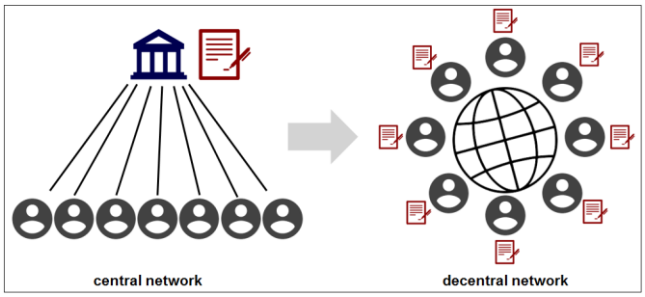
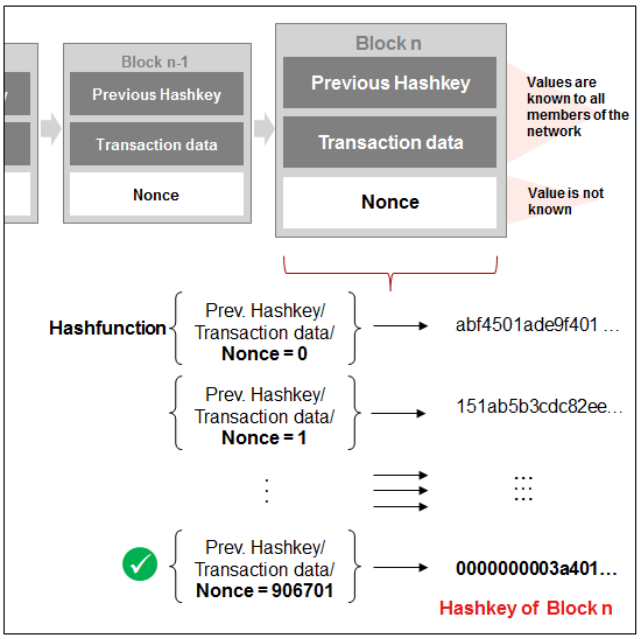
Bitcoin etc.: The innovation behind the hype

Towards the end of last year, there was a deluge of newspaper reports about bitcoin, and in the last few weeks some investors have presumably considered putting their money in the cryptocurrency. Even fear of a speculative bubble did not undo the trend, at least not last year. Instead, it seemed a new record high was reached one day after the next. But what is all the excitement about really?

Bitcoin is not disruptive because it is digital, virtual, or cryptographic, but rather because it does without an intermediary. In the depths of the financial crisis, when confidence in banks was shaky, the inventors of bitcoin asked how transactions could be made securely without using a central, trusted third party. When decentralized, the digital ledger ("blockchain") in which account balances and transactions are recorded is no longer kept at a safe bank, but must be accessible to all participants, each of whom can inspect and edit it. However, it must also be ensured that all copies of the blockchain match. So, a consensus must be found among many network participants, who do not know and possibly do not trust each other. The developers of bitcoin have found a solution to this problem for the first time using the blockchain as a consensus protocol.



As the name says, this protocol is a long list or "chain" consisting of blocks. In the case of bitcoin, the blocks contain transaction data with information about payers, payees, and amounts paid. In addition to the transaction data, the block contains a "hashkey" of the preceding block and a "nonce" ("number used once"). The hashkey is a string of characters that may be interpreted as a digital fingerprint, and the nonce is a random number. The transaction data and the hashkey of the previous block are known to all network participants, while the nonce is variable. Generating the next block requires a new hashkey to be found that is a function of these three factors. To that end, the nonce is varied as long as necessary until the result has the desired form. In this case, the desired form is simply that the hashkey begins with a number of zeros set in a bitcoin protocol. The rest of the characters in the string are unimportant.



In this, the hashkey function is not invertible, i.e., no input can be determined from the desired output (the string of characters with the determined number of zeros at the beginning). Instead, one must basically guess. This is done by randomly varying the nonce. This process is called mining. Miners randomly try out nonces until they finally find a value that results in the desired output (in the case above: 906,701). As soon as a suitable number is found, it is sent to the network. Verification can then be completed by simply entering the found nonce into the hashkey function. If the other participants validate the found block, it is attached to the chain.

Every network participant assumes that the longest chain in circulation is the correct one, since the most computational power has flowed into it, which means the most computers must have collaborated on it. Since the longst chain is always chosen, it is practically impossible to delete transfer payments from the protocol in order to enrich oneself. A malicious agent would have to regenerate all subsequent blocks (which likewise contain the hashkey of the preceding block) in order to obtain the longest chain again. That would only be possible, if the agent had more computational power than the other network participants together (at least 51%), since otherwise it would never catch up with the longest chain. This method of preventing fraud and ensuring consensus is called "proof of work". Economically and especially logistically, it is nearly impossible for an individual or institution to control 51% of the network's computational power, and there is no incentive because of the costs. The world's 500 most powerful super computers today have only about 0.01% of the bitcoin network's computational power. Decentralized consensus formation is the basic and, above all, innovative feature of the blockchain. It ensures that all participants have the same information and can access it while being unable to manipulate it.

However, because of its new popularity, bitcoin is now bringing to light some disadvantages of the blockchain. Its scalability is progressing very slowly for technological reasons. It is still not possible for the bitcoin network to process more than seven transactions per second. By comparison, the Visa network processes about 1,700 transactions per second. This leads to high fees and long wait times. That undermines bitcoin's original use case of fast and cheap transactions. The bitcoin network is also assuming problematic ecological dimensions. The total electrical power needed by miners now exceeds that of Denmark. That means power consumption of about 100 kWh for one transaction, which equals the weekly consumption of a single-family home in Germany.

In contrast to some competing blockchain projects, there is no association, group, or person behind bitcoin. The author of the bitcoin white paper, Satoshi Nakamoto, has constantly remained anonymous and withdrew from developing it some years ago. This accords with the goal of a completely decentralized network, but exactly there lies the problem. The result of having no management is a very slow development process, which could take on the above-mentioned problematic aspects. In particular, the problem of electrical power consumption must be solved for the future. A non-profit foundation is behind another crypto project called Ethereum, which has well-known founders and developers who are openly driving development forward.

In addition, the success of bitcoins has given rise to a new trust problem that cannot be solved by blockchain. It has become an object of extreme speculation. That cannot have been what its developers intended, since the basic presupposition for a currency's acceptance is a certain degree of value stability. Bitcoin is still far from achieving that. It is necessary for its future success that bitcoin be regulated and legal certainty be created for investors. But then there is the question whether because of the above-mentioned technical limitations, bitcoin will be replaced at some point by a newly developed cryptocurrency that solves the problem of scalability better.

If bitcoin were seen as a pocket calculator, the second best-known crypto currency, Ethereum, would probably be a smart phone, with any number of applications. This platform can be used to program "smart contracts," which are digital contract protocols that can retrieve and execute bodies of rules and regulations, laws, or external and internal terms and conditions. For example, when an event Z occurs, then A transfer x euros to B. In the case of bilateral contracts, the execution of such a protocol is still simple, but as soon as many parties in a network hold contracts that refer to one another or influence one another depending on events, an intermediary such as a stock exchange or agent has so far been needed to keep and constantly adjust a "contract ledger." A blockchain could ensure that this ledger is transparent, decentralized, and examinable by everyone, without being susceptible to manipulative change or without there being several versions. At the same time, parties who have in the past acted as guarantors of safety would be superfluous.

A decentralized electrical power grid, for example, would be one of the possible areas of application for smart contracts. Contrary to the conventional network topology consisting of a few power producers and millions of power customers, there would be many relatively small participants in a decentralized network that both consume and generate electricity. The energy transition is making this possible, with private individuals having solar panels on their roofs, for example. These "prosumers" ("producer-consumers") can use smart contracts to automatically arrange who will sell how much electricity to whom, when, and at what price. In the process, the smart contracts can include internal logic, such as minimum or maximum prices, or external factors, such as current power demand or the weather, in order to achieve the economically optimal outcome for all participants. Since this takes place by way of blockchain, the market participants need not know or trust one another personally and can nevertheless be certain that they will always be paid for the power they put into the network and always receive the best price when purchasing power from it.

These advantages can be transferred to various other areas such as logistics, insurance, land registry offices, governments (Democracy 2.0?), law, and other decentralized markets like those for data storage and computational power. Not only the banking sector, but also other industries have recognized the great potential. The Enterprise Ethereum Alliance includes well-known members such as Intel, IBM, Microsoft, BP, Cisco, and MasterCard. Other projects, such as the IOTA, which specializes in the internet of things, has strong partners like Bosch. The internet of things is the vision of a global infrastructure that links physical and virtual objects and makes communication between appliances and machines possible. A blockchain would enable the registration of objects in a global network and, above all, the confidential tracing and verification of the respective property rights. The technology might even break up the current oligopolistic structure of Google & Co with respect to data processing, interpretation, and commercial exploitation.

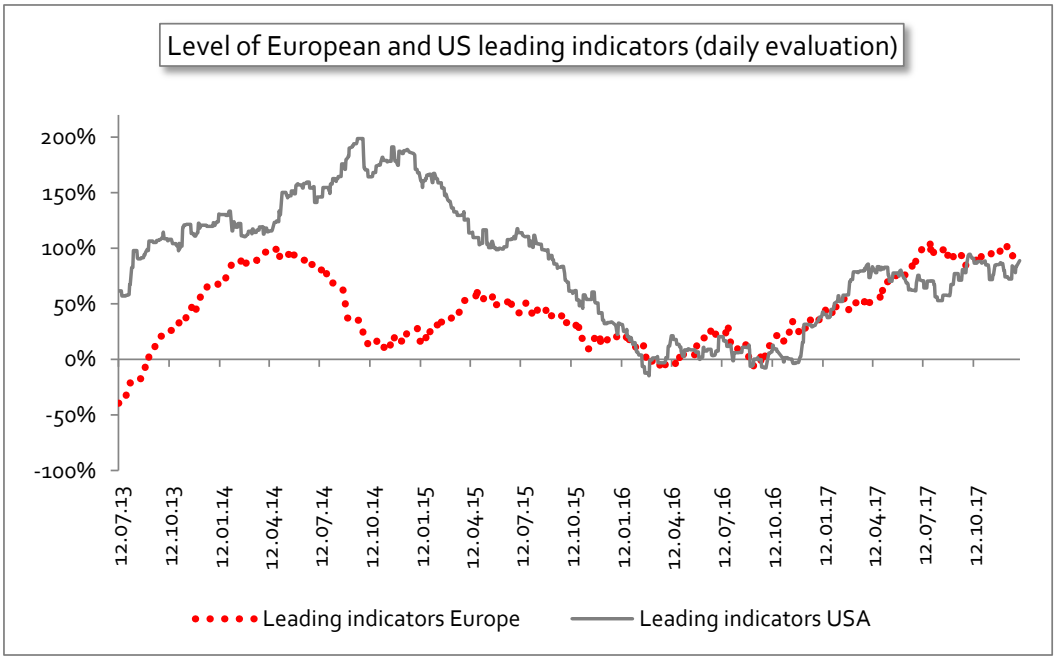
The blockchain is changing business models and creating new ones. To keep Germany an attractive place for businesses to locate, educational programs in universities, investments in pilot projects, and regulations to promote legal certainty should be implemented as soon as possible. While Germany does not have noteworthy players in the current field of internet companies, blockchain technology presents the opportunity to assume a pioneering role instead of being dependent on Silicon Valley. For, blockchain will remain even when bitcoin goes.

Weekly outlook for the January 8-22, 2018

	July	Aug.	Sept.	Oct.	Nov.	Dec.	Release
DE: New orders, m/m	-0.4%	4.1%	1.2%	0.5%	-1.2%		January 8
DE: New orders, y/y	5.2%	8.5%	9.7%	6.8%	7.5%		January 8
DE: Exports, m/m	0.0%	2.4%	-0.4%	-0.3%	1.2%		January 9
DE: Exports, y/y	7.5%	7.5%	7.6%	6.6%	5.0%		January 9
DE: Trade balance, in EUR bn	19.4	21.3	21.9	19.9	20.9		January 9
DE: Industrial production, m/m	-0.1%	2.6%	-0.9%	-1.4%	1.6%		January 9
DE: Industrial production, y/y	4.1%	4.5%	4.2%	2.7%	3.8%		January 9
EUR19: Industrial confidence	4.5	5.0	6.7	8.0	8.2	8.4	January 8
EUR19: Consumer confidence	-1.7	-1.5	-1.2	-1.1	0.1	0.5	January 8
EUR19: Retail sales, m/m	0.0%	-0.2%	0.8%	-1.1%	1.9%		January 8
EUR19: Retail sales, y/y	2.5%	2.3%	3.7%	0.7%	2.9%		January 8
EUR19: Unemployment rate	9.0%	9.0%	8.9%	8.8%	8.7%		January 9
EUR19: Industrial production, m/m	0.0%	1.8%	-0.5%	0.2%	0.4%		January 11
EUR19: Industrial production, y/y	3.4%	3.3%	3.5%	3.6%	3.2%		January 11

MMWB estimates in red

Chart of the Week: Europe persuasive with very good data



There is no perfect method of comparing economic data between different countries. In the case of leading indicators, problems already arise because they are often calculated and published by different data providers using different methods and processes and are thus not directly comparable. But if one wanted to compare "apples and oranges," one cannot get around standardizing often very different time series in such a way that direct comparisons can be made. Moreover, standardization has the advantage that several different leading indicators of a country or economic region can also be aggregated into an overall index. That is exactly what we have done in our Chart of the Week. It shows the cumulative development of various US and European leading indicators, and not in back-calculation, but in a daily real-time analysis. This means that the underlying model has been performing the necessary calculations every day for the United States and Europe since mid-2013 and has stored the results. In this way, we can obtain a good understanding of how the economic trend is evolving on a daily basis. It emerges that both the United States and Europe managed to stop their economic downtrend around the beginning of 2016. A phase of improving economic data then began at the end of 2016 that has continued to the present. Above all, there is no sign that the next downswing is imminent. Currently, data in the United States and Europe are moving sideways at a high level or even trending better. It is also notable that Europe has even surpassed the United States in the level of the data, whereas the United States was always in the lead in previous years. This may also explain why the euro has been able to hold its own against the US dollar lately. Overall, the good data argue in favor of sticking to a high portfolio weighting of stocks.

	As of	Change versus			
	05.01.2018	08.12.2017	14.11.2017	14.09.2017	30.12.2016
Stock marktes	16:42	-1 week	-1 month	-3 months	YTD
Dow Jones	25129	3,3%	7,3%	13,2%	27,2%
S&P 500	2730	2,9%	5,8%	9,4%	21,9%
Nasdaq	6857	0,2%	1,8%	6,6%	27,4%
DAX	13299	1,1%	2,0%	6,0%	15,8%
MDAX	26968	3,0%	2,3%	6,7%	21,5%
TecDAX	2638	4,9%	5,9%	11,4%	45,6%
EuroStoxx 50	3596	0,1%	1,1%	2,0%	9,3%
Stoxx 50	3222	1,4%	2,6%	3,5%	7,0%
SMI (Swiss Market Index)	9535	2,3%	4,4%	5,1%	16,0%
Nikkei 225	23715	4,0%	6,0%	19,7%	24,1%
Brasilien BOVESPA	78860	8,4%	11,3%	5,6%	30,9%
Russland RTS	1218	8,8%	7,2%	8,2%	5,7%
Indien BSE 30	34154	2,7%	3,7%	5,9%	28,3%
China Shanghai Composite	3392	3,1%	-1,1%	0,6%	9,3%
MSCI Welt (in €)	2143	0,9%	3,0%	6,8%	7,3%
MSCI Emerging Markets (in €)	1193	4,9%	4,2%	7,2%	21,3%
Bond markets					
Bund-Future	163,14	-34	75	158	-101
Bobl-Future	131,67	-92	-2	29	-196
Schatz-Future	111,96	-24	-31	-23	-34
3 Monats Euribor	-0,33	0	0	0	-1
3 Monats $ Libor	1,60	5	18	28	60
Fed Funds Future, Dec 2017	1,29	0	1	7	0
10 year US Treasuries	2,47	9	8	29	3
10 year Bunds	0,44	13	4	3	23
10 year JGB	0,06	2	1	3	1
10 year Swiss Government	-0,09	6	0	0	11
US Treas 10Y Performance	583,87	0,4%	0,5%	-0,9%	2,5%
Bund 10Y Performance	616,57	-0,1%	0,8%	1,0%	1,2%
REX Performance Index	480,62	-0,8%	-0,5%	-0,6%	-1,0%
US mortgage rate	0,00	0	0	0	0
IBOXX AA, €	0,56	2	-12	-18	-11
IBOXX BBB, €	1,13	2	-5	-17	-37
ML US High Yield	6,17	-2	-10	13	-29
JPM EMBI+, Index	835	0,2%	1,4%	-1,1%	8,1%
Convertible Bonds, Exane 25	7454	1,2%	1,4%	3,3%	7,8%
Commodities					
CRB Spot Index	429,73	-0,4%	-0,1%	0,3%	1,6%
MG Base Metal Index	336,22	2,1%	-2,3%	2,6%	20,2%
Crude oil Brent	67,72	6,9%	9,8%	21,1%	19,4%
Gold	1318,55	5,6%	3,1%	-0,5%	13,9%
Silver	15,84	0,5%	-6,9%	-10,6%	-1,3%
Aluminium	2033,25	2,1%	-1,3%	-1,7%	19,3%
Copper	6761,00	3,4%	0,6%	4,7%	22,4%
Iron ore	71,28	4,1%	15,4%	-3,3%	-10,6%
Freight rates Baltic Dry Index	1341	-21,2%	-4,6%	-1,5%	39,5%
Currencies					
EUR/ USD	1,2022	2,4%	2,4%	1,2%	14,0%
EUR/ GBP	0,8870	1,0%	-1,0%	-0,3%	3,9%
EUR/ JPY	136,11	2,1%	2,1%	3,5%	10,3%
EUR/ CHF	1,1749	0,4%	0,9%	2,2%	9,4%
USD/ CNY	6,4875	-2,0%	-2,3%	-1,1%	-6,7%
USD/ JPY	112,39	-1,0%	-0,9%	2,0%	-3,9%
USD/ GBP	0,74	-1,3%	-3,2%	-1,5%	-8,8%

Carsten Klude	+49 40 3282-2572	cklude@mmwarburg.com	Martin Hasse	+49 40 3282-2411	mhasse@mmwarburg.com
Dr. Christian Jasperneite	+49 40 3282-2439	cjasperneite@mmwarburg.com	Dr. Rebekka Haller	+49 40 3282-2452	rhaller@mmwarburg.com
Dr. Jörg Rahn	+49 40 3282-2419	jrahn@mmwarburg.com	Bente Lorenzen	+49 40 3282-2409	blorenzen@mmwarburg.com
Julius Böttger	+49 40 3282-2229	jboettger@mmwarburg.com			