Since the rally in 2017, the buzzwords bitcoin and blockchain have been omnipresent in the public. Still, the understanding of how much potential the technology actually offers is often rudimentary.

To shed more light onto the discussion, we discuss the manifold technological facets as well as the social changes that might come on the heels of the technology. In this analysis, we describe ten stages – each, in itself, a minor social revolution. All stages combined illustrate why the enthusiasts dream of a global blockchain revolution.

Of the ten stages, only two will revolutionise our monetary system. As the central innovation of a blockchain is the fixation of information, it provides a reliable data basis for many transactions beyond money such as, for instance, proprietary rights. Moreover, the communication between vehicles, machines and robots could also be managed via blockchains and, thanks to the storage of complex and code-based if-then logics, even contracts might eventually be fixed and executed. In theory, any binding agreement could be organised by means of blockchains.

After outlining the utopia, we point out the technical as well as the social hurdles that are standing in the way of the revolution. From our perspective, swift implementation is not to be expected. The more likely scenario is that it will take many years, possibly even decades, before high market penetration is achieved and the new technology becomes an integral part of our day-to-day lives.
The multiple stages of the blockchain revolution
The multiple stages of the blockchain revolution

Stage 1: A non-state means of payment

A group of libertarian computer experts calling themselves cypherpunks has been developing non-state currencies over the past decades. But all efforts to establish them as an alternative means of payment failed.

One reason why these attempts were unsuccessful was the centrality of the systems. Like most innovations, they were legally tied to the existence of a company. Many of these Bitcoin predecessors therefore foundered in the face of lacking market penetration, as well as refinancing risks and government bans. The development of bitcoin probably mirrors the negative experience of the Cypherpunks prior to 2009. Even though nobody knows who is hiding behind the pseudonym Satoshi Nakamoto, there is sufficient evidence to suggest an intellectual closeness to the Cypherpunks. To date, the market penetration of bitcoin as a means of payment is doubtlessly also low. The maximum number of bitcoin transactions per week is roughly 1 million, or 200,000 per day. Assuming an average number of 10 transactions per person and day, the global payment means bitcoin managed to support a town of 20,000 inhabitants. Alongside these so-called on-chain transactions, the Lightning Network went live in early 2018. These off-chain transactions are primarily used for small daily purchases and micropayments such as a cup of coffee or per-second billing of streaming services when watching videos, to name some standard examples. Although recent statistics suggest that nodes and payment channels in the Lightning Network are up sharply, its monetary capacity is just 100 bitcoins, or well below EUR 1 million at current market prices. If every inhabitant residing in our town of 20,000 carries EUR 100 of cash for daily transactions on them, currency in circulation in this town amounts to EUR 2 million, or twice the “purchasing power” of the Lightning Network. For now, on-chain and off-chain, bitcoin as a global payment means continues to be a niche product, at best.1

Stage 2: A hard-to-regulate object of speculation

As a means of payment, i.e. in exchange for goods or services, bitcoin may in fact be even less significant than we pointed out. Foremost, bitcoin is an object of speculation and the first vehicle of a new asset class. Eventually, investors want to exchange their anticipated profits for state currencies, or are sometimes forced to do so in order to pay taxes, for instance. Cryptocurrency investors remain hopeful that yields will continue to rise, thanks to user and investor growth. In the past, their number indeed increased, as the infrastructure surrounding cryptocurrencies was expanded. Shortly after the establishment of cryptocurrency exchanges through which bitcoin can be sold or purchased for euro or US dollar, traditional investment vehicles such as closed-end funds and ETNs (Exchange-Traded Notes) were launched, which support investment in the cryptocurrency market without requiring any specific knowhow. In 2017, futures markets with cash settlement were introduced, which means that losses from the futures positions are paid in US dollar. For 2019, the Intercontinental Exchange announced the introduction of futures markets with physical settlement allowing the direct settlement of losses in cryptocurrencies. Many investors therefore hope to see near-term mass adaption, if, for instance, ETFs are licensed by the US authorities or cryptocurrencies, for other reasons, become more widely accepted as an asset class by the family offices and institutional investors. Apart from the hoped-for continued uptrend in yields, cryptocurrencies can also be used as a hedging tool against financial market risks. As high public and private debt in many countries are likely to trigger new

crises, new non-state monetary systems could become more attractive. Outside times of crisis, however, the correlation between cryptocurrencies and equities, bond and real estate is also negligible. The risk/return ratio might hence improve, if cryptocurrencies are added to a portfolio. But given the high volatility of cryptocurrencies and the strong risk of meltdown, the optimum share in many clients’ portfolios is unlikely to exceed the (very) low single-digit percentage range.

Stage 3: Immutable recording of information

By means of the blockchain, a functional, relatively long-lived global non-state monetary system and hard-to-regulate object of speculation can be created. As the entire system also works without a central institution, it has attracted some attention – the more so as it is historically unique. Looking forward, however, the innovation potential of the technology by far exceeds the above uses, as is clearly illustrated when defining the blockchain as an information chain that is characterised by two essential features:

- First, the entire history of every information chain from the beginning to date can be accessed at all times.
- Second, the information chain cannot be manipulated, thanks to cryptography and thousands of copies, which are stored on computers in many countries. By recording information, such a system helps to build a basis of trust.

If, however, bitcoin is only a piece of digital information, why is every single information believed to be a coin of a currency? The answer is: Only because everybody thinks that everybody believes the piece of information to be a currency. Hence, the currency comes out of nowhere. Now, imagine a society in which an information is defined as a plot rather than a coin. If everybody thinks that everybody believes the information of a blockchain to represent a plot, property can be transferred to a new owner without a notary and, more importantly, without notary fees. Doubtless, this sounds utopian. But some countries are already working on pilot projects to manage ownership transfer of land and buildings on a blockchain in the probably still distant future.

If a piece of information on the information chain can represent either a cryptocurrency or a plot, what other information can be managed by means of a blockchain? If land ownership can be transferred, equities, bonds and derivatives may also be traded on a blockchain. The same holds for state cryptocurrencies, i.e. crypto euros or crypto dollars, as well as copyrights to songs and movies, personal health data or even entire digital identities. But thanks to cryptography, the blockchain – unlike the status quo – would allow people to retain full control over their data. Asked what information can be managed through a blockchain, enthusiasts would say; “all!”. They consequently expect a revolution in which all information from the service sector is shifted to the blockchain and all key actors, particularly those involved in the management and monitoring of information, potentially become obsolete.

---

Stage 4: Machine-to-machine communication across IT systems

In the end, not only the services sector might be turned inside out by the blockchain revolution, but manufacturing as well. Today, machine-to-machine communication or the "Internet of Things" (IoT) is primarily intra-plant, hence taking place within a company. For instance, if a robotic arm in the assembly line informs his "fellow robot": "That's my working zone, wait until I'm finished". Within a factory, i.e. a centrally-controlled hierarchy, it is easy to impose standards. If, however, machines communicate across different IT systems and legal entities, or even in the public domain, a digital basis of trust is crucial. Given their immutability, blockchains might be just the right basis, on which the machines resp. their programmers rely. Auto producers, for example, could set up a joint communication standard to manage their car as well as all road transport via a blockchain. Moreover, decentralised solutions could help to prevent the breakdown of digital systems and their potentially disastrous aftermath or, at least, substantially reduce the likelihood of such an event relative to centralised solutions. Courtesy of the decentralised distribution of information, which makes them more immune to cyber attacks than traditional IT systems, blockchains seem tailor-made for managing critical infrastructure. Whilst the implementation of decentralised solutions in road traffic is as yet a very remote prospect, though first pilot projects are under way, rail transport may benefit from blockchain solutions in the not too distant future. To this end, Deutsche Bahn is working intensively to manage more than one hundred railway companies in Germany via a joint blockchain, allowing real-time payment of their services.

Stage 5: Immutable codification of smart contracts

Beyond the recording of information, which supports the flexible management of complex control systems, complete and complex if-then logics can be archived in the blockchain. Contracts can thus be translated into code by the programmers and when embedded they are irrevocable. In the legal sense, these so-called smart contracts are the result of declarations of intent that are consistent in terms of content – just like any other contract. Would it not be a major step forward if there was an insurance for train delays whose contract is embedded in a blockchain, allowing automatic and non-bureaucratic compensation payments thanks to smart contract solutions? For flight delays, a blockchain-based solution has already been implemented. If used intensively, smart contracts have the potential to alter many aspects of our daily lives and make them simpler.

Stage 6: Smart contracts plus artificial intelligence (AI)

Once smart contracts have taken root in our everyday lives, the next revolution is just around the corner. With the deployment of artificial intelligence, the scope of smart contracts may virtually explode. Thanks to intelligent algorithms, a damaged car that is packed with cameras and sensors could in the future reconstruct the events leading to the crash. Within seconds after the accident, the artificial intelligence could call the ambulance and file a claim before its arrival. The financial funds to pay for the medical bills and the work-related income losses would thus be immediately available to the claimants.

---

There are numerous other examples of how our daily lives may benefit. The pharmaceutical sector, health insurances and the final consumer would communicate much more efficiently and be of greater mutual benefit to one another than today. Via sensors on their wrists recording blood pressure and pulse measurements at regular intervals on a blockchain, patients could, for instance, be monitored while taking their medication or when in the sanitary area. If the medication is taken as prescribed, health insurances could offer a bonus to the patient. Simultaneously, a host of information would be provided to the producer, including the dose, the medication intake frequency, the time of day, to name just a few examples. If this data is evaluated by means of artificial intelligence, taking into account patient-specific characteristics, future drug intake could be optimised by tailoring it to the individual needs of the patient.

Courtesy of cryptographically secure storage of the information on the blockchain, compliance with data protection regulations is ensured. To his health insurance, for example, the patient only grants access to the information "all medication was taken as prescribed", whilst providing his personal, albeit anonymised, data to the pharmaceutical producer against payment. Another role that might be redefined is that of the physician. If the healing process evolves in line with expectations, the number of consultations is reduced whereas an additional appointment can be automatically offered to the patient if the disease does not proceed as expected. In a controlled form, even sensitive data could hence become available to the society via the blockchain trust basis. Numerous other combinations of smart contracts and artificial intelligence could be major elements of the blockchain future.

Stage 7: The global AI society

In combination with artificial intelligence, blockchains could not only leave their mark in our day-to-day lives, but might also shift the boundaries of our knowledge society. Many complex scientific issues as regards, for instance, the development of new chemical substances or the calculation of climate models require the analysis of huge data sets. If in future these algorithms were increasingly performed via global computer networks, rather than central mainframes or supercomputers, huge computing capacities could be maintained, utilised and advanced in a flexible manner. Moreover, this approach also allows individual computers or part of the network to become highly specialised on specific AI algorithms. This may, on the one hand, help to enhance the efficiency of the entire network. On the other hand, complex calculations can be broken down into their constituent parts, which are then calculated by the specialised algorithms and reported to the network as partial solutions. Courtesy of the blockchain technology, it will become much easier to create and advance global computer and information networks. A cryptocurrency potentially allows the efficient allocation of computational problems to the different algorithms, thereby rewarding the programmers involved and creating incentives to persistently improve the system. Moreover, the partial results calculated by the algorithms can be stored on a blockchain and are therefore provided to the global computer network in a reliable manner. In this context, blockchains could be a crucial element of the growing role artificial intelligence will play for society and economy in the future.
Stage 8: Hopes of depolitisation through blockchains

The next stage of the blockchain revolution reflects the idea that an entirely new social and economic order may emerge in the future. This concept did not come out of the blue. From the very beginning, it was a key objective of the cypherpunks to end the involvement of third-party and central – in particular state – institutions in all human relations. To date, they continue to dream of replacing the current trust-building institutions and their – from the cypherpunks’ perspective – excessive concentration of power by blockchains solutions, which are incorruptible and entirely free of corruption or political tints.

Stage 9: Moving towards digital democracy

Another way to depolitise society by means of blockchains is more direct democracy. As outlined above, information such as a ballot vote can be recorded on a blockchain. The vote is cryptographically encrypted, assuring compliance with election secrecy, whilst the voter is provided with individual decryption keys to retroactively verify their vote whenever they wish. Thanks to the blockchain technology, election costs could be cut massively, as both postal voting and polling stations potentially become obsolete. The social implications, however, could be even greater than the savings potential. In the democratic countries, calls for more public participation in political decisions could have higher priority. In theory, a direct democracy is a possible scenario, in which parliamentary decisions are supplemented or even partially replaced by regular votes of the citizens.

Stage 10: Decentralised autonomous organisations (DAO)

Once many people can cast their votes in an efficient and transparent manner, the next revolution is on the horizon.Courtesy of blockchain solutions, the old proverb “too many cooks spoil the broth” will possibly become obsolete. Just as the democrats would be in the position to quickly and efficiently capture voter preferences via blockchains, the decision-making process at large organisations, at least, could also be managed by means of the technology. Potentially, members might jointly manage their associations via a blockchain or, in the same manner, stakeholders could reach major decisions without the company’s management. These so-called DAO will possibly redefine our economic and commercial life. Alongside the traditional hierarchical systems that have shaped our entire society in the past, the establishment of decentralised decision-making architectures within the context of the blockchain revolution is – in theory, at least – a conceivable scenario.

So much for the utopia, Now it is time for a critical assessment: The blockchain revolution is still a distant prospect

In the above sections, we have shed light on the dream and – we ourselves – are exalted by the current and future potential of the technology. Still, from our perspective, the global blockchain revolution is thwarted by several bottlenecks.
Blockchains

(1) are very expensive,
(2) can only be developed and programmed by few experts,
(3) often suffer from low scalability
(4) and many crypto projects are overambitious.
(5) Therefore, they are not safe from digital cyber attacks.

Apart from these technical and economic obstacles, the high energy consumption of cryptocurrencies is another argument that is often mentioned in this context. Whilst this moral problem is rightly stressed from the point of view of conservation and environmental protection, our other everyday consumption patterns ought to exceed cryptocurrencies in terms of wasting energy.

How expensive are blockchain solutions?

Blockchains are extremely expensive. Recently, the second most famous crypto developer after Satoshi Nakamoto, Ethereum founder Vitalik Buterin, estimated the costs.\(^5\) According to his calculation, the Ethereum blockchain is about a million times more expensive than centralised webservers, as all servers in a blockchain need to be synchronised. The existence of hundreds or thousands of copies is, apart from cryptopgraphic encryption, precisely what makes storage on a blockchain reliable and immutable. But potential changes to the system are complex and costly, due to high synchronisation requirements.

Developers and programmers are scarce and hence expensive

High synchronisation requirements as well as the use of cryptography – particularly in an exclusively consensus-based ecosystem – are the reason for the systemic complexity of blockchain solutions. As only a rare few developers and engineers can therefore maintain and advance the systems, hundreds of crypto projects are competing for few experts. Solidity programmers, in particular, are in high demand. Emerging only recently in conjunction with the cryptocurrency Ethereum, solidity is one of the key programming languages for coding smart contracts. As a consequence, many functionalities that are standard in other languages are not yet implemented or documentation is still incomplete. Given the challenges of solidity coding, solidity programmers are rare and hence excellently paid.

Scalability of blockchains is low

Another key reason arguing against swift mass adaption of the blockchain technology is its as yet low transaction capacity. Whilst centralised payment systems settle thousands of transactions per second every day – or even ten-thousands at peak times – the current maximum per-second capacity of decentralised cryptocurrencies is in the single- to double-digit range. Meanwhile, solutions are being developed to raise this technological barrier. Of the many approaches allowing higher transaction speed per second, the above-mentioned Lightning Network has probably received the most attention. Scalability could eventually increase rapidly, particularly if lightning technologies of different

---

cryptocurrencies are interconnected. Given the wide scope of potential blockchain applications beyond the payment sector – remember our discussions surrounding the Internet of Things, smart contracts, artificial intelligence, etc. – current centralised payment systems would also fall short of the task. If many of the technological dreams outlined above are to become reality, millions of transactions may have to be settled every second. In itself, the lack of technological scalability is likely to thwart the swift and broad-based implementation of blockchain projects for some time to come.

Many crypto projects are overambitious

Numerous crypto projects have never seen the light of day. Other projects – often initiated by very ambitious, relatively young entrepreneurs – are off to a vigorous start but eventually falter. Even projects which attract relatively widespread attention frequently fail to achieve their targets. Only a very limited number of cryptocurrencies are known to the wider public, no blockchain solution has achieved high market penetration, and an entry under deadcoins.com is all that is left of a relatively large number of projects. Alongside the complexity of the blockchain technology, several other factors are contributing to this imbalance, particularly overambitious targets and insufficient project management skills, but also a lack of life experience. Some project developers, for example, not only aim to upgrade the blockchain technology of bitcoin, but at the same time want to move from the binary hardware architecture – i.e. current on/off – to a ternary architecture. Other developers dream of immediately creating a world computer. One or two revolutions too many, perhaps. These projects simply took advantage of the hype of recent years to quickly collect money. In the face of the sharp price decline of recent months, however, some of these dreams have already come to nothing. That said, a lot of expertise is required – not only as regards crypto and IT issues but also with respect to market penetration at the final consumer level – to separate the good projects from the bad. Given the large share of poorly managed projects, the question arises, in our view, as to whether these developments may eventually cause a system breakdown. As many crypto systems are interconnected, errors in the interfaces of individual crypto projects and cryptocurrencies may ultimately have a technical – alongside the psychological – price effect.

Digital theft persists

One of the libertarian principles is individual responsibility. Using non-state money therefore directly implies that the holder is personally responsible for safekeeping and managing PINs and TANs, i.e. the passwords of the digital wallets. With the loss of access codes remaining an everyday phenomenon, however, the willingness to store cryptocurrencies on one’s own responsibility will likely be limited in the foreseeable future. Given overambitious projects as well as the lack of blockchain experts and the associated erroneous code, the number of stolen cryptocurrencies is up sharply. With these thefts, the libertarian dream turns into a nightmare.

More reasons pointing to a hesitant blockchain revolution

Apart from these systemic obstacles arguing against swift adaption, several other negative factors suggest that a blockchain revolution is unlikely to materialise in the near term.
The multiple stages of the blockchain revolution

(1) If adapted swiftly, the disruptive potential of decentralised solutions for present-day employment and society would be high.

(2) As blockchains are invisible to the consumer, potential users are hard to convince.

(3) Even the internet has not lived up to many revolutionary expectations.

The high disruptive potential of decentrality can act as a disincentive

If information is stored on blockchains, many control functions and administrative activities such as visits to public authorities may become obsolete in future. For example, if the blockchain technology is used for the storage of digital identities. Correspondingly, many traditional fields of employment and jobs might no longer be in demand. Even though digitisation and the introduction of blockchains will probably also create many new jobs, risks are that larger sections of the population vote against the new technologies, if they are adapted in a very swift fashion. The swift adaptation of cryptocurrencies as a global means of payment ought to have an equally disruptive potential for employment and society. Should the current niche product bitcoin suddenly play a major role when concluding new contracts and be established worldwide, the consequences might be overwhelming. Does global mass adaption require the conversion of old work and pension contracts to bitcoin? If so, at what price? How should a global decentralised currency be taxed? For many people, such fundamental issues are a cause of concern rather than enthusiasm. If adapted at a rapid pace, the global revolution that is awaited by some is likely to meet with swift and strict opposition from many.

Blockchains are primarily an abstract construct

The social impact of the blockchain technology is often compared to the internet. Given the immutability of the information stored on blockchains, this technology acts as a trust-building measure, even between strangers. This is exactly where the big difference between the blockchain and the internet lies. Trust is an abstract term. It cannot be seen or touched. Only the indirect impact of trust can be observed in the form of actions. Compared with the internet, this is the major, and possibly crucial, disadvantage of blockchain mass adaption. As the effects of the internet are experienced directly thanks to the transmission of pictures and sounds, even the conservatives and sceptics were easily convinced of its advantages. If you as a user visit a website to, for example, take out a flight delay insurance, you will not be able to tell whether you are using a blockchain or a purely digital solution. As regards high market penetration, this is a clear disadvantage, as – contrary to many experts who are thrilled by the fundamental potential of the blockchain technology – it is still all Greek to the wider public.

The internet's ambivalent effect on freedom and democracy

With the introduction of the internet in the early 1990s, the democratisation of information took a front seat in the public discussion. At that time, the utopia prevailed that universal cross-border access to information and the associated freedom of communication would trigger a social revolution. In the belief that everyone could be reader, editor, author of political articles, initiator of polls or voter, it was also hoped that the internet would foster more participation in the democratic process. The naive expectation of a quasi-automatic intensification
of freedom and democracy was not fulfilled. More than any other technology, perhaps, the internet has contributed to stronger social differentiation. The perception of the large internet companies' market power and their closed platforms, the so-called walled gardens, is turning increasingly negative. Against this backdrop, the impact on freedom and democracy is meanwhile seen in an ambivalent light.

Summary and outlook

Only a rare few have so far realised the potential of bitcoin and blockchain. But everyone who has a notion, at least, and begins to understand what impact the technology may potentially have for society is infected in a positive sense – thrilled by the vision of a world in which a technology creates trust resp. prevents fraudulence. Although we partially share the euphoria, we have also identified several restrictions, which ought to slow the blockchain revolution in the near term and possibly over the next years. In the meantime, not only the creators of cryptocurrencies but also many companies and governmental institutions are striving to embed the new technology in existing business operations and the regulatory framework. Similar to the internet revolution, the majority of products are likely to be provided by the private sector. The upshot is that – in analogy to the internet revolution of recent decades – the future blockchain world could have much more ambivalent social effects than the enthusiasts currently expect.

Jochen Möbert (+49 69 910-31727, jochen.moebert@db.com)
The multiple stages of the blockchain revolution - or into the crypto future and back ................. December 12, 2018
European Parliament elections 2019: The next "battle for Europe"? ..................................... October 24, 2018
Digital infrastructure: Bottlenecks hamper Europe's progress ................ October 12, 2018
Brexit impact on investment banking in Europe ............. July 2, 2018
PSD 2, open banking and the value of personal data ....... June 28, 2018
Digital economics: How AI and robotics are changing our work and our lives .................. May 14, 2018
Reform of the Common European Asylum System: A difficult undertaking ......................... April 12, 2018
Post-Brexit EU budget – the next hot button issue . February 28, 2018
Why would we use crypto euros? Central bank-issued digital cash – a user perspective ............ February 15, 2018
Bitcoin: Myths, misconceptions and misunderstandings ...... February 9, 2018

© Copyright 2018. Deutsche Bank AG, Deutsche Bank Research, 60262 Frankfurt am Main, Germany. All rights reserved. When quoting please cite "Deutsche Bank Research".

The above information does not constitute the provision of investment, legal or tax advice. Any views expressed reflect the current views of the author, which do not necessarily correspond to the opinions of Deutsche Bank AG or its affiliates. Opinions expressed may change without notice. Opinions expressed may differ from views set out in other documents, including research, published by Deutsche Bank. The above information is provided for informational purposes only and without any obligation, whether contractual or otherwise. No warranty or representation is made as to the correctness, completeness and accuracy of the information given or the assessments made. In Germany this information is approved and/or communicated by Deutsche Bank AG Frankfurt, licensed to carry on banking business and to provide financial services under the supervision of the European Central Bank (ECB) and the German Federal Financial Supervisory Authority (BaFin). In the United Kingdom this information is approved and/or communicated by Deutsche Bank AG, London Branch, a member of the London Stock Exchange, authorized by UK’s Prudential Regulation Authority (PRA) and subject to limited regulation by the UK’s Financial Conduct Authority (FCA) (under number 150018) and by the PRA. This information is distributed in Hong Kong by Deutsche Bank AG, Hong Kong Branch, in Korea by Deutsche Securities Korea Co. and in Singapore by Deutsche Bank AG, Singapore Branch. In Japan this information is approved and/or distributed by Deutsche Securities Inc. In Australia, retail clients should obtain a copy of a Product Disclosure Statement (PDS) relating to any financial product referred to in this report and consider the PDS before making any decision about whether to acquire the product.

Printed by: HST Offsetdruck Schadt & Tetzlafl GbR, Dieburg

ISSN (Print) 1612-0272 / ISSN (Online): 1612-0280