DOI: 10.1007/s10272-017-0706-3

Volker Brühl

Virtual Currencies, Distributed Ledgers and the Future of Financial Services

The phenomenon of virtual currencies has to be distinguished from the underlying distributed ledger technologies. Bitcoin and other cryptocurrencies need to be subject to strict financial regulation and supervision to ensure investor protection. At the same time, distributed ledger technologies will shape the future of the financial services in many respects. The disruptive potential is illustrated for selected financial products and processes.

The digitisation of the financial services industry is transforming the value chain of banks, insurance companies and other financial services providers. Established business models are challenged by new incumbents such as start-ups ("fintechs") and technology firms like Google, Facebook, Apple and Amazon. Hence, established players need to reinvent themselves by redesigning product offerings, modernising their IT infrastructure and restructuring the value chain.

As a consequence, internal processes are being streamlined, non-core activities are being outsourced on a large scale and the customer interface has been digitised by smartphone apps such as personal finance tools or wallet apps. Intelligent concepts for multichannel management, combining internet-based and physical distribution channels, have been a major challenge for financial institutions in recent years. In the meantime, more fundamental changes to business processes and product offerings have been triggered by artificial intelligence, big data, machine learning and the distributed ledger/blockchain technology.

The blockchain technology was originally developed for payment services based on virtual currencies, also called cryptocurrencies, as they use cryptographic methods to encode payments. Cryptocurrencies such as bitcoin were invented to facilitate instant payment services with no need for a central bank or financial intermediaries to execute payments. Using cryptographic functions, every user of the bitcoin system can transfer units of the virtual currency globally on an anonymous basis. The technological foundation is a peer-to-peer computer network that validates and executes each and every transaction in a tamper-proof manner, almost instantaneously and at very low marginal costs. However, financial supervisory authorities are about to increase regulation of virtual currencies due to concerns that the anonymous character of the system facilitates money laundering and the financing of illegal transactions.

Nevertheless, the underlying blockchain technology, or in broader terms, the distributed ledger technology, has the potential for disruptive changes in several segments of the financial services industry and beyond.[1] There is still a lot of uncertainty, including among regulators, as to whether or not virtual currencies have to be treated like currencies or even securities and to what extent related services fall under existing financial services regulations.

In 2015 the New York State Department of Financial Services approved a regulation that requires a business license (BitLicense) for companies in New York engaging in virtual currency activities – including storing, controlling, trading or exchanging bitcoins or any other cryptocurrency.[2] So far there is no nationwide regulation of the issuing and business activities of virtual currencies. Nevertheless, both the US Federal Reserve and the Securities and Exchange Commission (SEC) keep a close eye on developments in the field of cryptocurrencies, occasionally commenting on specific features or events around cryptocurrencies, e.g. the SEC on Initial Coin Offerings.[3]

Volker Brühl, Center for Financial Studies, Frankfurt, Germany.

1 See e.g. R. Wattenhofer: The Science of the Blockchain, Zurich 2016, CreateSpace Independent Publishing Platform.
2 New York State, Department of Financial Services: New York Codes, Rules and Regulations, Title 23. Department of Financial Services, Chapter I. Regulations of the Superintendent of Financial Services, Part 200. Virtual Currencies, 2015.
3 U.S. Securities and Exchange Commission: Investor Bulletin: Initial Coin Offerings, 25 July 2017.

The European Banking Authority has repeatedly pointed to the risks of virtual currencies.[4] On 5 July 2016, the European Commission suggested amending the Fourth Anti-Money Laundering Directive (EU 2015/849), adopted on 20 May 2015, to extend its scope by including exchange platforms and wallet providers for virtual currencies.[5] This could mean the de facto end of anonymous virtual currency networks in the EU. On the other hand, critical voices are concerned that the new regulatory initiatives would endanger the development of the innovative distributed ledger technology in Europe.

The discussion about the future of virtual currencies has been fuelled recently by the bitcoin price reaching US $10 000, a price increase of 1000% since the beginning of the year.

The purpose of this paper is to investigate the future potential of virtual currencies as innovative payment systems along with the possible impact of the underlying blockchain technology on transaction processing and corporate finance. The disruptive potential of peer-to-peer networks and distributed ledgers is illustrated for payments, securities settlements, trade finance as well as primary debt and equity capital markets.

Bitcoin, blockchain and distributed ledgers

Blockchain technology was originally developed as a platform for virtual currencies. Bitcoin and other cryptocurrencies such as Ripple, Ethereum or Litecoin are not money in a traditional sense. Rather, they are units of account used as a medium of exchange in multilateral private networks, in which the users agree on the mutual acceptance of such virtual currencies. An approval of their introduction and utilisation by financial supervisory authorities is usually not required as long as the usage is limited to private agreements and no additional services, such as the operation of exchange platforms or brokerage services, are introduced.[6]

Cryptocurrencies allow the initiation and execution of direct payments from senders to receivers of units of the respective virtual currency almost in real time and without financial intermediation. These web-based payment systems apply cryptographic methods in order to conduct payments safely, quickly and cost-efficiently through a peer-to-peer computer network.[7] Although the cryptographic algorithms differ in certain parameters, the functioning of all virtual currencies is based on the same principles, which are outlined below using bitcoin as an example.

Bitcoin is the first and so far most popular cryptocurrency. The open-source reference software Bitcoin Core was published in 2008.[8] All transactions with bitcoins are recorded in a distributed ledger, summarised in transaction blocks and interlinked in such a way that a full and tamper-proof chain of transactions and the respective blocks – i.e. a blockchain – is generated. All transactions are irreversible. Every user of the network can view and check the validity of any transaction in the blockchain at any point in time. However, the personal identity of the owner of the bitcoins remains confidential.

New bitcoins are not generated through the interaction of monetary policy instruments of central banks, commercial banks and bank customers, but rather through a specific incentive system that rewards those nodes of the network that are the first to prove the authenticity of encrypted transactions with a mathematical algorithm. The process of validating new transactions, combining them into new blocks and distributing the reward in the form of new bitcoins to the winning node of the network is called mining.[9] Hence, bitcoins and other virtual currencies are based on the trust of the participants in the security and integrity of a decentralised computer network, not on the credibility of a central bank. Each participant in the bitcoin network must use a suitable software program ("wallet") to get access to the bitcoin reference software that allows users to manage their own bitcoins and execute bitcoin transactions.

To execute a bitcoin transaction, the sender uses his wallet software to generate a cryptographic key pair, which consists of a private key and the corresponding public key. The private key is the private portion of a key pair which can create cryptographic signatures that other users can verify with the public key. The transfer of bitcoins requires a bitcoin address of the receiver, which is usually

4 European Banking Authority: Opinion on 'virtual currencies', EBA/Op/2014/08, 2014.

5 European Commission: Questions and Answers: Anti-money Laundering Directive, Fact Sheet, 5 July 2016.

6 J. Münzer: Bitcoins: Supervisory assessment and risks to users, German Federal Financial Supervisory Authority, 17 February 2014, available at https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2014/fa_bj_1401_bitcoins_en.html.

7 In contrast to client-server architectures, the nodes of a peer-to-peer network share resources without the use of a centralised administrative system. See e.g. C. Schindelbauer, P. Mahlmann: P2P Netzwerke: Algorithmen und Methoden, Berlin 2007, Springer.

8 S. Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System, White paper, 2008.

9 See J.A. Kroll, I.C. Davey, E.W. Felten: The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries, The Twelfth Workshop on the Economics of Information Security (WEIS 2013), Princeton University, Washington DC, 11-12 June 2013; and https://bitcoin.org/en/glossary/mining.

a string of 34 digits generated by the wallet software using a cryptographic method. Bitcoin addresses are usually used only once for security reasons.

Subsequently, the sender can generate a bitcoin transaction, which must contain the bitcoin address of the receiver in a predefined format, the amount of bitcoins to be sent and the references to all previous transactions, which confirms that the sender is the legitimate owner of the bitcoins to be spent. Next, the sender uses the signing algorithm of his private key to generate a signature of the data, which is then sent as an encrypted message along with the public key to the receiver and to the whole bitcoin network.

The receiver can then use the public key to verify the validity of the transaction, i.e. she can verify whether or not the sender has sent the bitcoins and whether he is the legitimate owner of the bitcoins, as the signature can only be generated by the owner of the private key corresponding to the public key sent. The receiver's wallet software displays the received number of bitcoins as spendable balance, which is categorised as "Unspent Transaction Output" by the network.

New transactions are broadcast in parallel to all nodes of the network, which check the validity of the transactions decentrally and try to combine them into a new block that will be added to the blockchain. The design of the blockchain for bitcoin also solves the "double spending problem", as it ensures that bitcoins can only be spent once.[10]

In order to ensure that all nodes have the same status of the blockchain at any given point in time and that the validity of all transactions – and ultimately of the blockchain as a whole – is continuously verified by the network, a proper incentive system is needed to generate new blocks. This is accomplished by the so-called mining process, which stipulates that for the generation of every new block, a mathematical problem has to be solved by the miner with cryptographic hash functions.

In order to generate a new block, a cryptographic function has to generate a hash value of the block header which is below a defined target value. Hash values are generated by hash functions that use cryptographic algorithms to transform arbitrary data into strings that seem to be random but are deterministic. The bitcoin system uses the SHA (security hash algorithm) 256 function that generates hexadecimal outputs with 64 digits and a length of 256 bits.[11] Even small changes of the input data lead to substantially unpredictable output data, which implies that for each input there is a unique deterministic output, but it is not possible to deduce the input data given the output data.

Each block has its own hash value that is a result of the hash values of all transactions in the block and the hash value of the previous block. Thus, a linear chain of blocks is established which reflects the full history of transactions in a time-stamped and tamper-proof manner.

Each block contains a number of new transactions that are saved in the transaction part of the block. Thereafter, copies of the transactions are repeatedly paired and hashed until a single hash value is generated. This value is called the "Merkle root" of the corresponding "Merkle tree" that maps the transactions in the block. The Merkle root reflects the cryptographic image which is saved in the block header. The block header also contains the hash value of the previous block and a dedicated field NONCE (Number Only Used Once).[12]

The miners, i.e. the nodes of the network intending to generate new blocks, have to search for a random number by applying search algorithms until they have found a specific value for the NONCE field so that the resulting hash value of the block header is below the required target value. Due to the characteristics of the SHA 256 function, the miners have to solve this mathematical problem through a trial-and-error process. This requires the investment of CPU (Central Processing Unit) time and energy. The costs associated with the process increase with the length of the blockchain and the determined target value for the hash value of the block. The average number of hash operations increases as the blockchain gets longer and the target hash value is set lower. The process of solving the cryptographic problem is called "proof of work", as the generation of a new valid block is the proof that the miner has invested economic resources to generate a new block. This factor is essential to ensure that there is no easy way of changing the transaction history and hence manipulating the flow of bitcoins between legitimate senders and receivers.[13] The newly generated block is then broadcast to all other nodes of the network,

10 The double spending problem refers to the fact that virtual currencies are digital tokens and may therefore easily be copied and hence spent several times.

11 See e.g. K. Schmeh: Kryptografie: Verfahren, Protokolle, Infrastrukturen, 6th edition, Heidelberg 2016, dpunkt.verlag.

12 R.C. Merkle: A Digital Signature Based on a Conventional Encryption Function, in: C. Pomerance (ed.): Advances in Cryptology – CRYPTO '87, Lecture Notes in Computer Science, Vol. 293, Berlin 1988, Springer, p. 369-378.

13 See e.g. M. Jakobsson, A. Juels: Proofs of Work and Bread Pudding Protocols, Communications and Multimedia Security, Deventer 1999, Kluwer Academic Publishers, pp. 258-272.

which verify the validity of the block and eventually add it to their image of the blockchain.

If competing miners find a new valid block at (nearly) the same time, forks in the blockchain can temporarily arise. However, as the network always adds new blocks to the longest blockchain, such forks usually disappear quickly. A complete, tamper-proof transaction history mapped into a blockchain evolves from the process of generating individual transactions and combining them in new interlinked blocks. Once the network has reached consensus on the accurate transaction history, each node of the network records a copy of the current status of the blockchain. This is a distributed ledger which is publicly accessible but preserves privacy, as only the owners of the respective Private Keys can view the details of the transactions they are involved in.

The cryptographic chaining of transactions and blocks implies that single transactions cannot be modified *ex post* without changing the corresponding block as a whole and all subsequent blocks. Therefore, the proof-of-work concept prevents easy manipulations of past transactions, as potential hackers would have to control more than 50% of the CPU power of the whole bitcoin network. This is theoretically possible but would be exorbitantly expensive.

The role of miners is pivotal to the integrity of the whole bitcoin system, as the miners, through the proof of work, ensure the authenticity of blocks, transactions and ultimately the entire blockchain. The miners, therefore, receive a reward in the form of new bitcoins for generating new blocks. The mining reward is halved every 210,000 blocks, and the maximum amount of bitcoins is 21 million.[14] Neither the absolute size of the mining reward nor the calibration of the bisection rhythm or the adjustment period were substantiated by the inventors of the bitcoin system. On the introduction of bitcoin in 2009, the mining reward was 50 bitcoins, which was cut to 25 bitcoins in November 2012. In July 2016, the mining reward was cut again to 12.5 bitcoins. As of 27 November 2017, approximately 16.7 million bitcoins have been issued.

The lower the threshold for the target hash value of a new block is set, the higher the average computing time miners have to invest to find new blocks. As the CPU power of the network increases over time, the difficulty of the proof of work has to be adjusted from time to time in order to keep the target average time of ten minutes to generate a new block.

14 See www.bitcoin.org.

Market development of bitcoin

The usage of bitcoins, measured by the average number of daily bitcoin transactions, has visibly increased over recent years. However, the current level of approximately 250,000 transactions per day is still low compared to established payment systems such as Visa, which handled almost 100 billion transactions in 2014. Overall growth dynamics and the dissemination of bitcoins or other virtual currencies appear too low to expect established payment systems to be challenged in the foreseeable future.

Lack of credibility and integrity

A major barrier to a higher acceptance rate for bitcoin may be rooted in the anonymity of the system and the lack of intermediaries. While bitcoin promotors view this as a major beneficial differentiating factor compared to traditional payment systems, it is precisely this lack of properly regulated financial intermediaries and appropriate supervisory processes – which ensure the stability, credibility and integrity of any financial system – that causes mistrust and concern about the integrity of the system itself.

There is already evidence that users of virtual currencies may experience substantial economic damages, e.g. through a theft of private keys by hackers who are protected by the anonymity of the system. There are several prominent examples of the abuse of the system, including Silk Road, an exchange platform for mostly illegal transactions on the darknet that was closed in 2013, the insolvency of the bitcoin exchange Mt. Gox in 2014 or the recent loss of at least US $70 million from the Hong Kong-based bitcoin exchange Bitfinex.

Although virtual currencies are not currencies in the sense of generally accepted mediums of payment, some customers, especially those with a limited level of financial literacy, might get the wrong impression. This mistaken impression would be reinforced by the fact that a growing number of countries permit the establishment of bitcoin ATMs, which allow the exchange of cash in a traditional currency into bitcoins and vice versa. These bitcoin ATMs look very similar to traditional ATMs, but they do not connect to a bank account. Instead, they allow the insertion of cash in exchange for bitcoins, which are given as a paper receipt or by moving money to a public key on the blockchain. Recent data published by Coin ATM Radar report a total of more than 1500 bitcoin ATMs, of which 75% are located in North America.[15] This physical

15 Coin ATM Radar: Share of Bitcoin ATMs by Continent, 14 September 2017, available at https://coinatmradar.com/charts/#by-continent.

access to bitcoins may also generate misperceptions that bitcoins are a trustworthy medium of payment.

Low barriers to entry

Since the introduction of bitcoin, a large number of new virtual currencies have been launched, the most notable of which are Ethereum, Ripple and Litecoin. As of the end of August 2017, more than 1000 virtual currencies have been registered. Each of the five largest in terms of market capitalisation shows a total value of circulating units of at least US $2 billion. When it comes to offering a new virtual currency, barriers to entry are low. All one needs is a cryptographic algorithm, a process of generating and distributing additional units of the respective currency (e.g. mining), and a consensus algorithm to ensure the network reaches a common understanding about the correct status of the distributed ledger. The high number of virtual currencies casts some doubt on the viability of most of the business models being pursued.

High volatility

The level of uncertainty about the future of bitcoin is also reflected in the volatility of the bitcoin price. On 13 August 2017, the bitcoin price exceeded US $4000 for the first time, a 400% increase since the beginning of 2017. This was followed by a sharp decline in September when BTCChina – the largest bitcoin exchange in China – stopped trading bitcoins following a ruling by the Chinese authorities. Then on 28 November, the price surpassed US $10 000 for the first time. Other prominent cryptocurrencies, like Ethereum and Ripple, showed similar patterns of price developments.

Market observers offer different explanations for the recent bitcoin boom. One frequently cited factor is the split of the original bitcoin blockchain through the establishment of a parallel chain, Bitcoin Cash, on 1 August 2017. The reason for this split lies in an ongoing discussion about the best strategy to accelerate the transaction process without increasing transaction costs. While the core bitcoin developer team is in favour of separating the transaction data from the respective signature (the so-called SegWit approach), the representatives of Bitcoin Cash have increased the average block size to free up capacity in the network. Another explanation for the rising bitcoin price is the growing customer acceptance of the cryptocurrency, e.g. in Japan. But the increase in bitcoin transaction volumes is too low, both in absolute and in relative terms, to trigger the recent price increase.

To sum it up, there is simply no plausible economically sound explanation for the boom in the bitcoin market, as the fundamental drivers that usually cause exchange rate movements – such as interest rate differences and diverging inflation and growth expectations – have not played any role. Instead, the bitcoin price development almost surely reflects a speculative bubble, fuelled by self-fulfilling prophecies or even market manipulation. However, neither this hypothesis nor the alternative presumption that bitcoin is the preferred vehicle of illegal transactions on the darknet can be tested in empirical studies. In any case, the sharp upward and downward movements of bitcoin prices represent further evidence that proper regulation and consistent supervision of cryptocurrencies is urgently needed on a global basis.[16]

Distributed ledgers and financial services

Obviously, the disruptive potential is less related to the virtual currencies themselves and more to the underlying blockchain technology, which has potential applications far beyond bitcoins. It has to be taken into account that the blockchain is only one form of the distributed ledger technology. In general terms, distributed ledgers are ledgers that share, replicate and synchronise digital data across various locations. The application of cryptographic methods allows for tamper-proof mapping of digitised transaction data in distributed databases. If transactions are grouped into blocks, with links building an irreversible history of transactions and a linear chain of blocks, the distributed ledger is called a blockchain. There are various types of distributed ledgers which differ in terms of cryptographic methods, number of users and the methodology applied to validate the integrity and accuracy of the database.

Virtual currencies use so-called public distributed ledgers that can be used by anybody who has access to the required client software. New transactions that lead to changes in the database are validated decentrally in a peer-to-peer network, grouped into new blocks and eventually added to the blockchain. Each node of the network validates new transactions and blocks independently. A predefined consensus algorithm ensures that the nodes of the network are continuously aligned to the correct state of the ledger. In order to avoid potentially negative aspects of anonymous distributed ledgers, particularly regarding regulations to prevent money laundering, restricted distributed ledgers may be more appropriate for financial markets applications. These “private” or “permissioned” ledgers are designed for a specific number of users or members. The application of cryptographic methods is supposed to facilitate tamper-proof, real-time

16 V. Brühl: Bitcoin: Höhenflug Grund zur Besorgnis?, in: Wirtschaftsdienst, Vol. 97, No. 9, 2017, p. 610.

execution of transactions in a multilateral trading and settlement system. Moreover, the joint use of data in a shared ledger may lead to efficiency gains in building and operating the underlying IT infrastructure. The registration of each participant is usually based on proof-of-identity procedures. This will at least reduce and possibly even eliminate the potential for fraud or other forms of system abuse for registered users. However, brute force cyber attacks remain a challenge, as in any IT system.

The design of permissioned distributed ledgers has to address privacy protection and the data security of the individual user on the one hand as well as the assignment of access rights, transparency and the monitoring of system integrity on the other hand. Nevertheless, in private distributed ledgers, certain surveillance functions need to be performed, e.g. by operators/owners of the ledger and/or trusted nodes. Hence, participants in closed distributed ledgers rely on a certain type of centralised institution or intermediary and not on the functioning of a decentralised system in its own right, as in open networks.

The development of distributed ledgers is still in a very early stage, and the disruptive potential of these technologies can only be roughly delineated, but there are clearly some areas, especially in the financial services sector, that may affect corporate finance and financial management in various dimensions. As distributed ledgers provide an innovative platform to initiate, execute and record transactions in a distributed database, it seems likely that transaction- and information-intensive services, in particular, will be subject to disruptive changes triggered by this new technology.

Three examples of uses for blockchain technology are outlined below. They illustrate the disruptive impact this technology could have on certain financial processes and products. For each of these examples, the status quo of the respective business processes is described and an alternative process based on the blockchain technology is presented. The first example looks at payment systems that may substantially benefit from the blockchain technology.

Payment systems

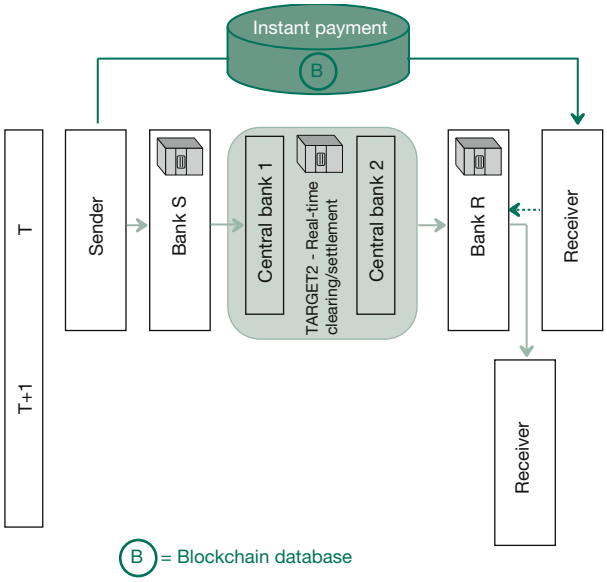
The execution of cross-border payments within the European Union has made significant progress with the introduction of the SEPA and TARGET2 systems. SEPA, the Single Euro Payments Area, has introduced a single set of payment instruments based on a common system for identifying and addressing bank accounts in the EU. The previously fragmented structure of national payment systems – which lacked interoperability – has been overcome, and a single market for euro-denominated payments has been created. TARGET2, the Trans-European Automated Real-Time Gross Settlement Express Transfer System, is the real-time gross settlement system of the central banks within the eurozone. It allows payment transactions to be settled on a continuous basis in central bank money with immediate finality. Payments to end customers of the participating banks are usually credited to the respective account on the next working day. Settlement times can be much longer if correspondent accounts have to be used, for example when international payments are handled through the SWIFT system (Society for Worldwide Interbank Financial Telecommunication).

Payment systems thus seem predestined for the application of distributed ledger technologies. Similarly to the bitcoin system, payments in any currency could be conducted directly between senders and receivers on a bilateral basis via a peer-to-peer network. The network would most likely be designed as a permissioned network, with operators being commercial banks, central banks or credit card organisations, since non-cash payments require a bank account. Figure 1 illustrates how a peer-to-peer network would allow a direct payment between sender and receiver on a real-time basis, provided the banks were obliged to offer real-time access to their legacy accounting system. In essence, the payment process would now be handled not through but rather alongside the banking ledger systems. Banks would no longer act as intermediaries, but only as repositories for money. However, it is possible that our current concept of deposits with banks could be replaced in the future by a transaction-oriented view of money as the right to use a digital entry into a shared database which is commonly accepted as a medium of exchange. In such an extreme scenario, banks would no longer be needed to conduct payments. In a sense, distributed ledgers may indeed revolutionise the payment sector, as currently even innovative payment solution providers like PayPal rely on the infrastructure of banks or credit card firms.

Such instant payment systems do not necessarily have to use distributed ledger technologies, as they may also be based on specific messenger services. In Europe, the European Central Bank (ECB) and the European Retail Payments Board are pursuing the advancement of TARGET2 and SEPA formats as a future platform for instant payments in the eurozone.[17] The ECB announced it would introduce a new system for instant payments by November 2018, known as the TARGET Instant Payments System. It is supposed to facilitate inter-bank transfers, accelerating

17 Euro Retail Payments Board: Statement following the fourth meeting of the Euro Retail Payments Board held on 26 November 2015, 2015.

Figure 1
Blockchain and real-time payments



Source: Author's illustration.

settlement from the present one-day standard down to a few seconds. The technical transaction scheme for pan-European payments is the SEPA Instant Credit Transfer, developed by the European Payments Council.[18]

Post-trading activities

Distributed ledgers may also enhance the efficiency of securities post-trading activities.[19] Buy or sell orders received by banks or brokers as intermediaries are generally routed to an electronic or physical trading platform, followed by clearing (the mutual reconciliation and matching of orders) and settlement (the transfer of securities and cash). Banks and brokers act as intermediaries between buyers, sellers and the central securities depository (CSD). Settlement periods differ widely depending on the type of security, trading platform, CSD and jurisdiction.

Currently, the processing of stock exchange trades without a central counterparty (i.e. "non-CCP") with collective safe custody (CSC) takes two days (T+2) from the order until the final settlement. The process can be sped up for securities that are routed through the Equity CCP to T+1 or even T+0. But one needs to take into account that these processing times are currently close to the ideal case and can often take much longer if additional interfaces are created between sellers and buyers of securities. This is the case for cross-border transactions in foreign securities, for example. Using the stock trade processing by Deutsche Börse and Clearstream Banking as an example, the settlement period depends on whether or not the securities are eligible for CSC pursuant to the German Securities Deposit Act. For securities kept in custody via an intermediary, Clearstream has a wide network of foreign custodians outside Germany. Post-trading processes are even more complex if at least one trading party resides outside the EU, as interfaces with banks, brokers, CSDs, custodians, collateral managers, correspondent banks, etc. are multiplied. Cash settlement against central bank money in euros takes place via the single shared platform TARGET2, while foreign currency settlements are carried out via correspondent banks. In such cases, settlement periods may be T+3 or even longer.

With the successive implementation of TARGET2 Securities (T2S) by the end of 2017, a pan-European platform for the settlement of cross-border securities transactions has been established. T2S is not a CSD but a platform which facilitates seamless cooperation among the national CSDs for the settlement of both exchange-traded and OTC-traded securities. It thus enables centralised delivery-versus-payment (DvP) settlement in central bank funds across all European securities markets. The implementation of T2S is an important step in terms of integrating and harmonising the highly fragmented securities settlement infrastructure in Europe.[20]

Figure 2 shows that distributed ledger technology may lead to a very lean settlement process, as the process steps of initiation, clearing and settlement merge, and real-time DvP procedures become feasible on a global scale. If securities and the corresponding cash can be transferred instantly and recorded in a distributed ledger in a tamper-proof manner, current CSDs might be diminished to pure repositories for securities. Even the custody services currently offered by banks may become an integral part of the blockchain in the form of so-called "smart contracts" that could automatically trigger actions such as dividend and coupon payments upon predefined triggering events.

Smart contracts

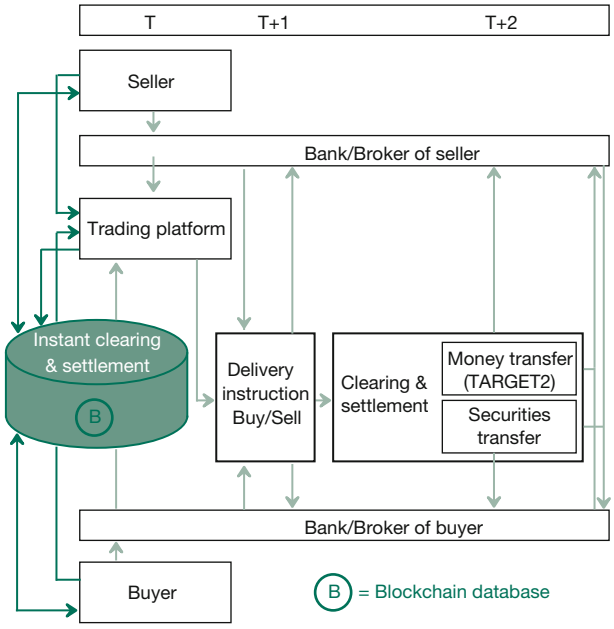
Smart contracts are digital images of contractual agreements between parties in the sense that rights, obligations and legal consequences are mapped onto algorithmic flow charts which are encoded as applications into the distrib-

18 European Central Bank: The new TARGET instant payment settlement (TIPS) service, June 2017, available at https://www.ecb.europa.eu/paym/intro/news/articles_2017/html/201706_article_tips.en.html.

19 A. Pinna, W. Ruttenberg: Distributed ledger technologies in securities post trading, ECB Occasional Paper No. 172, April 2016.

20 See Deutsche Bundesbank: TARGET2-Securities maximises settlement efficiency in the European securities market, Frankfurt 2015.

Figure 2
Blockchain and securities post-trading



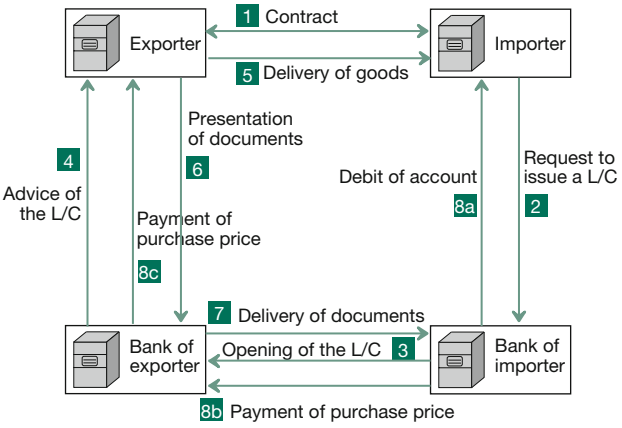
Source: Author's illustration.

uted ledger. The resulting programs are self-executing and may, therefore, trigger certain actions if the required conditions are fulfilled. This may apply, for instance, to coupon and redemption payments of loan contracts, the automatic payment of instalments in case of staggered purchase prices, or automated adjustments of insurance premiums according to the customer's damage history. The principles of distributed ledgers can be applied not only to financial transactions but also to tangible assets like real estate, machinery, equipment or intellectual property. As long as these objects can be digitally identified, for example using sensors, RFID transponders, QR codes or IP addresses, transactions involving such material or immaterial assets can be recorded in a distributed database such as a blockchain.

How distributed ledgers can facilitate corporate finance transactions shall be demonstrated using the example of trade finance. Figure 3 shows the transaction flow chart for a documentary letter of credit, which is a standard export finance product.

Let us assume there is a contractual agreement to buy and sell goods between an exporting and an importing company (1). The importer asks its bank to issue a Letter of Credit (L/C) to ensure payment to the exporter via the exporting bank, subject to the fulfilment of certain conditions which are in turn related to the delivery of documents (2). The opening of the L/C is performed by the exporter's bank (3), which in turn advises the exporter (4). Then the shipment

Figure 3
Transaction flow chart for a documentary letter of credit

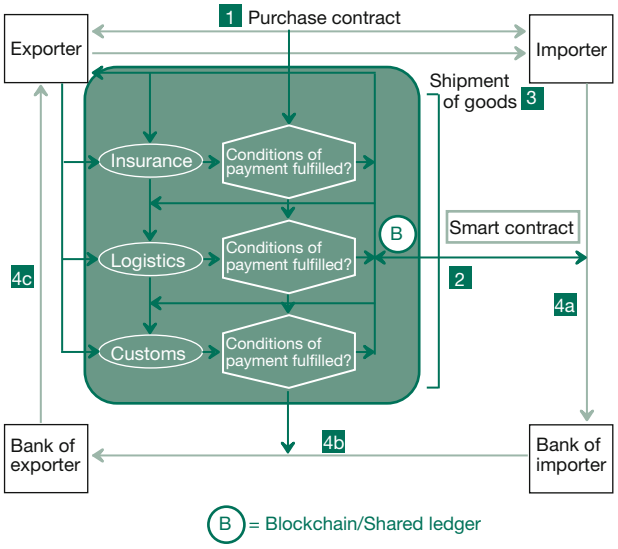


Source: Author's illustration.

of goods is carried out (5), and the agreed documents (e.g. freight, insurance, delivery note) are presented to the advising bank of the exporter (6). The documents are then delivered to the importer's bank (7). If the payment conditions set out in the contract are fulfilled, the account of the importer is debited (8a) and the payment to the exporter's bank is initiated (8b), so it credits the respective amount to the exporter (8c). The flow of activities is designed to ensure that both sides are protected. The importer releases the purchase price only if the contractual conditions are met and delivery of goods is secured, while at the same time the exporter is protected against non-payment. Depending on the nature of the products, the type of conditions agreed and the jurisdictions involved, the settlement of such trade finance transactions may take several days or even weeks, because it takes some time to reconcile the information needed on either side of the contract. Incompatible systems can require a number of manual activities, thus making processes time-consuming and costly.

Figure 4 demonstrates how distributed ledger technology could help to streamline and accelerate the information flow among the participants in such a transaction. Aside from the importer, exporter and their respective banks, customs, insurance companies and logistical service providers are also involved. If they all shared the same database with differentiated access rights, the information exchange among the parties would be improved and the flow of activities could be recorded in the distributed trade ledger in a tamper-proof manner. The risk of fraud would be reduced, instalments of payments could be conditioned upon the achievement of milestones in the process much more easily, and risk management could become more sophisticated, as a default history would be built up over time.

Figure 4
Documentary letter of credit on a blockchain



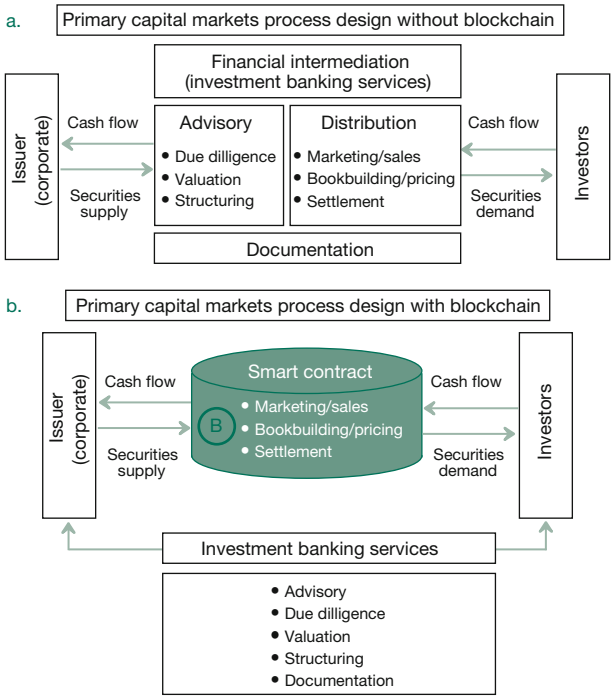
Source: Author's illustration.

Changing primary capital markets

The primary capital markets business, i.e. the issuance of new equity or debt securities to investors, can be structured as a public offering to private and institutional investors or as a private placement, usually focused on a limited number of institutional investors. Although the equity capital markets business is highly cyclical, the advisory, structuring and arranging of such transactions is still among the most profitable business lines in investment banking. Debt capital markets transactions, on the other hand, like the issuance of bonds or commercial papers, is a less cyclical business but also more of a commodity type of capital markets service. Figure 5a illustrates that the raising of equity capital through an initial public offering or a capital increase by listed companies is a particularly complex process involving investment banks as well as legal, commercial and financial advisors and covering topics ranging from valuation, due diligence and structuring to marketing, selling and settlement activities. All activities are usually handled by one or more investment banks, ensuring the smooth execution of the respective transaction.

Distributed ledger technology could have a disruptive impact on the primary capital markets as well, as illustrated in Figure 5b. A distributed ledger empowered by a tailor-made smart contract could be the future platform for these transactions, as it would facilitate information sharing, transparency and speed of execution in the non-advisory part of the transaction process. The knowledge-driven advisory activities are less likely to benefit from a distributed ledger, as the scope and content of these workstreams are very specific to the respective transaction, making them less suitable for digitisation.

Figure 5
Impact of blockchain on primary capital markets value chain



Source: Author's illustration.

Conclusion

Virtual currencies like Bitcoin are characterised by a lack of transparency, high price volatility and low barriers to entry. In order to ensure integrity, transparency and thereby investor protection, a proper regulatory framework and market supervision is urgently needed. However, the underlying distributed ledger technologies offer many opportunities to execute transactions in financial markets at lower costs while increasing the reliability, integrity and speed of the settlement processes. It can be expected that distributed ledgers will become a critical technology for financial market infrastructures such as stock exchanges, central securities depositories and the back-office functions of financial institutions in the future. The new technology will not only have a significant impact on the market structures and business models of financial institutions, but also on the supervisory and review processes of supervisory authorities. Furthermore, blockchain technology will enable innovative designs of securities and is likely to foster further disintermediation of primary capital markets. These factors will affect corporate financing in various ways. New capital market products may broaden the spectrum of financial instruments available to corporations. Moreover, new IT infrastructures facilitating direct access between corporates and institutional investors will reduce transaction costs and thereby impact the relationships between banks and their corporate customers.