BITCOIN IN 10 MINUTEN

Alles, was Sie schon immer zu Bitcoin wissen wollten

Brought to you by Relai

WAS IST BITCOIN?

Die höchst erfolgreiche Währung Bitcoin sorgt weltweit für Schlagzeilen und hat zahlreiche Diskussionen über Geld, Technologie und Investieren ausgelöst. Viele wollen an ihrem Erfolg mitprofitieren, andere geben sich gleichgültig oder gar skeptisch. Es ist von Spekulation und Blase die Rede, aber auch von Innovation, monetärer Revolution oder gar Erlösung aus dem heutigen Geldsystem.

Diverse Länder, unter anderem China, sehen Bitcoin als Bedrohung und haben der digitalen Währung den Kampf angesagt. Andere Regierungen, wie jene von El Salvador, haben Bitcoin in der Hoffnung auf wirtschaftlichen Aufschwung als offizielles Zahlungsmittel eingeführt.

Doch was ist Bitcoin? Ist es Geld? Digitales Gold? Eine vorübergehende Modeerscheinung für Informatiker und Spekulanten? Oder etwas ganzes Anderes?

Nachfolgend gehen wir diesen Fragen auf den Grund und beleuchten die neuartige Währung genauer, um die Funktionsweise und Philosophie hinter Bitcoin besser verstehen zu können. Hierzu ist es wichtig, ganz zu Beginn, also bei der Entstehungsgeschichte von Bitcoin, anzufangen.

DIE GESCHICHTE BITCOINS

Bitcoins Anfänge gehen bis in die frühen Neunzigerjahre zurück. Im Jahre 1992 startete eine Gruppe von Informatiker in Kalifornien einen Emailverteiler, um sich mit Gleichgesinnten über Kryptografie, Mathematik, Politik und Philosophie auszutauschen. Sie nannten sich 'Cypherpunks' – ein Wortspiel aus Cyberpunk (Person in der Sci-Fi Literatur, welche der Gesellschaft gegenüber misstrauisch ist – und dies zu Recht) und cipher (verschlüsseln).

Die Cypherpunks

Die Cypherpunks wuchsen bald zu einer bunt zusammengewürfelten Truppe heran. Trotz unterschiedlicher Herkunft vereinte sie die Überzeugung, dass das Internet in naher Zukunft zu einem der umkämpftesten Schauplätze für die menschliche Freiheit würde.

Um sich gegen die drohende Kontrolle, Überwachung und Zensur des Internets zu schützen und das freie und offene Internet zu bewahren, wussten sich die Cypherpunks einer mächtigen Waffe zu bedienen: Der Kryptografie, also der Verschlüsselung von Information.

In ihrem Manifest von 1993 hielten sie fest: «Cypherpunks schreiben Computercode. Wir wissen, dass jemand Software schreiben muss, um die Privatsphäre zu verteidigen, und [...] wir werden sie schreiben.» Kryptografie alleine aber würde für eine freie digitale Internet-Ökonomie nicht ausreichen. Denn, und davon

waren die Cypherpunks überzeugt: Das Internet kann nicht wirklich frei sein, wenn es nicht über sein eigenes Geld verfügt. Ein Geld, unabhängig von Staaten, Zentralbanken und Firmen, ein digitales Geld so fair und dezentralisiert wie das Internet selbst.

Geldexperimente

Doch stellte die Erschaffung eines unabhängigen, digitalen Geldes die Cypherpunks vor technische Herausforderungen. Bereits 1990 hatte der Kryptologe David Chaum mit eCash eine erste digitale Währung ins Leben gerufen, welche zwar nicht dezentralisiert war, aber dank Kryptografie Anonymität gewährleistete. eCash konnte sich längerfristig aber nicht gegen andere online Zahlungssysteme durchsetzen, weshalb die Firma nach 8 Jahren Konkurs anmelden musste und eCash verschwand.

Weitere Versuche folgten, von denen sich E-Gold besonders hervorzutun vermochte. E-Gold war eine durch Gold gedeckte digitale Währung, welche offen für jeden war. Während der Dotcom-Zeit im Jahr 1996 gegründet, traf das Unternehmen den Nerv der Zeit und prozessierte zu seinen besten Zeiten Transaktionen im Wert von über zwei Milliarden US-Dollar pro Jahr.

Aber auch E-Gold war von einer zentralen Stelle gesteuert und somit angreifbar. Bald folgten rechtliche Probleme und die US-Regierung ging gerichtlich gegen E-Gold vor. 2008 wurde E-Gold von einem US-Gericht wegen Geldwäscherei und Verstössen gegen das Geldübertragungsgesetz schuldig gesprochen. Sämtliche Vermögenswerte wurden eingefroren und E-Gold musste den Betrieb einstellen.

Den Cypherpunks waren durch diese fehlgeschlagenen Versuche zwei Tatsachen deutlich vor Augen geführt worden. Erstens: Sowohl eCash als auch E-Gold waren mit Sicherheiten hinterlegt gewesen. Diese Sicherheiten hatten sich als verwundbare Stelle herausgestellt, konnten diese doch von Staaten beschlagnahmt werden. Deshalb darf ein digitales Geld keine zentralen Angriffspunkte wie eine Bankkonto, eine (rechtliche) Person oder einen Serverstandort haben. Und zweitens: Regierungen und Regulatoren haben kein Interesse an einem staatsunabhängigen, digitalen Geld.

Die Grundfrage, für welche bisher keine Lösung gefunden worden war, blieb also: Wie kann digitales Geld ohne eine zentrale Instanz, welche die Bücher führt und sicherstellt, dass Geld nicht doppelt ausgeben wird, funktionieren? Denn sollte es gelingen, das Problem des doppelten Ausgebens zu lösen, ohne sich auf eine zentrale Partei verlassen zu müssen, könnte man möglicherweise ein digitales Geld schaffen, das dem Internet heimisch ist.

Ein mystischer Schöpfungsakt

Aus diesen Gründen begannen die Cypherpunks, Entwürfe für ein digitales Geld ohne zentrale Partei und ohne hinterlegte Sicherheiten zu diskutieren. Zwei der wichtigsten Konzepte hierbei waren b-money (1998) und BitGold (2005). Diese theoretischen Entwürfe, welche in der Praxis nie umgesetzt wurden, waren in ihrer Ausgestaltung Bitcoin bereits sehr ähnlich. Für die Verschlüsselung war ein öffentliches/privates Schlüsselpaar vorgesehen und zur Erschaffung digitaler Münzen sollte ein Arbeitsnachweis (Proof-of-Work) erbracht werden, wie dies bei Bitcoin ebenfalls der Fall ist. Der Erfinder Bitcoins bestätigte denn auch, von b-money und BitGold Kenntnis gehabt zu haben.

Da b-money und BitGold aber auf ein Wahlsystem für die Konsensfindung (die Übereinstimmung, wem welche Geldeinheiten zum jetzigen Zeitpunkt gehören) bauten, waren sie anfällig für böswillige Hackerattacken, welche die Wahlen manipulieren und so die Eigentumsverhältnisse verfälschen konnten.

Für dieses letzte Problem, welches der Erschaffung eines neuen Internetgeldes noch im Weg stand, wurde am Freitag, dem 31. Oktober 2008 eine Lösung präsentiert. An diesem Tag wurde das Bitcoin Whitepaper, in welchem Satoshi Nakamoto sein Konzept für ein dezentralisiertes Zahlungsnetzwerk erklärt, per E-Mail an die Cypherpunks versandt. Zwei Monate später, am 3. Januar 2009, ging das Bitcoin-Netzwerk live.

Die Reaktionen auf das neue Netzwerk fielen verhalten aus. Einige wenige Enthusiasten begannen das Netzwerk zu testen und Fehler zu rapportieren. Zu Beginn war es aber vor allem Satoshi Nakamoto selbst, der das Netzwerk am Laufen hielt. Doch langsam bereitete sich die Neuigkeit des neuen Internetgeldes auf Computer- und Technikforen aus und das Interesse am Netzwerk wuchs. Nach einem Jahr zählte das Bitcoin-Netzwerk bereits einige Nutzer. Bitcoin selbst aber hatte noch keinen Wert.

Wer ist Satoshi Nakamoto?

Das Bitcoin-Whitepaper sowie die E-Mail-Kommunikation des Bitcoin-Erfinders wurden jeweils mit den Namen Satoshi Nakamoto unterzeichnet. Die wahre Identität des Bitcoin Erfinders ist aber bis heute unbekannt, denn bei diesem Namen scheint es sich um einen Decknamen zu handeln. Um sich an Gleichgesinnte und später an die Bitcoin-Entwicklergemeinschaft zu wenden, verwendete Nakamoto mindestens drei E-Mail-Adressen, welche er aufwendig verschlüsselte, damit die wahre Identität des Absenders nicht zurückverfolgt werden konnte.

Diverse Personen haben bereits von sich behauptet, Satoshi Nakamoto zu sein. Doch bis heute bleibt ein jeder den Beweis schuldig. Denn der ultimative Beweis, nämlich das Verschicken eines Bitcoins von einer der Adressen, welche mit grösster Wahrscheinlichkeit Satoshi gehören, hat noch niemand erbracht.

Zudem ist die Gruppe derjenigen, welche «persönlich» via Internet mit Satoshi Nakamoto kommuniziert haben, sehr klein. Seine letzte Nachricht an die Bitcoin-Community verfasste Satoshi Nakamoto am 12. Dezember 2010. Dies war aber keinesfalls eine Abschiedsnachricht – Satoshi hörte danach einfach auf zu schreiben.

Sein Rückzug galt jedoch nur der breiten Community. Nakamoto scharte weiterhin eine kleine Gruppe von Kernprogrammierern um sich und informierte diese über die weiteren Entwicklungsschritte des Bitcoin-Netzwerks. Im April 2011 schickte er auch dieser Gruppe eine letzte Nachricht. Genauso geheimnisvoll wie Nakamoto auf der Bühne erschien, verschwand er drei Jahre später wieder.

Bitcoins «Pizza-Tag»

Wie hat nun Bitcoin überhaupt einen Wert erhalten? Zu Beginn konnte man Bitcoin zwar schürfen und verschicken, doch hatten die digitalen Einheiten keinen Wert. Auch war der Kreis derer, welche Bitcoin kannten, geschweige denn versenden und empfangen konnten, noch sehr klein.

Dies änderte sich am 22. Mai 2010. An diesem Tag erschien auf dem Internetforum «bitcointalk.org» eine ungewöhnliche Anfrage. Ein 28-Jähriger namens Laszlo Hanyecz aus Florida bot derjenigen Person 10'000 Bitcoin, die ihm zwei Pizzen nach Hause bestellen würde. Ein kalifornischer Student ging auf das Angebot ein und liess ihm zwei grosse Pizzen im Wert von 41 Dollars nach Hause liefern. Im Gegenzug schickte ihm Hanyecz die 10'000 Bitcoin.

Seit diesem Tag wird der 22. Mai von Bitcoinern jährlich als Bitcoin «Pizza-Tag» gefeiert. Der Tag ist deshalb so populär, weil er drei Dinge veranschaulicht:

- Bitcoins haben seither einen Wert
- Bitcoins eignen sich als Tausch- und Zahlungsmittel
- Bitcoin als Währung ist disinflationär.

Die Anzahl an zusätzlich in Umlauf gesetzten Bitcoin nimmt stetig ab, was zu einer Wertsteigerung führen kann.

Diese beiden Pizzen sind als die teuersten der Welt in die Geschichtsbücher eingegangen. Nimmt man den Bitcoin-Kurs von Ende 2021 wurden für sie unglaubliche 430 Million Schweizer Franken bezahlt. Das ist eine Menge Geld. Doch auch der Empfänger der 10'000 Bitcoin hat diese nach eigenen Angaben bereits wieder ausgegeben, und zwar für einen Roadtrip – nach heutigem Bitcoin-Kurs wohl auch der teuerste Roadtrip der Menschheitsgeschichte. Der Bitcoin «Pizza-Tag» veranschaulicht zudem eindrücklich, weshalb das 'Hodln' – abgeleitet von 'hold' (halten) – unter den Bitcoinern so populär ist. Gemeint ist das ewige Halten der eigenen Bitcoins mit dem Ziel, diese niemals zu verkaufen. Denn wer möchte schon heute seine Bitcoin ausgeben, wenn sie in den nächsten Jahren das Doppelte, Dreifache oder sogar das Zehnfache wert sein könnten?

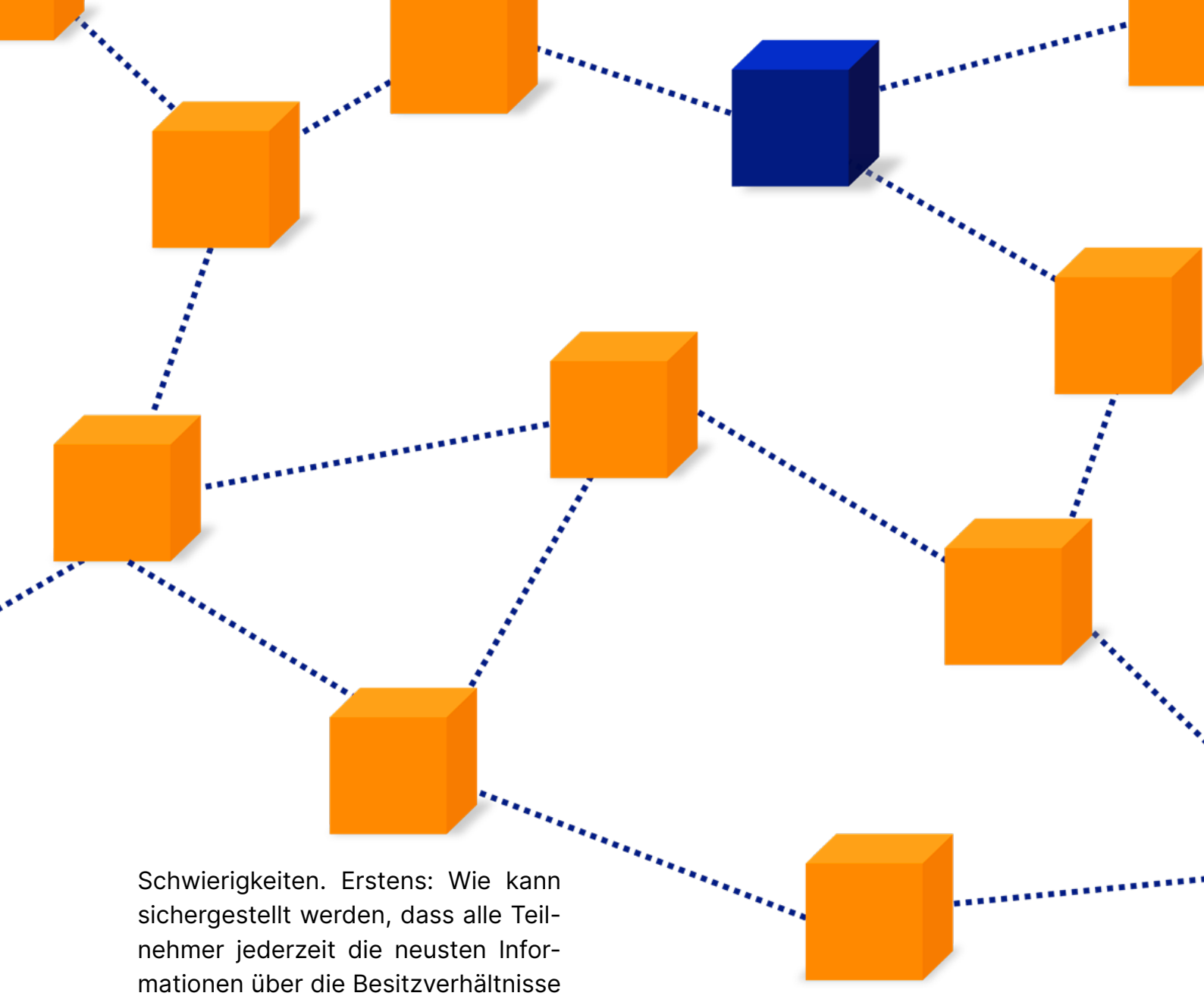
WIE FUNKTIONIERT BITCOIN?

Nachdem wir die Entstehungsgeschichte Bitcoins kennengelernt haben, tauchen wir nun in die Funktionsweise der digitalen Währung ein. Ziel ist es zu verstehen, wie das Bitcoin-Netzwerk funktioniert, welche Probleme es löst und was der praktische Nutzen davon ist.

Die Absicht hinter Bitcoin ist es, ein möglichst dezentralisiertes Netzwerk zu sein. Kein Netzwerkteilnehmer soll alleine über das Netzwerk bestimmen können – die Entscheidungsgewalt und Aufsicht ist auf alle Teilnehmer verteilt. Das ist wichtig, weil so kein Individuum, keine Regierung und keine Firma das Netzwerk eigenständig abändern kann, sondern Änderungen nur im Kollektiv möglich sind.

Bitcoin funktioniert so, dass jeder Netzwerkteilnehmer zu jeder Zeit eine identische Kopie der aktuellen Eigentumsverhältnisse besitzt – das heisst, alle wissen immer, wem wann welche Bitcoin gehören. Somit kann auch niemand behaupten, er besitze mehr Bitcoin als er hat, da alle anderen diese Aussage überprüfen und als falsch entlarven können.

Vor der Lancierung von Bitcoin stand diese Art von dezentralisierten Netzwerken vor zwei grossen

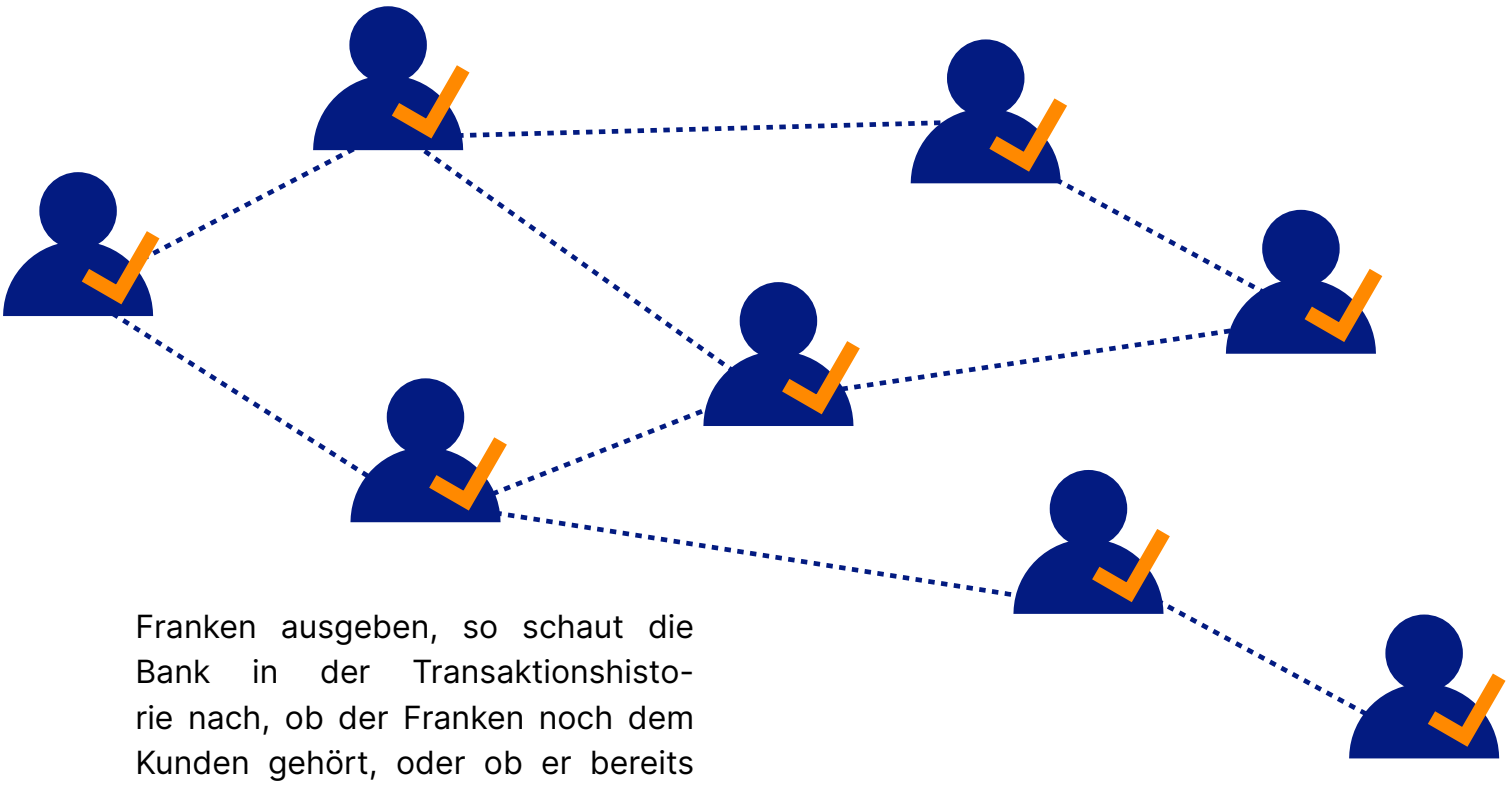


Schwierigkeiten. Erstens: Wie kann sichergestellt werden, dass alle Teilnehmer jederzeit die neusten Informationen über die Besitzverhältnisse erhalten - also das Wissen darüber, welche Bitcoin ausgegeben worden sind. Und zweitens: wie können Teilnehmer überprüfen, ob diese Informationen zu 100% korrekt sind.

Die Blockchain

Diese Schwierigkeiten konnten dank der Erfindung der Blockchain überwunden werden. Eine Blockchain (Block-Kette) ist die zeitliche Aneinanderreihung von Information. Im Fall von Bitcoin sind alle Transaktionen seit der Entstehung von Bitcoin in chronologischer Reihenfolge in einzelnen Blöcken auf der Bitcoin-Blockchain gespeichert. Jeder Netzwerkteilnehmer, welcher wissen will, wem welche Bitcoin gehören, kann die Transaktionshistorie auf der Blockchain nachvollziehen und so genau feststellen, wem zum jetzigen Zeitpunkt wie viele Bitcoin gehören. Will also jemand einen Bitcoin versenden, so kann jedermann überprüfen, ob dieser Bitcoin auch wirklich der entsprechenden Person gehört.

Bis hierhin ist dies nichts Spezielles, macht doch eine Bank genau dasselbe. Will ein Kunde einen



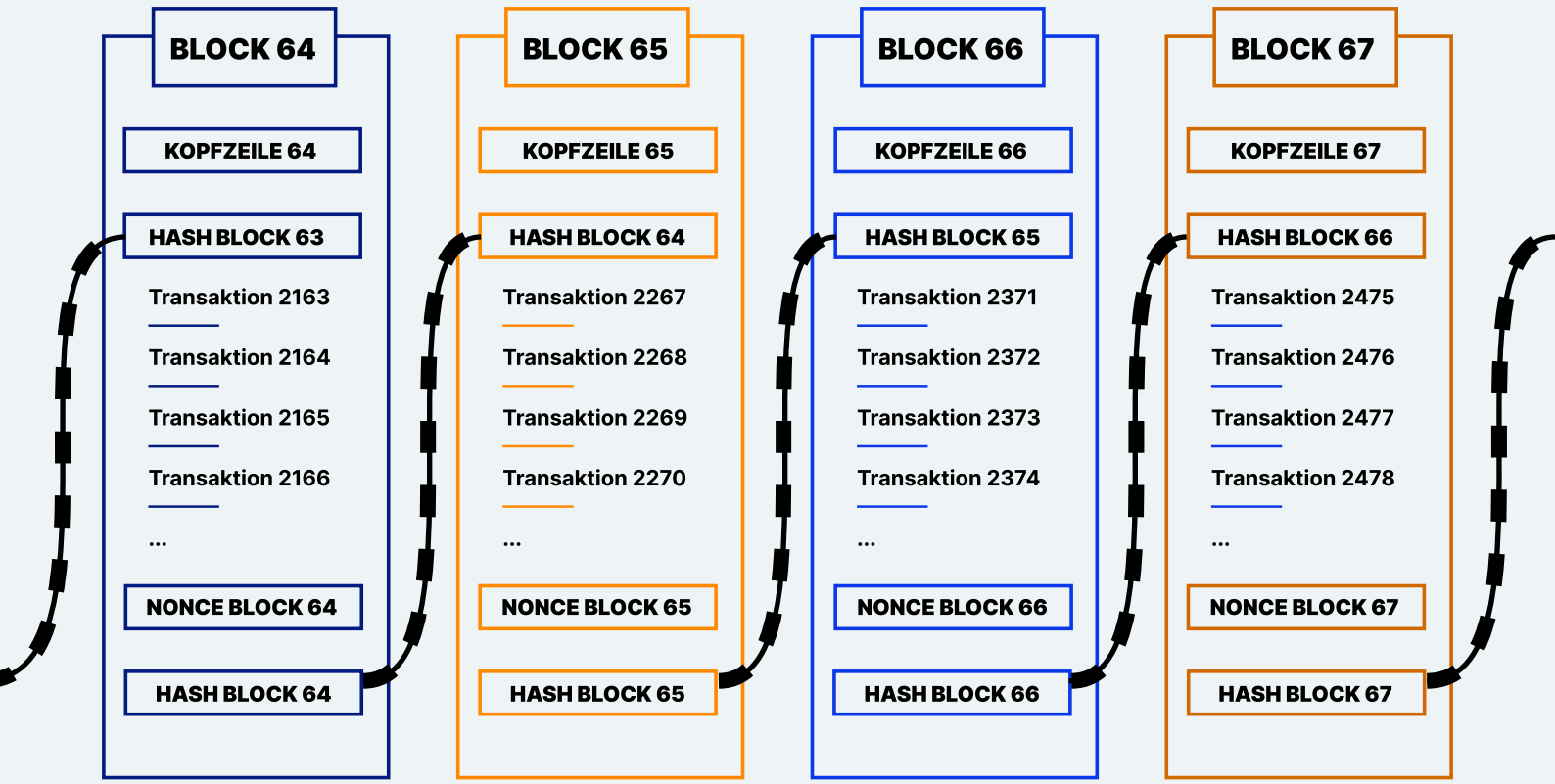
Franken ausgeben, so schaut die Bank in der Transaktionshistorie nach, ob der Franken noch dem Kunden gehört, oder ob er bereits ausgegeben wurde. Das Besondere an der Blockchain ist aber, dass sie nicht auf einem zentralen Bankenserver, sondern auf den jeweiligen Computern der Netzwerkteilnehmer (sogenannten Full Nodes) abgespeichert ist und somit in zehntausendfacher Ausführung weltweit existiert. Dies ist auch der Grund, weshalb Bitcoin nicht einfach gelöscht werden kann – hierfür müsste man die identische Blockchain Kopie von allen teilnehmenden Computern weltweit gleichzeitig löschen.

Die Krux liegt nun darin, dass jeder Netzwerkteilnehmer mit absoluter Sicherheit feststellen können muss, dass seine Kopie der Blockchain korrekt ist und ihm keine fehlerhaften Transaktionen mitgeteilt werden. Da der Blockchain laufend neue Blöcke mit neuen Transaktionen angehängt werden, wächst sie ständig und muss auf allen teilnehmenden Computern weltweit stetig aktualisiert werden. Und diese neu angehängten Blöcke müssen wiederum von allen verifiziert werden können.

Dieses Verifizieren geschieht durch unveränderbare Regeln, welche im Computercode des Netzwerks festgelegt sind. Diese definieren genau, welche Transaktionen zugelassen sind und welche nicht. Jeder Nutzer, der die Kopie der Blockchain herunterlädt, kann deshalb verifizieren, ob alle Transaktionen den Regeln entsprechen. Verstösst eine Transaktion gegen die Regeln, ist sie also falsch oder betrügerisch, wird sie von den Netzwerkteilnehmern (Full Nodes) abgestossen und nicht in die Transaktionshistorie aufgenommen.

Proof-of-Work (PoW) Mining

Darüber hinaus verfügt das Bitcoin-Netzwerk über einen Mechanismus, um das Anhängen neuer Blöcke zu beschränken. Könnten neue Transaktionen und Blöcke von jedermann an die Blockchain angehängt werden,



Die Kopfzeile, das Resultat der Hashfunktion des vorangehenden Blockes, alle Transaktionen des aktuellen Blockes sowie die Nonce (willkürliche Zahl) werden in eine mathematische Hash-Funktion geben. Die Nonce wird dabei so lange geändert, bis das Resultat der Funktion genügend vorangehende Nullen hat. Dieser Prozess wird Mining genannt.

könnte es leicht zu einer Überlastung des Netzwerks kommen, da sich die Blockchain weltweit nicht schnell genug auf den gleichen Stand bringen kann.

Um das zu verhindern, arbeitet Bitcoin mit einem Proof-of-Work Mechanismus. Damit jemand einen neuen Block an die Blockchain anhängen darf, muss er einen Arbeitsnachweis erbringen. Ein treffender Vergleich ist die Suche nach Nadeln in einem Heuhaufen. Nur wer eine Nadel gefunden hat, darf einen neuen Block an die Blockchain anhängen und wird dafür mit neuen Bitcoin-Einheiten sowie den im Block enthaltenen Transaktionsgebühren belohnt.

Mathematisch gesehen handelt es sich hierbei um das Ausführen einer Hashfunktion (SHA-256 Hash-Algorithmus). Die Hashzahl des vorherigen Blockes, die Transaktionen des aktuellen Blockes sowie eine zufällige Zahl (Nonce) werden zusammen verhasht. Die Nonce wird so lange verändert, bis die Hashfunktion ein Resultat mit einer Mindestanzahl an führenden Nullen ausspuckt. Der Block #700000, erstellt am 11. September 2021, hatte zum Beispiel die gültige Hashzahl: 000000000000000000590fc0f3eba193a27853422 0b2b37e9849e1a770ca959.

Die Suche nach dieser Zahl, auch genannt schürfen oder mining, wird von sogenannten Miner vorgenommen und hat zwei Hauptfunktionen: Sie verknüpft erstens die Blöcke auf mathematisch-kryptografische Weise miteinander, so dass für jeden die Reihenfolge klar nachvollziehbar und prüfbar ist. Gleichzeitig ist es nahezu unmöglich, diese Reihenfolge im Nachhinein zu verändern. Zweitens verzögert dieser Mechanismus das Hinzufügen neuer Blöcke, so dass im Durchschnitt nur alle 10 Minuten ein neuer Block an die Blockchain angehängt wird. Somit wird allen Netzwerkteilnehmern weltweit genügend Zeit gegeben, sich auf den gleichen, neusten Stand zu bringen.

Zusammengefasst kann mal sagen: Die Miner halten das Bitcoin-Netzwerk am Laufen. Dank ihnen werden immer neue Transaktionen verarbeitet und an die Blockchain angehängt. Die Full-Nodes kontrollieren das Netzwerk und stellen sicher, dass keine betrügerischen Transaktionen in die Blockchain gelangen.

21 Millionen Bitcoin

Obwohl laufend weitere Blöcke an die Bitcoin-Blockchain angehängt werden und die Miner für diese Arbeit mit neuen Bitcoins belohnt werden, ist die Gesamtanzahl an Bitcoin auf 21 Millionen Bitcoin beschränkt. Es wird nie mehr als 21 Millionen Bitcoin geben. Doch waren diese 21 Millionen Münzen nicht von Anfang an im Umlauf. Vielmehr werden sie durch den Bitcoin-Code gemäss eines strikten Emissionsplans freigesetzt. Als Bitcoin lanciert wurde, hat der Code ungefähr alle 10 Minuten 50 neue Bitcoin an die Miner freigegeben. Vier Jahre nach der Lancierung hat sich diese Menge der pro zehn Minuten freigesetzten Bitcoins halbiert. Dieser Vorgang wird als Halving bezeichnet und beschreibt die Tatsache, dass die Blockbelohnung für die Miner alle 4 Jahre um die Hälfte abnimmt. Zurzeit sind bereits knapp 19 Millionen Bitcoin im Umlauf. Die restlichen Bitcoin werden bis im Jahr 2140 geschürft werden. Danach werden die Miner nur noch über die Transaktionsgebühren abgegolten.

Die absolut begrenzte Menge an Bitcoin-Einheiten ist eine der fundamentalen Eigenschaften der Kryptowährung und macht Bitcoin zu einem äusserst knappen Gut. Diese absolute digitale Knappheit ist denn auch eine wichtige Voraussetzung für seine Funktion als Wertaufbewahrungsmittel über lange Zeiträume und ist der Grund, weshalb Bitcoin oftmals also digitales Gold oder Gold 2.0 bezeichnet wird.

Das Resultat: Digitales Eigentum

Betrachtet man alle Eigenschaften des Bitcoin-Netzwerkes zusammen, erkennt man die Bedeutung dieser Erfindung. Das erste Mal in der Geschichte hat man ein digitales Gut vor sich, das es nur in einer limitierten Zahl gibt. Bitcoins können nicht kopiert und nicht vervielfältigt werden.

Dank dieser Einzigartigkeit werden Bitcoins gerne auch als digitale Grundstücke bezeichnet. Denn so wie jedes Stück Land auf dieser Erde einmalig ist und nur einmal existiert, so ist auch jede Bitcoin-Einheit einmalig und existiert nur einmal im digitalen Raum.

Diese Bitcoin-Einheiten können wahrhaftig besessen werden. Nur wer im Besitz des entsprechenden privaten Schlüssels ist, also einer Zahlen- und Buchstabenkombination aus 64 Zeichen, kann über die dazugehörigen Bitcoin bestimmen. Das heisst, ohne diesen privaten Schlüssel können Bitcoin weder gestohlen, noch beschlagnahmt oder blockiert werden. Dies ermöglicht es dem Besitzer, die absolute Kontrolle über die eigenen finanziellen Mittel zu haben, unabhängig davon, ob dieser Millionär, politischer Flüchtling oder ein verfolgter Gläubiger ist. Das erste Mal seit der Erfindung des Computers ist es also möglich, digitales Eigentum wirklich zu besitzen.

WARUM BITCOIN?

Doch warum dieser Hype um Bitcoin? Die Möglichkeit, digitales Eigentum wahrhaftig besitzen zu können, mag revolutionär sein. Aber warum sollte man Bitcoin überhaupt besitzen wollen?

Das Beste aus zwei Welten

In vergangenen Jahrhunderten waren mehrheitlich Edelmetalle und später Bargeld in Form von Münzen und Noten als Zahlungsmittel im Einsatz. Diese Zahlungsmittel hatten den Vorteil, dass sie unabhängig von Drittparteien aufbewahrt und ausgegeben werden konnten. Nicht umsonst pflegte man zu sagen: Bargeld ist gedruckte Freiheit. Der Nachteil des Edelmetalls, aber auch des Bargelds, ist, dass sie in der neuen, digitalen Internetwelt schwer zu gebrauchen sind. Spätestens seit dem Aufkommen des Online-Shoppings haben sich deshalb Kreditkarten in der breiten Bevölkerung etabliert.

Da die Menschen nun aber vermehrt von digitalem Geld auf Bankkonten und Kreditkarten Gebrauch machen, steigen die Gegenparteienrisiken, denen sie ausgesetzt sind. Was, wenn ein Finanzinstitut Insolvenz anmelden muss und die Ersparnisse verloren gehen? Oder wenn, wie im Jahre 2013 auf Zypern geschehen, Bargeldbezüge stark limitiert, Zahlungen ins In-und Ausland blockiert werden und sogar eine Zwangsenteignung auf Sparkonti stattfindet? Oder Bankkunden einem Bekannten kein Geld schicken dürfen, weil er auf Kuba oder im Iran lebt?

Mit dem Umstieg auf digitales Geld, gelagert auf Bankkonten, sind wir in letzter Konsequenz nicht mehr Herr über unser eigenes Geld. Bislang war dieser Umstand allerdings der Preis, den wir zahlen mussten, um an einem digitalisierten Alltag teilnehmen zu können.

Für dieses Dilemma bietet Bitcoin eine Lösung. Als digitales Geld ist es bestens für die Verwendung in der digitalen Sphäre geeignet. Gleichzeitig kann man Bitcoin als digitales Eigentum selbst verwahren, ohne auf die Verwahrung durch Drittparteien (Banken) angewiesen zu sein. Man kann Bitcoin also im wahrsten Sinne des Wortes unter der Matratze lagern, indem man die privaten Schlüssel dort verwahrt, wo es einem am sichersten dünkt.

Bitcoin Genesis Block

Raw Hex Version

```
00000000  01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000010  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000020  00 00 00 00 3B A3 ED FD  7A 7B 12 B2 7A C7 2C 3E  ....;£íýz{.²zÇ,>
00000030  67 76 8F 61 7F C8 1B C3  88 8A 51 32 3A 9F B8 AA  gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040  4B 1E 5E 4A 29 AB 5F 49  FF FF 00 1D 1D AC 2B 7C  K.^J)«_Iÿÿ...¬+|
00000050  01 01 00 00 00 01 00 00  00 00 00 00 00 00 00 00  ................
00000060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000070  00 00 00 00 00 00 FF FF  FF FF 4D 04 FF FF 00 1D  ......ÿÿÿÿM.ÿÿ..
00000080  01 04 45 54 68 65 20 54  69 6D 65 73 20 30 33 2F  ..EThe Times 03/
00000090  4A 61 6E 2F 32 30 30 39  20 43 68 61 6E 63 65 6C  Jan/2009 Chancel
000000A0  6C 6F 72 20 6F 6E 20 62  72 69 6E 6B 20 6F 66 20  lor on brink of
000000B0  73 65 63 6F 6E 64 20 62  61 69 6C 6F 75 74 20 66  second bailout f
000000C0  6F 72 20 62 61 6E 6B 73  FF FF FF FF 01 00 F2 05  or banksÿÿÿÿ..ò.
000000D0  2A 01 00 00 00 43 41 04  67 8A FD B0 FE 55 48 27  *....CA.gŠý°þUH'
000000E0  19 67 F1 A6 71 30 B7 10  5C D6 A8 28 E0 39 09 A6  .gñ¦q0·.\Ö¨(à9.¦
000000F0  79 62 E0 EA 1F 61 DE B6  49 F6 BC 3F 4C EF 38 C4  ybàê.aÞ¶Iö¼?Lï8Ä
00000100  F3 55 04 E5 1E C1 12 DE  5C 38 4D F7 BA 0B 8D 57  óU.å.Á.Þ\8M÷º..W
00000110  8A 4C 70 2B 6B F1 1D 5F  AC 00 00 00 00           ŠLp+kñ._¬....
```

Passender Zeitpunkt

Bitcoin wurde inmitten der weltweiten Finanzkrise von 2008/09 ins Leben gerufen. Auf dem ersten Block der Bitcoin Blockchain – auch Genesis-Block genannt – hat Satoshi Nakamoto denn auch eine klare Botschaft hinterlassen. Dort zitiert er eine Schlagzeile der «The Times»-Zeitung mit den Worten: «Kanzler kurz vor der zweiten Rettungsaktion der Banken».

Mit diesem Akt brachte Satoshi die staatskritische Philosophie der Cypherpunks zum Ausdruck. In der Finanzkrise von 2008 haben die Zentralbanken Unmengen an neuem Geld in Umlauf gebracht, um die Banken zu retten. Indirekt dafür bezahlt haben aber die Sparer, deren Ersparnisse durch die Geldschwemme an Wert verloren. Diese Tatsache bestätigte die Cypherpunks in ihrem Misstrauen gegenüber dem Staat und bekräftige sie in ihrer Überzeugung, dass ein staatlich unabhängiges Geld dringlich gebraucht wurde.

Das gleiche Spiel, nur noch grösserem Ausmass, wiederholte sich seit dem Ausbruch der Covid-19 Pandemie. Allein im Jahr 2020 wurde die US-Geldmenge um 50 Prozent ausgeweitet und auch in anderen Ländern – inklusive der Schweiz – läuft die digitale Druckerpresse konstant. Eine direkte Folge davon sind rekordtiefe Zinsen – in der Schweiz sogar Negativzinsen – und eine starke Inflation von Vermögenswerten.

Absicherung gegen Geldentwertung

Bitcoin wurde daher zum bestmöglichen Zeitpunkt ins Leben gerufen. Noch selten war die Geldthematik aktueller und die Fragezeichen grösser als heute. Mit seinem absolut beschränkten Angebot von 21 Million setzt Bitcoin einen wohltuenden Kontrast zu den endlos wachsenden Bilanzen der Zentralbanken. Sein begrenztes Angebot bietet Schutz vor der Verwässerung des eigenen Kapitals, wie sie über die letzten Jahrzehnte bei allen Währungen weltweit zu beobachten war.

Aufgrund seiner spezifischen Ausgestaltung sollte Bitcoin den Erhalt der Kaufkraft über lange Zeiträume hinweg sicherstellen. Da Bitcoin absolut knapp ist, dürfte es dieser Aufgabe sogar besser gewachsen sein als Gold, das jedes Jahr einen Neuzufluss von 1-2% hat. Darüber hinaus sind auch die Kosten für die Aufbewahrung und den Transport von Bitcoin gegenüber Gold deutlich tiefer, was ebenfalls einen besseren Werterhalt ermöglicht.

Eigentumsschutz

Eine weitere Problematik, welche Bitcoin entschärft, ist der Schutz von Eigentum. Während Gold oder Bargeld meist unter Aufwand von Kosten sicher gelagert werden müssen, um sie vor Diebstahl zu schützen, kann Bitcoin quasi zum

Nullkostentarif verwahrt und transportiert werden. Selbst substanzielle Beträge können mit einem aus zwölf oder vierundzwanzig Wörtern bestehenden Code weltweit überall mitgenommen werden. Einmal auswendig gelernt und physisch vernichtet, kann dieser Code von niemandem mehr gestohlen werden, womit die Vermögenswerte hinter dem Code absolut sicher sind und von seinem Besitzer, falls gewünscht, bis mit ins Grab genommen werden können.

BITCOIN KAUFEN

Um in den Besitz von Bitcoin zu kommen, gibt es grundsätzlich zwei Möglichkeiten. Entweder man wird als Miner tätig oder kauft Bitcoin einer anderen Person ab. Da Mining heutzutage mit Heimgeräten quasi unmöglich geworden ist, bleibt dem Einsteiger nur den Weg des Erwerbs.

Kryptobörsen

Der einfachste Weg Bitcoin zu kaufen, führt über eine Handelsbörse. Diese funktionieren ähnlich wie Aktienhandelsplattformen. Nach dem Eröffnen eines persönlichen Kontos können Schweizer Franken, Euro oder US-Dollar per Banküberweisung oder Kreditkarte überwiesen werden. Ist das Geld auf dem persönlichen Konto bei der Handelsbörse angekommen, können rund um die Uhr an sieben Tagen die Woche Bitcoin mit wenigen Mausklicken zum aktuellen Marktpreise gekauft werden. In Europa können Bitcoin dank der beliebten Bitcoin-Investment-App Relai auch ohne Registrierung, Verifizierung oder vorherige Banküberweisung erworben werden.

Peer-to-peer

Alternativ zu Kryptobörsen kann Bitcoin auch direkt von anderen Marktteilnehmern ohne Einbezug einer Börse über Peer-zu-Peer Plattformen erworben werden. Dies ermöglicht eine grössere Anonymität, da für eine solche Transaktion keine persönlichen Daten hinterlegt werden müssen.

Bitcoin ATMs

Ebenfalls gibt es die Möglichkeit, Bitcoin über Geldautomaten zu

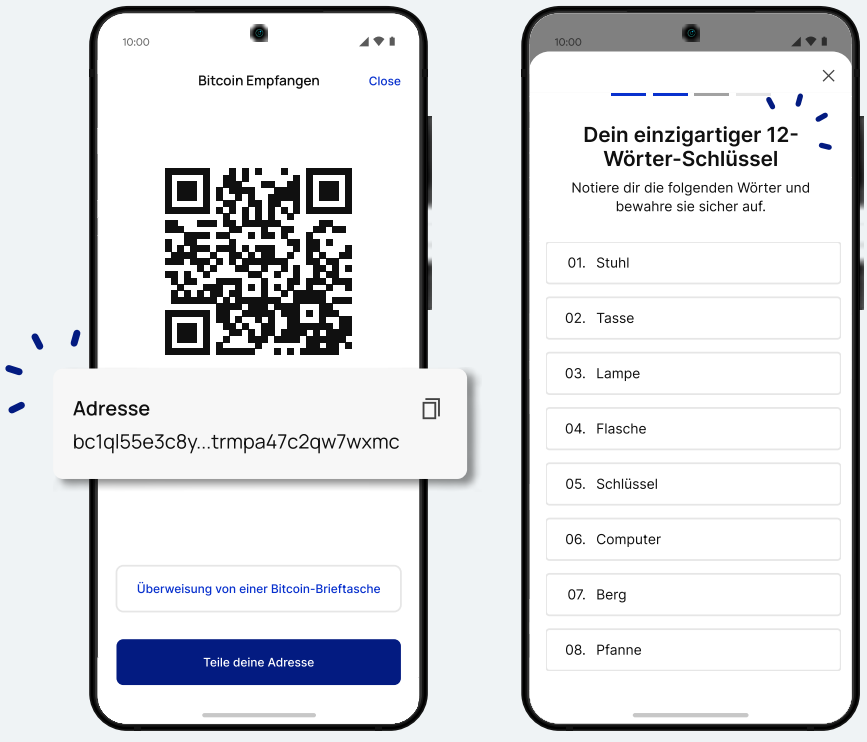
beziehen. Diese sind bereits in vielen Ländern, unter anderem in der Schweiz, Deutschland, and Österreich, zahlreich vorhanden.
An Bitcoin Geldautomaten kann die digitale Währung anonym mit Bargeld oder Kreditkarte bezogen werden. Dazu ist weder ein Konto noch eine Krypto-Wallet notwendig.

Bitcoin sicher verwahren

Sobald Bitcoins erworben wurden, stellt sich die Frage der sicheren Handhabung und Aufbewahrung derselben. Bei Bitcoin und Kryptowährungen im Allgemeinen gilt der Grundsatz: «Not your keys, not your coins», zu Deutsch «nicht deine Schlüssel, nicht dein Geld». Um seine Bitcoin wirklich zu besitzen, muss man im Besitz der entsprechenden privaten Schlüssel sein. Diese etwas technische Ausdrucksweise will sagen, dass man nur dann wirklich die Kontrolle über seine Bitcoin hat, wenn man sie in einer persönlichen digitalen Geldbörse (wallet) lagert, zu der man die privaten Schlüssel besitzt. Solange die Bitcoin auf einer Kryptobörse deponiert sind, sind diese unter der Kontrolle der Börse. Sollte die Börse gehackt werden, bankrottgehen oder betrügerische Absichten verfolgen, könnten die Bitcoin für immer verloren gehen.

Selbstverwahrung

Anders als bei einem Bankkonto hat man bei Bitcoin die Möglichkeit, sein Geldeinheiten auf einer persönlichen Wallet zu lagern. Damit kann man seine eigene Bank sein. Dies hat den Vorteil, dass man die absolute Kontrolle über seine Bitcoin hat. Umgekehrt bringt dies auch Eigenverantwortung mit sich. Der private Schlüssel, welcher oft in Form von zwölf oder vierundzwanzig Wörter daherkommt, muss nämlich vom Inhaber der jeweiligen Bitcoin selber aufbewahrt werden.



Ein Falscher oder fahrlässiger Umgang damit kann zum unwiderruflichen Verlust der Bitcoin führen.

Wallets: Digitale Geldbörsen

Wallets, also digitale Geldbörsen, helfen bei der sicheren Verwahrung der Bitcoin, oder genauer gesagt, der privaten Schlüssel. Die Bitcoin selber befinden sicher nämlich immer auf der Blockchain und können nicht in ein Wallet transferiert werden. Nur die Zugangsschlüssel zu den Bitcoin können in einem Wallet verwahrt werden.

Wallets wurden also dazu geschaffen, die privaten Schlüssel sicher und einfach zu verwahren. Ausserdem ermöglichen sie das Versenden und Empfangen von Bitcoin mit wenigen Klicken. Somit sind Wallets ein nützliches Hilfsmittel für die Handhabung von Bitcoin.

Software Wallet

Die am meisten verbreiteten Wallets sind Software Wallets. Software Wallets können als Desktop-Anwendungen oder als Smartphone-App eingerichtet werden. Beim Aufsetzen werden die privaten Schlüssel zur Wallet in Form von zwölf oder vierundzwanzig Wörtern aufgelistet. Diese Wörter sind synonym mit den Bitcoin in dieser Wallet. Wer diese Wörter kennt, hat die Verfügungsgewalt über die Coins. Die Wörter gilt es deshalb analog, am besten auf Papier, im Geheimen aufzuschreiben und sicher zu verwahren. Sollte das Mobiltelefon einmal verloren gehen, kann mit diesen Worten die Wallet jederzeit wiederhergestellt werden.

Software Wallets haben den Vorteil, dass sie schnell aufgesetzt und einfach in der Handhabung sind. Da Soft Wallets jedoch als Computerprogramme auf einem Gerät installiert und direkt mit dem Internet verbunden sind, besteht grundsätzlich das Risiko von Hackerangriffen.

Hardware Wallet

Wer Wert auf maximale Sicherheit legt, sollte auf ein Hardware Wallet zurückgreifen. Diese kleinen Geräte speichern die Zugangscodes für die Bitcoin auf einem USB-Stick ähnlichen Gerät, welches nur bei Bedarf an den Computer angeschlossen wird. Das Gerät ist so konzipiert, dass selbst ein mit schädlicher Software infizierter Computer nicht auf die Codes zugreifen kann.

Beim Aufsetzen dieser Geräte werden ebenfalls zwölf oder vierundzwanzig Wörter aufgelistet, welche es analog aufzuschreiben und sicher zu verwahren gilt. Sollte die Hardware Wallet einmal verloren gehen, kann diese mit Hilfe der Wörter wiederhergestellt werden. Beispiele für Anbieter von Hardware Wallets sind BitBox und Trezor.

Made in Switzerland

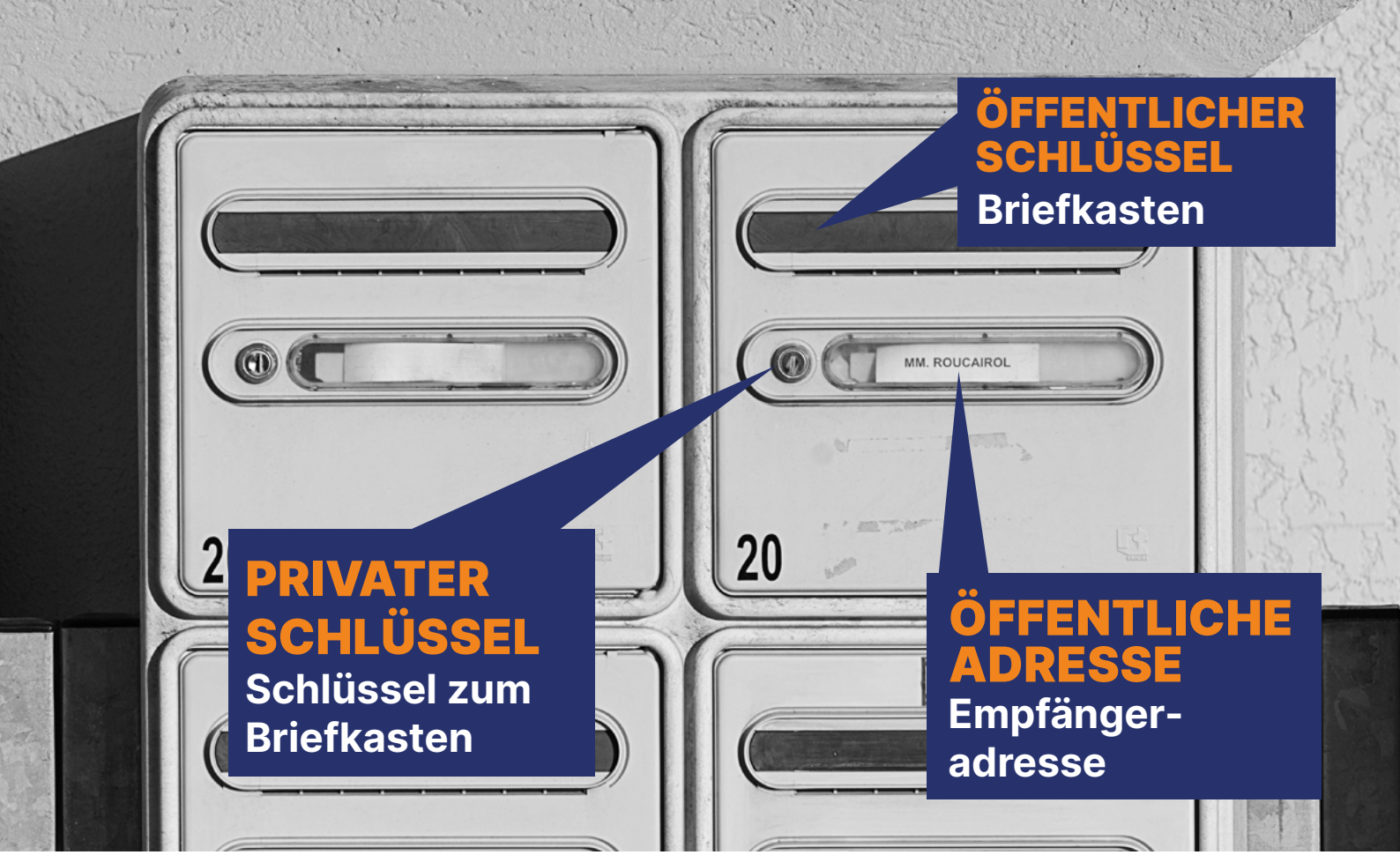
EUROPAS EINFACHSTE BITCOIN APP

Relai

Download on the App Store

GET IT ON Google Play

Kaufen Sie Bitcoin in 1 Minute ab einem Betrag von 10 EUR/CHF ohne Verifizierung.



Bitcoin senden und empfangen

Senden und empfangen von Bitcoin ist kinderleicht. Jede Bitcoin Wallet hat eine eigene öffentliche Adresse, die aus dem sogenannten Public-Key generiert wird. Diese dient ähnlich einer IBAN-Nummer als Empfangsadresse. Jeder, der diese Adresse hat, kann Bitcoin an die entsprechende Wallet senden. Die Adresse wird oftmals auch als QR-Code dargestellt, was die Handhabung vereinfacht.

Möchte man jemandem Bitcoin senden, kann in der persönlichen Wallet unter 'senden' entweder die Bitcoin-Adresse des Empfängers eingetragen oder aber der entsprechende QR-Code gescannt werden. Die anfallenden Transaktionsgebühren werden automatisch von der Wallet des Senders abgezogen. Die Höhe der Transaktionsgebühren variiert dabei je nach Auslastung des Netzwerks und kann hier nachgeschaut werden. Bis die Überweisung beim Empfänger eintrifft, dauert es im Durchschnitt 10 Minuten. Es kann aber auch länger dauern, abhängig von der Höhe der Transaktionsgebühren, die man zu zahlen bereit ist.

Mit Bitcoin zahlen

Beim Aufkommen von Bitcoin hatte man die Hoffnung, dass Bitcoin eines Tages für das Zahlen alltäglicher Dinge verwendet werden kann. Und grundsätzlich ist dies heute möglich. Einzelne Steuerämter, gemeinnützige Organisation und Firmen akzeptieren Bitcoin als Zahlungsmittel. Da Transaktionen über das Bitcoin-Netzwerk heute aber mehrere

Franken kosten können und mindestens 10 Minuten brauchen, macht dies nur für grössere Beträge Sinn. Um Bitcoin günstig und schnell zu versenden, braucht es deshalb eine alternative Lösung.

Lightning Netzwerk - schneller und günstiger

Deshalb wurde auf das Bitcoin-Netzwerk ein zusätzliches Netzwerk gebaut. Dieses Netzwerk mit Namen Lightning ermöglicht das Zahlen mit Bitcoin in Sekundenschnelle zu minimalen Kosten. In Ländern wie El Salavdor ist das Lightning-Netzwerk bereits rege und erfolgreich in Gebrauch.

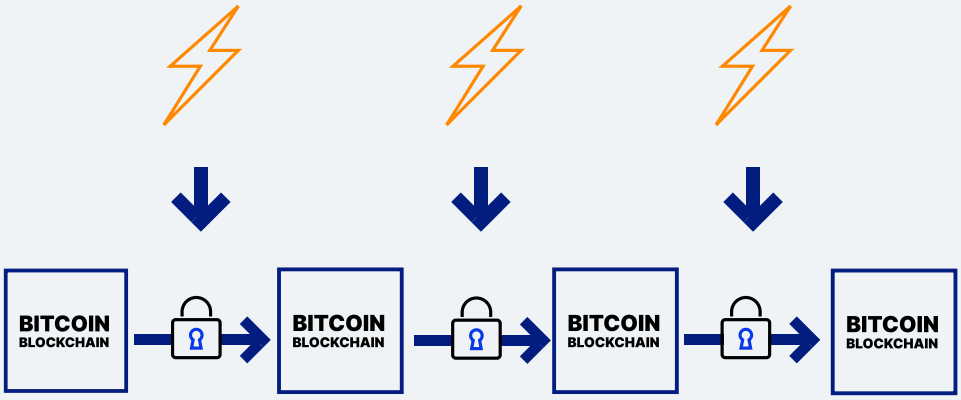
Das Bezahlen von alltäglichen Gütern mit Bitcoin wird deshalb in Zukunft zum grössten Teil über das Lightning-Netzwerk vonstattengehen. Die Entwicklungen in diesem Bereich laufen denn auch auf Hochtouren. So hat zum Beispiel Twitter kürzlich eine 'Trinkgeld'-Funktion eingeführt, welche ebenfalls über das Lightning-Netzwerk funktioniert. Weiter bietet die App Strike weltweite Zahlungen in verschiedenen Währungen zum Nullkostentarif über das Lightning Netzwerk an. Zu erwarten ist deshalb, dass in Zukunft nur noch grössere Beträge direkt über das Bitcoin-Netzwerk abgewickelt werden, während alle anderen Transaktionen über das Lightning Netzwerk laufen.

Da im Lightning Netzwerk oftmals kleinere Beträge versandt werden, wird nicht primär Bitcoin als Einheit verwendet, sondern Satoshis, kurz Sats. 1 Bitcoin ist dabei gleich 100'000'000 Sats. Für das Benutzen des Lightning-Netzwerks muss eine Lightning-Wallet eingerichtet werden.

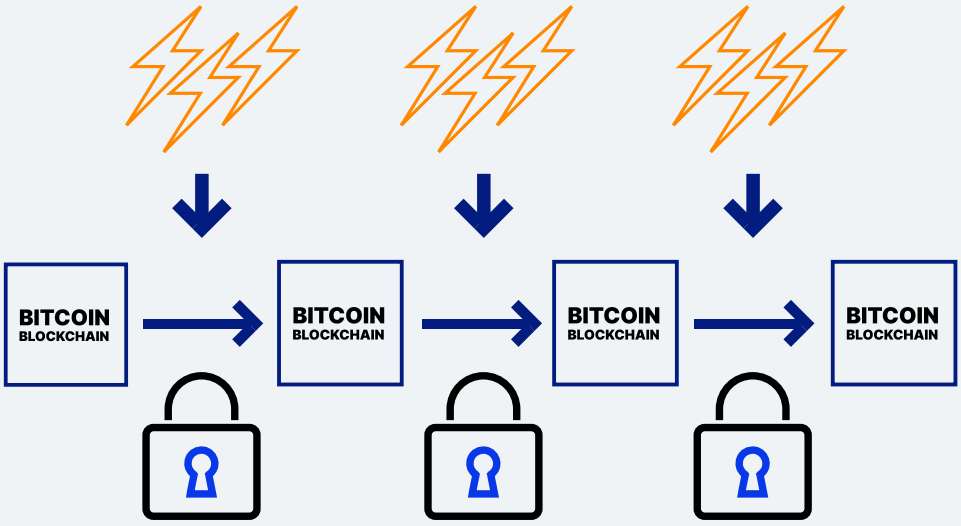
EIN BLICK IN DIE ZUKUNFT

In seinem über zehnjährigen Bestehen hat Bitcoin viel bewegt und durchlebt. Mehrmals wurde die digitale Währung totgesagt oder geriet nach starken Kursverlusten in der breiten Öffentlichkeit in Vergessenheit. Bitcoin aber hat sich unaufhaltsam um den Globus verbreitet.

Je weniger Energie in Form von Rechenleistung in die Produktion der Bitcoin Blockchain fliesst, desto einfach kann diese im Nachhinein verändert werden.



Je mehr Energie in Form von Rechenleistung in die Herstellung der Bitcoin Blockchain fliesst, desto schwieriger wird es, diese im Nachhinein zu verändern.



Bitcoin und Energie

Einer der ersten Fragen, die bezüglich der Entwicklung von Bitcoin immer wieder aufgeworfen wird, ist der Energieverbrauch des Bitcoin-Netzwerks. Das Bitcoin-Mining beansprucht bereits heute weltweite eine grosse Menge an Strom. Und dieser Verbrauch dürfte in Zukunft noch weiter ansteigen, wenn mehr Leute ins Bitcoin-Mining einsteigen.

Hierbei ist es wichtig zu verstehen, dass die Menge an Energie, welche ins Bitcoin-Netzwerk fliesst, entscheidend für die Sicherheit des Netzwerks ist. Je mehr Energie ins Netzwerk fliesst, desto sicherer ist es. Denn damit die Bitcoin-Blockchain im Nachhinein verändert werden kann, muss die gleiche Menge an Rechenleistung - und damit an Energie - aufgewendet werden, die bereits für die Herstellung der Blockchain investiert wurde. Da aber weltweit Millionen von Computern dem Bitcoin-Netzwerk Rechenleistung zur Verfügung stellen, ist es als einzelne Person, Organisation oder als Staat beinahe unmöglich, jemals genügend Rechenleistung aufzubringen, um auch nur kleinste Änderungen an der Blockchain vornehmen zu

können. Deshalb ist die Rechenleistung (English: Hashpower) und der damit verbundene Energieverbrauch ein wichtiges Sicherheitsmerkmal des Bitcoin-Netzwerks.

Des Weiteren haben Bitcoin-Mining Computer den Vorteil, dass sie überall auf der Welt aufgestellt werden können. Da Miner möglichst günstigen Strom benötigen, um profitabel zu sein, siedeln sie sich oft an Orten an, wo viel überschüssige und damit günstige Energie vorhanden ist. Längerfristig dürfte dies vor allem an Orten sein, wo viel erneuerbare Energiequellen vorhanden sind, da diese den günstigsten Strom produzieren.

Laut dem Bitcoin Mining Council benutzen Bitcoin-Miner derzeit ca. 56 % erneuerbare Energie und die Tendenz ist steigend. Viele Bitcoin Experten sind der Meinung, dass Bitcoin-Mining in Zukunft mit bis zu 100 % erneuerbarer Energie angetrieben werden wird.

Bis das der Fall ist, läuft Bitcoins Energieverbrauch aber auf die Frage hinaus, ob ein sicheres und unverfälschliches Geld und Wertaufbewahrungsmittel diesen Energieaufwand wert ist - oder eben nicht.

El Salvador -
Bitcoin als Landeswährung

Bereits vor einigen Jahren hielten es Visionäre für möglich, dass Bitcoin dereinst von Nationalstaaten als gesetzliches Zahlungsmittel anerkannt werden würde. Im Sommer 2021 war es dann soweit: El Salvador führte Bitcoin als erstes Land weltweit als gesetzliches Zahlungsmittel ein. In Läden, Restaurants und bei Dienstleistern aller Art kann nicht mehr nur mit US-Dollar bezahlt werden, sondern auch mit Bitcoin. Den Bewohner wurde hierzu eine Bitcoin-Wallet zur Verfügung gestellt, welche Zahlungen über das Lightning-Netzwerk in Sekundenschnelle und zu minimalen Kosten ermöglicht.

Weitere Länder wie die Ukraine, Brasilien oder Panama diskutieren zurzeit ähnliche Gesetzesentwürfe. Sollten noch andere Länder dem Beispiel von El Salvador folgen, würde dies einerseits die Nachfrage nach Bitcoin weiter erhöhen, andererseits aber vor allem dessen Glaubwürdigkeit als ‘Geld’ untermauern. Die Akzeptanz von Bitcoin als gesetzlichem Zahlungsmittel in immer mehr Ländern stellt deshalb eine entscheidende Phase im weltweiten Adaptionsprozess von Bitcoin dar.

Gesetze und Vorschriften

Dies führte dazu, dass sich Staaten, Zentralbanken und Firmen intensiv mit Kryptowährungen auseinandersetzten müssen. Diverse Staaten, darunter die Schweiz, haben erste Vorschriften und Richtlinien bezüglich

Kryptowährungen erlassen. Dieser Schritt wird von vielen Marktteilnehmern begrüsst, da er sowohl für Kryptoprojekte als auch für involvierte Firmen Rechtssicherheit schafft.

Auch in den USA, welche bisher eher einen Laissez-faire Ansatz verfolgte, zeichnen sich Regulierungen ab. Die genauen Ausgestaltungen dieser werden von der weltweiten Kryptogemeinschaft genauestens verfolgt, da diese grosse Auswirkungen auf den gesamten Kryptobereich haben werden.

Andere Kryptowährungen

Bitcoin ist heutzutage bei weitem nicht mehr die einzige Kryptowährung. Mittlerweile gibt ca. über 21'000 verschiedene Kryptowährungen und -werte. Diese Währungen habe alle verschiedenen Eigenschaften und Funktionsweisen und sind lange nicht alle als 'Währungen' oder Geld konzipiert worden. Einige gleichen mehr Aktien, da ihr Wert den Erfolg eines Kryptoprojektes widerspiegelt. Andere braucht man, um einen bestimmten Dienst oder Service in Anspruch zu nehmen. Und wieder andere - sogenannte Meme-Tokens – sind vor allem Spasswährungen.

Um Verluste zu vermeiden, empfiehlt es sich deshalb, sich vor einer allfälligen Investition genauer mit der jeweiligen Währung und dem dahinterstehenden Projekt auseinanderzusetzen.

Digitale Währungen von Zentralbanken (CBDC)

Kryptowährungen befinden sich im Übergang von der anfänglich unregulierten Wild West Phase hin zu einer regulierten, geordneteren Kryptofinanzwelt. Diese Entwicklung ist auch an den Zentralbanken nicht spurlos vorüber gegangen und Ideen wurden laut, dass Zentralbanken ihre eigenen Kryptowährungen herausgeben sollten. Diese «Central Bank Digital Currencies», kurz CBDCs, würden, so die Befürworter, die Stabilität einer staatlichen Währung mit den Vorteilen einer blockchain-basierten Währung verbinden. Kurz, man würde sozusagen digitales Bargeld schaffen.

Je nach Ausgestaltung kann eine CBDC aber grundlegend verschiedene Züge annehmen. Diverse Länder haben Pilotversuche mit unterschiedlichen Arten von CBDCs gestartet und in einigen wenigen Ländern wurden bereits CBDCs lanciert. Mit Spannung erwartet wird aber, ob und in welcher Form wirtschaftsstarke Währungsräume wie die USA, EU oder China ihre CBDCs lancieren werden.

Geldwettbewerb

Unsere Gesellschaft hat sich in den vergangenen Jahrzehnten so stark an staatliche Währungen gewöhnt, dass andere Arten von Geld bis vor kurzem für Viele kaum vorstellbar waren.

Doch vor noch nicht allzu langer Zeit gehörte es zum Alltag, dass verschiedene Geldarten parallel im Umlauf waren. Da gab es Banknoten von verschiedensten Banken, Münzen aus unterschiedlichen Edelmetallen und andere geldige Werte, welche als Zahlungsmittel gebraucht werden konnten.

Mit Bitcoin steht nun wieder nichtstaatliche Währunge als Alternative zur Verfügung. Diese wurde von staatlicher Seite bisher mehrheitlich geduldet, auch dank ihrer Dezentralität, welche diese Währung nur schwer angreifbar macht. Für Bürger bedeutet dies, dass nun neben Gold und Silber auch eine digitale Alternative zu staatlichem Geld zur Verfügung steht. Die Auswirkungen dieser zusätzlichen Geldkonkurrenz dürfte in der Zukunft spannend zu beobachten sein.

BITCOIN, WAS NUN?

Wenn Du dich nun fragst, was du nun mit all den Informationen anstellen solltest, dann lass mich dir einen Vorschlag unterbreiten. In die Welt von Bitcoin einzusteigen kostet quasi nichts, weder Zeit noch Geld. Dafür aber lernst du eine Technologie kennen, die gerade dabei ist, unsere Welt und deren Zukunft zu verändern.

Deshalb: Lade auf deinem Mobiltelefon eine Wallet herunter und kaufe einmalig Bitcoin für 50 CHF. Oder lass dir von einem Kollegen Bitcoin auf deine persönliche Wallet schicken. Aber komm zumindest einmal in Berührung mit Bitcoin. Danach musst du die Wallet meinetwegen nie mehr anrühren, versprochen.

Denn sollte Bitcoin den Durchbruch schaffen und so allgegenwärtig werden wie das Internet, weisst du nach diesem Booklet nicht nur theoretisch Bescheid, sondern hast Bitcoin auch selbst einmal genutzt. Dieses praktische Wissen wird dir helfen, dich schneller in der neuen Welt der digitalen Währungen zurechtzufinden.

ABOUT

THE AUTHOR

Daniel Jungen ist Ökonom und Finanzjournalist mit Schwerpunkt Kryptoassets. Daniel ist Mitgründer von InsightDeFi, einer Research Boutique spezialisiert auf Kryptothemen. Zusammen mit seinen Partnern von InsightDeFi publiziert er alle zwei Wochen den gleichnamigen deutschen Newsletter InsightDefi, welcher den Lesern Einblicke in aktuelle Themen rund um Bitcoin, DeFi und Krypto bietet.

RELAI

Relai wurde von Julian Liniger und Adem Bilican in der Schweiz gegründet, weil die beiden Gründer Schwierigkeiten hatten, einen sicheren und unkomplizierten Ort für den Kauf von Bitcoin zu finden. Dank Relai ist das Sparen und Investieren in Bitcoin nun für jeden zugänglich. Die Bitcoin-App ist einfach und intuitiv gestaltet und ermöglicht es jedem in Europa, innerhalb weniger Minuten Bitcoin zu kaufen und zu verkaufen, ohne dass eine Registrierung, Verifizierung oder Banküberweisung erforderlich ist. Unabhängig geprüft und mit über CHF 35 Millionen Bitcoin, die bereits über die Plattform investiert wurden, bietet Relai seinen Kunden die Möglichkeit, neue Wege des Sparens und Investierens zu erschließen.

Erfahre mehr unter Relai.app.

This booklet is also available in English.