30. Januar 2025

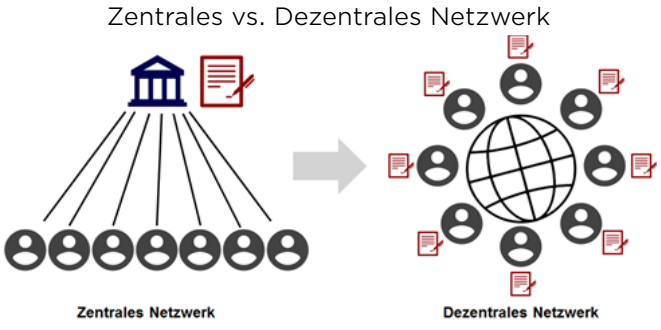
Bitcoin verstehen (Teil I/II): Die Technologie hinter der digitalen Währung

Vor knapp 16 Jahren kam mit Bitcoin die weltweit erste Kryptowährung auf den Markt. Seitdem gleicht der Aufstieg von Bitcoin einer beispiellosen Entwicklung. Der erstmalige Durchbruch der 100.000-Dollar-Marke beim Bitcoin-Kurs Anfang Dezember symbolisiert mehr als nur einen Preisanstieg er steht für einen grundlegenden Wandel der dezentralen Finanzarchitektur und die zunehmende Akzeptanz von Kryptowährungen im Mainstream-Finanzsektor.

Vor diesem Hintergrund stellt sich die Frage, wie Bitcoin genau funktioniert, welche technologischen Mechanismen seinem Wertzuwachs zugrunde liegen und welche ökonomischen Prinzipien für die Preisbildung ausschlaggebend sind. Mit unserer zweiteiligen Miniserie, die in die Welt von Bitcoin eintaucht, versuchen wir auf diese Fragen eine passende Antwort zu finden. In diesem ersten Teil unserer Dilogie erkunden wir die Grundlagen von Bitcoin. Wir beleuchten die Grundidee und innovative Technologie hinter der Kryptowährung und erklären, was Bitcoin eigentlich ist. Aufbauend auf dieser Grundlage widmen wir uns im zweiten Teil der Wertbestimmung von Bitcoin und untersuchen, anhand welcher Kriterien und Faktoren eine Bewertung der Kryptowährung erfolgen kann.

Die Grundidee von Bitcoin

Das Bitcoin-Netzwerk ist ein digitales, sogenanntes Peer-to-Peer-Zahlungssystem, das am 31. Oktober 2008 durch ein Whitepaper von Satoshi Nakamoto vorgestellt wurde. Die Grundidee besteht darin, ein dezentrales digitales Zahlungssystem zu schaffen, das ohne vertrauenswürdige Intermediäre wie Banken funktioniert. Die Idee entstand während der Finanzkrise, als das Vertrauen in traditionelle Finanzinstitutionen erschüttert war. Bitcoin nutzt Kryptographie, um anonyme und zensurresistente Transaktionen zu ermöglichen. Dabei liegt die wahre Innovation nicht in der digitalen oder virtuellen Natur von Bitcoin, sondern in seiner Fähigkeit, sichere Transaktionen ohne einen zentralen Finanzintermediär durchzuführen.



Quelle: Eigene Darstellung

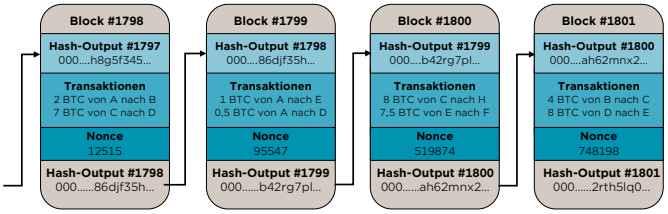
Das Transaktionsbuch, in dem Kontostände und Transaktionen verzeichnet werden, ist im dezentralen Fall nicht mehr bei einer sicheren Bank hinterlegt, sondern muss für jeden Teilnehmer zugänglich, einsehbar und mitgestaltbar sein. Jedoch muss auch gleichzeitig sichergestellt werden, dass das Transaktionsbuch bei jedem Teilnehmer identisch ist. Es muss also ein Konsens zwischen vielen sich unbekannten Netzwerkteilnehmern gefunden werden, die sich möglicherweise nicht vertrauen. Die Entwickler von Bitcoin haben mit der Blockchain als Konsensus-Protokoll erstmals eine Lösung für dieses Problem gefunden.

Blockchain: Das digitale Fundament der Bitcoin-Technologie

Doch was ist überhaupt eine Blockchain? Einfach ausgedrückt ist die Blockchain eine öffentliche, verteilte Datenbank, die alle Transaktionen im Netzwerk überprüft und aufzeichnet. Wie der Name schon sagt, besteht sie aus einer Kette von Blöcken.

Im Falle von Bitcoin enthalten diese Blöcke Transaktionsdaten mit Informationen darüber, wer an wen wie viele Bitcoins gezahlt hat. Dabei initiiert ein Nutzer eine Bitcoin-Überweisung durch die Signierung einer Transaktion mittels seines privaten Schlüssels. Diese signierte Transaktion wird dann im Bitcoin-Netzwerk verbreitet, das von sogenannten ***Minern*** betrieben wird. Diese Miner arbeiten daran, Transaktionen zu überprüfen und in Blöcken auf der Blockchain zu speichern. Dabei wird jede Transaktion auf ihre Gültigkeit überprüft und sichergestellt, dass sie den Regeln des Bitcoin-Netzwerks entspricht. Sobald eine Transaktion bestätigt wurde, wird sie in einen Block, zusammen mit weiteren aktuellen Transaktionen, an die Blockchain angehängt. Jeder Block enthält eine Reihe von Transaktionsdaten einen sogenannten ***Hash-Wert*** des vorherigen Blocks und eine ***Nonce***. Ein Hash-Wert ist eine Zeichenfolge, die als digitaler Fingerabdruck interpretiert werden kann und die Nonce (Abkürzung für "number used once") ist eine beliebige Zahlenkombination, die nur ein einziges Mal in ihrem jeweiligen Kontext verwendet wird. Allen Teilnehmern des Netzwerkes sind die Transaktionsdaten sowie der Hashwert der vorherigen Blocks bekannt, nur die Nonce ist variabel.

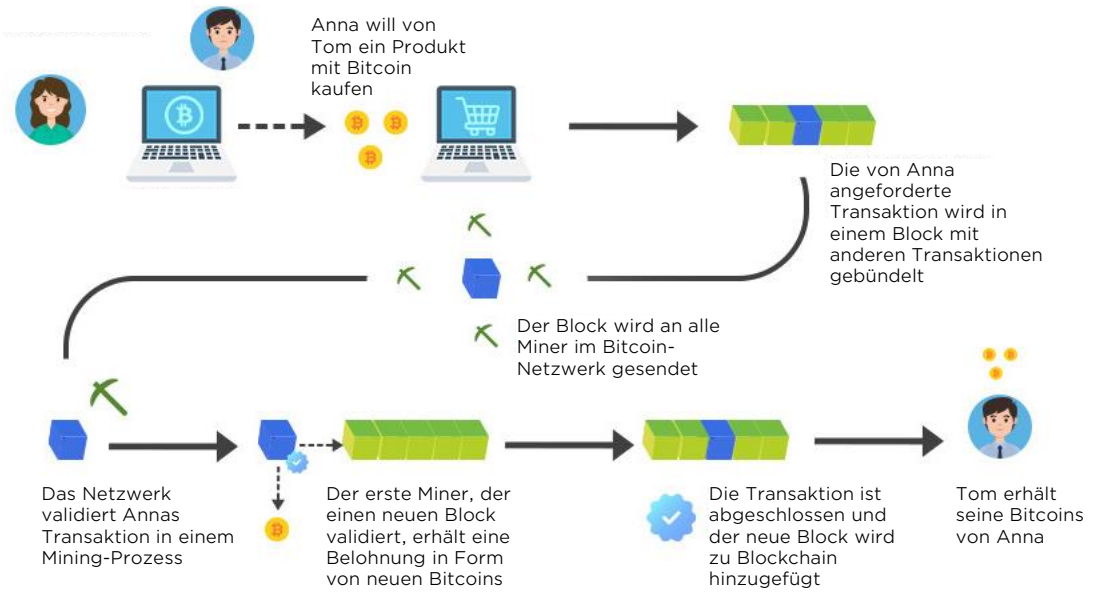
Vereinfachte Illustration der Bitcoin-Blockchain



Quelle: Eigene Darstellung in Anlehnung an Deutsche Bundesbank, 2021

Um den nächsten Block zu erzeugen, muss ein neuer Hash-Wert gefunden werden, der kleiner als ein vorgegebener Zielwert ist. Um dieses komplexe mathematische Rätsel zu lösen, wird die Nonce so lange variiert, bis die richtige Lösung gefunden ist. Da nur der Miner entlohnt wird, der als Erstes diese Aufgabe löst, steigert eine höhere Rechenleistung die Chancen auf Erfolg. Dieses bewusst rechenintensive Verfahren wird als ***Mining*** bezeichnet. Sobald eine gültige Lösung gefunden worden ist verifizieren die anderen Teilnehmer die Gültigkeit des Blocks und der darin enthaltenen Transaktionen. Nach erfolgreicher Validierung wird der Block von den Teilnehmern akzeptiert und der Blockchain hinzugefügt. Die enthaltenen Transaktionen gelten nun als bestätigt.

Funktionsweise einer Bitcoin-Transaktion



Quelle: Eigene Darstellung in Anlehnung an geeksforgeeks

Dieser ***Proof-of-Work-Mechanismus*** (das Vorweisen einer Lösung gilt als Nachweis dafür, dass Rechenleistung investiert worden ist) gewährleistet nicht nur die Verarbeitung der Transaktionen, sondern auch die Sicherheit und Integrität des Bitcoin-Netzwerks. Dieser Zyklus wiederholt sich durchschnittlich alle zehn Minuten, wobei die Schwierigkeit des Mining-Prozesses regelmäßig adjustiert wird, um diese Zeitspanne konstant zu halten. Der erfolgreiche Miner erhält als Anreiz für seine Rechenleistung pro Block eine Belohnung in Form neu ausgegebener Bitcoins sowie die akkumulierten Transaktionsgebühren des Blocks.

Derzeit beträgt diese Belohnung 3,125 Bitcoins pro Block, aber sie wird alle 210.000 Blöcke halbiert, was etwa alle vier Jahre geschieht. Das letzte sogenannte ***Halving*** fand am 20. April 2024 statt und ist ein programmierter Mechanismus, der in festgelegten Intervallen auftritt und mehrere technische Ziele verfolgt. Primär dient es der Inflationskontrolle, indem die Rate, mit der neue Bitcoins generiert werden, halbiert wird. Dies verstärkt die Knappheit von Bitcoin und festigt seine Position als digitales Gut, denn die Gesamtmenge der insgesamt verfügbaren Bitcoins konvergiert durch die regelmäßigen Halvings zur Maximalmenge von 21 Millionen Stück. Darüber hinaus sorgt das Halving für ein transparentes und vorhersehbares Angebotswachstum und schafft Anreize für die Miner, ihre Effizienz zu steigern und in fortschrittliche Technologien zu investieren.

Die Entwicklung von Bitcoin zeigt eindrucksvoll, dass es sich nicht mehr um eine Nische handelt und Kryptowährungen zunehmend im Mainstream angekommen sind. Wie der Wert hinter dem Bitcoin zu beurteilen ist und ob Kryptowährungen mittlerweile als eigene Anlageklasse zu betrachten sind, untersuchen wir in der kommenden Ausgabe von Konjunktur und Strategie. Eines ist jedoch sicher: Die Technologie hinter Bitcoin ist kein vorübergehender Trend und wird bleiben!

Tilman Deißinger, Sebastian Kuhnert, Jan Mooren

Überblick über Marktdaten

	Stand	Veränderung zum				
	30.01.2025	23.01.2025	27.12.2024	29.10.2024	29.01.2024	31.12.2024
Aktienmärkte	11:57	-1 Woche	-1 Monat	-3 Monate	-12 Monate	YTD
Dow Jones	44714	0,3%	4,0%	5,9%	16,6%	5,1%
S&P 500	6091	-0,5%	2,0%	4,4%	23,6%	3,6%
Nasdaq	19632	-2,1%	-0,5%	4,9%	25,6%	1,7%
Russell 2000	2283	-1,4%	1,7%	2,0%	13,5%	2,4%
DAX	21709	1,4%	8,6%	11,5%	28,1%	9,0%
MDAX	26617	2,6%	3,5%	-1,6%	2,0%	4,0%
TecDAX	3708	1,4%	7,4%	8,6%	10,9%	8,5%
EuroStoxx 50	5267	0,9%	7,5%	6,4%	13,5%	7,6%
Stoxx 50	4578	1,3%	6,3%	3,4%	8,7%	6,2%
Nikkei 225	39514	-1,1%	-1,9%	1,6%	9,7%	-1,0%
MSCI Welt	3828	-0,7%	1,9%	3,0%	18,3%	3,3%
MSCI Welt SRI	3516	-3,6%	-1,0%	-0,6%	11,5%	0,4%
MSCI Emerging Markets	1092	1,0%	0,9%	-3,9%	10,3%	1,6%
Zinsen und Rentenmärkte						
Bund-Future	131,34	-22	-168	-117	-365	-210
Bobl-Future	116,99	12	-66	-177	-110	-87
Schatz-Future	106,62	3	-34	-21	54	-37
3 Monats Euribor	2,61	-6	-7	-44	-130	-10
3M Euribor Future, Dez 2025	2,16	5	24	-59	-31	26
3 Monats $ Libor	4,31	-5	0	-39	-111	-6
Fed Funds Future, Dez 2025	3,86	-8	-9	-64	-20	-5
10-jährige US Treasuries	4,50	-14	-12	24	43	-7
10-jährige Bunds	2,52	0	13	18	31	15
10-jährige Staatsanl. Japan	1,21	3	12	27	52	13
10-jährige Staatsanl. Schweiz	0,43	0	14	-4	-47	15
IBOXX AA, €	3,13	1	8	11	-8	9
IBOXX BBB, €	3,57	1	10	8	-28	11
ML US High Yield	7,40	-2	-21	0	-48	-25
Rohstoffmärkte						
Rohöl Brent	76,41	-2,6%	3,2%	7,6%	-7,6%	2,2%
Gold	2777,79	1,1%	6,2%	0,4%	37,1%	5,8%
Silber	30,81	1,6%	3,8%	-10,1%	33,4%	3,8%
Kupfer	8943,80	-1,9%	0,8%	-4,7%	5,8%	3,4%
Eisenerz	101,33	0,0%	-2,5%	-2,7%	-25,2%	-2,2%
Frachtraten Baltic Dry Index	726	-11,9%	-27,2%	-48,2%	-50,3%	-27,2%
Devisenmärkte						
EUR/ USD	1,0400	0,0%	-0,3%	-3,5%	-3,9%	0,1%
EUR/ GBP	0,8368	-0,8%	1,0%	0,8%	-1,7%	1,2%
EUR/ JPY	160,62	-1,2%	-2,4%	-3,0%	0,3%	-1,5%
EUR/ CHF	0,9438	0,0%	0,4%	0,7%	1,1%	0,3%

Quelle: Refinitiv Datastream

Carsten Klude
+49 40 3282-2572
cklude@mmwarburg.com

Dr. Rebekka Haller
+49 40 3282-2452
rhaller@mmwarburg.com

Martin Hasse
+49 40 3282-2411
mhasse@mmwarburg.com

Dr. Christian Jasperneite
+49 40 3282-2439
cjasperneite@mmwarburg.com

Simon Landt
+49 40 3282-2401
mlandt@mmwarburg.com

Jan Mooren
+49 40 3282-2992
jmooren@mmwarburg.com