Distributed ledger technologies in payments and securities settlement: potential and risks

Distributed ledger technology (DLT) has made huge strides in recent years, and it has now become a major testing ground for financial service providers, financial market infrastructure operators, central banks and the like. The Bundesbank's interest in this topic centres around how DLT could be incorporated into the world of payments and settlement systems. The term "distributed ledger" (DL) is generally used to describe a database shared across a network which gives participants ("nodes") joint rights to write, read and store entries to the ledger. Potentially, DLT offers a number of benefits due to the distributed storage of data, which can simplify reconciliation processes associated with complex labour-sharing value added chains. DLT is seen as having disruptive potential since it generally allows transactions to be carried out directly – that is, without intermediaries. Developed originally for the virtual currency Bitcoin, DLT will nonetheless require extensive modification if it is to be adapted to the needs of the financial sector. For one thing, the legal framework as it stands requires participants to be identifiable, transactions to be kept secret from third parties, and transactions to be settled with absolute finality. For another, transaction throughput needs to be high. Given the current state of the art, it is rather unlikely that DLT will be put to use in large-value or retail payments. In the field of securities settlement, though, the shrinking processing times and reconciliation costs might prove to be a more important factor and suggest that DLT may have its uses in this area. The Deutsche Bundesbank is analysing the pros and cons of DLT in a project it is running with Deutsche Börse. While this project indicates that DLT does indeed have its functional merits, it is still unclear whether DLT also has the edge over today's technology in terms of security, efficiency, costs and speed. This article then goes on to discuss the possibility of providing central bank-issued digital currency. Probably the most pressing design question here is whether central bank-issued digital currency should be issued to non-banks as well. However, the implications of central bank-issued digital currency for monetary policy and financial stability and for the structure and business models of banks are hard to fathom, which is why there appears to be no realistic prospect of central bank-issued digital currency being rolled out for non-banks in the foreseeable future. In its capacity as an operator, supervisor and catalyst, the Bundesbank is continuing to analyse this technology so that it can actively shape the ongoing conversation about DLT by contributing insights of its own.

Introduction

DLT: a prominent testing ground in the financial sector

Distributed ledger technology (DLT) has made huge strides in recent years, and it has now become a major testing ground for financial service providers, financial market infrastructure operators, central banks and the like. Many regard DLT as a disruptive technology – one that could trigger fundamental change, or even structural breaks, in the industries in which it is applied. In the financial sector, for instance, it could make intermediaries obsolete or pave the way for new, more efficient processes in areas such as payments and securities settlement. This development was originally set in motion by mounting interest in "virtual currencies" – first and foremost in Bitcoin, which still ranks as the best-known field in which DLT has been put to use. But attention is now increasingly turning to the underlying technology itself.

DLT's role in payments and securities settlement an interesting topic for the Bundesbank

This article focuses on the role of DLT in payments and securities settlement – two areas which are highly important for the Bundesbank, given that section 3 of the Bundesbank Act *(Gesetz über die Deutsche Bundesbank)* requires the Bank to "arrange for the execution of domestic and cross-border payments and […] contribute to the stability of payment and clearing systems."

The Bundesbank fulfils this statutory mandate by performing three different roles. First, it develops and operates major payment and settlement systems, often in conjunction with other central banks, and in this context explores innovative technical capabilities which can contribute to their stability and efficiency. Second, the Bundesbank acts as a catalyst to forge improvements in payment operations and settlement structures. The better the Bundesbank grasps the practical implications of technologies or processes, the more forcefully it will be able to present its arguments, which always aim to preserve the stability and enhance the efficiency of payment and settlement systems. Third, in addition to its role as a banking supervisor, in which it oversees individual institutions (market players), the Bundesbank also monitors the stability of systems and tools used in the field of payments and settlement. Being able to gauge the relative merits of state-of-the-art technology is a key skill in this regard. That is why the Bundesbank – much like other central banks worldwide – has been putting a great deal of thought into DLT, even though this technology is still very much in its infancy.

This article introduces readers to the topic of DLT, illuminates the opportunities and challenges it presents, shows its potential for driving market change and explores the possible repercussions for the Bundesbank's role in payments and securities settlement.

Functional analysis of DLT

Understanding how DLT works from a technical perspective and what sets it apart from the traditional payment and settlement system architecture is the first step in gauging the opportunities and risks it presents.

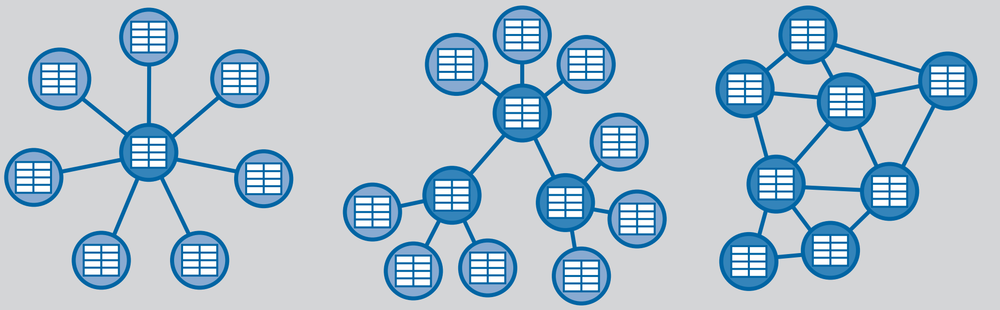
How DLT works

Distributed ledger with joint rights to write, read and store ledger entries

DLT is a special type of electronic data processing and storage system. The term "distributed ledger" (DL) is generally used to describe a database shared across a network which gives participants ("nodes") joint rights to write, read and store entries to the ledger. While traditional distributed databases likewise distribute and store data across the entire network, entries there can only be created or updated by a central administrator.[1] DL networks differ from traditional databases in that no such central administrator is needed to manage the database or ledger. New information can be provided by nodes at any time and added to the database by means of a validation process. These new data entries are added to each

1 See E Benos, R Garratt and P Gurrola-Perez (2017), The economics of distributed ledger technology for securities settlement, Bank of England Staff Working Paper No 670.

A comparison of network models*



* Based on Baran, 1964.

Deutsche Bundesbank

node's copy of the DL so that each node will always have the latest version of the entire database.[2] The above chart shows different types of network model. The ability to write to the DL – that is, the power of control over ledger updates – dictates which of these three models a network is assigned to according to this definition: in a centralised set-up, control lies with a single administrator; in a decentralised model, with multiple nodes; and in a distributed model in the narrower sense, with every single node.

Blockchain: a special form of DLT for recording transaction histories

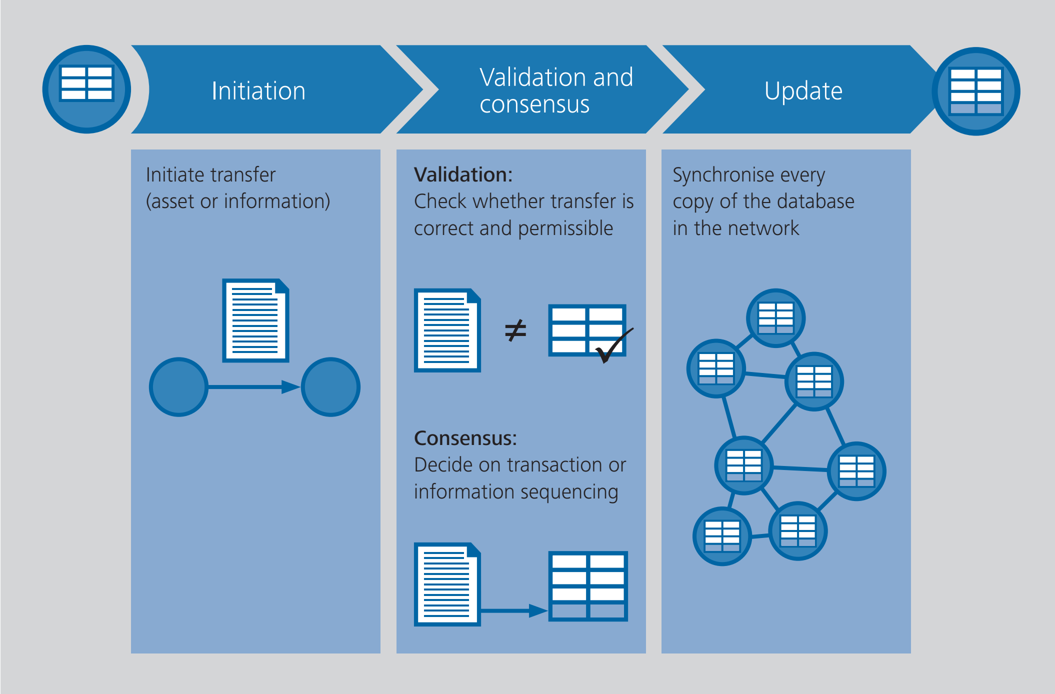
The most common DLT applications are based on blockchain technology, which has proven to be particularly useful for recording transaction histories and will be used for illustrative purposes in the remainder of this article.[3] In the case of the blockchain, the distributed ledger is made up of a chain of chronologically sequenced blocks containing one or more transactions.[4] The ledger is updated by generating a new transaction block and adding it to the existing chain of transaction blocks.

Consensus mechanisms needed for validation

To synchronise additions to every node's copy of the distributed ledger, the nodes need to have a reconciliation and validation process in place.[5] This is normally done using what are known as consensus mechanisms such as proof of work (PoW), proof of stake (PoS) or practical byzantine fault tolerance (PBFT). The consensus mechanism defines the condition which has to be met for new valid transactions to be added to the ledger. Conditions might include the demonstrative use of a node's computing power (proof of work), evidence of the node's share of units of value transferred within the network (proof of stake), or a minimum number of nodes agreeing on the validity of a given transaction (PBFT). These protocols serve two purposes. First, they help forge agreement on

2 Further background reading on DLT and Blockchain can be found in Bank for International Settlements (BIS) (2017), Distributed ledger technology in payment, clearing and settlement – an analytical framework, report by the Committee on Payments and Market Infrastructures; P Roßbach (2016), Blockchain-Technologien und ihre Implikationen, Banking and Information Technology, 17(1), pp 54-69; V Brühl (2017), Bitcoins, Blockchain und Distributed Ledgers. Funktionsweise, Marktentwicklungen und Zukunftsperspektiven, Wirtschaftsdienst, 97(2), pp 135-142; and L Geiling (2016), Distributed Ledger: Die Technologie hinter den virtuellen Währungen am Beispiel der Blockchain, Bafin technical article.
3 As a rule, DLT applications can also be run without blockchain. In this case, the database can contain either the entire history (not in block format), the net state of assets or information distributed across the network, or a node's individual ledger updates applied to the preceding version of the ledger (see, for example, Deloitte (2016), Bitcoin, blockchain & distributed ledgers: caught between promise and reality).
4 Information contained in a transaction block are not stored directly in a blockchain but reduced to what are known as cryptographic hashes. Each new data block contains the preceding data block's hash, thus creating the chain structure by which the history of any transaction can be traced back immutably.
5 See the chart on p 38.

Updating a distributed ledger



Deutsche Bundesbank

transactions to be added to the chain (consensus); second, they help validate transactions so as to prevent misuse or counterfeiting, eg due to the renewed use of previously used assets by the same payer (the double-spending problem).

Cryptography guarantees authentication

Cryptographic tools are used to authenticate nodes and verify their rights. Nodes wishing to add new transactions to the DL, for instance, have to authenticate themselves by providing their digital signature. Cryptographic mechanisms can also be used to preserve the integrity of the DL.

Smart contracts allow contingent transfers

Since DLT generally allows any kind of digital information to be stored and distributed, it can also be used to record more complex contingent transactions. The nodes can choose to make a particular transfer of assets contingent on certain predefined criteria being met. The automated process by which an algorithm reviews those conditions and subsequently executes the transfers is often referred to as a smart contract. It is not, then, a special type of contractual agreement but a piece of programming code that is automatically executed whenever certain conditions are met and can play a role in contractual performance.

Networks can be public or private

Generally speaking, the network of nodes in which the distributed ledger is used can be configured as a public ("permissionless") or private ("permissioned") network. A public network would be open to anyone satisfying the basic technical requirements, while a private configuration would restrict data access to certain individuals or institutions. Confining network access to a selected group of users can make sense on a number of counts, for instance if there is a restricted group of counterparties, or participants are expected to meet certain minimum standards. It also hides the ledger from unauthorised third parties. Where, for instance, DLT is used to settle trade finance transactions, a permissioned system could restrict the group of authorised blockchain users to the business partners (exporter and importer) involved in the transaction as well as their respective principal banking partners.

Functional comparison with existing systems

DLT enables direct exchange without intermediaries

DLT mainly differs from traditional financial market infrastructures in that it is designed to facilitate a direct electronic transfer of assets between nodes without the need for any account-holding agent to be involved. Financial market infrastructures, on the other hand, act as intermediaries in the sense of a hub and spoke system – that is, users route transfers of assets via a central institution (the hub) to other users. That central institution operates accounts for each user and runs the system. Financial market infrastructures, ie payment systems, securities settlement systems, central securities depositories (CSDs) and central counterparties (CCPs), are core components of today's financial system and serve as conduits between different markets and participants.

Payments

Payments sometimes need more than one intermediary

In today's financial system, there are a multitude of intermediaries in the field of payments. Their number and variety depends on factors including the "institutional distance" between the parties sending and receiving payment.[6] If both parties are customers with the same bank, that bank will be the sole intermediary. But if they bank with different credit institutions, there will be at least two intermediaries, plus a clearing house if the two banks do not have accounts with each other. Larger amounts are normally routed via a large-value payment system like TARGET2. Payments across currency areas will involve foreign payment systems or correspondent banks, and perhaps also the central infrastructure known as continuous linked settlement (CLS).

DLT potentially replaces clearing, settlement and accounting

When DLT is used, payment is first initiated by the sender, followed by a consensus mechanism; when that is concluded, the payment is added to the DL. Adding the payment to the DL replaces, as it were, clearing (= the process of determining mutual claims or liabilities and netting), settlement (= the settlement of existing claims or liabilities), and potentially also internal accounting, provided the parties involved agree that the entry they have initiated in the distributed ledger entails a transfer of title.

Securities settlement

Greater number and variety of intermediaries needed for securities settlement

Compared to payments, today's securities trading and post-trade operations involve a far greater number and variety of intermediaries. Securities traders, exchanges, clearing houses or CCPs, CSDs, registrars, custodians and potentially also sub-custodians all have a role to play in a security's life cycle. There will be cases where some of these functions have been pooled to a degree within a single institution. Complexity levels are high and processes are error-prone, making reconciliation a very laborious task. DLT has the technical capability to reduce securities settlement to just a few process steps. Thus, if two nodes make a matching declaration in the distributed ledger, the entry in the distributed ledger could be simultaneously interpreted as the trade, clearing, settlement and accounting.[7] All the nodes can access the same data pool.

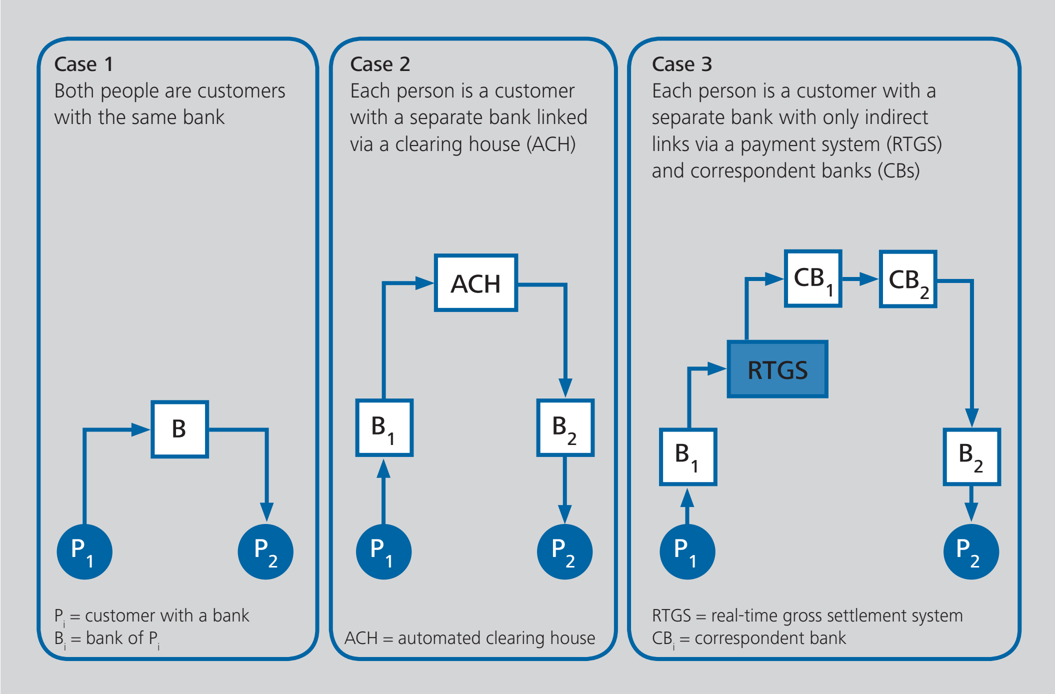
Prospective benefits

Due to its network structure and synchronised access to a common database, DLT promises to take transparency, operational efficiency, security and resilience, independence from intermediaries and automated contract performance to the next level.

---

6 See the chart on p 40.
7 See report by European Securities and Markets Authority (ESMA) (2017), The distributed ledger technology applied to securities markets.

Examples of how a payment can be settled: person 1 pays money to person 2



Deutsche Bundesbank

Transparency and immutability

DLT generally offers a high level of transparency

A DL enables the nodes of a DLT network (unless defined otherwise) to view the entire data history.[8] Transfers of assets and exchanges of information are thus visible to the entire network. Information can be stored in a way that prevents it from being manipulated. That allows a tamper-proof record of transactions to be stored without any need for the nodes to trust each other.

Operational efficiency

Reconciliation workload might decline

Another way in which DLT might have an edge over traditional financial market infrastructures is that it could reduce complexity in the settlement of financial market transactions requiring a great deal of reconciliation. Direct reconciliation between nodes and the accompanying documentation could automate multiple process-heavy intermediate steps and shorten transfer times, particularly for labour-sharing processes such as trade finance. The use of DLT might also drive down settlement costs, not so much for transaction settlement itself but potentially for all the downstream post-trade processes. While nodes will all need to have greater storage capabilities to maintain the data, it will probably be far easier to view the data.

Security and resilience

No single point of failure in the network

A decentralised system could boost the security of assets or information transferred across the network. Unlike a centralised settlement platform, DLT has no single point of failure – that is, a point in a system that, if it failed to work correctly, would lead to a failure of the entire system. DLT's ability to compensate for an inoperable or compromised node is often seen as

8 More recent developments, however, have begun to make a distinction between nodes, with the result that some of them are prevented from seeing the entire data history.

providing enhanced protection against failure. If one copy of the DL is subverted by a malicious actor, other copies of the DL containing the original data can be used to correct those changes. However, having multiple nodes with identical rights exposes a DLT to multiple possible points of attack, potentially driving up the cost of shielding the system from cyber risks.

Independence from intermediaries

Direct P2P transactions

DLT generally enables transactions or information to be exchanged between peers (P2P) without the need for any intermediaries, something which is otherwise only possible with cash payments. In theory, DLT could do away with the need for dedicated systems run by intermediaries. That would render the intermediate agents which traditionally validate financial transactions obsolete from a purely technical perspective.

Automated contract performance

Automated performance of complex processes

DLT promises huge potential for optimising processes through the automated execution of contractual rights using what are known as smart contracts. Particularly transactions which require counterparties to reconfirm or issue a guarantee stand to become more efficient as a result of being automated with smart contracts. DLT could, for example, be used to automate interest or dividend payouts in securities business. These benefits do, however, depend on the specific design of the DLT application in question.

Challenges

DLT from Bitcoin blockchain requires modification

The original blockchain for Bitcoin was created for a virtual currency. Its key characteristics are the intermediary-free, direct (P2P) transfer of Bitcoins, its accessibility for any participant who is not required to operate under their real name (and may operate under multiple pseudonyms), the complete transparency it provides across all transactions for all nodes, the use of the proof of work protocol as a consensus mechanism, the designation of the longest blockchain as authoritative, regardless of when the blocks were created, and the fact that transfers are confined to Bitcoin. The Bitcoin blockchain would need a variety of adjustments in order to be migrated to the real financial system. Some advances in DLT have already resolved the real-world challenges to a degree,[9] but this might also lessen the potential benefits. If DLT is to be a viable proposition in the financial sector, however, certain rules must be complied with.

Identifiability

Anti-money laundering legislation requires participants to be identifiable

Anonymous transfers of assets of the kind seen on public DLT platforms (public ledgers) do not allow participants to be identified. Anti-money laundering legislation, however, states that it must be possible to unambiguously identify natural and legal persons. This requirement to "know your customer" means ascertaining the identity of network participants, which is why an application like Bitcoin – where transactions take place anonymously – is ineligible. A transfer as a P2P transaction would then only be possible subject to rules which no longer guarantee anonymity. Thus, any application of DLT in the financial sector would only be possible with a private ledger, rather than a public one.

Confidentiality

Participants want to settle transactions confidentially

DLT generally enables any participant to view the transaction history, which means that the confidentiality of financial transactions cannot

9 See inter alia G Danezis and S Meiklejohn (2015), Centrally banked cryptocurrencies, https://arxiv.org/pdf/1505.06895.pdf; V Buterin (2016), Ethereum: platform review – opportunities and challenges for private and consortium blockchains, http://www.r3cev.com/blog/2016/6/2/ethereum-platform-review; J Poon and T Dryja (2016), The Bitcoin lightning network: scalable off-chain instant payments, https://lightning.network/lightning-network-paper.pdf; Hyperledger Fabric Model, https://hyperledger-fabric.readthedocs.io/en/latest/fabric_model.html; R Brown, J Carlyle, I Grigg and M Hearn (2016), Corda: an introduction, https://docs.corda.net/_static/corda-introductory-whitepaper.pdf. Owing to the multitude of advances made, just a few applications are mentioned here by way of example.

be assured without encryption. Even encrypted storage of data at every node would still not offer sufficient safety. If future improvements in hardware or software components enabled data to be decrypted, that would expose the transaction history again to all the nodes at which the data had been stored. This compromise of future confidentiality ("forward secrecy") could be resolved by not having all the data stored at every node but exchanging them in sub-networks of a kind. This safeguard would, however, mark a significant departure from the fundamental principles of full transparency and comprehensibility of a distributed database, and make DLT less tamper-proof.

Scalability and performance

Current DLT too slow for high-volume applications

Scalability and performance – as measured, for instance, in terms of system latency periods – are crucially important criteria when applying DLT to infrastructures with high throughput rates and/or high transaction volumes during peak times. The scalability of DLT solutions depends on the choice of technical configuration and especially on the consensus mechanism. Depending on which consensus mechanism is used, DLT solutions require far more data storage capacity, data instructions and time to settle a single transaction than a centralised financial market infrastructure. If DLT systems fail to reach the transaction throughput rates achieved by today's financial market infrastructures, it would only make sense to apply them to systems which are highly complex but run at relatively low transaction volumes. By way of comparison, the Bitcoin network settles a peak of roughly 350,000 transactions worldwide every day, and given its current configuration, it is thought to be running at almost full capacity. The German payment system alone, by contrast, processes more than 75 million transactions on average every business day.[10]

Resilience compromised

New developments of hierarchical structures in DLT lower resilience

Some DLT developers keen to boost performance have introduced hierarchical role concepts which assign different rights to different nodes. Some are given more extensive read, write and validation rights; others are only authorised to propose transactions, say. This could ultimately compromise the very operational resilience which the elimination of a single point of failure set out to achieve. If a node with extended rights came under attack, a malicious actor could potentially inflict greater damage and could furthermore focus its efforts on the least protected node (the weakest link). Under certain circumstances, then, it is far more difficult to guarantee data security than in the case of a centralised system. However, this weakest link dilemma would not be confined to read access rights. Depending on the consensus mechanism used, a malicious actor could feed faulty data into the network. Where the PBFT protocol, which is currently a popular consensus mechanism in hierarchical DLT networks, is used, that form of unauthorised write access would, however, require a successful attack on the majority of validating nodes.

Finality

Some consensus mechanisms offer only probabilistic finality

Financial transactions require both clearly defined *de jure* and *de facto* finality, ie a specific point in time as from which a transaction may be considered valid. State-of-the-art RTGS systems immediately reuse incoming funds, while in the field of securities, financial institutions sometimes sell or lend securities or use them as collateral immediately after settlement finality. Some DLT consensus mechanisms, however, such as the proof of work protocol, only offer probabilistic finality. In this particular consensus mechanism, the longest chain of blocks is the valid one. There is a certain degree of probability, however, that various nodes will have added different blocks to the valid chain, creating bifurcations (forks) in the chain which make it difficult at first to be sure which chain is the valid one. Only when one chain of blocks grows more quickly will it prevail as the au-

10 See https://blockchain.info and Deutsche Bundesbank, payment statistics for 2016.

thoritative chain. Transactions in the shorter part of the chain from the bifurcation are cancelled retroactively. That is why these consensus mechanisms are said to offer only probabilistic finality.

How virtual assets relate to real assets

Trustless transfers by third parties only possible in cyberspace

Bitcoins, which circulate in the currently best-known DL network, are only ever a virtual currency; that is, they do not exist outside the blockchain. Bitcoins can only be transferred across the blockchain and cannot leave the blockchain. A security, by contrast, embodies a claim in the real world. While that security can be transferred via DLT, its migration onto the blockchain depends on the existence of a body, such as a central securities depository, to link real, off-ledger assets with the digital world. In other words, there needs to be a trusted body at least at the interface between the real world and DLT.[11] That is not the case in the Bitcoin blockchain. To put it more broadly, while the sale of a good can be documented in a distributed ledger, that is not enough to validate the very existence of that good, its specifications and possibly also its previous ownership status. DLT's assertion that it can make trustless transfers a reality, then, would be confined to the purely virtual realm and have no points of reference in the real world.

Possible changes in the market

Some sectors experimenting with DLT

DLT is a technical concept which is being tested simultaneously in a number of sectors and fields of application. The following section of this article will discuss how DLT might transform the markets for payments and securities settlement. Judging by the above description of DLT's functionalities, its actual use in the financial sector would generally appear to be beneficial whenever extensive reconciliation is required between multiple independent participants and/or repeated recourse to the database is necessary, and whenever a complex value chain is involved. It goes without saying that it must be possible to digitalise assets for use in DLT.

Payments

Some believe that DLT has a high degree of disruptive potential in the field of payments. The P2P network architecture in particular is regarded by some market participants as being instrumental to an efficient, globally accessible asset transfer capability. Yet a nuanced analysis reveals that the special structural features of DLT will not *per se* revolutionise the world of payments.

Payments in the euro area

Fairly unlikely that DLT will be used in European large-value or retail payments

The trend in the European payments space is towards ever-faster systems which settle payments as close to real time as possible. In large-value payments business, it is customary for payments to be settled with finality in central bank money directly between two banks via RTGS systems. In future, the TARGET Instant Payment Settlement Service (TIPS) is expected to make the direct transfer of funds in real time a reality for retail payments as well. RTGS systems such as TARGET2 process payments efficiently, and are optimised for fast transfers, besides requiring a minimum of reconciliation. So far, there is nothing to suggest that the use of DLT for payments in a single currency area can achieve any efficiency gains over the established settlement systems. As it happens, payment settlement using DLT will probably even become slower and more costly, depending on how the consensus mechanism is designed and which database structure is selected. From the perspective of today's technical capabilities, there is little prospect of DLT being put to widespread use in large-value and retail payments in Europe.

11 See G Neyer (2017), The future of blockchain, Journal of Digital Banking, 2 (1), pp 74-94.

Payments across currency areas/trade finance

Correspondent banking and trade finance seem more suited to DLT

The situation is different with regard to payments across currency areas. In order to become a participant in RTGS systems, a bank must generally have a registered office, a subsidiary or a branch office in the relevant currency area. If this is not the case, it has the possibility of maintaining what are known as correspondent banking relationships with a credit institution that belongs to the currency area in question. Correspondent banking is less standardised than centralised payment systems and often calls for extensive reconciliation processes between those involved. Settlement takes a long time (as a rule, more than one day) and causes relatively high transaction costs. DLT and the use of smart contracts could simplify some of the process stages in correspondent banking or even make them superfluous and allow quicker and cheaper settlement for end users. The development of a number of DLT-based pilot projects for correspondent banking relationships has led financial service providers currently operating in that field to review their own procedures in terms of boosting efficiency.

It is furthermore conceivable that DLT solutions could help to improve financial inclusion in some countries which have a poorly developed financial infrastructure.

In addition to this, the use of DLT in trade finance seems to offer advantages where several process stages have to be executed and confirmed step by step. DLT could, above all, make reconciliation between those involved easier and faster by automating processes that are settled manually at present.

Securities settlement

Many observers ascribe major potential to DLT in securities settlement and other post-trade areas. There, too, possibilities of deployment are seen in those areas where there are complex transaction chains and there is a relatively large need for manual reconciliation between the parties involved in the transaction.

Reduced reconciliation workload

Distributed but uniform database could lower reconciliation costs

In the life cycle of a security, actual settlement of the trade is followed in many instances by a need to balance the amounts, say, in the case of capital measures such as interest payments. This matching process is known as reconciliation. DLT could offer advantages at this point. Owing to the distributed, but uniform database, no differences should occur at least within a DL. All those involved are using the same pool of data. Reconciliation between the CSDs and custodians as well as between custodians and account-keeping banks could be simplified by the use of DLT.[12]

Shortening process chains

Smart contracts could shorten process chains

The biggest potential advantage of DLT in securities settlement lies in the possibility of combining or greatly simplifying process stages.[13] Smart contracts, which allow complex sequences of transactions to be conducted as a single transaction, are one major instrument for this purpose. In fact, more than two parties can be involved as well as more than one currency and several securities. This could save time and would be of particular benefit if risks are reduced by conducting different parts of a transaction simultaneously.

Corporate actions and custody

Measures in the life cycle of a security could be executed more simply via DLT

The distributed storage of data when using DLT promises to make it easier to determine the current and historic securities holders, since the relevant information is distributed automatically in the system and is directly available. This

12 See BIS (2017), op cit; and D Mills et al (2016), Distributed ledger technology in payments, clearing and settlement, Federal Reserve Board, Finance and Economics Discussion Series 2016-095.
13 See ESMA report (2017), op cit.

would simplify the processing of corporate actions (eg interest payments, redemption upon maturity, stock splits). Above and beyond that, various corporate actions could be (partly) automated by using smart contracts by, for example, automatically generating and conducting the transactions for the coupon payment.[14] In an extreme case, the complete life cycle of a security would be represented in a smart contract. After issuance, such a security would not need any kind of additional action in order to be settled.

Reference data and identification solutions

Decentralised maintenance of reference data using DLT

Many DL applications use the immutability of the data once they have been written and the distributed structure in order to store and administer unambiguous reference data and classifications on it using smart contracts. Even though such solutions are not designed for the transfer of money or securities, they do offer a number of applications which are indispensable for the settlement of financial transactions, such as identity management.[15] This might relate to updating the master data of participants in a financial market infrastructure, for example. In such kinds of tasks, DLT is characterised by a large degree of automation in the processing of information. This is the case because the authorised participants in a network are able to enter changes to their data directly into the network for validation. Once they have been validated, the data are updated immediately at all nodes. Solutions of this kind could be an advantage precisely in correspondent banking, where it is vital to identify the participants in a transaction unambiguously in order to allow the implementation of the "know your customer" principle on a transnational and secure basis.[16] For the majority of applications in the field of finance, making changes to reference data without externally authorised verification is unlikely to be acceptable, however.

Central bank-issued digital currency

Central bank-issued digital currency under discussion

In current payment systems, market participants insist on settlement in central bank money where large amounts are involved. When using DLT, the question might arise in future as to whether central bank-issued digital currency could be provided for the safe settlement of such larger transactions. Central bank-issued digital currency would rank alongside cash and credit balances with the central bank – the latter essentially being the preserve of commercial banks and general government – as another form of central bank money, and it would have to be posted in the same way as a central bank liability on the balance sheet. There are several technical options in terms of the form this could take. Transfers could be value-based (like cash) or account-based (like deposits), anonymous or registered, its use could be restricted – in terms of amount or payment purpose, say – and it could be remunerated or, like cash, earn no interest.

The actual way this is implemented would ultimately determine its macroeconomic impact, and it is precisely this which has to be taken into account when making any comprehensive assessment.

Should non-banks also have central bank-issued digital currency at their disposal?

Arguably, the most important question here concerns who should be authorised to use central bank-issued digital currency, or, to be more precise, whether central bank-issued digital currency should be issued to non-banks as well. This is because, if that were the case, substitution effects between the different forms of money would have to be expected. In particular, non-banks could convert their sight deposits at banks into central bank-issued digital currency if storage as an entry on the distributed ledger appears more secure and more

14 See report by Euroclear and Slaughter and May (2016), Blockchain settlement – regulation, innovation and application.
15 See BIS (2017), op cit.
16 See ESMA report (2017), op cit.

convenient than hoarding it as cash. Significant parts of non-banks' sight deposits being shifted onto a blockchain, however, and no longer being available to the credit institutions as virtually unremunerated funding might have considerable repercussions for the interest margin, the scale of lending as well as the business models in the banking system, and the banking system's structure. Furthermore, a simple expansion of the monetary base, accompanied by a shift from sight deposits into central bank-issued digital currency and thus an increase in central bank liabilities, would require a corresponding increase in balance sheet assets, say, in the form of additional refinancing operations that would have to be appropriately collateralised. The effects on the structure and the risk profile of central bank balance sheets would be considerable.

Implications currently hard to assess; central bank-issued digital currency therefore unrealistic at present

Seen in that light, the potential monetary policy and stability policy implications of introducing central bank-issued digital currency, say on the basis of DLT, are manifold and – even though they are currently being studied by some central banks – all but impossible to predict.[17] Even leaving aside current uncertainty about the technological potential of DLT, which is a factor here, too, this makes its application to central bank-issued digital currency seem unrealistic at present.

Implications and outlook

Possible implications for the roles of the Bundesbank

Role as an operator

Bundesbank looking into suitability and efficiency of DLT in its own project

By operating payment and settlement systems, above all for settlement between banks, the Bundesbank supports – along with other central banks – the stable settlement of payments in the Eurosystem. In the case of DLT, the Bundesbank sees the use of permissioned systems as the sole option – in other words, private ledgers which allow the identification of participants. The Bundesbank is currently conducting a conceptual study together with Deutsche Börse in order to make a more exact assessment of DLT's potential. This study explores whether DLT is suitable for use in the field of digitally transferable currency units and securities and how efficient and stable it is. Initial results confirm the general functional suitability of DLT. The technical performance and the scalability of such a system will have to be examined in further stages, however, in order to be able to tell whether DLT is fit for practical use.

Role as a catalyst

In its role as a catalyst, the Bundesbank supports ongoing development in payments and securities settlement with the aim of fostering stability and efficiency. New procedures and techniques have to hold out the promise of added value and fit into the existing regulatory system. In order to assess this, it is necessary to understand the procedures. One way to do this is to apply and analyse them oneself.

Network externalities and path dependence necessitate the role as a catalyst in the public interest

There is a need to bring together the various participants with diverging interests, as the industry has pronounced network features. At the same time, it is important not to distort market developments or competition between rival systems. Changes in the procedures and processes require acceptance by a majority of participants so that potential benefits are realised. Partial changes may even be economically harmful, especially without complete interoperability with existing systems. The generally high investment costs involved in system change coupled with low variable costs in production also promote technological path dependencies. Without the convincing prospect of significant efficiency gains, it is difficult to per-

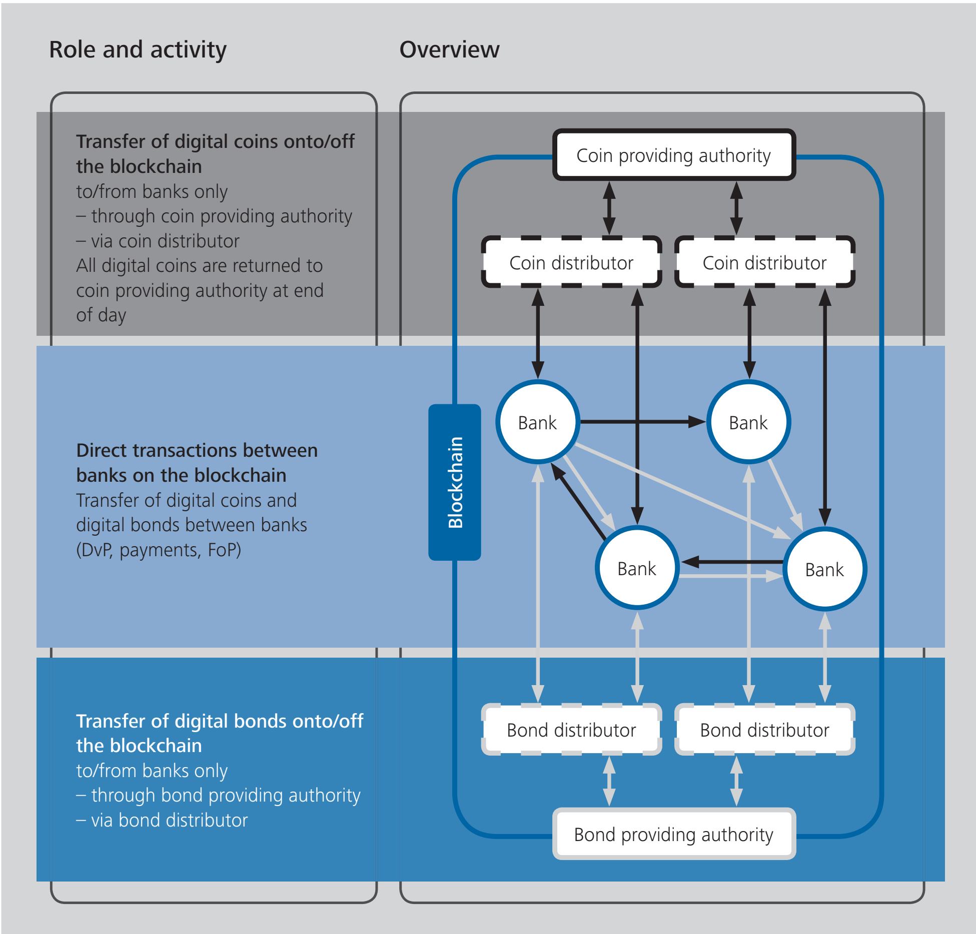
17 See, inter alia, B Broadbent (2016), Central banks and digital currencies, speech at the London School of Economics, 2 March 2016; J Powell (2017), Innovation, technology, and the payments system, speech at Yale Law School Center for the Study of Corporate Law, 3 March 2017; C Skingsley (2016), Should the Riksbank issue e-krona?, speech at FinTech Stockholm, 16 November 2016.

Blockchain research project

The Deutsche Bundesbank and Deutsche Börse are cooperating on a research project on the use of blockchain technology in payment and securities settlement between banks. The jointly developed prototype enables the settlement of security purchases on a delivery-versus-payment basis in exchange for centrally issued digital coins, as well as the pure transfer of digital securities. In addition, it is capable of executing basic corporate actions such as interest payments and the redemption of securities at maturity. In technical terms, it uses a permissioned blockchain based on Hyperledger Fabric.[1] In principle, the prototype could also be based on other DLT versions.

1 See Hyperledger Fabric Model at https://hyperledger-fabric.readthedocs.io/en/latest/fabric_model.html

Schematic illustration of the prototype for blockchain technology-based settlement presented by the Deutsche Bundesbank and Deutsche Börse



Sources: Deutsche Börse and Deutsche Bundesbank.

Deutsche Bundesbank

Prototype is neutral in terms of monetary policy

For the blockchain-based settlement processes, the coin providing authority transfers digital coins from an external cash cycle onto the blockchain at the start of each business day. They are available for network participants during the trading day. The coins are returned to the external cash cycle at the end of the day. Securities are made available for trading within the blockchain network by a bond providing authority. The securities remain on the blockchain throughout and do not leave the network until instruction has been received from the participant or upon maturity.

Prototype meets regulatory requirements in principle

The prototype ensures the confidentiality of transaction content using an adaptable rights framework. It takes into consideration the existing regulatory requirements and covers all business-related procedures for internal and external accounting and for regulatory reporting. This means that the prototype generally provides the basis for a practical application. However, it is a conceptual study and thus far from being market-ready. In a further stage of the project, the prototype will be further developed to allow technical performance and scalability to be analysed in more detail.

suade market participants of the merits of new procedures.

In order to contribute to the cross-application harmonisation of DLT, the Bundesbank is also taking part in an initiative for the standardisation of "Blockchain and Distributed Ledger Technologies" organised by the International Organization for Standardisation. The aim of the initiative is to apply a uniform framework of reference in order to promote interoperability and the exchange of data between users, applications and systems which use this technology.

Role as an overseer

Operation on DLT basis examined applying the same criteria as for existing systems

In its role as overseer of payments and settlement systems, the Bundesbank analyses all relevant developments in terms of their impact on the security and efficiency of the financial sector. At the present time, oversight in the case of DLT is confined to monitoring the market. If large DLT-based systems wished to start up operations in Germany, they would be assessed on the basis of the same criteria as those for the current systems.

Outlook

DLT continues to be the subject of in-depth research and development in the expectation that its use will be able to lower transaction costs. Transferring its original role as the technology behind the virtual currency Bitcoin to applications in payments and securities settlement is proving to be a veritable challenge. It is becoming apparent that a large number of adjustments to the original Bitcoin procedure will be necessary. A purely P2P implementation without intermediaries is unlikely to be practicable in the financial sector. Added to this are non-functional criteria: the scalability and performance of DLT are still too limited to be considered for use in high-volume applications.

At present, research is being undertaken both into the underlying principles – the technical design of DLT *per se* – as well as the application-related interfaces and the legal forms it could take. The fact that these developments are taking place simultaneously makes predictions especially difficult. The actual benefits of DLT are likely to be apparent not so much in its use in traditional structures and processes, but rather come to bear more strongly in modified structures and processes. This is countered, however, not only by the potential for persistence of the existing service providers but also by the technology-related inertia of developments in payments and securities settlement (path dependency/network effects). Certainly, there may be some isolated rapid applications of DLT that do not result immediately in system change. Nevertheless, introducing it on a broad front would call for a simultaneous cooperative effort on the part of virtually all those involved. At all events, DLT has already led to further work being performed on some traditional procedures in order to improve their efficiency.

Depending on one's point of view, DLT is currently encountering a period of disillusionment in the face of its by no means trivial application in the financial system or receiving increasingly wide attention as a result of a growing number of feasibility studies, not least by central banks. The outcome of such experiments is uncertain. On the one hand, major challenges have not yet been mastered. On the other hand, it has often been the case that the real advantage of an innovation was not yet apparent at the early stages of its development. As the Bundesbank sees it, there are, for now, good grounds to go on exploring the practical applicability of DLT in payments and in securities settlement.