, hängt deshalb auch von den Sicherheitsanforderungen und den technischen Möglichkeiten ab.

Verwenden heutige Bitcoin-Wallets diese Methode?

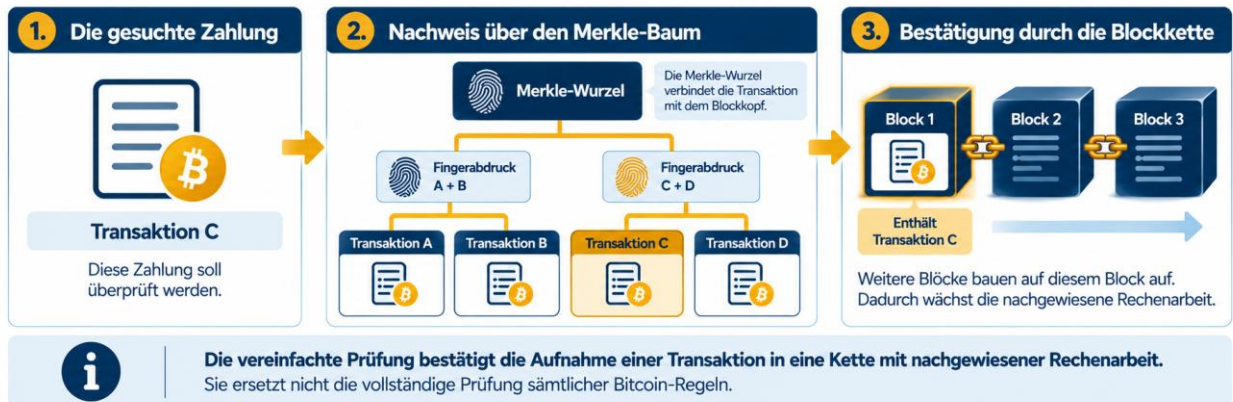
Das grundlegende Konzept der vereinfachten Zahlungsprüfung hat die Entwicklung von Bitcoin-Wallets beeinflusst. Allerdings arbeiten heute nicht sämtliche Wallets nach genau demselben Verfahren, das Satoshi Nakamoto im Whitepaper beschrieben hat. Manche Anwendungen verwenden eigene Prüfverfahren. Andere beziehen Informationen von spezialisierten Servern. Wieder andere können mit einem selbst betriebenen vollständigen Prüfknoten verbunden werden. Eine Wallet, die Informationen von einem fremden Server anzeigt, führt deshalb nicht automatisch eine vereinfachte Prüfung anhand der Blockköpfe und eines Merkle-Nachweises durch. Hier müssen wir zwischen dem ursprünglichen Konzept aus dem Jahr 2008 und unterschiedlichen heutigen technischen Umsetzungen unterscheiden. Für das Verständnis des Whitepapers ist vor allem eine Erkenntnis entscheidend: Bitcoin wurde so konstruiert, dass sich die Aufnahme einer Transaktion in die Blockchain auch mit vergleichsweise wenigen Daten nachweisen lässt. Dieser Nachweis bietet jedoch nicht dieselbe unabhängige Sicherheit wie eine vollständige Überprüfung aller Netzwerkregeln.

MERKSATZ:

Satoshi Nakamoto beschreibt im Whitepaper ein Verfahren, mit dem die Aufnahme einer Bitcoin-Zahlung in die Blockchain vereinfacht überprüft werden kann. Dafür werden die Blockköpfe und ein Merkle-Nachweis verwendet. Der Nutzer muss nicht sämtliche Transaktionen dauerhaft selbst speichern. Die Methode überprüft jedoch nicht alle Bitcoin-Regeln unabhängig und bietet deshalb weniger Sicherheit als ein vollständiger Prüfknoten.

GRAFIK 8

Eine Bitcoin-Zahlung überprüfen, ohne den gesamten Block zu speichern



SWISSRATION+
WERTE. WISSEN. VORSORGE.

swissration.ch

Ein Merkle-Nachweis verbindet eine bestimmte Transaktion mit der Merkle-Wurzel eines Blocks. Die Kette der Blockköpfe ermöglicht zusätzlich die Überprüfung der nachgewiesenen Rechenarbeit. Diese vereinfachte Methode ersetzt jedoch nicht die vollständige Prüfung aller Bitcoin-Regeln.

9. Wie können Bitcoin-Beträge aufgeteilt und zusammengeführt werden?

Verständliche Erklärung des Originalabschnitts «Combining and Splitting Value»

Im neunten Abschnitt seines Whitepapers erklärt Satoshi Nakamoto, wie Bitcoin unterschiedliche Zahlungsbeträge verarbeiten kann. Denn im Alltag bezahlen wir selten immer genau denselben Betrag. Manchmal möchten wir eine kleine Summe ausgeben. Manchmal benötigen wir mehrere vorhandene Beträge, um eine grössere Zahlung auszuführen. Ausserdem kommt es häufig vor, dass wir mehr Geld zur Verfügung haben, als wir gerade ausgeben möchten. Bei Bargeld kennen wir dafür eine einfache Lösung. Wir können mehrere Münzen oder Banknoten zusammenlegen. Und wenn wir mit einer grösseren Banknote bezahlen, erhalten wir gegebenenfalls Wechselgeld zurück. Bitcoin verwendet für vergleichbare Aufgaben ein eigenes technisches Verfahren. Satoshi Nakamoto erklärt dazu, dass eine Bitcoin-Transaktion mehrere Eingänge und mehrere Ausgänge besitzen kann.

Warum müssen Bitcoin-Beträge teilbar sein?

Stell dir vor, Bitcoin würde ausschliesslich aus einzelnen, unveränderlichen Einheiten bestehen. Jede dieser Einheiten müsste vollständig übertragen werden. Dann wäre es umständlich, einen bestimmten Betrag zu bezahlen. Für jede kleine Teilzahlung müsste möglicherweise eine eigene Transaktion erstellt werden. Satoshi Nakamoto wollte deshalb ein System, das unterschiedliche Beträge flexibel verarbeiten kann. Die Lösung besteht darin, dass Transaktionen vorhandene Beträge verwenden und daraus neue verfügbare Beträge erzeugen können.

So lassen sich kleinere Beträge zusammenführen. Grössere Beträge können aufgeteilt werden. Und bei Bedarf kann ein Restbetrag wieder dem ursprünglichen Nutzer zugeordnet werden.

Was bedeutet Eingang und Ausgang einer Transaktion?

Bei Bitcoin besteht eine Transaktion aus bestimmten technischen Bestandteilen. Besonders wichtig sind ihre Eingänge und Ausgänge. Ein Eingang verweist auf einen bereits vorhandenen, noch nicht ausgegebenen Betrag aus einer früheren Transaktion. Ein Ausgang legt fest, welcher neue Betrag unter welchen Bedingungen künftig ausgegeben werden darf. Das klingt zunächst kompliziert. Ein Alltagsvergleich hilft beim Verständnis. Stell dir vor, du bezahlst in einem Geschäft mit einer 100-Franken-Note. Du kaufst etwas für 35 Franken. Der Verkäufer gibt dir 65 Franken zurück. Du hast also einen vorhandenen Betrag von 100 Franken verwendet. Daraus sind zwei neue Beträge entstanden. 35 Franken erhält der Verkäufer. 65 Franken bekommst du zurück. Bei Bitcoin kann eine Transaktion etwas Ähnliches bewirken. Ein vorhandener Betrag wird verwendet und anschliessend auf mehrere neue Beträge verteilt. Allerdings werden bei Bitcoin keine physischen Banknoten oder Münzen übergeben. Die verfügbaren Beträge werden anhand der Transaktionsregeln digital verwaltet.

Was sind verfügbare Transaktionsausgänge?

Um diese Technik genauer zu verstehen, müssen wir einen wichtigen Begriff kennenlernen. Bitcoin verwaltet verfügbare Beträge in Form von noch nicht ausgegebenen Transaktionsausgängen. Im Englischen heisst das «Unspent Transaction Output». Die Abkürzung lautet UTXO. Auf Deutsch bedeutet dies sinngemäss: Ein Betrag aus einer früheren Transaktion, der noch nicht ausgegeben wurde. Ein solcher Betrag kann später als Eingang einer neuen Transaktion verwendet werden. Du kannst dir einen UTXO vereinfacht wie einen einzelnen verfügbaren Geldbetrag vorstellen. Dabei ist wichtig, dass er nicht mit einer physischen Münze gleichgesetzt werden darf. Ein UTXO ist eine technische Information innerhalb der Bitcoin-Transaktionshistorie. Wenn dieser Betrag ausgegeben wird, wird der bisherige Transaktionsausgang vollständig verwendet. Falls nicht der gesamte Wert an den Empfänger gehen soll, kann die Transaktion einen neuen Restbetrag für den Absender erzeugen.

Wie funktioniert eine Zahlung mit Wechselgeld?

Wir betrachten ein einfaches Beispiel. Anna besitzt einen verfügbaren Bitcoin-Betrag von 100'000 Satoshi. Ein Satoshi ist die kleinste Einheit eines Bitcoin auf der Blockchain. 100 Millionen Satoshi entsprechen einem Bitcoin. Anna möchte Beat 60'000 Satoshi senden. Für die Transaktion nehmen wir in diesem erfundenen Beispiel eine Gebühr von 1'000 Satoshi an. Anna verwendet ihren vorhandenen Betrag von 100'000 Satoshi als Eingang. Die Transaktion erzeugt zwei neue Ausgänge. Der erste Ausgang weist Beat 60'000 Satoshi zu. Der zweite Ausgang weist Anna 39'000 Satoshi zurück. Die verbleibenden 1'000 Satoshi bilden die Transaktionsgebühr. Die Rechnung lautet: Vorhandener Betrag: 100'000 Satoshi Zahlung an Beat: 60'000 Satoshi Restbetrag für Anna: 39'000 Satoshi Transaktionsgebühr: 1'000 Satoshi Zusammen ergeben die neuen Ausgänge und die Gebühr wieder 100'000 Satoshi. Damit ist die Rechnung ausgeglichen. Der ursprüngliche verfügbare Betrag wurde vollständig verwendet. An seiner Stelle existieren nun die neuen verfügbaren Beträge.

Warum erhält Anna einen neuen Restbetrag?

Ein wichtiger Unterschied zum gewöhnlichen Bankkonto besteht darin, dass der ursprüngliche verfügbare Transaktionsausgang nicht einfach um den überwiesenen Teilbetrag verkleinert wird. Wenn Anna einen Betrag von 100'000 Satoshi verwendet, wird dieser Ausgang vollständig ausgegeben. Anschliessend entstehen neue Ausgänge. Einer gehört zu Beats Zahlung. Ein weiterer kann den verbleibenden Betrag wieder Anna zuordnen. Diesen Vorgang nennt man Wechselgeld. Im Englischen wird dafür der Begriff «Change» verwendet. Die Wallet organisiert solche Restbeträge normalerweise automatisch. Anna muss also nicht bei jeder Zahlung selbst berechnen, wie ein bestimmter Transaktionsausgang aufgeteilt werden soll. Die technische Funktionsweise bleibt jedoch wichtig. Denn dadurch wird verständlich, weshalb eine Bitcoin-Zahlung häufig mehr als einen Ausgang besitzt. Auch erklärt dies, warum sich der technisch verfügbare Bestand einer Wallet aus mehreren einzelnen Beträgen zusammensetzen kann.

Wie werden mehrere kleinere Beträge zusammengeführt?

Nun betrachten wir den umgekehrten Fall. Anna besitzt zwei verfügbare Bitcoin-Beträge. Der erste beträgt 70'000 Satoshi. Der zweite beträgt 40'000 Satoshi. Zusammen besitzt Anna damit 110'000 Satoshi. Sie möchte Beat 85'000 Satoshi senden. Ein einzelner ihrer beiden verfügbaren Beträge reicht dafür nicht aus. Deshalb kann ihre Wallet beide Beträge als Eingänge derselben Transaktion verwenden. Die Eingänge lauten: Eingang 1: 70'000 Satoshi Eingang 2: 40'000 Satoshi Gesamtbetrag: 110'000 Satoshi Nun werden daraus neue Ausgänge gebildet. Ausgang 1: 85'000 Satoshi an Beat Ausgang 2: 23'000 Satoshi zurück an Anna Gebühr: 2'000 Satoshi Die Rechnung lautet: $110'000 \text{ Satoshi} = 85'000 + 23'000 + 2'000 \text{ Satoshi}$ Damit werden zwei kleinere vorhandene Beträge in einer Transaktion zusammengeführt. Aus ihnen entsteht eine grössere Zahlung. Gleichzeitig erhält Anna einen neuen Restbetrag.

BEISPIEL:

Du besitzt zwei verfügbare Bitcoin-Beträge. Der erste beträgt 70'000 Satoshi. Der zweite beträgt 40'000 Satoshi. Du möchtest 85'000 Satoshi bezahlen. Deine Wallet kann beide Beträge gemeinsam verwenden. Dabei entsteht eine Transaktion mit zwei Eingängen. Nach der Zahlung werden dir gegebenenfalls ein neuer Restbetrag und dem Miner eine Transaktionsgebühr zugeordnet. Die Wallet erledigt diese Berechnungen normalerweise automatisch.

Warum funktioniert Bitcoin nicht wie ein gewöhnliches Kontoguthaben?

Bei einem Bankkonto sehen wir normalerweise einen einzigen Kontostand. Wenn du 1'000 Franken besitzt und 200 Franken überweist, zeigt dein Konto anschliessend vereinfacht 800 Franken an. Bei Bitcoin kann dir deine Wallet ebenfalls einen einzigen Gesamtbestand anzeigen. Technisch kann dieser Bestand jedoch aus zahlreichen einzelnen verfügbaren Transaktionsausgängen bestehen. Die Wallet berechnet daraus den für dich verfügbaren Gesamtbetrag. Wenn du eine Zahlung ausführst, wählt sie geeignete Beträge aus. Diese werden als Eingänge der neuen Transaktion verwendet. Anschliessend entstehen die neuen Ausgänge.

Das Netzwerk führt also nicht für jeden Nutzer ein gewöhnliches Bankkonto mit einem einzigen laufend veränderten Saldo.

Es prüft, welche Transaktionsausgänge verfügbar sind und ob sie nach den geltenden Regeln ausgegeben werden dürfen. Das ist ein grundlegender Bestandteil der Bitcoin-Technik.

Kann eine Transaktion mehrere Empfänger haben?

Ja. Satoshi Nakamoto beschreibt im Whitepaper insbesondere das einfache Beispiel einer Zahlung mit einem möglichen Restbetrag. Das bedeutet aber nicht, dass Bitcoin grundsätzlich auf zwei Ausgänge begrenzt ist. Eine Transaktion kann auch mehrere Ausgänge besitzen. Dadurch lassen sich in einer einzigen Transaktion Beträge an unterschiedliche Empfänger zuordnen. Stell dir vor, ein Unternehmen möchte mehrere Rechnungen bezahlen. Unter geeigneten Bedingungen kann es dafür eine Transaktion erstellen, die mehrere Empfängerbeträge enthält. Die technische Umsetzung hängt davon ab, welche Software verwendet wird und welche Transaktionsbedingungen erfüllt werden müssen. Für das Verständnis des Whitepapers ist vor allem wichtig: Bitcoin-Transaktionen können vorhandene Beträge zusammenführen und daraus mehrere neue Beträge erzeugen. Dadurch wird das System wesentlich flexibler als ein Modell, bei dem jede digitale Münze nur vollständig und einzeln übertragen werden könnte.

Warum besitzen Bitcoin-Transaktionen eine Vorgeschichte?

Jeder gewöhnliche Transaktionseingang verweist auf einen früheren verfügbaren Transaktionsausgang. Dieser frühere Ausgang stammt wiederum aus einer bereits bestehenden Transaktion. Auch diese Transaktion kann ihrerseits auf noch ältere Transaktionen zurückgehen. Dadurch entsteht eine miteinander verbundene Geschichte von Zahlungen. Stell dir einen Baum mit vielen Verzweigungen vor. Mehrere frühere Beträge können in einer neuen Transaktion zusammengeführt werden. Ein grösserer Betrag kann später wieder in mehrere neue Beträge aufgeteilt werden. Diese können anschliessend erneut für weitere Zahlungen verwendet werden. So entsteht ein Netzwerk aus miteinander verbundenen Transaktionen. Satoshi Nakamoto weist im Whitepaper darauf hin, dass solche Verzweigungen kein grundsätzliches Problem darstellen. Das System benötigt nicht für jede einzelne Zahlung eine vollständig abgeschlossene Kopie ihrer gesamten Vorgeschichte. Die Transaktionshistorie und die geltenden Prüfregele ermöglichen es, die benötigten Zusammenhänge zu überprüfen.

Warum beeinflusst diese Technik auch die Gebühren?

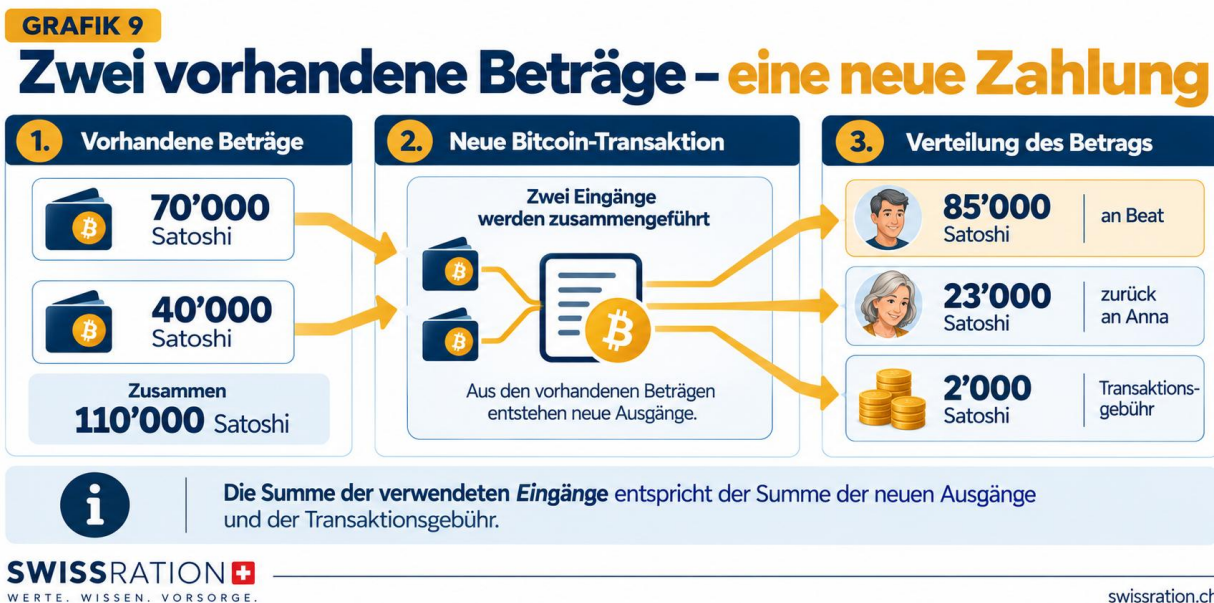
Das Zusammenführen und Aufteilen von Beträgen hat Auswirkungen auf die Grösse einer Bitcoin-Transaktion. Eine Transaktion mit mehreren Eingängen benötigt normalerweise mehr Daten als eine vergleichbare Transaktion mit nur einem Eingang. Auch zusätzliche Ausgänge können den benötigten Platz erhöhen. Bei Bitcoin hängen die Netzwerkgebühren unter anderem davon ab, wie viele Daten eine Transaktion beansprucht und wie stark der verfügbare Platz in neuen Blöcken nachgefragt wird. Deshalb kann eine Zahlung mit vielen Eingängen teurer sein als eine einfachere Zahlung. Das gilt selbst dann, wenn beide Zahlungen denselben Bitcoin-Betrag übertragen. Die Gebühr hängt also nicht ausschliesslich davon ab, wie viel Bitcoin bezahlt wird. Für Einsteiger ist diese Unterscheidung wichtig. Eine kleine Zahlung kann unter bestimmten Umständen eine verhältnismässig hohe Netzwerkgebühr verursachen. Umgekehrt kann eine grosse Zahlung technisch vergleichsweise wenig Platz beanspruchen. Wie eine Wallet ihre verfügbaren Beträge auswählt, kann deshalb auch die entstehenden Gebühren beeinflussen.

Warum ist diese Technik für den Datenschutz relevant?

Wenn eine Bitcoin-Transaktion mehrere Eingänge verwendet, werden diese Eingänge öffentlich innerhalb derselben Transaktion sichtbar. Dadurch können Beobachter Rückschlüsse auf Zusammenhänge zwischen den verwendeten Beträgen ziehen. Satoshi Nakamoto greift dieses Problem im nächsten Abschnitt seines Whitepapers ausdrücklich auf. Er weist darauf hin, dass gemeinsam verwendete Eingänge häufig auf einen gemeinsamen Eigentümer hindeuten. Allerdings ist diese Schlussfolgerung nicht in jedem Fall zwingend richtig. Heute gibt es auch Verfahren, bei denen mehrere Personen gemeinsam an einer Transaktion beteiligt sein können. Die Verbindung mehrerer Eingänge ist deshalb ein möglicher Hinweis auf einen Zusammenhang, aber nicht immer ein sicherer Beweis für dieselbe Person. Trotzdem zeigt sich bereits hier: Die Art, wie Bitcoin-Beträge zusammengeführt und aufgeteilt werden, hat nicht nur technische Folgen. Sie kann auch beeinflussen, welche Informationen über Zahlungen öffentlich nachvollziehbar sind.

MERKSATZ:

Bitcoin arbeitet mit verfügbaren Beträgen aus früheren Transaktionen. Diese können bei einer neuen Zahlung zusammengeführt oder aufgeteilt werden. Eine Transaktion kann mehrere Eingänge und mehrere Ausgänge besitzen. Nicht ausgegebene Restbeträge können als neue verfügbare Beträge an den Absender zurückgehen. Dadurch lassen sich mit Bitcoin unterschiedliche Zahlungsbeträge flexibel verarbeiten.



Eine Bitcoin-Transaktion kann mehrere vorhandene Beträge zusammenführen. Anschliessend können daraus eine Zahlung, ein Restbetrag für den Absender und eine Transaktionsgebühr entstehen. Die Rechnung muss nach den Netzwerkregeln vollständig aufgehen.

10. Wie funktioniert der Datenschutz bei Bitcoin?

Verständliche Erklärung des Originalabschnitts «Privacy»

Im zehnten Abschnitt seines Whitepapers beschäftigt sich Satoshi Nakamoto mit dem Schutz persönlicher Informationen. Dabei entsteht bei Bitcoin eine besondere Herausforderung. Einerseits müssen Transaktionen öffentlich überprüfbar sein. Andererseits möchten viele Menschen nicht, dass jeder ihre persönlichen Zahlungen mit ihrem Namen verbinden kann. Satoshi Nakamoto beschreibt deshalb, wie ein öffentliches Zahlungssystem aufgebaut sein kann, ohne die Identität sämtlicher beteiligter Personen direkt in der Transaktionshistorie zu veröffentlichen. Der englische Titel dieses Abschnitts lautet «Privacy». Auf Deutsch bedeutet das Privatsphäre oder Datenschutz. Es geht dabei vor allem um die Frage, welche Informationen über Zahlungen öffentlich sichtbar sind und welche Rückschlüsse daraus auf die beteiligten Personen gezogen werden können.

Wie funktioniert der Datenschutz bei einer Bank?

Bei einem gewöhnlichen Bankkonto kennt die Bank normalerweise die Identität ihrer Kunden. Sie führt die Konten und verarbeitet die entsprechenden Zahlungen. Wenn du Geld an eine andere Person überweist, werden die Zahlungsinformationen nicht automatisch in einem weltweit öffentlich zugänglichen Register veröffentlicht. Die Informationen stehen vor allem den beteiligten Finanzinstituten und den jeweils berechtigten Stellen zur Verfügung. Dadurch entsteht ein bestimmter Schutz gegenüber der allgemeinen Öffentlichkeit. Allerdings müssen die Kunden darauf vertrauen, dass die beteiligten Institutionen mit ihren Daten korrekt umgehen. Ausserdem können gesetzliche Pflichten bestehen, bestimmte Informationen an Behörden weiterzugeben. Satoshi Nakamoto beschreibt dieses Modell als eine Form von Datenschutz, bei der der Zugang zu den Zahlungsinformationen auf bestimmte Beteiligte begrenzt wird. Bitcoin funktioniert anders. Denn bei Bitcoin muss die gemeinsame Transaktionshistorie öffentlich überprüfbar sein.

Warum sind Bitcoin-Transaktionen öffentlich?

Das Bitcoin-Netzwerk benötigt eine gemeinsame Grundlage, um die Gültigkeit von Zahlungen zu überprüfen. Deshalb werden die technischen Informationen der Transaktionen öffentlich verfügbar gemacht. Andere Teilnehmer können dadurch nachvollziehen, welche verfügbaren Beträge bereits ausgegeben wurden. Sie können ausserdem überprüfen, ob die geltenden Regeln eingehalten werden. Diese Offenheit ist ein wichtiger Bestandteil des Systems. Sie verhindert, dass eine einzelne Organisation die verbindliche Transaktionshistorie geheim verwaltet. Gleichzeitig bedeutet dies aber, dass Zahlungen nicht einfach unsichtbar sind.

Auf der Bitcoin-Blockchain lassen sich unter anderem die übertragenen Beträge und ihre technischen Verbindungen nachvollziehen. Die Blockchain enthält jedoch normalerweise keine direkt zu den einzelnen Transaktionen gehörenden Felder mit den vollständigen Namen und Wohnadressen der beteiligten Personen. Genau an diesem Unterschied setzt Satoshi Nakamotos ursprüngliches Datenschutzkonzept an.

Was bedeutet es, wenn Bitcoin-Adressen keine Namen enthalten?

Bei Bitcoin werden Zahlungen an technische Ausgabebedingungen gebunden. Im Alltag begegnen dir diese Bedingungen häufig in Form von Bitcoin-Empfangsadressen. Eine solche Adresse besteht aus einer Zeichenfolge. Sie ist nicht mit einem persönlichen Namen vergleichbar. Wenn du eine Bitcoin-Zahlung erhältst, muss dein Name deshalb nicht direkt in der Blockchain stehen. Ein Beobachter kann möglicherweise erkennen, dass ein bestimmter Betrag an eine bestimmte Adresse übertragen wurde. Er weiss dadurch aber nicht automatisch, welche Person hinter dieser Adresse steht. Satoshi Nakamoto beschreibt dieses Grundprinzip im Whitepaper anhand öffentlicher Schlüssel. Die eigentliche Idee besteht darin, dass die öffentlich sichtbaren Zahlungsdaten nicht unmittelbar mit einer persönlichen Identität verbunden sein müssen. Allerdings ist dabei Vorsicht notwendig. Dass eine Adresse keinen Namen enthält, bedeutet nicht, dass die zugehörige Person dauerhaft unbekannt bleiben muss.

Ist Bitcoin anonym?

Bitcoin wird häufig als anonymes Zahlungssystem bezeichnet. Diese Beschreibung ist jedoch ungenau. Bei einem vollständig anonymen System dürfte sich aus den verfügbaren Informationen grundsätzlich nicht erkennen lassen, welche Person an einer bestimmten Zahlung beteiligt war. Bitcoin bietet einen solchen umfassenden Schutz nicht automatisch. Die Transaktionshistorie ist öffentlich nachvollziehbar. Wenn eine Bitcoin-Adresse einer bestimmten Person zugeordnet werden kann, lassen sich möglicherweise auch weitere Zahlungen mit dieser Person in Verbindung bringen. Deshalb wird Bitcoin häufig als pseudonym bezeichnet. Ein Pseudonym ist eine Bezeichnung, die nicht unmittelbar den richtigen Namen einer Person offenlegt. Bei Bitcoin können Adressen oder andere öffentlich sichtbare Kennzeichnungen eine ähnliche Rolle spielen. Solange keine Verbindung zu einer tatsächlichen Person bekannt ist, bleibt ihre Identität möglicherweise verborgen. Sobald eine solche Verbindung hergestellt wird, können zusätzliche Informationen sichtbar werden.

Ein Beispiel für die Zuordnung einer Bitcoin-Adresse

Stell dir vor, Anna betreibt ein kleines Geschäft. Auf ihrer öffentlichen Webseite veröffentlicht sie eine Bitcoin-Empfangsadresse. Daneben steht ihr vollständiger Name. Ein Kunde verwendet diese Adresse, um eine Zahlung an Anna zu senden. Die Zahlung erscheint in der öffentlich nachvollziehbaren Bitcoin-Transaktionshistorie. Nun kann ein Beobachter die Adresse mit Annas Geschäft verbinden. Damit ist zumindest diese Adresse nicht mehr unabhängig von ihrer Identität. Wenn Anna dieselbe Adresse später erneut verwendet, können weitere Zahlungen an diese Adresse ebenfalls mit ihrem Geschäft in Verbindung gebracht werden. Das bedeutet nicht automatisch, dass der Beobachter sämtliche Bitcoin-Bestände von Anna kennt. Es zeigt aber, wie durch die Verbindung einer öffentlichen Adresse mit einem Namen zusätzliche Informationen sichtbar werden können.

BEISPIEL:

Anna veröffentlicht eine Bitcoin-Adresse auf ihrer Geschäftswebseite. Jeder Besucher kann erkennen, dass diese Adresse zu Annas Geschäft gehört. Wenn Zahlungen an diese Adresse erfolgen, lassen sie sich auf der Blockchain nachvollziehen. Die Adresse enthält zwar keinen ausgeschriebenen Namen. Durch die Veröffentlichung auf der Webseite ist ihre Verbindung zu Anna jedoch bekannt. Das Beispiel zeigt: Bitcoin-Adressen sind nicht automatisch dauerhaft anonym.

Warum empfiehlt Satoshi Nakamoto neue Schlüssel für neue Zahlungen?

Im Whitepaper schlägt Satoshi Nakamoto vor, für neue Transaktionen möglichst neue Schlüsselpaare zu verwenden. Ein Schlüsselpaar besteht aus einem privaten und einem zugehörigen öffentlichen Schlüssel. Der Gedanke dahinter ist einfach. Wenn unterschiedliche Zahlungen immer dieselben öffentlichen Kennzeichnungen verwenden, lassen sie sich leichter miteinander verbinden. Wer dagegen neue Schlüssel beziehungsweise geeignete neue Empfangsadressen verwendet, erschwert bestimmte direkte Verknüpfungen. Stell dir vor, du verwendest für jede erhaltene Zahlung dieselbe Bitcoin-Adresse. Ein Beobachter kann dann erkennen, welche Zahlungen an diese Adresse gerichtet wurden. Verwendest du dagegen unterschiedliche Empfangsadressen, sind diese Zahlungen nicht allein aufgrund einer identischen Adresse miteinander verbunden. Das bietet einen gewissen zusätzlichen Datenschutz. Allerdings bedeutet auch diese Vorgehensweise nicht, dass die Zahlungen vollständig anonym sind. Es können andere Informationen vorhanden sein, durch die sich unterschiedliche Adressen derselben Person zuordnen lassen.

Warum können mehrere Eingänge den Datenschutz schwächen?

Im vorherigen Kapitel haben wir gesehen, dass Bitcoin-Transaktionen mehrere Eingänge besitzen können. Damit lassen sich unterschiedliche vorhandene Beträge für eine grössere Zahlung zusammenführen. Satoshi Nakamoto weist im Datenschutzabschnitt darauf hin, dass dadurch eine neue Verbindung entstehen kann. Wenn eine Transaktion mehrere Eingänge verwendet, sind diese Eingänge öffentlich innerhalb derselben Transaktion sichtbar. Ein Beobachter könnte daraus schliessen, dass die zugehörigen Beträge von derselben Person kontrolliert wurden. Stell dir vor, Anna verwendet drei verschiedene Bitcoin-Adressen. Sie erhält auf jede Adresse einen separaten Betrag. Solange diese Beträge getrennt bleiben, ist ihre gemeinsame Zugehörigkeit möglicherweise nicht offensichtlich. Nun möchte Anna eine grössere Zahlung ausführen. Dafür verwendet ihre Wallet Beträge aus allen drei Adressen als Eingänge derselben Transaktion. Ein Beobachter kann nun erkennen, dass diese Beträge gemeinsam verwendet wurden. Damit entsteht ein Hinweis auf einen Zusammenhang zwischen den Adressen. Im Whitepaper beschreibt Satoshi Nakamoto diese Verbindung als eine wichtige Grenze seines Datenschutzmodells. Aus heutiger Sicht ist allerdings eine Präzisierung notwendig. Nicht jede Transaktion mit mehreren Eingängen wird zwingend von einer einzigen Person erstellt. Es existieren auch Verfahren, bei denen mehrere Personen gemeinsam eine Transaktion aufbauen. Deshalb ist die gemeinsame Verwendung von Eingängen ein möglicher Hinweis auf einen gemeinsamen Eigentümer, aber nicht immer ein endgültiger Beweis.

Was geschieht, wenn eine Adresse nachträglich einer Person zugeordnet wird?

Ein besonderer Aspekt der Bitcoin-Blockchain besteht darin, dass historische Transaktionen weiterhin nachvollziehbar bleiben. Stell dir vor, eine Person verwendet über längere Zeit verschiedene Bitcoin-Adressen. Zu Beginn weiss niemand, wer hinter diesen Adressen steht. Später wird eine der Adressen öffentlich mit ihrem Namen verbunden. Nun können Beobachter die zugehörigen Transaktionen untersuchen. Wenn sich weitere technische Verbindungen zu anderen Adressen erkennen lassen, können möglicherweise zusätzliche Rückschlüsse entstehen. Das bedeutet: Die spätere Bekanntgabe einer Identität kann auch frühere Zahlungen betreffen.

Deshalb ist der Schutz persönlicher Informationen bei Bitcoin nicht nur im Augenblick einer Zahlung relevant. Er kann auch langfristige Folgen haben.

Welche Rolle spielen Bitcoin-Handelsplattformen?

Das ursprüngliche Whitepaper beschäftigt sich vor allem mit dem technischen Aufbau des Netzwerks. Seit seiner Veröffentlichung haben sich zahlreiche Unternehmen entwickelt, die den Kauf, Verkauf und die Verwahrung von Bitcoin ermöglichen. Bei solchen Handelsplattformen müssen Kunden je nach Anbieter und geltenden Vorschriften ihre Identität nachweisen. Dazu können beispielsweise persönliche Angaben und amtliche Ausweisdokumente verlangt werden. Wenn Bitcoin von einer solchen Plattform an eine eigene Wallet übertragen werden, können Informationen über die Auszahlung beim Anbieter vorhanden sein. Dadurch kann unter bestimmten Umständen eine Verbindung zwischen einer persönlichen Identität und einer Bitcoin-Adresse entstehen. Die Blockchain selbst benötigt für gewöhnliche Transaktionen keine direkte Angabe des vollständigen Namens. Das bedeutet aber nicht, dass ausserhalb der Blockchain keine entsprechenden Informationen existieren. Dieser Unterschied ist für die heutige Nutzung besonders wichtig. Das Datenschutzmodell des ursprünglichen Whitepapers darf deshalb nicht mit vollständiger Anonymität im heutigen Bitcoin-Ökosystem verwechselt werden.

Können Bitcoin-Zahlungen technisch nachverfolgt werden?

Ja. Weil die Bitcoin-Blockchain öffentlich ist, können Transaktionen und ihre Verbindungen untersucht werden. Dafür gibt es spezielle Software. Solche Programme können beispielsweise nachvollziehen, wie verfügbare Beträge aus früheren Transaktionen in neue Transaktionen eingeflossen sind. Sie können ausserdem bekannte Adressen oder bestimmte Transaktionsmuster auswerten. Wenn zusätzliche Informationen vorhanden sind, lassen sich daraus möglicherweise Hinweise auf bestimmte Personen oder Unternehmen gewinnen. Allerdings sind solche Auswertungen nicht immer eindeutig. Eine technische Verbindung zwischen zwei Transaktionen bedeutet nicht zwangsläufig, dass dieselbe Person beide Zahlungen kontrolliert hat. Auch die Zuordnung einer Adresse zu einer bestimmten Person kann fehlerhaft sein. Deshalb müssen solche Analysen sorgfältig interpretiert werden. Für unseren Leitfaden ist vor allem wichtig: Bitcoin-Zahlungen sind öffentlich nachvollziehbar, aber die persönliche Identität der Beteiligten wird nicht automatisch bei jeder Transaktion in der Blockchain veröffentlicht.

Warum vergleicht Satoshi das System mit einer Börse?

Im Whitepaper verwendet Satoshi Nakamoto einen Vergleich mit öffentlich sichtbaren Börsengeschäften.

Bei einer Börse können bestimmte Informationen über gehandelte Mengen und Preise veröffentlicht werden. Die Öffentlichkeit kann dadurch Handelsvorgänge nachvollziehen. Das bedeutet jedoch nicht, dass bei jeder veröffentlichten Handelsinformation automatisch die Namen sämtlicher beteiligter Käufer und Verkäufer erscheinen. Satoshi Nakamoto verwendet diesen Vergleich, um sein Datenschutzkonzept zu erklären. Die Zahlungsinformationen sollen öffentlich überprüfbar sein. Die persönlichen Identitäten der Beteiligten sollen dagegen nicht zwingend direkt mit diesen Informationen veröffentlicht werden. Der Vergleich zeigt allerdings auch die Grenze dieses Ansatzes.

Wenn zusätzliche Informationen über die Beteiligten bekannt werden, können Verbindungen zwischen den öffentlichen Transaktionen und den tatsächlichen Personen entstehen.

Welche Datenschutzrisiken beschreibt das Whitepaper nicht vollständig?

Das ursprüngliche Whitepaper erschien im Jahr 2008. Seitdem haben sich die technischen Möglichkeiten zur Untersuchung öffentlicher Transaktionsdaten erheblich weiterentwickelt. Heute müssen deshalb zusätzliche Aspekte berücksichtigt werden. Beispielsweise können Informationen von Handelsplattformen mit öffentlich sichtbaren Transaktionen verbunden werden. Auch die wiederholte Verwendung derselben Empfangsadresse kann Rückschlüsse ermöglichen. Weitere Hinweise können aus öffentlich veröffentlichten Zahlungsinformationen oder technischen Verbindungen zwischen verschiedenen Transaktionen entstehen. Ausserdem können bei der Übermittlung von Transaktionen über das Internet zusätzliche technische Informationen anfallen. Das Whitepaper beschreibt die grundlegende Trennung zwischen öffentlichen Transaktionsdaten und persönlichen Identitäten. Es liefert jedoch keine Garantie für vollständige Anonymität. Auch die Verwendung neuer Empfangsadressen beseitigt nicht automatisch sämtliche Risiken einer späteren Zuordnung.

Wie lässt sich das Datenschutzkonzept zusammenfassen?

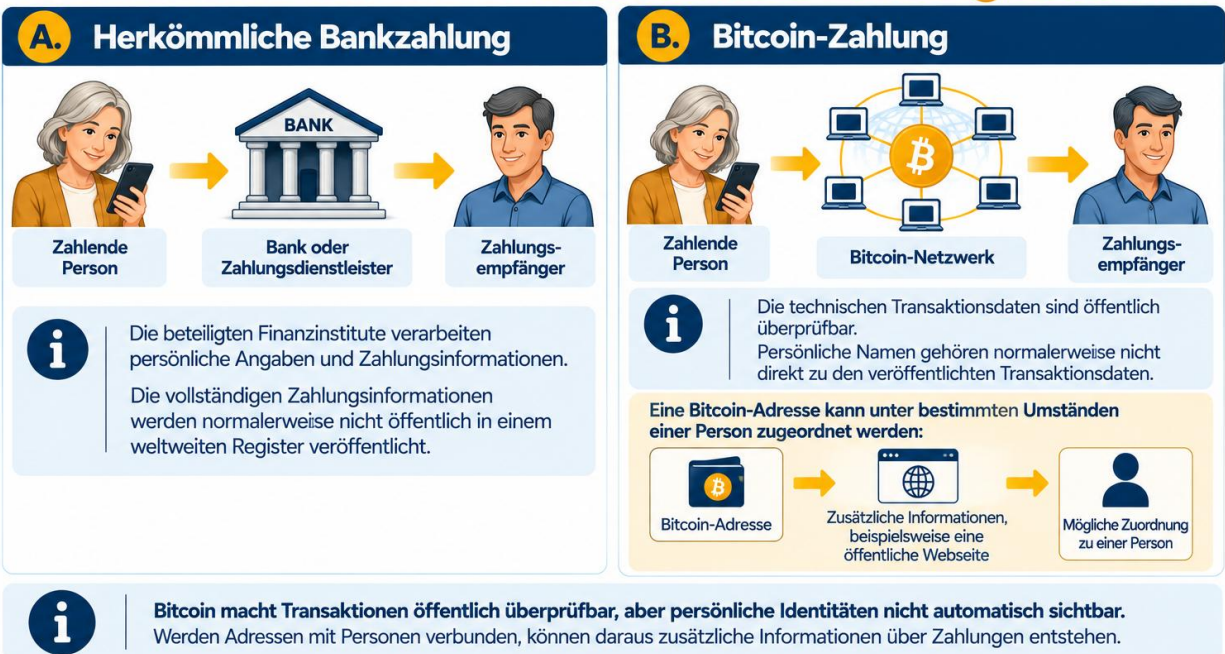
Satoshi Nakamoto musste bei Bitcoin zwei unterschiedliche Anforderungen miteinander verbinden. Einerseits sollte das Netzwerk ohne zentrale Buchungsstelle funktionieren. Dafür müssen die technischen Transaktionen öffentlich überprüfbar sein. Andererseits sollten die persönlichen Identitäten der Nutzer nicht automatisch Bestandteil dieser öffentlichen Transaktionshistorie sein. Sein Lösungsansatz bestand darin, die Transaktionsdaten öffentlich zu machen, aber die Verbindung zu persönlichen Identitäten nicht zwingend in das System einzubauen. Zusätzlich sollten möglichst neue Schlüssel beziehungsweise Empfangsadressen verwendet werden, um bestimmte Verknüpfungen zu erschweren. Diese Konstruktion bietet einen gewissen Schutz der Privatsphäre. Sie verhindert jedoch nicht, dass öffentliche Transaktionsdaten später mit realen Personen in Verbindung gebracht werden können. Genau deshalb ist Bitcoin nicht mit einem vollständig anonymen Zahlungssystem gleichzusetzen.

MERKSATZ:

Die Bitcoin-Blockchain ist öffentlich nachvollziehbar. Die persönlichen Namen der Beteiligten stehen jedoch normalerweise nicht direkt in den Transaktionsdaten. Dadurch können Zahlungen zunächst ohne unmittelbare Namenszuordnung sichtbar sein. Wenn eine Adresse später einer Person zugeordnet wird, können möglicherweise auch weitere Transaktionen mit ihr in Verbindung gebracht werden. Bitcoin bietet deshalb keine automatische vollständige Anonymität.

GRAFIK 10

Welche Informationen sind bei einer Zahlung sichtbar?



Bei einer Bankzahlung verarbeiten die beteiligten Finanzinstitute persönliche Angaben und Zahlungsinformationen. Bei Bitcoin sind die technischen Transaktionsdaten öffentlich nachvollziehbar, ohne dass die persönlichen Namen automatisch in der Blockchain stehen. Durch zusätzliche Informationen können jedoch Verbindungen zwischen Adressen und Personen entstehen.

11. Wie sicher ist Bitcoin gegen einen Angreifer?

Verständliche Erklärung des Originalabschnitts «Calculations»

Im elften Abschnitt seines Whitepapers beschäftigt sich Satoshi Nakamoto mit einer besonders wichtigen Frage: Wie wahrscheinlich ist es, dass ein Angreifer eine bereits bestätigte Bitcoin-Zahlung nachträglich verändert? In den bisherigen Kapiteln haben wir gesehen, dass Bitcoin seine Transaktionshistorie durch miteinander verbundene Blöcke und einen Arbeitsnachweis absichert. Wir haben auch erfahren, dass Miner Rechenleistung einsetzen müssen, um neue gültige Blöcke zu finden. Nun möchte Satoshi Nakamoto zeigen, weshalb dieses Verfahren eine bereits bestätigte Zahlung mit zunehmender Zahl weiterer Blöcke immer besser gegen bestimmte Manipulationsversuche schützen kann. Dafür verwendet er mathematische Wahrscheinlichkeitsrechnungen. Diese Berechnungen bilden einen wichtigen Bestandteil des ursprünglichen Whitepapers.

Du musst die einzelnen mathematischen Formeln nicht selbst berechnen können. Entscheidend ist, dass du verstehst, welche Situation Satoshi untersucht, welche Annahmen er trifft und welche Schlussfolgerungen sich daraus ergeben.

Dabei ist eine Unterscheidung besonders wichtig:

Bitcoin bietet keine mathematische Garantie, dass eine bestätigte Zahlung unter allen Umständen endgültig bleibt. Stattdessen lässt sich unter bestimmten Voraussetzungen berechnen, wie unwahrscheinlich eine erfolgreiche nachträgliche Veränderung wird.

Welchen Angriff untersucht Satoshi Nakamoto?

Satoshi Nakamoto betrachtet einen Angreifer, der versucht, eine alternative Version der Bitcoin-Blockchain aufzubauen. Diese alternative Blockchain soll eine frühere eigene Zahlung des Angreifers rückgängig machen. Stell dir folgende Situation vor. Anna möchte bei Beat einen wertvollen Gegenstand kaufen. Sie vereinbaren, dass Anna den Kaufpreis mit Bitcoin bezahlt. Anna erstellt eine gültige Bitcoin-Zahlung an Beat. Beat sieht, dass die Zahlung in einem Block bestätigt wurde. Anschliessend übergibt er Anna den gekauften Gegenstand. Anna hat jedoch einen betrügerischen Plan. Sie möchte den Gegenstand behalten und gleichzeitig erreichen, dass ihre ursprüngliche Bitcoin-Zahlung an Beat aus der später akzeptierten Transaktionshistorie verschwindet. Dafür versucht sie, eine konkurrierende Blockchain aufzubauen. In dieser alternativen Geschichte soll derselbe ursprüngliche Bitcoin-Betrag nicht an Beat, sondern wieder an eine von Anna kontrollierte Empfangsadresse gehen. Wenn Anna ihre alternative Blockchain erfolgreich durchsetzen könnte, würde Beats ursprüngliche Zahlung aus der nun bevorzugten Transaktionshistorie verdrängt. Beat hätte dann möglicherweise den Gegenstand bereits übergeben, ohne die vereinbarte Bitcoin-Zahlung dauerhaft erhalten zu haben. Genau diese Art von Angriff untersucht Satoshi Nakamoto. Sie wird als Doppelausgabeangriff bezeichnet. Im Englischen spricht man von einem Double-Spending-Angriff.

Was kann ein solcher Angreifer nicht?

Bevor wir die Berechnung betrachten, müssen wir eine wichtige Grenze verstehen. Ein Angreifer mit grosser Rechenleistung kann nicht einfach beliebige Bitcoin erzeugen oder fremde Bitcoin ohne die notwendigen Freigaben ausgeben. Die unabhängig prüfenden Computer des Netzwerks kontrollieren weiterhin die geltenden Regeln. Ein Block, der gegen diese Regeln verstösst, wird zurückgewiesen. Das gilt beispielsweise für eine Transaktion, mit der jemand ohne die erforderlichen privaten Schlüssel fremde Bitcoin ausgeben möchte. Auch die geltenden Regeln zur Ausgabe neuer Bitcoin können nicht einfach durch zusätzliche Rechenleistung ausser Kraft gesetzt werden. Satoshi Nakamoto stellt deshalb ausdrücklich klar, dass die Möglichkeit einer konkurrierenden Blockchain keine allgemeine Erlaubnis bedeutet, beliebige Buchungen vorzunehmen. Der untersuchte Angreifer versucht vielmehr, eine eigene frühere Zahlung durch eine alternative Transaktion zu ersetzen.

Es geht also darum, einen bereits verwendeten eigenen Betrag in einer konkurrierenden Geschichte anders auszugeben. Die Manipulation der Transaktionsreihenfolge ist etwas anderes als das Fälschen fremder digitaler Signaturen.

MERKSATZ:

Ein Angreifer mit grosser Rechenleistung kann versuchen, eine eigene frühere Bitcoin-Zahlung durch eine konkurrierende Transaktionshistorie rückgängig zu machen. Er kann dadurch aber nicht einfach fremde private Schlüssel ersetzen, beliebige Bitcoin erschaffen oder unabhängig prüfenden Teilnehmern ungültige Blöcke aufzwingen.

Warum entsteht ein Wettlauf zwischen zwei Blockketten?

Stell dir vor, Annas Zahlung an Beat wurde in einen gültigen Block aufgenommen. Die ehrlichen Miner arbeiten nun daran, den nächsten Block zu finden. Anna versucht gleichzeitig, im Verborgenen eine andere Fortsetzung der Blockchain zu erzeugen. In ihrer alternativen Geschichte ist die Zahlung an Beat nicht enthalten. Stattdessen soll der betreffende Betrag wieder an Anna selbst gehen. Nun beginnt ein Wettlauf. Auf der einen Seite steht die vom übrigen Netzwerk fortgesetzte Blockchain. Auf der anderen Seite steht Annas konkurrierende Blockchain. Immer wenn die ehrlichen Miner einen neuen Block finden, wächst der Vorsprung ihrer Kette. Immer wenn Anna einen gültigen Block für ihre alternative Kette findet, kann sie ihren Rückstand verkleinern. Dabei entscheidet nicht einfach die Anzahl der beteiligten Computer. Massgeblich ist die insgesamt geleistete Rechenarbeit. Deshalb hängt Annas Erfolgschance wesentlich davon ab, wie viel Rechenleistung sie im Vergleich zu den ehrlichen Minern kontrolliert.

Ein Wettlauf mit unterschiedlicher Geschwindigkeit

Um die Situation zu verstehen, hilft ein Vergleich mit zwei Personen bei einem Wettlauf. Person A läuft normalerweise schneller als Person B. Ausserdem besitzt Person A bereits einen Vorsprung. Person B möchte diesen Vorsprung aufholen. Solange Person A im Durchschnitt schneller vorankommt, ist Person B im Nachteil. Das bedeutet allerdings nicht, dass Person B niemals aufholen könnte. Vielleicht macht Person A vorübergehend weniger Fortschritte, während Person B mehrere besonders erfolgreiche Schritte hintereinander schafft.

Je grösser der Vorsprung von Person A wird, desto unwahrscheinlicher wird jedoch, dass Person B diesen noch aufholen kann. Bei Bitcoin ist die Situation ähnlich. Die ehrlichen Miner finden mit ihrer gemeinsamen Rechenleistung neue Blöcke. Der Angreifer versucht gleichzeitig, eine konkurrierende Kette aufzubauen. Wenn die ehrlichen Miner im Durchschnitt mehr Rechenleistung besitzen, wächst ihr Vorsprung langfristig schneller. Einzelne Blöcke werden allerdings zufallsabhängig gefunden. Deshalb kann auch ein unterlegener Angreifer zeitweise schneller vorankommen. Satoshi Nakamoto verwendet Wahrscheinlichkeitsrechnungen, um dieses Risiko zu untersuchen.

Was bedeutet der Anteil der Rechenleistung?

Für seine Berechnung verwendet Satoshi Nakamoto zwei wichtige Grössen. Die erste bezeichnet er mit dem Buchstaben p . Sie steht für die Wahrscheinlichkeit, dass die ehrlichen Miner den nächsten Block finden. Die zweite bezeichnet er mit dem Buchstaben q .

Sie steht für die Wahrscheinlichkeit, dass der Angreifer den nächsten Block findet. Diese Wahrscheinlichkeiten hängen im vereinfachten Modell vom jeweiligen Anteil an der gesamten Rechenleistung ab. Stell dir vor, die ehrlichen Miner kontrollieren zusammen 90 Prozent der Rechenleistung. Der Angreifer kontrolliert die übrigen 10 Prozent.

Dann lautet die vereinfachte Annahme: $p = 90$ Prozent $q = 10$ Prozent Das bedeutet nicht, dass die ehrlichen Miner bei genau neun von zehn aufeinanderfolgenden Blöcken gewinnen müssen. Es handelt sich um durchschnittliche Wahrscheinlichkeiten. Der Angreifer könnte gelegentlich mehrere Blöcke hintereinander finden. Die ehrlichen Miner könnten ebenfalls mehrere Blöcke hintereinander finden. Über längere Zeiträume besitzt die Seite mit der grösseren Rechenleistung jedoch den statistischen Vorteil.

Warum ist die Mehrheit der Rechenleistung wichtig?

Satoshi Nakamoto unterscheidet zwei grundlegende Situationen. In der ersten Situation kontrollieren die ehrlichen Miner gemeinsam mehr Rechenleistung als der Angreifer. Dann besitzt die ehrliche Blockchain den statistischen Vorteil. Wenn der Angreifer bereits mehrere Blöcke zurückliegt, wird es mit zunehmendem Rückstand immer unwahrscheinlicher, dass er diesen jemals aufholen kann. In der zweiten Situation besitzt der Angreifer mindestens ebenso viel Rechenleistung wie die ehrlichen Miner. Dann gelten diese günstigen Sicherheitsannahmen nicht mehr. Ein Angreifer mit mindestens der Hälfte der Rechenleistung kann unter den vereinfachten Bedingungen des Modells langfristig mit einem Aufholen rechnen. Das bedeutet jedoch nicht, dass er augenblicklich jede beliebige Transaktion verändern kann. Ebenso wenig kann er dadurch die übrigen Bitcoin-Regeln ausser Kraft setzen. Die zentrale Erkenntnis lautet: Die Widerstandsfähigkeit gegen den untersuchten Angriff beruht wesentlich darauf, dass die ehrlich arbeitenden Miner gemeinsam über mehr Rechenleistung verfügen als der Angreifer.

Wie berechnet Satoshi die Wahrscheinlichkeit des Aufholens?

Satoshi Nakamoto betrachtet zunächst einen Angreifer, der bereits eine bestimmte Anzahl von Blöcken zurückliegt. Er möchte wissen, wie wahrscheinlich es ist, dass der Angreifer diesen Rückstand irgendwann vollständig aufholt. Dafür verwendet er ein mathematisches Modell, das mit einem Glücksspiel verglichen werden kann. Stell dir einen Spieler vor, der mehrere Punkte im Rückstand liegt. Bei jeder Runde kann er entweder einen Punkt aufholen oder einen weiteren Punkt zurückfallen. Wenn seine Gewinnchance bei jeder Runde kleiner ist als die seines Gegners, wird es mit wachsendem Rückstand immer unwahrscheinlicher, dass er den Gleichstand erreicht. Ein vergleichbares mathematisches Problem wird als Ruinproblem eines Spielers bezeichnet. Im Englischen spricht man vom Gambler's Ruin Problem. Satoshi verwendet dieses Modell, um die Wahrscheinlichkeit zu berechnen, mit der eine unterlegene Angreiferkette ihren Rückstand irgendwann aufholen könnte.

Die erste Formel des Whitepapers einfach erklärt

Für diese erste Berechnung verwendet Satoshi drei Grössen. p bezeichnet die Wahrscheinlichkeit, dass die ehrlichen Miner den nächsten Block finden. q bezeichnet die Wahrscheinlichkeit, dass der Angreifer den nächsten Block findet. z bezeichnet die Anzahl Blöcke, um die der Angreifer bereits zurückliegt. Solange die ehrlichen Miner den grösseren Anteil der Rechenleistung besitzen, ergibt sich eine einfache mathematische Beziehung. Die Wahrscheinlichkeit des späteren Aufholens entspricht dem Verhältnis zwischen der Rechenleistung des Angreifers und jener der ehrlichen Miner, mehrfach mit sich selbst multipliziert. Wie oft dieses Verhältnis multipliziert wird, hängt von der Anzahl der aufzuholenden Blöcke ab. Das klingt abstrakt. Ein Beispiel macht es verständlich.

DIE ERSTE FORMEL:

Satoshi verwendet folgende vereinfachte Berechnung: Wahrscheinlichkeit des Aufholens = $(q / p)^z$
hoch z Dabei gilt: p = Wahrscheinlichkeit, dass die ehrlichen Miner den nächsten Block finden q = Wahrscheinlichkeit, dass der Angreifer den nächsten Block findet z = Anzahl Blöcke, die der Angreifer zurückliegt Diese Formel gilt für den Fall, dass p grösser als q ist. Wenn der Angreifer mindestens ebenso viel Rechenleistung besitzt wie die ehrlichen Miner, beträgt die langfristige Aufholwahrscheinlichkeit in diesem vereinfachten Modell 100 Prozent. Die Formel beschreibt zunächst einen bereits bestehenden Rückstand. Für die Berechnung des Risikos während einer noch laufenden Zahlung berücksichtigt Satoshi anschliessend weitere Faktoren.

Warum genügt diese erste Formel noch nicht?

Stell dir vor, Beat wartet nach Annas Zahlung mehrere neue Blöcke ab. Während dieser Wartezeit arbeiten die ehrlichen Miner an der gewöhnlichen Blockchain. Anna könnte aber gleichzeitig an ihrer geheimen, konkurrierenden Blockchain arbeiten. Wenn Beat schliesslich entscheidet, dass genügend Blöcke entstanden sind, weiss er nicht, wie viele Blöcke Anna im Verborgenen bereits gefunden hat. Vielleicht ist sie weit zurückgeblieben. Vielleicht hat sie aber während derselben Zeit mehrere eigene Blöcke gefunden. Deshalb genügt es nicht, nur den sichtbaren Vorsprung der ehrlichen Blockchain zu betrachten. Satoshi Nakamoto berücksichtigt in einer zweiten Berechnung zusätzlich den möglichen Fortschritt des Angreifers während der Wartezeit. Damit wird die Untersuchung realistischer als eine Berechnung, die davon ausgeht, dass der Angreifer während des Wartens überhaupt keine Fortschritte macht.

Welche Rolle spielt die zufällige Entstehung neuer Blöcke?

Bitcoin-Blöcke entstehen nicht in einem festen zeitlichen Takt. Ein neuer Block kann schon nach kurzer Zeit gefunden werden. Manchmal dauert es deutlich länger. Die Entstehung neuer Blöcke hängt von vielen einzelnen Berechnungsversuchen ab. Deshalb verwendet Satoshi Nakamoto ein mathematisches Modell für zufällig eintretende Ereignisse. Dieses Modell wird Poisson-Verteilung genannt. Du musst dir den Namen nicht merken. Wichtig ist die Grundidee. Die Poisson-Verteilung ermöglicht es, abzuschätzen, wie häufig ein bestimmtes Ereignis innerhalb eines betrachteten Zeitraums eintreten könnte. Bei Bitcoin geht es darum, wie viele Blöcke ein Angreifer möglicherweise findet, während die ehrlichen Miner weitere Blöcke erzeugen. Satoshi kombiniert diese Abschätzung mit der Frage, wie wahrscheinlich der Angreifer einen anschliessend noch bestehenden Rückstand aufholen kann.

Wie funktioniert diese zweite Berechnung?

Satoshi Nakamoto geht von folgendem Beispiel aus. Eine Zahlung wurde in einen Block aufgenommen. Der Empfänger wartet nun ab, bis auf diesem Block weitere Blöcke aufgebaut wurden. Während dieser Zeit arbeitet ein möglicher Angreifer an einer geheimen alternativen Blockchain. Der Empfänger kennt den tatsächlichen Fortschritt des Angreifers nicht. Satoshi berechnet deshalb mehrere mögliche Situationen. Vielleicht hat der Angreifer während der Wartezeit keinen einzigen Block gefunden. Vielleicht hat er einen oder zwei Blöcke gefunden. Vielleicht hatte er ungewöhnlich viel Glück und konnte bereits mehrere Blöcke erzeugen. Für jede dieser Möglichkeiten wird berücksichtigt, wie wahrscheinlich sie ist.

Anschliessend wird berechnet, wie gross die verbleibende Chance des Angreifers wäre, die ehrliche Blockchain noch einzuholen. Aus der Kombination dieser Möglichkeiten ergibt sich eine geschätzte gesamte Erfolgswahrscheinlichkeit. Satoshi gibt dafür im Whitepaper eine mathematische Formel und zusätzlich ein kleines Computerprogramm an. Das Programm berechnet die Wahrscheinlichkeiten für unterschiedliche Anteile der Rechenleistung und unterschiedliche Wartezeiten.

Was bedeutet das zusätzliche mathematische Zeichen Lambda?

In seiner zweiten Berechnung verwendet Satoshi Nakamoto den griechischen Buchstaben Lambda. Er wird mit dem Zeichen λ dargestellt. Lambda beschreibt in diesem Zusammenhang, wie viele Blöcke der Angreifer während der betrachteten Wartezeit durchschnittlich finden könnte. Dafür verwendet Satoshi die bereits bekannten Grössen p , q und z . Die Rechnung lautet: $\text{Lambda} = z \times q / p$. Auch hier musst du keine mathematischen Kenntnisse mitbringen. Die Aussage ist einfach. Je grösser der Anteil der Rechenleistung des Angreifers ist, desto mehr Fortschritt kann er während einer bestimmten Wartezeit durchschnittlich erzielen. Je kleiner sein Anteil ist, desto weniger Blöcke wird er im Durchschnitt finden. Satoshi nutzt diese Abschätzung anschliessend, um die möglichen Ergebnisse des Wettlaufs miteinander zu verrechnen.

Was zeigen die Zahlen des ursprünglichen Whitepapers?

Satoshi Nakamoto berechnet im Whitepaper mehrere Beispiele. Wir betrachten zunächst einen Angreifer, der 10 Prozent der gesamten Rechenleistung besitzt. Die ehrlichen Miner kontrollieren damit die übrigen 90 Prozent. Satoshi untersucht, wie sich die Erfolgswahrscheinlichkeit verändert, wenn der Zahlungsempfänger zusätzliche Blöcke abwartet. Dabei bezeichnet z im Rechenbeispiel die Anzahl weiterer Blöcke, die nach dem Block mit der betreffenden Zahlung entstanden sind. Wichtig ist deshalb: Wenn z den Wert 5 besitzt, wurde die Zahlung bereits in einen Block aufgenommen und anschliessend sind fünf weitere Blöcke entstanden. Nach der heute gebräuchlichen Zählweise entspricht dies insgesamt sechs Bestätigungen. Die folgenden Zahlen stammen aus Satoshis mathematischem Modell. Sie sind keine aktuellen Messwerte des Bitcoin-Netzwerks.

BEISPIELRECHNUNG AUS DEM ORIGINAL:

Angenommen, ein Angreifer kontrolliert 10 Prozent der Rechenleistung. Die ehrlichen Miner kontrollieren 90 Prozent. Satoshi berechnet unter seinen Modellannahmen folgende ungefähren Erfolgswahrscheinlichkeiten: 1 weiterer Block nach dem Zahlungsblock: 20,46 Prozent 3 weitere Blöcke nach dem Zahlungsblock: 1,32 Prozent 5 weitere Blöcke nach dem Zahlungsblock: 0,091 Prozent 6 weitere Blöcke nach dem Zahlungsblock: 0,024 Prozent 10 weitere Blöcke nach dem Zahlungsblock: 0,00012 Prozent Die Werte zeigen: Unter den angenommenen Bedingungen sinkt die berechnete Erfolgswahrscheinlichkeit mit jedem zusätzlichen Block deutlich. Diese Wahrscheinlichkeiten beziehen sich ausschliesslich auf den untersuchten Doppelausgabeangriff. Sie sind keine allgemeine Statistik über die Sicherheit sämtlicher Bitcoin-Zahlungen.

Was bedeutet eine Wahrscheinlichkeit von 0,091 Prozent?

Eine Wahrscheinlichkeit von 0,091 Prozent ist sehr klein. Sie bedeutet jedoch nicht, dass ein Erfolg mathematisch ausgeschlossen wäre. Eine solche Wahrscheinlichkeit entspricht ungefähr neun möglichen Erfolgen bei zehntausend vergleichbaren, unabhängig betrachteten Versuchen. Das ist nur eine anschauliche Grössenordnung. Die tatsächlichen Ergebnisse einzelner Versuche können davon abweichen. Wichtig ist deshalb: Eine sehr geringe Wahrscheinlichkeit ist nicht dasselbe wie absolute Unmöglichkeit. Genau diese Unterscheidung ist für das Verständnis der Bitcoin-Sicherheit entscheidend. Satoshi zeigt mit seinen Berechnungen, dass ein unterlegener Angreifer mit zunehmendem Rückstand immer schlechtere Erfolgsaussichten besitzt. Er zeigt nicht, dass unter allen denkbaren Umständen jede bestätigte Bitcoin-Zahlung unumkehrbar wäre.

Was geschieht bei einem stärkeren Angreifer?

Nun betrachten wir einen anderen Fall. Angenommen, der Angreifer kontrolliert 30 Prozent der gesamten Rechenleistung. Die ehrlichen Miner besitzen zusammen 70 Prozent. Auch in diesem Fall ist der Angreifer statistisch im Nachteil. Allerdings ist sein Anteil wesentlich grösser als im vorherigen Beispiel. Deshalb besitzt er eine deutlich höhere Chance, während der Wartezeit eigene Blöcke zu finden. Satoshi Nakamoto berechnet für diesen Fall ebenfalls mehrere Beispiele. Nach fünf weiteren Blöcken beträgt die berechnete Erfolgswahrscheinlichkeit ungefähr 17,74 Prozent. Nach zehn weiteren Blöcken beträgt sie ungefähr 4,17 Prozent. Nach zwanzig weiteren Blöcken beträgt sie ungefähr 0,25 Prozent. Auch hier sinkt die Wahrscheinlichkeit mit zunehmendem Rückstand. Allerdings geschieht dies deutlich langsamer als bei einem Angreifer mit nur 10 Prozent der Rechenleistung. Damit zeigt Satoshi einen wichtigen Zusammenhang: Nicht nur die Anzahl zusätzlicher Blöcke ist entscheidend. Ebenso wichtig ist der Anteil der Rechenleistung, den ein möglicher Angreifer kontrolliert.

VERGLEICH ZWEIER ANGRIFFSSZENARIEN:

Satoshi untersucht zwei unterschiedliche Angreifer. Angreifer A kontrolliert 10 Prozent der Rechenleistung. Angreifer B kontrolliert 30 Prozent der Rechenleistung. Beide versuchen, eine konkurrierende Blockchain durchzusetzen. Nach fünf weiteren Blöcken ergibt das Modell: Angreifer A: Ungefähr 0,091 Prozent Erfolgswahrscheinlichkeit. Angreifer B: Ungefähr 17,74 Prozent Erfolgswahrscheinlichkeit. Der Unterschied ist erheblich. Ein stärkerer Angreifer besitzt unter denselben übrigen Annahmen wesentlich bessere Erfolgsaussichten. Deshalb hängt die Sicherheit nicht allein von der Anzahl der Bestätigungen ab.

Warum wartet ein Empfänger auf mehrere Bestätigungen?

Die Berechnungen erklären, weshalb Bitcoin-Empfänger bei bestimmten Zahlungen mehrere Bestätigungen abwarten. Stell dir vor, Beat verkauft einen Gegenstand mit hohem Wert. Wenn er den Gegenstand sofort nach dem Erscheinen einer unbestätigten Bitcoin-Transaktion herausgibt, übernimmt er ein erhöhtes Risiko. Wartet er dagegen auf die Aufnahme der Zahlung in einen gültigen Block, besitzt er bereits einen stärkeren Nachweis. Wenn anschliessend weitere gültige Blöcke entstehen, wird eine erfolgreiche nachträgliche Veränderung unter den üblichen Sicherheitsannahmen zunehmend unwahrscheinlicher. Allerdings gibt es keine einzige Anzahl von Bestätigungen, die für sämtliche Zahlungen gleichermassen geeignet ist.

Bei kleineren Zahlungen können andere Sicherheitsanforderungen gelten als bei sehr grossen Beträgen. Auch die konkrete technische Situation und die wirtschaftlichen Folgen eines möglichen Angriffs spielen eine Rolle. Die Berechnungen des Whitepapers erklären deshalb das grundlegende Sicherheitsprinzip. Sie ersetzen jedoch keine individuelle Beurteilung des Risikos einer bestimmten Zahlung.

Warum verwendet Satoshi einen neuen öffentlichen Schlüssel?

Im elften Abschnitt beschreibt Satoshi Nakamoto noch eine weitere Vorsichtsmassnahme. Der Empfänger einer Zahlung soll für diese Zahlung ein neues Schlüsselpaar erzeugen. Den zugehörigen öffentlichen Schlüssel teilt er dem Absender erst kurz vor der Erstellung der Zahlung mit. Satoshi verfolgt damit ein bestimmtes Ziel. Er möchte verhindern, dass ein betrügerischer Absender schon lange im Voraus eine passende konkurrierende Blockchain vorbereiten kann. Stell dir vor, Anna weiss bereits sehr früh, welche genaue Zahlung sie später an Beat leisten soll. Sie könnte versuchen, bestimmte Angriffsvorbereitungen vor dem eigentlichen Zahlungsvorgang zu treffen. Wenn die entscheidenden Zahlungsinformationen dagegen erst kurz vor der Zahlung feststehen, wird eine solche gezielte Vorbereitung erschwert. Das ist der Gedanke hinter Satoshis Beschreibung. Aus heutiger Sicht ist allerdings wichtig: Das Erzeugen einer neuen Empfangsadresse allein verhindert keinen Doppelausgabeangriff. Es ersetzt weder die Prüfung der Zahlung noch das Abwarten angemessener Bestätigungen. Satoshis Überlegung gehört zu seinem konkreten mathematischen Angriffsszenario und darf nicht als allgemeine Sicherheitsgarantie verstanden werden.

Warum enthält das Whitepaper ein Computerprogramm?

Nach seinen mathematischen Formeln zeigt Satoshi Nakamoto ein kurzes Computerprogramm. Dieses wurde in der Programmiersprache C geschrieben. Eine Programmiersprache ermöglicht es, einem Computer genaue Anweisungen für Berechnungen zu geben. Das Programm dient dazu, die zuvor beschriebenen Wahrscheinlichkeiten auszurechnen. Es verarbeitet insbesondere zwei Angaben. Die erste ist der Anteil der Rechenleistung des Angreifers. Die zweite ist die Anzahl zusätzlicher Blöcke, die der Empfänger abwartet. Anschliessend berechnet es unter den Modellannahmen die Erfolgswahrscheinlichkeit des Angreifers. Die verwendeten mathematischen Schritte entsprechen den zuvor erläuterten Überlegungen. Das Computerprogramm ist deshalb kein eigener Sicherheitsmechanismus des Bitcoin-Netzwerks. Es ist ein Hilfsmittel, mit dem Satoshi seine theoretischen Berechnungen nachvollziehbar macht. Für das Verständnis des Whitepapers musst du dieses Programm nicht selbst schreiben oder ausführen können. Wichtig ist, dass du verstehst, weshalb Satoshi die Wahrscheinlichkeiten berechnet und welche Aussage seine Ergebnisse ermöglichen.

Was bedeuten Satoshis mathematische Ergebnisse?

Die Ergebnisse zeigen einen grundlegenden Zusammenhang. Wenn die ehrlichen Miner gemeinsam mehr Rechenleistung besitzen als der Angreifer, ist die ehrliche Blockchain statistisch im Vorteil. Ein Angreifer kann zwar zeitweise Glück haben und mehrere Blöcke finden. Wenn er jedoch immer weiter zurückfällt, werden seine Aussichten auf ein späteres Aufholen zunehmend schlechter. Wie schnell diese Wahrscheinlichkeit sinkt, hängt wesentlich vom Anteil der Rechenleistung ab.

Bei einem kleinen Angreifer kann bereits eine begrenzte Anzahl zusätzlicher Blöcke zu einer sehr geringen berechneten Erfolgswahrscheinlichkeit führen. Bei einem stärkeren Angreifer sind dafür wesentlich mehr Blöcke notwendig. Das Whitepaper beschreibt damit eine Form zunehmender Sicherheit. Die Schutzwirkung wächst mit der nachgewiesenen Rechenarbeit, die nach einer Zahlung auf der akzeptierten Blockchain aufgebaut wird.

Was können diese Berechnungen nicht beweisen?

Die mathematischen Ergebnisse beruhen auf einem vereinfachten Modell. Sie setzen bestimmte Bedingungen voraus. Dazu gehört insbesondere, dass der Angreifer und die ehrlichen Miner mit festgelegten Anteilen der Rechenleistung betrachtet werden. Ausserdem wird die Blockentstehung mit mathematischen Wahrscheinlichkeiten modelliert. In einem realen Netzwerk können zusätzliche Faktoren eine Rolle spielen. Beispielsweise kann sich die Verteilung der Rechenleistung verändern. Auch technische Störungen, ungleiche Informationsverbreitung und strategisches Verhalten einzelner Teilnehmer können Auswirkungen besitzen. Darüber hinaus untersucht Satoshi in diesem Abschnitt nicht sämtliche denkbaren Sicherheitsprobleme. Die Berechnungen schützen beispielsweise nicht vor gestohlenen privaten Schlüsseln. Sie verhindern auch nicht, dass jemand freiwillig Bitcoin an einen Betrüger sendet. Ebenso wenig sagen sie etwas über den zukünftigen Marktpreis von Bitcoin aus. Deshalb dürfen die angegebenen Wahrscheinlichkeiten nicht als allgemeine Sicherheitsgarantie verstanden werden. Sie erläutern die Widerstandsfähigkeit des ursprünglichen Bitcoin-Konzepts gegenüber einem bestimmten Angriff unter festgelegten Annahmen.

Warum ist dieser Abschnitt für Bitcoin so wichtig?

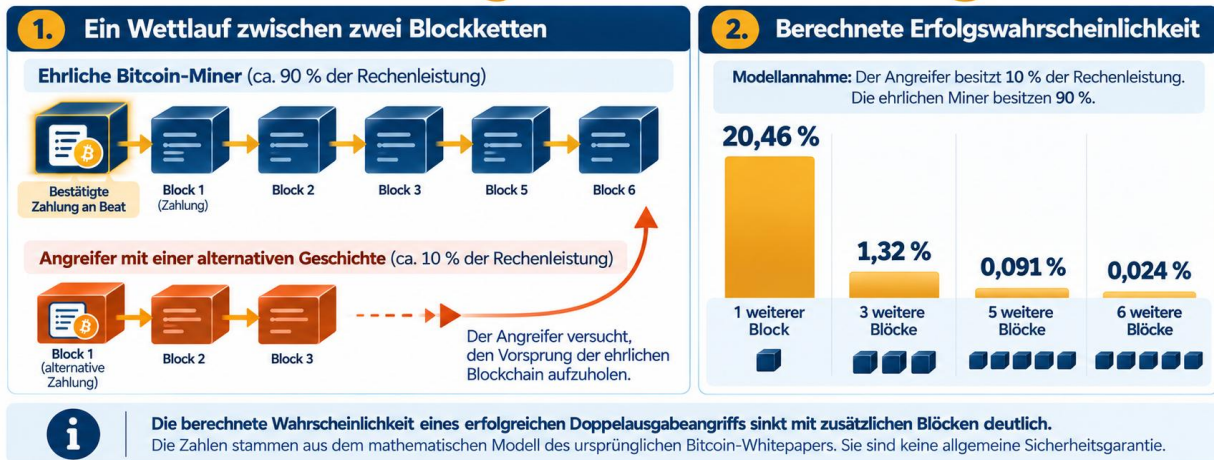
Der elfte Abschnitt des Whitepapers zeigt, dass Satoshi Nakamoto die Sicherheit seines Systems nicht einfach mit einer Behauptung begründet. Er versucht, die Widerstandsfähigkeit gegenüber einem bestimmten Angriff mathematisch nachvollziehbar zu machen. Dabei untersucht er, wie sich die verfügbare Rechenleistung und die Anzahl zusätzlicher Blöcke auf die Erfolgsaussichten eines Angreifers auswirken. Die Ergebnisse erklären, weshalb Bitcoin-Bestätigungen eine wichtige Rolle spielen. Eine Zahlung wird nicht allein deshalb sicherer, weil einige Minuten vergangen sind. Entscheidend ist, dass zusätzliche gültige Blöcke entstehen und dadurch weitere nachgewiesene Rechenarbeit auf der akzeptierten Transaktionshistorie aufbaut. Das ist ein grundlegender Unterschied zwischen einer blossen Wartezeit und der technischen Absicherung durch das Bitcoin-Netzwerk.

MERKSATZ:

Satoshi Nakamoto zeigt mit mathematischen Berechnungen, weshalb ein Angreifer mit weniger Rechenleistung als die ehrlichen Miner zunehmend schlechtere Chancen besitzt, eine bestätigte Zahlung nachträglich zu verändern. Je mehr gültige Blöcke auf einer Zahlung aufbauen, desto geringer wird unter den untersuchten Annahmen die Wahrscheinlichkeit eines erfolgreichen Doppelausgabeangriffs. Die Sicherheit hängt aber auch vom Anteil der Rechenleistung des Angreifers ab. Eine absolute Garantie ergibt sich daraus nicht.

GRAFIK 11

Wie sinkt die Erfolgschance eines Angreifers?



SWISSRATION 
WERTE. WISSEN. VORSORGE.

swissration.ch

Satoshi Nakamoto berechnet, wie sich die Erfolgschance eines Angreifers mit zunehmender Zahl weiterer Blöcke verändert. Das Beispiel geht von einem Angreifer mit 10 Prozent der gesamten Rechenleistung aus. Unter diesen Modellannahmen sinkt die berechnete Wahrscheinlichkeit deutlich, erreicht aber keine absolute Null.

12. Was hat Satoshi Nakamoto mit Bitcoin geschaffen?

Verständliche Erklärung des Originalabschnitts «Conclusion»

Im zwölften und letzten Abschnitt seines Whitepapers fasst Satoshi Nakamoto die wichtigsten Ergebnisse seiner Überlegungen zusammen. Der englische Titel «Conclusion» bedeutet auf Deutsch «Schlussfolgerung». Satoshi wollte ein elektronisches Zahlungssystem entwickeln, bei dem Menschen digitale Geldbeträge direkt untereinander übertragen können, ohne dass eine zentrale Institution die gesamte Buchhaltung führen muss. Die besondere Herausforderung bestand darin, sicherzustellen, dass derselbe digitale Betrag nicht mehrfach ausgegeben werden kann. In den vorherigen elf Abschnitten hat Satoshi die verschiedenen Bestandteile seiner Lösung beschrieben. In seiner Schlussfolgerung zeigt er nun, wie diese Bestandteile zusammenwirken und weshalb daraus ein funktionsfähiges Zahlungssystem entstehen kann.

Die entscheidende Lösung liegt im Zusammenspiel verschiedener Verfahren

Satoshi Nakamoto hat nicht sämtliche technischen Grundlagen von Bitcoin neu erfunden. Digitale Signaturen, kryptographische Fingerabdrücke und Verfahren zur zeitlichen Dokumentation digitaler Informationen waren bereits bekannt. Seine entscheidende Leistung bestand darin, verschiedene Verfahren so miteinander zu verbinden, dass sie gemeinsam ein grundlegendes Problem elektronischer Zahlungen lösen können.

Digitale Signaturen ermöglichen die technische Freigabe einer Zahlung. Eine öffentlich überprüfbare Transaktionshistorie macht nachvollziehbar, welche Beträge bereits ausgegeben wurden. Die Verbindung der Datenblöcke und der Arbeitsnachweis erschweren nachträgliche Veränderungen dieser Geschichte. Unabhängige Netzwerkteilnehmer überprüfen, ob Transaktionen und Blöcke den geltenden Regeln entsprechen. Keiner dieser Bestandteile würde für sich allein das gesamte Problem lösen. Erst ihr Zusammenspiel ermöglicht die von Satoshi Nakamoto vorgeschlagene Form elektronischer Zahlungen ohne eine zwingend notwendige zentrale Abrechnungsstelle.

Wie entsteht eine gemeinsame Transaktionshistorie ohne zentrale Leitung?

Bei einer Bank führt eine zentrale Organisation die verbindliche Buchhaltung. Bei Bitcoin übernehmen viele unabhängige Computer die Überprüfung der gemeinsamen Transaktionshistorie. Neue Zahlungen werden über das Netzwerk verbreitet. Miner stellen daraus mögliche neue Blöcke zusammen und suchen nach einem gültigen Arbeitsnachweis. Andere Netzwerkteilnehmer können überprüfen, ob diese Blöcke den geltenden Regeln entsprechen. Entstehen unterschiedliche gültige Fortsetzungen der Blockchain, orientieren sich die Teilnehmer an der Kette mit der grössten gesamten nachgewiesenen Rechenarbeit. Dadurch kann das Netzwerk eine gemeinsame Geschichte gültiger Transaktionen aufbauen, ohne dass eine einzelne Organisation deren Reihenfolge für alle verbindlich festlegen muss. Die Sicherheit dieses Verfahrens hängt jedoch von bestimmten Voraussetzungen ab. Insbesondere geht das ursprüngliche Whitepaper davon aus, dass die ehrlich arbeitenden Miner gemeinsam über mehr Rechenleistung verfügen als eine zusammenarbeitende Gruppe von Angreifern.

Warum benötigt Bitcoin keine zentrale Koordinationsstelle?

Satoshi Nakamoto hebt in seiner Schlussfolgerung ausdrücklich hervor, dass das Bitcoin-Netzwerk mit vergleichsweise wenig zentraler Koordination auskommt. Die teilnehmenden Computer müssen sich weder persönlich kennen noch bei einer zentralen Stelle anmelden, um grundsätzlich am offenen Netzwerk teilnehmen zu können. Neue Informationen werden zwischen miteinander verbundenen Computern weitergegeben. Dabei ist nicht erforderlich, dass jede Nachricht sofort sämtliche Teilnehmer erreicht. Einzelne Computer können vorübergehend ausfallen oder ihre Verbindung zum Netzwerk verlieren, ohne dass dadurch das gesamte System stillsteht. Wenn ein Teilnehmer später wieder beitrifft, kann er die zwischenzeitlich entstandenen Informationen von anderen Netzwerkteilnehmern beziehen. Ein vollständig prüfender Computer kann anschliessend selbst kontrollieren, ob die erhaltenen Blöcke den geltenden Regeln entsprechen. Diese offene Organisation macht das Netzwerk weniger abhängig vom Betrieb einzelner Computer oder Unternehmen. Sie bedeutet allerdings nicht, dass Bitcoin ohne funktionierende Kommunikationswege, Stromversorgung oder ausreichend aktive Netzwerkteilnehmer auskommt.

Welche Rolle spielen Rechenleistung und Zustimmung?

Im ursprünglichen Whitepaper beschreibt Satoshi Nakamoto die Beteiligung am Arbeitsnachweis als eine Art Abstimmung durch Rechenleistung. Damit meint er, dass Miner durch ihre Arbeit zur Fortsetzung einer bestimmten gültigen Blockchain beitragen. Wer einen Block als gültig anerkennt und darauf aufbaut, unterstützt mit seiner Rechenleistung diese Fortsetzung der Transaktionshistorie.

Heute ist bei dieser Beschreibung eine wichtige Unterscheidung notwendig. Miner schlagen neue Blöcke vor und liefern die erforderlichen Arbeitsnachweise. Unabhängige Prüfknoten kontrollieren dagegen, ob diese Blöcke den von ihnen verwendeten Bitcoin-Regeln entsprechen. Ein Miner kann deshalb nicht allein durch zusätzliche Rechenleistung erreichen, dass alle anderen Teilnehmer einen Block akzeptieren, der gegen ihre geltenden Regeln verstößt. Der Arbeitsnachweis entscheidet darüber, welche gültige Kette sich bei konkurrierenden Fortsetzungen durchsetzt. Die unabhängige Regelprüfung legt dagegen fest, welche Blöcke ein Teilnehmer überhaupt als gültig betrachtet. Beide Aufgaben ergänzen sich und sind für das Verständnis des Bitcoin-Netzwerks entscheidend.

Warum sind wirtschaftliche Anreize notwendig?

Ein weiteres Element von Satoshis Konzept sind die wirtschaftlichen Anreize für die Netzwerkteilnehmer. Miner müssen Computer betreiben und Energie einsetzen, um neue gültige Blöcke zu finden. Dafür können sie nach den geltenden Regeln eine Vergütung erhalten. Diese besteht aus neu erzeugten Bitcoin und den Gebühren der im Block enthaltenen Transaktionen. Satoshi Nakamoto wollte damit erreichen, dass die Unterstützung des Netzwerks wirtschaftlich attraktiv sein kann. Gleichzeitig soll es für Miner einen Anreiz geben, sich an die Regeln zu halten, statt ihre Rechenleistung für Angriffe einzusetzen. Diese Überlegung ist ein wichtiger Bestandteil des ursprünglichen Konzepts. Sie garantiert jedoch nicht, dass alle Teilnehmer jederzeit ehrlich handeln. Bitcoin verbindet deshalb wirtschaftliche Anreize mit technischen Prüfregeln und dem Arbeitsnachweis. Das System soll nicht allein davon abhängen, dass sich sämtliche Beteiligten freiwillig korrekt verhalten.

Was hat das ursprüngliche Whitepaper tatsächlich bewiesen?

Das Bitcoin-Whitepaper beschreibt einen technischen Lösungsansatz für die Übertragung digitaler Geldbeträge ohne eine zwingend notwendige zentrale Abrechnungsstelle. Satoshi Nakamoto erklärt, wie digitale Signaturen, eine gemeinsame Transaktionshistorie und Proof of Work zusammenarbeiten können. Ausserdem untersucht er mathematisch, unter welchen Voraussetzungen es für einen Angreifer zunehmend unwahrscheinlich wird, eine bestätigte Zahlung nachträglich durch eine konkurrierende Transaktionshistorie zu ersetzen. Das Whitepaper liefert damit eine technische Begründung für das vorgeschlagene System. Es beweist jedoch nicht, dass Bitcoin unter allen denkbaren Umständen unangreifbar ist. Ebenso wenig enthält es eine Garantie für die zukünftige wirtschaftliche Entwicklung oder den Marktpreis von Bitcoin. Auch spätere Technologien wie moderne Hardware-Wallets oder das Lightning Network gehören nicht zum ursprünglichen Dokument von 2008. Diese Unterscheidung ist wichtig, weil wir die ursprüngliche technische Idee verstehen möchten, ohne ihr nachträglich Eigenschaften oder Versprechen zuzuschreiben, die Satoshi Nakamoto darin nicht formuliert hat.

Die wichtigste Erkenntnis aus Satoshis Schlussfolgerung

Die eigentliche Besonderheit von Bitcoin liegt nicht in einem einzelnen Computerprogramm oder einer bestimmten mathematischen Berechnung. Sie liegt in der Verbindung mehrerer technischer Verfahren zu einem gemeinsamen System. Digitale Zahlungen können nach öffentlich bekannten Regeln überprüft werden. Viele unabhängige Computer können sich an dieser Überprüfung beteiligen.

Ein Arbeitsnachweis erschwert es, die akzeptierte Transaktionshistorie nachträglich zu verändern. Wirtschaftliche Anreize sollen dafür sorgen, dass ausreichend Rechenleistung für den Netzbetrieb bereitgestellt wird. Dadurch entsteht ein Zahlungssystem, bei dem keine einzelne Bank die verbindliche Buchhaltung führen muss. Die Teilnehmer können sich stattdessen auf überprüfbare technische Regeln und eine durch Rechenarbeit abgesicherte Transaktionshistorie stützen. Genau das ist die grundlegende Lösung, die Satoshi Nakamoto im Jahr 2008 vorgestellt hat.

MERKSATZ:

Satoshi Nakamotos entscheidender Beitrag bestand darin, verschiedene bekannte technische Verfahren zu einem neuen elektronischen Zahlungssystem zu verbinden. Digitale Signaturen ermöglichen die Freigabe von Zahlungen. Eine gemeinsame Transaktionshistorie verhindert die mehrfache Ausgabe desselben Betrags innerhalb der gültigen Geschichte. Proof of Work erschwert nachträgliche Veränderungen. Unabhängige Netzwerkteilnehmer überprüfen die Einhaltung der geltenden Regeln. So können elektronische Zahlungen ohne eine zwingend notwendige zentrale Abrechnungsstelle verarbeitet werden.

Abschliessender Gedanke

Das Bitcoin-Whitepaper beantwortet eine grundlegende Frage: Wie können Menschen digitale Geldbeträge direkt untereinander übertragen, wenn keine einzelne Institution die verbindliche Buchhaltung führt? Satoshi Nakamoto zeigte, dass sich dieses Problem durch die Kombination kryptographischer Verfahren, eines offenen Computernetzwerks und wirtschaftlicher Anreize lösen lässt. Das Ergebnis war die technische Grundlage von Bitcoin. Seit der Veröffentlichung des Whitepapers hat sich das Netzwerk weiterentwickelt. Seine praktische Nutzung, seine wirtschaftliche Bedeutung und sein Marktpreis können sich auch in Zukunft verändern. Die ursprüngliche technische Idee lässt sich jedoch unabhängig davon untersuchen und nachvollziehen. Wer das Whitepaper verstanden hat, erkennt deshalb, dass Bitcoin mehr ist als ein handelbarer digitaler Vermögenswert. Bitcoin ist zunächst ein technisches System, das die Übertragung und Überprüfung digitaler Geldbeträge ohne eine zwingend notwendige zentrale Buchungsstelle ermöglicht. Ob und in welchem Umfang diese Technologie langfristig genutzt wird, bleibt eine wirtschaftliche und gesellschaftliche Frage. Die technische Konstruktion, auf der sie beruht, ist dagegen öffentlich dokumentiert und kann unabhängig überprüft werden.

ABSCHLUSS DES SWISSRATION-WHITEPAPER-LEITFADENS:

Bitcoin wurde nicht entwickelt, um digitale Dateien wie gewöhnliche Informationen beliebig kopieren zu können. Satoshi Nakamoto wollte ein elektronisches Zahlungssystem schaffen, das genau diese mehrfache Verwendung desselben digitalen Geldbetrags verhindert. Seine Lösung verbindet digitale Signaturen, eine öffentlich überprüfbare Transaktionshistorie, Proof of Work und ein weltweit verteiltes Computernetzwerk. Damit schuf er die Grundlage für ein System, in dem digitale Geldbeträge direkt zwischen Teilnehmern übertragen werden können, ohne dass eine einzelne zentrale Institution sämtliche Zahlungen verwalten muss. Das ist die zentrale Idee des Bitcoin-Whitepapers von 2008.

GRAFIK 12

Wie die Bestandteile des Bitcoin-Systems zusammenarbeiten



Bitcoin verbindet digitale Signaturen, eine öffentlich überprüfbare Transaktionshistorie, Arbeitsnachweise und unabhängige Regelprüfungen. Erst das Zusammenwirken dieser Bestandteile ermöglicht die von Satoshi Nakamoto beschriebene technische Lösung.

Quellen und wissenschaftliche Grundlagen des Bitcoin-Whitepapers

Das ursprüngliche Bitcoin-Whitepaper

Die Grundlage dieses Swissration-Leitfadens ist das ursprüngliche englische Bitcoin-Whitepaper von Satoshi Nakamoto.

Originaltitel: Bitcoin: A Peer-to-Peer Electronic Cash System

Autor: Satoshi Nakamoto

Veröffentlichung: 31. Oktober 2008

Originaldokument: <https://bitcoin.org/bitcoin.pdf>

Die vorliegende Swissration-Ausarbeitung folgt der ursprünglichen Reihenfolge der zwölf Abschnitte. Sie ist keine wortwörtliche Übersetzung des Originaldokuments. Ihr Ziel ist es, die technischen Aussagen in verständlicher deutscher Sprache zu erläutern. Dabei wurden ergänzende Erklärungen, Beispiele und Hinweise zur heutigen technischen Funktionsweise eingefügt. Diese Ergänzungen dienen dem Verständnis und sind nicht automatisch Bestandteil des ursprünglichen Whitepapers.

Welche wissenschaftlichen Arbeiten nennt Satoshi Nakamoto?

Satoshi Nakamoto entwickelte Bitcoin nicht unabhängig von sämtlichen früheren Arbeiten. Im ursprünglichen Whitepaper verweist er auf acht bereits veröffentlichte wissenschaftliche und technische Quellen.

Diese beschäftigen sich unter anderem mit digitalem Geld, der zeitlichen Dokumentation elektronischer Informationen, kryptographischen Verfahren und mathematischen Wahrscheinlichkeiten. Die nachfolgenden Quellen entsprechen dem Literaturverzeichnis des ursprünglichen Whitepapers.

Literaturverzeichnis des Originals

[1] W. Dai (1998) b-money Ein früher Vorschlag für ein digitales Geldsystem.

<http://www.weidai.com/bmoney.txt>

[2] H. Massias, X. S. Avila und J.-J. Quisquater (1999) Design of a Secure Timestamping Service with Minimal Trust Requirements Eine wissenschaftliche Arbeit über die sichere zeitliche Dokumentation digitaler Informationen.

[3] S. Haber und W. S. Stornetta (1991) How to Time-Stamp a Digital Document Eine grundlegende wissenschaftliche Arbeit über die zeitliche Absicherung elektronischer Dokumente.

[4] D. Bayer, S. Haber und W. S. Stornetta (1993) Improving the Efficiency and Reliability of Digital Time-Stamping Eine weiterführende Arbeit zur Verbesserung der Effizienz und Zuverlässigkeit kryptographischer Zeitrachweise.

[5] S. Haber und W. S. Stornetta (1997) Secure Names for Bit-Strings Eine wissenschaftliche Arbeit über kryptographisch abgesicherte Bezeichnungen digitaler Informationen.

[6] A. Back (2002) Hashcash – A Denial of Service Counter-Measure Eine technische Arbeit über einen Arbeitsnachweis, bei dem Rechenaufwand eingesetzt wird.

<http://www.hashcash.org/papers/hashcash.pdf>

[7] R. C. Merkle (1980) Protocols for Public Key Cryptosystems Eine grundlegende wissenschaftliche Arbeit über kryptographische Verfahren mit öffentlichen Schlüsseln.

[8] W. Feller (1957) An Introduction to Probability Theory and Its Applications Ein mathematisches Grundlagenwerk über Wahrscheinlichkeitsrechnung.

Hinweis zur Verwendung dieser Quellen

Die genannten Arbeiten zeigen, dass verschiedene Bestandteile des Bitcoin-Systems bereits vor der Veröffentlichung des Whitepapers wissenschaftlich untersucht wurden. Satoshi Nakamotos entscheidender Beitrag bestand darin, mehrere dieser Ansätze zu einem neuen System für elektronische Zahlungen zusammenzuführen. Für das Verständnis des Swisstration-Leitfadens ist es nicht notwendig, sämtliche wissenschaftlichen Originalarbeiten selbst zu lesen. Wer die technischen Grundlagen vertiefen möchte, kann sie jedoch als weiterführende Quellen verwenden.