M.M.WARBURG & CO
BANK

Economic Situation and Strategy

23 January 2025

Understanding Bitcoin (Part I/II): The technology behind the digital currency

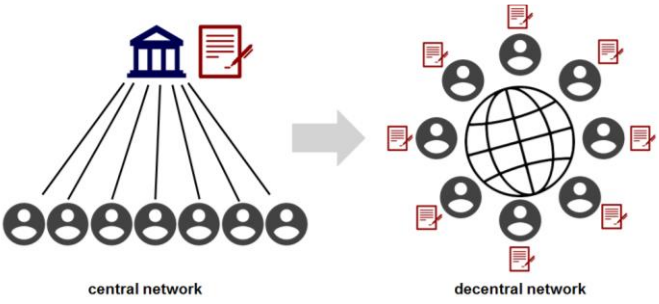
Bitcoin, the world's first cryptocurrency, came onto the market almost 16 years ago. Since then, the rise of Bitcoin has resembled an unprecedented development. The first breakthrough of the 100,000 dollar mark in the Bitcoin price at the beginning of December symbolizes more than just a price increase ¬ it stands for a fundamental change in the decentralized financial architecture and the increasing acceptance of cryptocurrencies in the mainstream financial sector.

Against this backdrop, the question arises as to how exactly Bitcoin works, what technological mechanisms underlie its increase in value and what economic principles are decisive for price formation. In our two-part mini-series, which delves into the world of Bitcoin, we try to find an appropriate answer to these questions. In this first part of our mini-series, we explore the basics of Bitcoin. We shed light on the basic idea and innovative technology behind the cryptocurrency and explain what Bitcoin actually is. Building on this foundation, in the second part we look at the valuation of Bitcoin and examine the criteria and factors that can be used to value the cryptocurrency.

The basic idea behind Bitcoin

The Bitcoin network is a digital, so-called peer-to-peer payment system that was introduced on October 31, 2008 in a white paper by Satoshi Nakamoto. The basic idea is to create a decentralized digital payment system that works without trustworthy intermediaries such as banks. The idea was born during the financial crisis, when trust in traditional financial institutions was shaken. Bitcoin uses crypto-graphy to enable anonymous and censorship-resistant transactions. The true innovation lies not in the digital or virtual nature of Bitcoin, but in its ability to conduct secure transactions without a central financial intermediary.

Centralized vs. decentralized network



Source: Own illustration

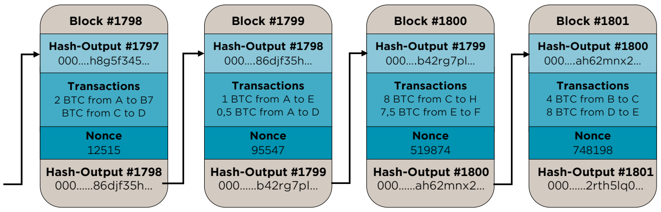
In the decentralized case, the transaction ledger, in which account balances and transactions are recorded, is no longer stored at a secure bank, but must be accessible, viewable and configurable for every participant. However, it must also be ensured that the transaction ledger is identical for every participant. A consensus must therefore be found between many unknown network participants who may not trust each other. The developers of Bitcoin have found a solution to this problem for the first time with the blockchain as a consensus protocol.

Blockchain: the digital foundation of Bitcoin technology

But what is a blockchain anyway? Put simply, a blockchain is a public, distributed database that checks and records all transactions in the network. As the name suggests, it consists of a chain of blocks.

In the case of Bitcoin, these blocks contain transaction data with information about who paid how many Bitcoins to whom. A user initiates a Bitcoin transfer by signing a transaction using their private key. This signed transaction is then distributed in the Bitcoin network, which is operated by so-called miners. These miners work to verify transactions and store them in blocks on the blockchain. This involves checking the validity of each transaction and ensuring that it complies with the rules of the Bitcoin network. Once a transaction has been confirmed, it is appended to the blockchain in a block together with other current transactions. Each block contains a series of transaction data, a so-called hash value of the previous block and a nonce. A hash value is a character string that can be interpreted as a digital fingerprint and the nonce (abbreviation for “number used once”) is an arbitrary number combination that is only used once in its respective context. The transaction data and the hash value of the previous blocks are known to all participants in the network, only the nonce is variable.

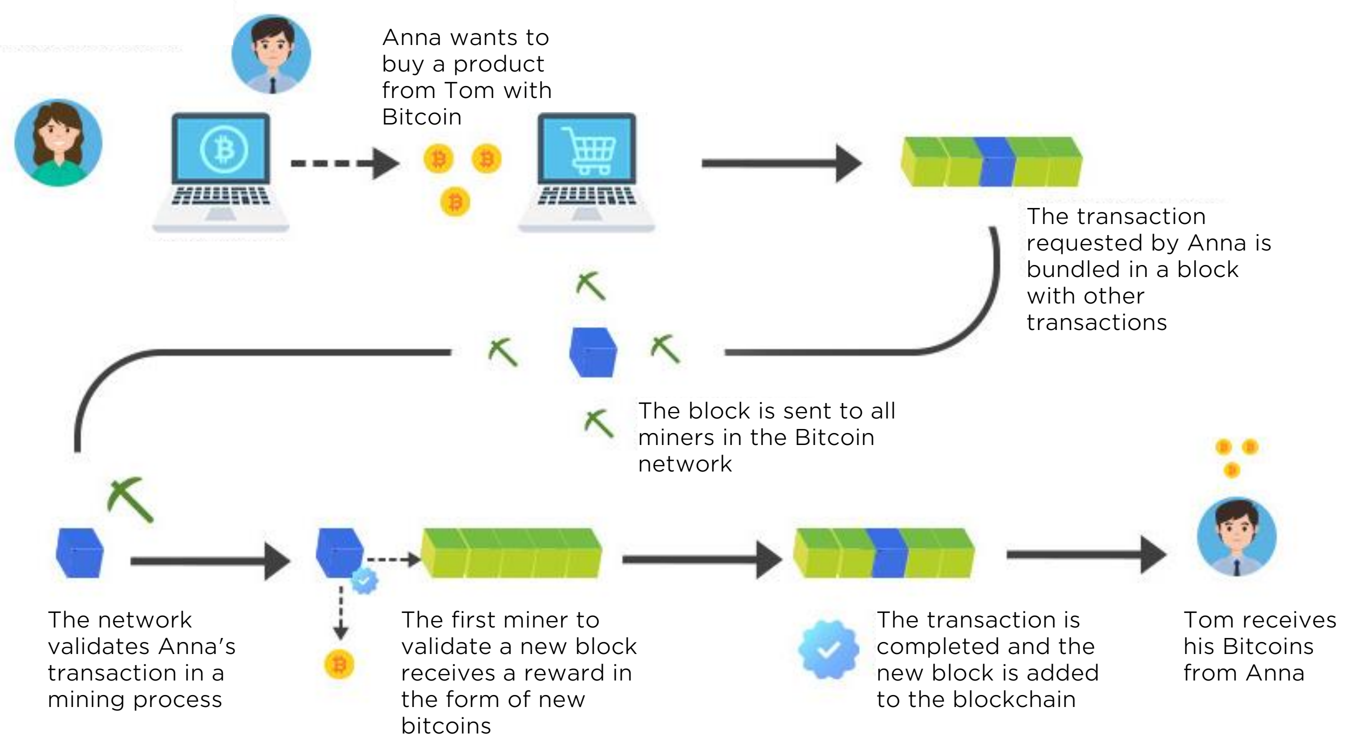
Simplified Illustration of the Bitcoin Blockchain



Source: Own illustration based on Deutsche Bundesbank, 2021

To generate the next block, a new hash value must be found that is smaller than a predefined target value. To solve this complex mathematical puzzle, the nonce is varied until the correct solution is found. As only the miner who solves this task first is rewarded, higher computing power increases the chances of success. This deliberately computationally intensive process is known as mining. As soon as a valid solution has been found, the other participants verify the validity of the block and the transactions it contains. After successful validation, the block is accepted by the participants and added to the blockchain. The transactions it contains are now considered confirmed.

How a Bitcoin Transaction works


Anna wants to buy a product from Tom with Bitcoin
The transaction requested by Anna is bundled in a block with other transactions
The block is sent to all miners in the Bitcoin network
The network validates Anna's transaction in a mining process
The first miner to validate a new block receives a reward in the form of new bitcoins
The transaction is completed and the new block is added to the blockchain
Tom receives his Bitcoins from Anna

Source: Own illustration based on geeksforgeeks

This proof-of-work mechanism (the presentation of a solution is considered proof that computing power has been invested) ensures not only the processing of transactions, but also the security and integrity of the Bitcoin network. This cycle is repeated every ten minutes on average, whereby the difficulty of the mining process is regularly adjusted in order to keep this time span constant. The successful miner receives a reward per block in the form of newly issued bitcoins and the accumulated transaction fees for the block as an incentive for their computing power.

Currently, this reward is 3.125 Bitcoins per block, but it is halved every 210,000 blocks, which happens approximately every four years. The last so-called halving took place on April 20, 2024 and is a programmed mechanism that occurs at fixed intervals and pursues several technical goals. Primarily, it serves to control inflation by halving the rate at which new Bitcoins are generated. This increases the scarcity of bitcoin and consolidates its position as a digital good, as the total amount of bitcoins available converges to a maximum of 21 million through regular halvings. In addition, halving ensures transparent and predictable supply growth and incentivizes miners to increase their efficiency and invest in advanced technologies.

The development of Bitcoin shows impressively that it is no longer a niche market and that cryptocurrencies are increasingly becoming mainstream. In the next issue of Economic Situation and Strategy, we will examine how the value behind Bitcoin should be assessed and whether cryptocurrencies should now be regarded as an asset class in their own right. One thing is certain, however: the technology behind Bitcoin is not a passing trend and is here to stay!

Tilman Deißinger, Sebastian Kuhnert, Jan Mooren

Market data

	As of	Change versus				
	31.01.2025	24.01.2025	30.12.2024	30.10.2024	30.01.2024	31.12.2024
Stock marktes	10:57	-1 week	-1 month	-3 months	-1 year	YTD
Dow Jones	44882	1,0%	5,4%	6,5%	16,7%	5,5%
S&P 500	6125	0,4%	3,7%	5,3%	24,4%	4,1%
Nasdaq	19682	-1,4%	1,0%	5,8%	26,9%	1,9%
DAX	21790	1,8%	9,4%	13,2%	28,4%	9,4%
MDAX	26816	2,7%	4,8%	0,7%	3,1%	4,8%
TecDAX	3731	2,3%	9,2%	11,4%	11,2%	9,2%
EuroStoxx 50	5311	1,8%	9,1%	8,7%	13,9%	8,5%
Stoxx 50	4633	2,3%	8,2%	6,1%	9,9%	7,5%
SMI (Swiss Market Index)	12695	3,3%	9,4%	6,1%	10,9%	9,4%
Nikkei 225	39572	-0,9%	-0,8%	0,8%	9,7%	-0,8%
Brasilien BOVESPA	126913	3,6%	5,5%	-2,9%	-0,4%	5,5%
Indien BSE 30	77493	1,7%	-1,0%	-3,1%	8,9%	-0,8%
China CSI 300	3817	-0,4%	-4,6%	-1,9%	17,6%	-3,0%
MSCI Welt	3853	-0,1%	3,6%	4,0%	19,1%	3,9%
MSCI Emerging Markets	1096	0,5%	1,6%	-2,7%	11,7%	1,9%
Bond markets						
Bund-Future	131,90	65	-154	-7	-263	-154
Bobl-Future	117,37	71	-49	-90	-47	-49
Schatz-Future	106,80	31	-19	19	83	-19
3 Monats Euribor	2,61	-3	-7	-44	-129	-10
3M Euribor Future, Dec 2025	2,08	-9	18	-73	-47	18
3 Monats $ Libor	4,30	-5	-7	-37	-112	-7
Fed Funds Future, Dec 2025	3,88	-5	-3	-64	-25	-3
10 year US Treasuries	4,53	-9	-1	25	48	-4
10 year Bunds	2,47	-7	11	10	23	11
10 year JGB	1,24	4	16	32	56	16
10 year Swiss Government	0,40	-6	12	-8	-50	12
US Treas 10Y Performance	596,32	0,8%	0,6%	-0,8%	0,3%	0,8%
Bund 10Y Performance	559,88	0,5%	-0,8%	-0,4%	0,6%	-0,8%
REX Performance Index	451,02	0,2%	-0,4%	-0,1%	1,6%	-0,4%
IBOXX AA, €	3,07	-8	4	-2	-18	3
IBOXX BBB, €	3,51	-9	6	-5	-37	5
ML US High Yield	7,38	-3	-24	-1	-51	-27
Commodities						
MG Base Metal Index	413,12	-1,8%	0,7%	-4,0%	7,0%	1,9%
Crude oil Brent	76,62	-2,4%	3,0%	5,4%	-7,5%	2,5%
Gold	2794,36	0,7%	7,5%	0,4%	37,4%	6,4%
Silver	31,40	2,2%	5,8%	-7,5%	35,8%	5,8%
Aluminium	2624,76	-0,3%	4,0%	1,6%	17,4%	3,9%
Copper	9008,68	-1,6%	2,4%	-4,1%	5,8%	4,1%
Iron ore	101,33	0,0%	-2,4%	-2,6%	-25,3%	-2,2%
Freight rates Baltic Dry Index	715	-8,1%	-28,3%	-48,7%	-48,8%	-28,3%
Currencies						
EUR/ USD	1,0381	-0,9%	-0,6%	-4,0%	-4,3%	-0,1%
EUR/ GBP	0,8357	-0,8%	0,7%	0,1%	-2,3%	1,1%
EUR/ JPY	160,55	-2,0%	-2,4%	-3,2%	0,4%	-1,5%
EUR/ CHF	0,9452	-0,4%	0,2%	0,6%	0,9%	0,4%
USD/ CNY	7,2507	-0,1%	-0,7%	1,9%	1,0%	-0,8%
USD/ JPY	154,31	-1,1%	-1,6%	0,6%	4,5%	-1,8%
USD/ GBP	0,81	0,6%	0,8%	4,8%	2,0%	0,9%

Source: 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 3282-2132
jmooren@mmwarburg.com

This article does not constitute an offer or an invitation to submit an offer but is solely intended to provide guidance and present possible business activities. This information does not purport to be complete and is therefore not binding. The information provided should not be considered a recommendation to purchase financial instruments individually but serves only as a proposal for a possible asset allocation. The opinions expressed herein are subject to change without notice. Where statements were made with respect to prices, interest rates or other indications, these solely refer to the time when the information was prepared and do not imply any forecasts about future development, particularly regarding future gains or losses. In addition, this information does not constitute advice or a recommendation. Before completing any deal described in this information, a product-specific consultation tailored to the customer's individual needs is required. This information is confidential and exclusively intended for the addressee described herein. Any use by parties other than the addressee is not permissible without our approval. This particularly applies to reproductions, translations, microfilms, saving and processing in electronic media as well as publishing the entire contents or parts thereof.

This article is freely available on our website.