B 3 Blockchain

B 3-1 Blockchain technologies: Greater security for decentralized applications

Blockchain is a recent technology that enables data to be digitally stored and transmitted in a process that renders it both immutable and tamper-proof.[355] Rather than being stored by a single institution, in blockchains, data is stored by numerous actors simultaneously. As a result, there is no central authority that has control over the stored data (cf. figure B 3-2).

Box B 3-1 demonstrates the significance of this technological accomplishment using the example of international supply chains.

Besides the transactions of goods along the supply chain, blockchains can also store numerous other types of transactions and render them tamper-proof. Current uses of blockchain technologies include processing financial transactions, organizing decentralized electricity trading, administrating digital identities, facilitating the flow of information between public authorities and helping regulatory bodies and companies to comply with reporting requirements.

However, blockchain technologies and their applications are still in an early developmental stage. The majority of example applications are yet to move beyond the pilot stage. Nevertheless, domain experts expect the technology and its applications to develop successfully in future. The ongoing development of blockchain technologies could engender substantial cost savings and substantially simplify transaction processes. As a result, there is huge potential for both further innovation and significant upheaval in existing economic structures. One reason for this is the crucial importance of data for business and wider society combined with the novel approach to data storage provided by blockchain technologies. There is no longer any need for a central, mediating authority.

Barriers to the future development of blockchain technologies arise from unanswered technological issues, uncertain legal and regulatory framework conditions and a lack of acceptance at both political and societal levels. Germany is in a promising position for shaping the development of blockchain technologies and realizing potential economic and societal benefits. Berlin in particular is a location of global significance for the blockchain developer community. Political actors should leverage this location advantage to promote the future development and application of blockchain technologies.

Key features of blockchain technologies B 3-2

The design and operating principle of blockchain technologies create a series of features that potentially influence the success and diffusion of these technologies. These features include blockchain governance, security, the distinction between blockchains as infrastructure and as an application, and the economic incentives for various actors in the blockchain ecosystem.

The absence of a single, central authority is not only the objective of blockchain technology applications but also serves as the guiding principle for their future development.[356] Decisions on the direction of this development require either the formation of an informal process or definition of a formal one. Informally, for example, the most active developers might come to decisions on the technology's future direction, which are then adopted by others involved in the process. A formal process, on the other hand, could require a system in which every user of a

specific blockchain technology has a voice to help shape direction-dictating decisions. These options are discussed as part of blockchain governance (for further aspects of blockchain governance, cf. box B 3-4). Governance can therefore influence issues such as the quality and pace of the development of blockchain technologies.

The aforementioned features and economic incentives (cf. box B 3-3) mean that blockchain technologies offer a high level of security. However, absolute security is not possible. As a result, there have been repeated cases in which cryptocurrencies have been stolen – such thefts are estimated to have amounted to almost €1 billion in the first half

Box B 3-1

Blockchain applications for supply chains

Every year, goods worth €16 trillion are shipped internationally. 80 percent of the goods we consume every day are the result of international trade.[357] The supply chains this entails are highly complex. For instance, to transport a shipment of avocados from Mombasa to Rotterdam, 30 institutions and over 100 people might be involved in over 200 distinct exchanges of data.[358] This high degree of complexity leads to high administrative costs throughout the supply chain. Such costs can significantly exceed the physical costs of delivering the goods. It is also difficult to trace the overall make-up of such supply chains. Tests with packaged fruit have shown that it can take several days to trace a supply chain and identify the origin of a product. Recent food scandals have highlighted the importance of being able to trace supply chains. Only then is it possible to correctly identify the source of contaminants – which could include pathogens. The objective must therefore be to make it as easy to trace and understand international supply chains with numerous actors as it is to track and trace a package shipped by a courier.

To document a supply chain and the various actors it comprises, all events during a shipment must be recorded and stored in one place.[359] In the past, however, companies have been loath to work together to map supply chains, as it would mean entrusting information on business processes to other companies and relying on a third party's security provisions. If a single company were made the central institution for supply chain information, they would have detailed insights into the transactions made by the companies involved and could then attempt to profit from this information.

Blockchain technologies can render such a central institution superfluous. Rather than having a central institution collect and store the data, the companies involved save information on supply chain processes in a digital ledger: the blockchain. The companies involved can then each store a copy of the blockchain, so that the data is not concentrated in a single, central institution. At the same time, the access rights to the blockchain can be specified; doing so allows only companies involved in a specific shipment to read and write entries in the blockchain. Furthermore, technological features of the blockchain prevent data from being manipulated at a later point in time (cf. box B 3-3).

As a result, blockchain technologies offer a high degree of transparency and security with regard to the stored data; they also help to remove barriers and make tracing supply chains more straightforward. A pilot project has demonstrated that, after introducing a blockchain to track supply chains, the origin of packaged fruit can be tracked in just a few seconds – a task that can otherwise take several days. In another case, improved transparency made it possible to reduce the time required to transport a shipment of packaging material to a US production line by 40 percent.[360]

In August 2018, the technology firm IBM and container shipping company Maersk introduced a blockchain for supply chains following a twelve-month test period. At that time, 94 organizations were involved in the project, including various port operators, shipping companies, customs authorities and logistics providers.[361]

Fig. B 3-2

Download data

How a transaction works – both with and without blockchain technology

Anton and Anna want to initiate a transaction with Kim

Anton – without blockchain

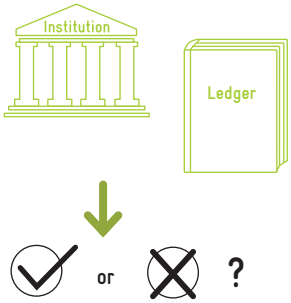
Anton sends the order to a central institution, e.g. a bank.

Anna – with blockchain

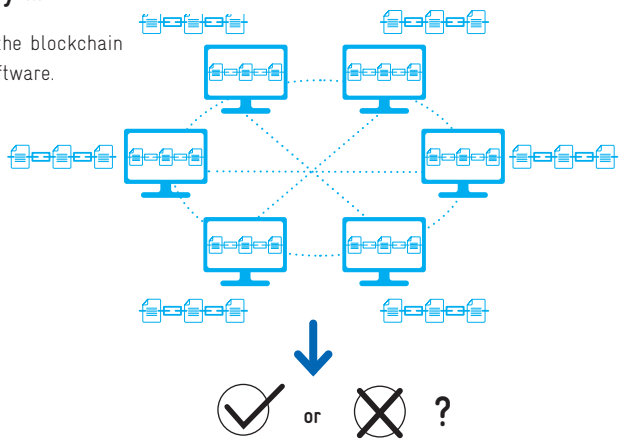
Anna sends the order to a blockchain network.

Whether the transaction is permissible is checked by …

… the central institution using its centrally managed ledger.



… the blockchain software.



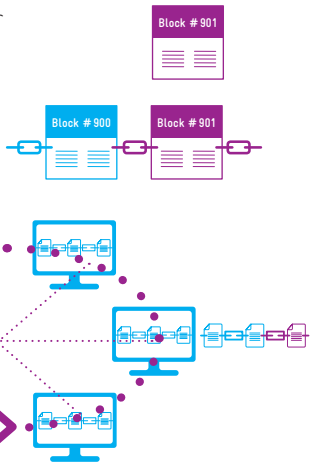
If the transaction is permissible, then …

… an entry is made in the central ledger.

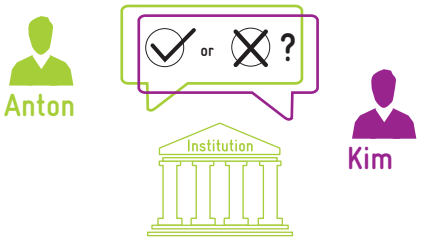
… the transaction is bundled together with other legitimate transactions to form a so-called block,

cryptographically chained to the preceding block,

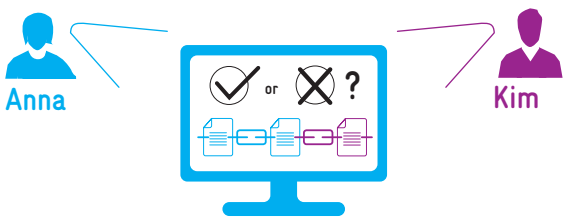
and communicated to the entire blockchain network.



To check whether the transaction has been completed …



… Anton and Kim can submit a query to the central institution.



… Anna and Kim can refer to the blockchain.

Transaction process	Differences between the transactions
Anton and Anna each agree a transaction with Kim in which Kim is to receive €50. Anna makes the transaction using a blockchain, while Anton uses a central authority such as a bank.	In the case of transactions without blockchain technology, the central institution has to be trusted to carry out the transaction reliably, keep data secure and only use data for the authorized purposes. Such services often incur high fees. When using blockchain technologies, one has to be confident that the blockchain technology works properly.
Anton instructs the bank to transfer €50 to Kim. The bank uses its central cash book to check whether the transaction can be permitted. Anna sends the value of €50 via the blockchain. In the blockchain, the participants check whether the transaction is permissible.	Blockchain technologies clearly define and state which transactions are permitted. In transactions without blockchain technology, the central institution's conditions of use need to be examined and interpreted to understand which transactions are legitimate. However, the central institution might interpret these conditions differently – and can change them unilaterally. The computers of the blockchain network have to build a consensus. The necessary consensus mechanisms, however, can consume a lot of energy, as in the case of the Bitcoin blockchain.
The bank executes Anton's transaction, debiting Anton's account with the amount of €50 and crediting €50 to Kim's account. The transaction is recordedin the ledger. Anna's transaction is combined with other transactions in a block, marked with a digital fingerprint (known as a hash) and then communicated to the entire blockchain network. The new block is chained to the previous block by referring to the hash of its predecessor.	Transactions stored in a blockchain cannot be changed at a later date. A central institution, on the other hand, is able to change or delete transactions. In addition, a successful cyber-attack on a central institution can result in its services being unavailable. In a blockchain, the ledger is stored on many different computers, meaning that data remains available even if some computers fail. Recording a transaction in a central ledger is a quick process that requires few resources. Recording a transaction in a blockchain, on the other hand, requires more resources because the transactions are sent to and stored by all computers in the network. This also requires greater memory capacity.
To review the transaction with Anton, Kim can check her bank account. To review the transaction with Anna, Kim can check the block with her transaction.	To inspect the current status of stored transactions, a request has to be sent to the central institution. Blockchain participants can directly access and view the transactions stored in a blockchain. In addition to transactions, a central institution also stores data about its users, such as their names, passwords and credit card details. While these institutions do have security features in place to protect against theft, various hacks have shown that such provisions do not offer complete security.

Glossary:

A **ledger** records and stores transactions (potentially digitally). A transaction is a sequence of steps that form a logical unit. The nature of transactions can vary considerably – and include tasks such as transferring money from one person to another, posting on social media or sharing information between companies or authorities.

A **central institution** maintains the ledger. As a result, the institution holds sole control over the recording and storing of transactions. Examples of central institutions include banks, legal advisers and social media.

A **network** is composed of computers that are connected and therefore able to exchange information.

A **blockchain** is a digital ledger simultaneously stored on numerous different computers. A blockchain is composed of blocks connected in a chain.

Blocks bundle transactions, similar to a page in a ledger. In addition, each block contains information that connects it to the previous block and thereby renders its content immutable. This renders both the transactions within a block and the sequence of blocks immutable.

Consensus describes a situation in which all computers agree on the correct state of the blockchain and the transactions stored in it.

Consensus mechanisms ensure that the computers form a consensus, even if there might be computers within the network seeking to disrupt it, such as by sending false information.

Box B 3-3

Operating principle of blockchain technologies

Blockchain is a technology that enables the digital storage and transmission of data. All transactions are stored by numerous computers[362] and information about new transactions is shared between the computers in the blockchain network. New transactions are compiled in a block of a specific size and cryptographically connected with all previous blocks in a chain (cf. figure B 3-2).[363]

This process does not feature a central authority – such as a bank – that checks that transactions are correct. Therefore, no trust is required between the participants ex ante. This is ensured by technical functions and economic incentives.

Blockchains can either be open to everyone (public) or limited to a specific group of participants (private or permissioned). Examples of public blockchains include the Ethereum and Bitcoin blockchains.[364] In consortium blockchains, only a specific group of people are authorized to view or save transactions. This could include various companies who want to record transactions together but wish to ensure that such transactions do not become publicly accessible. In a private blockchain, the access rights are further restricted, for example to allow only one specific company to save transactions in the blockchain.

The high level of security that blockchains offer rests, among other things, upon the consistent and systematic use of cryptographic processes. These processes are used to ensure that the identity of the transaction partners and the transactions themselves are correct, i.e. that they have not been falsified, and to make sure that past transactions cannot be altered.[365] When checking the legitimacy of a transaction, the network ensures, among other aspects, that only new transactions can be added to the blockchain and that the resources to be transferred actually exist. Transactions which have already been saved cannot be manipulated. As a result, the entries in a blockchain are immutable. This feature is ensured by cryptographic hash functions that allocate an easily identifiable fingerprint (known as a hash) to transactions within a block. If just one character within the transaction is changed, it would be obvious that the hash is not correct. The hash function SHA-256 would give the transaction

Anna sends €50 to Kim.

the following hash:

bfc31d9b353de84eb1ddaf1aa13bf02a34dae95287498b5d5653fa10c086812a.

This hash is stored in the original block with the transaction between Anna and Kim. If Anna wished to change the transaction at a later date and debit Anne instead, the same hash function would give the transaction

Anne sends €50 to Kim.

the following hash:

cc00ae6db2eedfbc703f95de9a82700a9778281c67ef8a7d9d2a592abf24ea08.

This hash is obviously in conflict with the hash saved in the original block. Furthermore, the following block includes its predecessor's hash as a reference – thereby the blocks are chained to each other. Therefore, a transaction can only be successfully manipulated if all subsequent blocks are also changed accordingly.

This is why the legitimation of new blocks by computers in the blockchain network is so important. The rules for this constitute so-called consensus mechanisms. The choice of the consensus mechanism depends to a large extent on the access rights of the computers in the network. In a consortium blockchain in which the participants know each other's identities, security and reliability can also be enforced outside the blockchain. This makes it possible to use other consensus mechanisms, such as those based on plurality voting systems. By contrast, the users of public blockchains by and large remain anonymous. This means that, as the security of such blockchains cannot be enforced

outside of the blockchain, such provisions need to be integrated in their protocols. There are various approaches to achieve this, such as proofofwork (PoW) and proofofstake (PoS). These approaches use economic incentives and financially penalize misconduct, such as confirming non-legitimate blocks.

To create a new block for a PoW blockchain, a computing-intensive cryptographic problem must be solved. This process is known as mining. The task is to find a number, known as the nonce, so that the block's hash starts with a specific number of zeroes. The nonce, like the target value for the number of zeroes, is stored in the block. This makes it possible to check straight away whether the work to create the block has actually been carried out – hence the name proofof-work. The first miner to create a correct block and find an applicable nonce receives a fee in the corresponding blockchain currency (e.g. Bitcoin) as payment for their work.

The computing power required to solve this cryptographic problem consumes high levels of electricity. Electricity costs form an economic incentive that prevents many new blocks of the blockchain from being generated to manipulate an earlier transaction in the blockchain. The incentive for manipulation arises from weighing the profit of manipulation and the associated costs of mining – in this case the costs for electricity and computers.

PoW is a very secure consensus mechanism that can also enforce the rules of a blockchain when participation is unrestricted and when the network could contain faulty computers or participants with malicious intentions. However, such mechanisms require so much power that, in 2018, the Bitcoin blockchain consumed about as much energy as Austria.[366]

An alternative to PoW in public blockchains is the PoS consensus mechanism. PoS consumes markedly less energy than PoW and includes incentives to discourage mistakes by requiring a deposit to be paid before a user can validate blocks.

Once a new block has been created, it has to be sent to the entire network and saved by the participating computers. This process is considerably more demanding than saving a transaction in a central ledger because it has to be repeated for all computers in the network. The eschewal of a central storage system means that blockchain technology is also less susceptible to malfunctions.

In addition to the fundamental operating principle of blockchain technologies, there are a range of extensions with varying degrees of maturity. The aims of current development projects include increasing transaction throughput[367] and creating a connection between different blockchains. Another extension has already been introduced with the introduction of the Ethereum Blockchain: the automatic execution of processes on the blockchain by so-called smart contracts. Smart contracts are computer programmes that are also stored in the blockchain.[368] They make it possible, for instance, to implement if-then relationships, such as: "If Kim delivers the shipment of gummi bears to Anna, then €50 will be transferred from Anna to Kim". Smart contracts have the potential to reduce transaction costs by formalizing the conditions for transactions and executing them automatically. This gives rise to a further motivation to dispense with central institutions.

of 2018.[369] However, the security precautions of blockchain technologies are usually not overcome in these thefts. Instead, such thefts often occur in central cryptocurrency exchanges.[370] Nevertheless, there have been repeated cases in the past in which small blockchain networks – i.e. blockchains in which the miners (cf. box B 3-3) have relatively little computing power – have been the victims of so-called 51 percent attacks.[371] Blockchains with high levels of computing power are significantly less likely to become victims of 51 percent attacks. The security that blockchain applications provide (cf. also box B 3-3) is a key reason for their use. The notion that blockchain technologies may not be secure can therefore negatively impact their diffusion.

An important distinction must be made between a blockchain such as Ethereum, which represents infrastructure, and the applications which build on it. This distinction is comparable to the difference between TCP/IP internet protocols on the one hand and applications, such as the World Wide Web with its webpages and email, on the other. Decentralized applications that build on a blockchain are known as dApps (decentralized apps). For example, dApps acting as a browser or wallet facilitate the interaction with a blockchain. Furthermore, they provide applications such as social networks, trading platforms or identity management. dApps thereby make it possible to use blockchain technologies without an in-depth technical understanding. They also generate additional functionalities for users and thereby contribute to the technology's diffusion.

The most important actors in the blockchain ecosystem include: institutions behind certain blockchains, such as the Ethereum Foundation; miners, who undertake validation in proof-of-work blockchains; companies that offer applications on the basis of blockchain technologies, and companies that provide complete blockchain solutions. The latter group includes major technology firms such as IBM, Amazon, SAP and Microsoft, that offer blockchain solutions in the form of software-as-a-service.

In the past, start-ups that develop blockchain applications or blockchain infrastructure have often used a new financing instrument known as initial coin offering (ICO). An ICO involves selling digital tokens that can later be used, for instance, to use the services of the blockchain application. Such methods are supplemented by rounds of classic financing using venture capital to finance blockchain companies.

Blockchain applications generate revenue from their users by applying usage charges such as freemium or subscription models. Miners receive payments for their work in the cryptocurrency of the blockchain for which they confirm a block.

Applications and potential of blockchain technologies B 3–3

Blockchain applications can be found in many different fields. The motivation for using or testing blockchain technologies is often a combination of three distinct considerations: i) securing transactions, ii) automating transactions and iii) decentralized data storage and access management.

The use of blockchain technologies in international supply chains (cf. box B 3-1) is an example of cross-company (and therefore decentralized) data storage. Public authorities can also deploy blockchain technologies to intensify the exchange of information, automate process steps and thereby improve cooperation between authorities. Box B 3-5 provides an example of the successful use of blockchain technologies in the asylum process.

When regulatory authorities and companies implement blockchain technologies, this can lead to enhanced transparency and lower the costs involved in fulfilling transparency requirements. This was demonstrated by a pilot project conducted by the UK Financial Conduct Authority (FCA) in cooperation with two global banks.[372] The banks in question were able to fulfil their reporting obligations for mortgages much more easily than in the past.[373] So far, banks and regulatory authorities have spent up to four weeks preparing and providing data. By using blockchain technologies, the banks were able to significantly reduce the time taken up by reporting processes. This new approach also made it possible to produce reports almost in real-time; previously, reports were only made available on a quarterly basis at most.[374]

Data saved in blockchains cannot be deleted or changed. Consequently, blockchain technologies are suitable for making information verifiable and reliable.[374] The immutability of data is used to file

tax-relevant information, as for example invoices in the online trade, in a forgery-proof form. In medical research, this aspect is used to secure automatically generated data from analysis systems. This rules out the possibility that the data will be manipulated.[376]

An example of process automation through sart contracts can be found in the insurance sector. By taking publicly accessible data on flight times as a basis, a major international insurance company offers insurance against flight delays. Due to

Box B 3-4

Blockchain governance

Governance describes the manner in which an organization – in this case the blockchain and its stakeholders – is managed or governed. For blockchains, governance includes the set of rules contained in the blockchain protocol, often described as on-chain governance. Onchain governance includes, for example, a consensus mechanism (cf. box B 3-3). Offchain governance, on the other hand, comprises decision-making rules for amendments to the blockchain's protocol or criteria by which to select people who validate transactions (in the case of restricted groups of validators). In contrast to elements of onchain governance, elements of offchain governance are not compiled and codified but instead arise as a result of lived experience. In the case of public blockchains, for example, an opinion leadership of prominent persons of the blockchain developer community is often established.

The design of governance systems can play an important role in realizing the potential benefits of blockchain technologies. For instance, the use of blockchain technologies is often aimed at reducing dependence on an intermediary or a central authority. However, the use of blockchain technologies does not necessarily guarantee the avoidance of central authorities. This recentralization of blockchain technologies can result from the governance of the blockchain if prominent persons have been able to establish opinion leadership or if a closed group of actors is responsible for validating transactions in private blockchains.

In addition, less strict onchain and offchain governance and blockchain security often have conflicting objectives. At the very least, ensuring the blockchain's security requires either strict on-chain governance or strict off-chain governance. Public blockchains – in which anyone can validate transactions (as participants usually remain anonymous) therefore usually use proof-of-work as a consensus mechanism in order to ensure adherence to the blockchain's regulations (cf. box B 3-3). On the other hand, private blockchains in which transactions can only be confirmed by participants whose identities are known can be based on other consensus mechanisms as adherence to the regulations can also be enforced outside the blockchain. This makes it possible to avoid the drawbacks of proof-of-work systems, such as the high energy requirements. Public blockchains in which anyone can validate transactions are referred to as public unpermissioned blockchains. By contrast, public blockchains in which only certain participants can validate transactions are known as public permissioned blockchains.

Public permissioned blockchains can also be made open to all validating participants (or organizations) who fulfil specific criteria. These criteria might relate to having business operations in a particular sector of the economy, as applied by the Energy Web Foundation,[377] or require participants to be not-for-profit organizations, as is the case for the Interplanetary Database (IPD).[378] Selecting participants in this way can help to create transparent governance structures without recentralizing the blockchain to a closed group of validating participants.

Box B 3-5

The use of blockchain technology in the asylum process

Blockchain technology has already been used in Germany as part of a proof-of-concept for the reliable and expedient exchange of information in asylum processes.[379] In this case, it supported the exchange of information between reception centres, the Federal Office for Migration and Refugees (BAMF) and the immigration authorities. The evaluation identified "significant benefits in terms of process reliability, transparency and efficiency".[380]

In the asylum process, asylum seekers are registered at an initial reception centre before being allocated to a reception centre. If an application is lawfully submitted, the BAMF holds a hearing to examine the case. If the BAMF decides to approve the asylum application, the immigration authorities then issue a residence permit. To ensure that this process proceeds both quickly and reliably, the various authorities must at all times observe and apply the regulations governing the asylum procedure and must have access to up-to-date information on each case. Blockchain technology improves on the current situation in both regards.

Decentralized data storage (cf. box B 3-3) means that the relevant authorities can always check the current status of an asylum case. As a result, data from the various systems in different departments – such as the workflow and document management system at the BAMF or the personalization infrastructure components at the initial reception centres – can be integrated and made available to all participating authorities. Furthermore, by using smart contracts stored in the blockchain (cf. box B 3-3), processes can be automated, making it possible to avoid deviations from established processes or document them in full as and when they occur. This minimizes waiting times between the authorities' work steps and renders the entire process markedly more reliable.[381]

The blockchain architecture for the asylum process, analysed using proof-of-concept development, was implemented in 2018 as part of a pilot project overseen by the BAMF, the immigration authorities and the Dresden AnkER Centre.

transparent smart contracts, insurance cases are processed automatically as soon as flight delays occur.[382] In addition to insurance policies, blockchain technologies are used for various other applications relating to financial transactions, such as payment infrastructure between banks.[383]

Several European countries[384] are currently piloting blockchain-based land registers. This would automate processes such as requesting a land register excerpt or creating a land register entry. The services of intermediaries such as notaries and banks would no longer be required to the same extent for such tasks, while the administrative costs of maintaining a land register could also be reduced. In countries without a functioning land register, this would make it possible to establish a reliable register for real estate, even where public trust in state authorities has been damaged.[385]

Blockchain technologies can also be used to create digital keys that should not be copied – such as keys to apartments, houses and cars. In the case of locks, the property owner can use a smart contract on the blockchain to define the conditions for opening the lock. These conditions might include paying a deposit or paying rent in advance. The tenant can then use their smartphone to confirm their identity and will be given access to the apartment if confirmation that these conditions have been fulfilled is entered in the blockchain.[386]

Such applications are evidence that many actors are currently developing, testing and introducing blockchain technologies to create marketable products. Yet these still represent just a small subsection of the areas in which blockchain technologies are used. The blockchain's potential extends far beyond these applications; indeed,

blockchain technologies can lead to radical changes in existing industries. In the energy industry, for example, blockchain technologies can be used to provide transparent information about the costs of operating a power network, thereby allowing network charges to be levied efficiently and fairly based on consumers' actual usage. Box B 2-7 describes potential applications of blockchain technologies for the energy sector.

On an even more fundamental level, however, blockchain technologies are transforming the way in which we store data. Blockchain technologies allow data to be stored securely and in a decentralized manner. On this basis, individuals have the ability to retain control of their own data rather than having to cede this control to central institutions such as major internet companies. This gives hope that citizens and companies could make their data more accessible and allow it to be used under controlled conditions.[387]

Decentralized data storage is ultimately also associated with hopes of easing the market concentration in data-driven industries and dismantling barriers to entry in such markets. Blockchain technologies therefore have the potential to engender significant changes in market structures and induce radical transformations.

Yet despite the range of highly promising applications and the potential of such technologies to disrupt existing structures, it remains to be seen whether blockchain technologies will be able to become a cross-cutting technology in future. Whether the expectations placed upon it will actually prove feasible depends to a large degree on blockchain governance (cf. box B 3-4).

B 3-4 Germany as a blockchain location

Germany is home to an active community of developers working on blockchain technologies. Almost half of all German blockchain start-ups are based in Berlin.[388] Domain experts believe that this concentration of development activity makes Germany – and Berlin in particular – a key international location for blockchain technologies.[389] Berlin has a high concentration of developers who work to develop blockchain infrastructure. Prominent organizations in this regard include: the Web3 Foundation, which promotes the development of a decentralized internet; the Energy Web Foundation, which works to create open blockchain technology for energy markets, and the IOTA Foundation, which develops blockchain technology for IoT applications. The Ethereum Foundation plays a particularly important role,[391] as Ethereum is currently a quasi-standard in the blockchain community.[392]

However, it is difficult to conduct a precise assessment of Germany's performance in an international comparison. There are various reasons for this. For one, blockchain development activities and their objectives are heterogeneous. Developments relating to the fundamental infrastructure of blockchains, such as the work conducted by the Ethereum Foundation, is often the result of a group of developers working on open source software. These developers collaborate internationally, which makes it difficult to pinpoint a single location. At the same time, working on open source software makes it impossible to compare development activities by analysing patent figures because open source software is, by its nature, not patented. Another approach is to attempt to compare the number of blockchain start-ups in different countries.[393] However, such lists (and in particular those which make international comparisons) are often incomplete and can therefore produce a distorted image of the international distribution of blockchain start-ups.

Nevertheless, it is clear that Germany finds itself in a dynamic, competitive market in which other countries are becoming increasingly attractive locations. The world's largest initial coin offerings (ICOs), a financing instrument used by blockchain-related start-ups, took place outside Germany.[394] Of the 20 largest ICOs to date only one took place in a European country: Switzerland. One of these start-ups, Tezos, is working to develop a blockchain technology in which all users have a right to co-determine the future development direction of the technology.

B 3-5 Barriers to the diffusion of blockchain technologies

There are still various barriers making it hard to develop blockchain technologies further and thereby realize their potential in commercial and societal applications. These barriers primarily relate to technological development, regulation and legislative as well as political and societal acceptance.

As a result, technological solutions that deliver higher scalability of public blockchains are still yet to be launched. Moreover, popular blockchains such as Bitcoin and Ethereum have so far used energy-intensive PoW consensus mechanisms which create serious negative climate externalities (cf. box B 3-3).[395]

In terms of the legal and regulatory framework conditions for the use of blockchain technologies, Germany has for the most part adopted a cautious, watchful approach.[396] At present, there is a lot of uncertainty around the application of the General Data Protection Regulation in the context of blockchain technologies, the classification of ICOs, the taxation of cryptocurrencies, and the use of blockchain technologies in regulated markets such as the energy sector.[397] To reduce this uncertainty, qualified people must be appointed in ministries and public authorities. Barriers to communication between the political, administrative sphere on the one hand and the blockchain community on the other need to be dismantled.[398] There are also barriers with respect to the potential users of blockchain technologies. For instance, the wider public lacks a broad understanding of the potential uses and benefits of blockchain technologies, due in part to the overly abstract and technical descriptions of blockchain technology, with too little connection to practical applications available today.

B 3-6 Recommendations

The Commission of Experts considers blockchain technology to have significant potential to benefit companies, citizens and administrative bodies. To realize this potential, the Commission of Experts recommends that the Federal Government enact the following measures:

- The Federal Government's planned Blockchain Strategy should contain an analysis of Germany's strengths and weaknesses as a location for blockchain technology. This would include analysis of current legal and regulatory framework conditions which inhibit innovation.
- The strategy should include proposals for Regulatory Test Beds, which would allow the identified barriers to innovation to be tested and legal amendments prepared.
- The Blockchain Strategy should specify interfaces with other strategies formulated by the Federal Government in relation to digital policy, such as the AI Strategy and the implementation strategy for digitalization. Synergies generated by these strategies should also be identified and exploited.
- Companies' legal uncertainty has to be reduced by developing skills and domain expertise of relevant people in ministries and authorities. These enhanced competencies should also be used to analyse application concepts for blockchain technologies and, where prudent, to initiate pilot projects.
- Finally, citizens and companies should be better informed of the benefits and drawbacks of blockchain technologies; this would equip them with the skills and knowledge required to handle blockchain applications with confidence.