Central bank money and blockchain: A payments perspective

Jürgen Bott* and Udo Milkau**

Received (in revised form): 23rd May, 2017

*University of Applied Sciences Kaiserslautern — Zweibrücken, Amerikastrasse 1, Zweibrücken 66482, Germany
E-mail: juergen.bott@hs-kl.de

**Goethe University Frankfurt, Frankfurt am Main 60323, Germany; and DZ BANK AG, Platz der Republik, Frankfurt am Main 60265, Germany
E-mail: udo.milkau@dzbank.de

Jürgen Bott *is Professor of Finance Management at the University of Applied Sciences in Kaiserslautern, and visiting professor and guest lecturer at a number of other universities and business schools. He studied business administration at the Julius Echter University of Würzburg, and statistics and operations research at Cornell University. He received his doctorate from Goethe University Frankfurt. Prior to his academic career, he worked with J.P. Morgan, Deutsche Bundesbank and McKinsey & Company. He has been involved in projects with the International Monetary Fund and the European Commission and remains an academic adviser to the latter, helping to prepare legislative acts and policy initiatives on banking issues.*

Udo Milkau *is Chief Digital Officer, Transaction Banking at DZ BANK. He received his PhD from Goethe University, Frankfurt. He has been a part-time lecturer at Goethe University Frankfurt and Frankfurt School of Finance and Management, and has worked as a research scientist at major European research centres, including CERN, CEA de Saclay and GSI. He is presently Chair of the Digitalisation Working Group and a member of the Payments Services Working Group of the European Association of Cooperative Banks and the European Central Bank's Operation Managers Group.*

Abstract

Although distributed ledger technology (DLT, aka 'blockchain') is associated with high production costs and low capacity, it represents a practical solution for 'electronic cash' and a starting point for the innovation of new kinds of transactions in digitised economies. Among other institutions, the European Central Bank is committed to exploring the potential of such new technologies. This paper provides a first reflection of central bank money on blockchain, and evaluates the possible scenarios. It argues that the digitisation of central bank money (backed by trust) via DLT can open new perspectives on a digital economy with efficient and secure market infrastructures, linking new technological concepts with existing benefits.

Keywords: distributed ledger technology, blockchain, payment systems, central bank money, interoperability

Jürgen Bott

Udo Milkau

INTRODUCTION

Many central banks consider payments services as core activities. For example, the Deutsche Bundesbank defines its tasks as follows [emphasis added]:

> 'Payments are therefore one of the key tasks of the European System of Central Banks (ESCB) and by extension also of the Deutsche Bundesbank. The Bundesbank ensures the smooth functioning of domestic and foreign payments.
>
> 1. For this purpose, it *provides settlement and clearing services*.

Journal of Payments Strategy & Systems
Vol. 11, No. 2 2017, pp. 145–157

2. Moreover, the Bundesbank, as part of the ESCB, is involved in *creating a common standard* for European payments.
3. It is also responsible for *monitoring payments*; in doing so, it makes an important contribution to maintaining and strengthening the stability of the financial system'.[1]

Central banks must keep pace with technological developments and changing market needs, and as such, their role must necessarily evolve.

Digitisation in the banking industry will change the dichotomy of clearing and settlement. Within Europe, one development is the European Retail Payment Board's 'SEPA Instant Payments' initiative — real-time payments with funds immediately available for use by the recipient (beneficiary). As the Eurosystem is continuously exploring ways to develop the infrastructure of the payments market to meet the needs and requirements of the market, in June 2017, the Governing Council of the European Central Bank (ECB) has decided to develop a new service for the settlement of instant payments: the 'TARGET instant payment settlement' (TIPS[2]), as a service to facilitate 'atomic' payments transactions. With the TIPS service, the exchange of real-time messages and the settlement of funds with central bank money (ie on central bank accounts) will be an integrated process.

Another alternative is the so-called blockchain, which be will the focus of the present paper. The motivation can be illustrated by Bank of Canada's 'Jasper' project as: 'An ongoing collaboration initiated by Payments Canada and the Bank of Canada to explore the possibility of issuing, transferring and settling central bank-issued assets on a distributed ledger network'.[3]

The subject of 'central bank money on blockchain' is therefore of topical interest, being discussed by many central banks around the world, and will be elaborated in this paper in detail.

DISTRIBUTED LEDGER TECHNOLOGIES (DLT): EVOLUTION AND REVOLUTION

In December 2016, Yves Mersch, Executive Board Member of the ECB, gave a speech on 'Distributed ledger technology: role and relevance of the ECB'. He concluded with a summary that:

> 'Exploring the potential of new technologies such as DLT is high on the ECB's strategic agenda … how could a central bank interface and interoperate with DLT-based settlement services which are not necessarily offered by the central bank itself? For example, it needs to be assessed whether "a central bank could inject and control the amount of central bank money circulating in a DLT environment". Or whether, for example, a private sector trustee could ensure that the values circulated in a DLT-based solution are fully backed by a corresponding amount of central bank money held "off-chain". Such concepts could alter the existing central bank role as operator and impact monetary policy implementation. Therefore, joint analysis by the Eurosystem will be required. We are on a journey which could radically alter the financial ecosystem as we know it. The ECB is committed to be part of this journey.'[4]

Two years before this, the Bank of England highlighted DLT's relevance beyond Bitcoin as the first implementation of a blockchain.[5] DLT has the potential to redesign established processes and underlying business models. According to transaction cost economics, business models can be classified schematically as 'distributed' (ie market-like with a number of peers) or centralised (ie with a hierarchical structure in a company or in a group).[6]

DLT's underlying technical components and building blocks were developed over a long period (see Table 1) and are already applied in existing information technology.

Table 1: Existing elements in distributed computing reused in DLT (selected examples)

Basis concept	*Explanation*
The 'two generals' or 'Byzantine generals' problem (Akkoyunlu *et al.* 1975[8]) Byzantine fault tolerance (Lamport *et al.* 1982[9])	Impossibility of synchronising two or more participants via a *network of unknown* (ie trustless) nodes in a finite time. It must be remarked that this concerns the synchronisation in general and not the exchange of secure, encrypted messages. Possibility of resilience of a *network of known nodes* against failure or manipulation based on a voting consensus with a predefined fallback option in case of timeout (typically hand-over to an external third party such as human pilots in the event that the triple autopilot system cannot 'agree').
Impossibility of distributed consensus (Fischer *et al.*[10])	Impossibility of a consensus in a distributed network with the conditions that (i) one process/node may fail and (ii) the consensus should be reached in finite time.
Chain of blocks with time-stamping (Haber and Stornetta 1991[11])	'… time-stamping could … enhance the authenticity of documents … This is the case for a large class of documents which we call "tamper-unpredictable". We further conjecture that no purely algorithmic scheme can add any more credibility to a document than time-stamping provides'.
Proof of work concept (Dwork and Naor 1992[12])	Basis for a probabilistic approach to select a neutral referee in a network of *ex-ante* trustless nodes. As any voting in an open, ie anonymous, computer network for a quorum consensus can be compromised by a single faulty entity simulating multiple identities (eg 'Sybil Attack'), proof of work provides a 'game theoretical' solution for consensus under some conditions.
Introduction of the concept of 'software aging' (Parnas 1994[13])	Understanding that software systems always have errors resulting from the interaction of the different layers, but especially that software can 'get old' and will develop 'unexpected' errors over time due to the complexity and the interaction of multiple layers — which have to be corrected by 'changing'.
CAP-Theorem (Brewer 2000[14])	Impossibility in any networked shared-data system that one can achieve all three desirable properties, namely: *C*onsistency, *A*vailability and *P*artition tolerance (= fault tolerance, if part of the system fails).
Development of 'Secure HashAlgorithm 2' (SHA-2 2001[15])	SHA-2 — as an example of hash functions — is a set of injective hash 'one-way' functions designed by the US National Security Agency (NSA) and published by the US National Institute of Standards and Technology (NIST) for the cryptographic protection of sensitive information against manipulation; especially when stored in or transmitted via open networks.
Double spending problem (Osipkov *et al.* 2007[16] and Hoepman 2008[17])	Possibilities to prevent so called 'double spending' as a failure mode of electronic cash schemes, as any electronic message, ie a bit string of 0s and 1s, can be copied and send to manifold different beneficiaries in a network.

These building blocks comprise well-known components, such as encryption, hashing and techniques to synchronise decentralised databases and peer-to-peer networks. Therefore, DLT is sometimes dismissed as 'old wine in new bottles' with limited benefits for improving existing infrastructure. Indeed, some researchers have concluded that the technology is not yet mature.[7]

In contrast, moderate analysts understand DLT as smart new assembly of proven components. Engaging with DLT can have a 'catalyst effect' for an industry-wide discussion. It opens up minds and sometimes even expands horizons to release creativity and to encourage thinking about common standards, new process design and, consequently, new business models with new roles.

THE USE OF DLT FOR PAYMENT, CLEARING AND SETTLEMENT

If DLT is used in systems for payment, clearing and settlement, careful analysis is necessary to identify both the opportunities

and challenges associated with the new design (or redesign) of those processes that are critical to the financial system. It is a core principle of the Bank for International Settlements Committee on Payment and Settlement Systems that financial market infrastructures (ie those used for payment, clearing and settlement processes) should conduct their money settlements in central bank money wherever it is practical and available.[18] Where central bank money is not used, an alternative settlement asset should be used with little or no credit or liquidity risk. If settlement is conducted in commercial bank money, strict monitoring and management of the arising risks will be requested.[19]

Accordingly, settlement in central bank money is a characteristic of the highest quality. This paper evaluates possible scenarios that may apply when using central bank money to achieve finality in payments, clearing and settlement processes based on DLT, ie blockchain mechanisms, and the possible consequences if central bank money is not available or not practical to use.

ESSENTIAL ELEMENTS OF PAYMENTS, CLEARING AND SETTLEMENT

To complete a financial transaction — initiated by an exchange of messages — participants (counterparties) transfer an asset or sets of assets. Assets can be any financial instrument, such as security, commodity, derivative or money.

A term, often used synonymously for the procedures and obligations necessary to complete a financial transaction, is 'post-trade processes'. Post-trade processes usually start with the confirmation of the conditions agreed among the counterparties. The next step is clearing, in which an entity calculates the counterparties' obligations with respect to delivering the traded assets. The obligations may be computed on a transaction-by-transaction basis or on a net basis. The last step is settlement, during which the relevant obligations of the counterparties are discharged. All in all, there is a de-synchronisation between pre-trade ('exchange of message') and post-trade ('transfer of assets').

Arrangements and systems used for settlement differ by the underlying assets. If a system transfers only money, the system is called a 'payment system'. The Federal Reserve defines a 'payment system' as a set of instruments, procedures and rules for the transfer of funds between or among participants. This includes, among other things, large-value funds transfer systems, the automated clearing house, cheque clearing houses, and credit and debit card settlement systems. Other assets have their own settlement infrastructure. In the settlement process for securities, central securities depositories are often involved. The settlement of derivatives may be executed via central counterparties. The settlement arrangements for one specific asset are often referred as a 'settlement leg'. The completion of a financial transaction usually requires actions in at least two settlement legs (eg transfer of securities from the seller to the buyer in one leg and the transfer of the payment from the buyer to the seller in the second leg).

In financial market, the counterparties usually communicate with each other by sending electronic messages. They act in networks with different participants. Participants in some networks are limited to financial institutions, such as banks or broker-dealers. Other networks include users such as households or businesses.[20]

RISKS DURING PAYMENTS, CLEARING AND SETTLEMENT PROCESSES

The settlement process is complete following the final (unconditional) transfer of assets from the seller to the buyer (delivery) and final transfer of funds — ie a specific asset

called money — from the buyer to the seller (payment).[21] The money involved in such processes could be a claim against a central bank (liability of a central bank) — in which case the settlement asset is called central bank money, or a claim against a commercial bank — in which case the settlement asset is called commercial bank money. In general, it is possible to replace money with other valuable assets, such as gold.

Some markets have mechanisms to ensure delivery only once payment occurs. Such mechanisms are called 'delivery versus payment mechanisms'. Without such a mechanism, counterparties are exposed to principal risk, that is, the risk that the seller of an asset (eg a security) could deliver but not receive payment or that the buyer could make payment available to the seller but not receive delivery.[22]

Principal risk can occur in the settlement process of any asset. For example, the settlement of foreign exchange trades requires the payment of one currency and the receipt of another. In the absence of delivery versus payment mechanisms, one of the counterparties to a foreign exchange trade could pay out the currency it sold but not receive the currency it bought. Principal risk in the settlement of foreign exchange transactions is variously known as foreign exchange settlement risk, cross-currency settlement risk or 'Herstatt risk'.[23]

Even if arrangements are in place to eliminate principal risks, participants are still exposed to replacement cost risk and liquidity risk. Liquidity risk occurs in the settlement process if one of the counterparties is unable to deliver the promised asset when it is due. The other counterparty may then be forced to borrow the missing asset for the period of the delayed settlement of the transaction. If the counterparty is never able to deliver the promised asset, a replacement, ie a new transaction, with another counterparty might be necessary. The replacement, ie the new trade, could have less favourable conditions (eg the price of the purchased security) than the original one.

RISKS OF MONEY SETTLEMENT WITH OTHER ASSETS THAN CENTRAL BANK MONEY

Analysis of risks in settlement systems must not only determine the strength of the linkage between delivery and payment but must also assess the finality (irrevocability) of the transfer of the assets involved in the trade and the soundness of the claim against the settlement entities that hold the asset.

The legal definitions of the moment that finality (irrevocability) is reached have taken decades of comprehensive research and legislative effort. Extensive regulatory, statutory and contractual arrangements support these definitions.

Whenever the transfer of the asset is not performed physically (eg gold shipped from vault of the seller into the vault of the buyer) but only a claim for the asset is transferred (eg before the transaction, 'Alice' had a claim against Bank A, and after the transaction, 'Bob' has a claim against Bank A), there is, in additional to the risks prior to the irrevocable transfer of the asset, the danger of the potential failure of the entities holding the assets.

As it is considered a near certainty that a central bank will be able to fulfil all legal claims in its own currency, a claim against a central bank (in its home currency) represents the highest standard of claim. By contrast, a claim against a commercial bank always bears the risk that the commercial bank may fail.[24]

The value of payments executed in fiduciary money (money which is issued on the credit of a bank or government) depends to a large extent on the standing of the issuer, its organisational efficiency, and the structure of the money market.[25] The higher the standing of the issuer of the fiduciary money, the higher the quality of

the received payment will be. The higher the creditworthiness of the entity against which the claim is held, the lower the credit risk associated with the claim.

The value of a claim depends on the usability of the claim, too. Can the claim be used as a settlement asset on different platforms or in different settlement systems?

It has been argued that in a multi-currency environment, settlement in central bank money is impractical because there is no 'global' central bank to provide finality in a variety of currencies.[26] In general, it might be argued that the quality of fiduciary money as an asset used for payments in settlement processes depends on its disposability with respect to different (important) clearing and settlement systems. The availability and flexibility of using central bank money as a settlement asset on several (important) platforms might also be a quality factor to differentiate between currencies issued by different central banks.

There is in some respect a concealed 'competition' among central banks. When looking at international settlement processes, there are differences in the attractiveness of currencies. For example, the US dollar is more popular — ie is more commonly used — than the euro.[27] Indeed, some forms of central bank money are almost meaningless for international settlement processes.

The international role of a currency is primarily determined by market forces. Leading central banks neither hinder nor promote the international use of their currency; they merely emphasise it. The international use of a currency is analysed and depends mainly on its relevance as a basis for international reserves, investment and as a payment currency. The share of the demand for foreign central bank money as an invoicing or settlement currency for 'outside area trades' is often reflected only by the net shipments of banknotes.

However, when analysing settlement procedures more deeply, there should be no doubt that settlement procedures (eg gross or net settlement) have an impact — at least on intra-day positions — on the amount of liquidity needed for smooth operations. International settlement runs over multiple time zones. Different definitions of the 'end of a business day' cause situations where foreign currency positions are held for operational purposes, not just intra-day, but also overnight. The amount of foreign central bank money needed overnight is influenced by trade volumes, operational cut-off-times, and the clearing and settlement algorithms of the foreign/international platforms, among other things.

DLT WITH THE POTENTIAL TO CHANGE PAYMENT, CLEARING AND SETTLEMENT

Core components of DLT, eg tools for cryptographic or synchronisation of databases, are widely used in information technology for payments, clearing and settlement. Participants of payments, clearing and settlement systems) ie financial institutions and financial market infrastructures) apply technologies to propose, validate and update ledgers securely. The technology is used to synchronise distributed ledgers so that transactions may be carried out without necessarily relying on central authorities.

Using the example of the blockchain technology, it can be shown that the functionalities of payment, clearing and settlement platforms, which traditionally have a centralised design, could — from a technical point of view — also have a decentralised design that uses decentralised ledger technologies and runs on distributed ledger platforms. The developments to leverage DLT beyond Bitcoin have spawned a whole spectrum of different blockchain derivatives. Indeed, some of these derivatives have evolved so far from the original concept that one might reasonably ask just how much 'blockchain' they still contain.

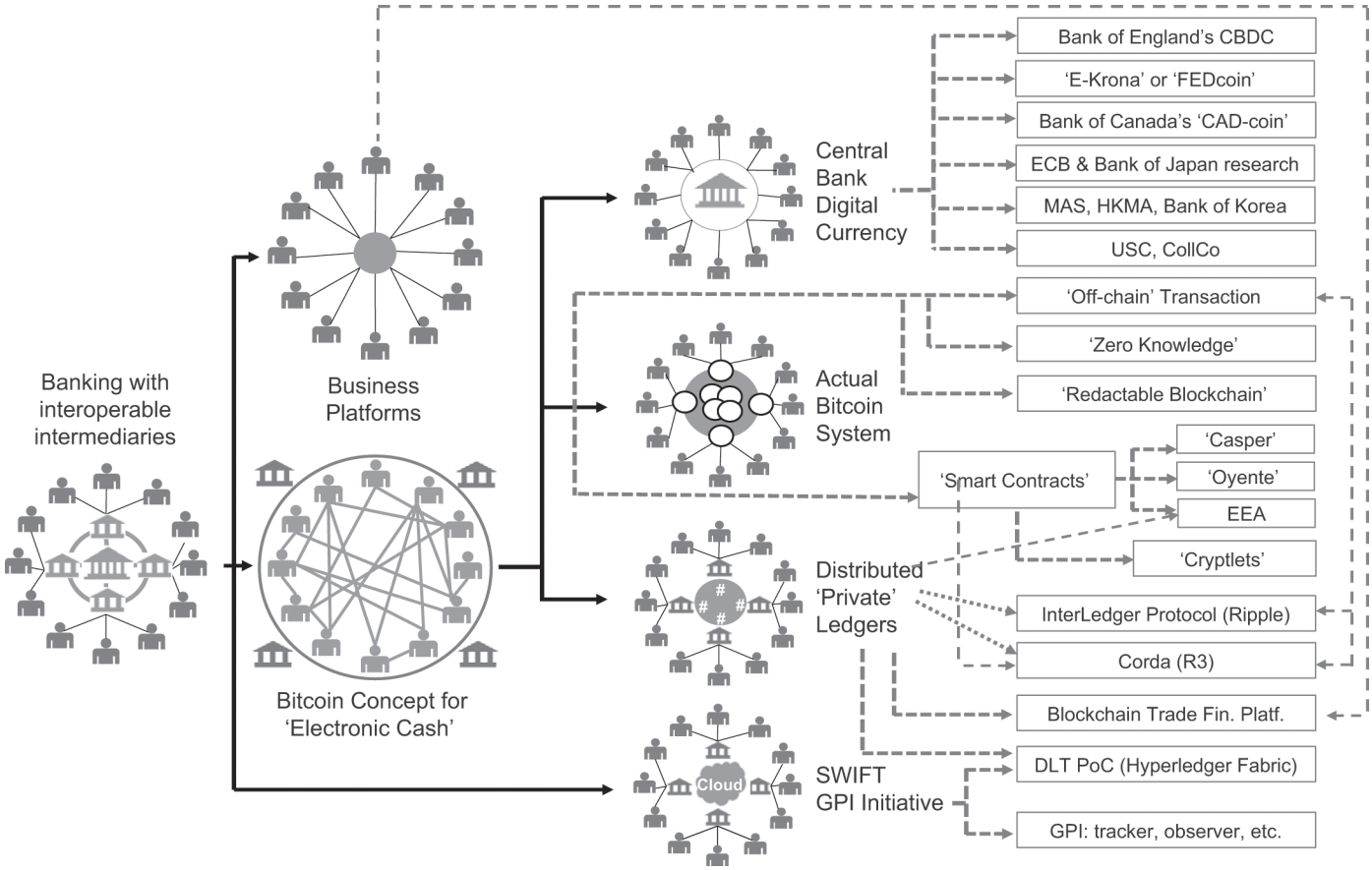

Figure 1: The four main development streams in the evolution of distributed ledger technology (DLT)

Figure 1 illustrates this dynamic development with some, by no means exhaustive, examples of current initiatives, including a number of activities being undertaken by central banks across the globe.

The four main streams are comprised as follows:

- central bank initiatives including types of 'central bank digital currency';
- blockchain developments to improve deficits in the original blockchain implementation (with off-chain transaction for capacity, eg for micropayments, zero knowledge for anonymity and redactable blockchain for editing) or extension with so-called 'smart contracts' (including scope for further improvement of 'Casper', use in enterprise environments in the 'Enterprise Ethereum Alliance', or linkage via 'cryptlets' to systems outside the blockchain);
- the development of distributed 'private' ledger technology towards protocols for the 'synchronisation' of transactions between participants in permissioned networks; and
- the extension of initiatives (such as SWIFT GPI) based on conventional technology with distributed 'private' ledger technology.

DLT's potential for central banks has been discussed in a number of recent publications and projects, most notably:

- in the UK, 'Central banks and digital currencies'[28] and 'The macroeconomics of central bank issued digital currencies';[29]

- in Sweden, 'Should the Riksbank issue e-krona?';[30]
- in the USA, 'Should the Fed issue its own Bitcoin?';[31]
- in Canada, the so-called 'Project Jasper'[32] and 'CAD-coin';[33]
- in Germany, the 'CollCo' concept proposed by Deutsche Börse[34] in addition to cooperation between the Deutsche Bundesbank and Deutsche Börse Group;[35]
- in Europe, ECB in with Bank of Japan;[36]
- proof-of-concept announcements by the Monetary Authority of Singapore,[37] Hong Kong Monetary Authority[38] and Bank of Korea;[39] and
- globally, the 'Utility Settlement Coin', launched in September 2015 to emulate central bank money on blockchain.[40]

CENTRAL BANK MONEY AS A 'NATIVE ASSET' AND 'NON-NATIVE ASSET'

It is technically possible to issue central bank money on blockchain. The process for this as follows:

1. The central bank requires an algorithm that allows a special spending condition.
2. The issuance transaction by the central bank comprises the hash of the amount and the hash of the receiver (eg the public key of Bank A, participating in an open market transaction of the central bank), for example: Hash (PubKA; Amount).
3. The hash is then signed with the 'private issuance key' of the central bank (this key is different from the verification key).
4. On the output side, the transaction is formatted as a 'normal' transaction (Amount, public key Bank A).

If the central bank wants to take volumes of central bank money out of use in the blockchain, it can execute simple 'redemption transactions' by transferring central bank money back to the central bank. For example:

- Bank A processes a normal transaction in favour of the central bank (using the public key of the central bank).
- The hash of 'previous out' is signed with the private key of Bank A and the output of the transaction shows the amount and the public key of the central bank (amount, public key central bank).

The central bank money stays on the blockchain; however, the central money in circulation (outside the central bank) is reduced. This is similar to banknotes, which are stored in the vaults of the central bank. Banknotes in the vaults of the central bank are considered only as 'printed paper' rather than central bank money.

This is just one example of how central bank money could be issued on a blockchain. There are several alternatives regarding how to originate central bank money as a digital asset on decentralised ledgers. Once issued directly on the decentralised ledger, central bank money can technically be used like any other 'native asset' (also known as 'native token'). DLT can either record assets that are native to the ledger or work with claims of assets which are held outside the DLT arrangement. Instead of issuing central bank money directly on a blockchain, it is possible to represent only central bank money on the ledger. Such a presentation is typically referred to as 'non-native asset' or 'non-native token'.

One example how to design operations around the concept of 'non-native assets' is the so called 'I owe you' (IOU) concept. The asset — in this case, the central bank money — is held outside the DLT arrangement in a kind of an escrow account. The IOU acts like a declaration of debt. Anyone who trusts the entity — or a group of entities — who declares that a defined amount of the asset is available outside the DLT arrangement

can use the representative of the asset (the non-native token) within the DLT.

Mechanisms complementing the core arrangement allow the participants of the DLT to convert the non-native token into the 'real asset'. There are exchange rates between the representative of the asset (the non-native token) and the 'real asset'. The exchange rates can be fixed (eg one non-native token equals one unit of the real asset) or they can be flexible exchange rates.

The central bank could provide central bank money as native assets or as non-native assets to be used in DLT. However, it is also possible that a trustworthy entity (eg a large financial institution with the best credit rating or a group of financial institutions) could guarantee the exchange of non-native assets (IOUs) used on a DLT to central bank money outside the DLT. Such trusted entities act like gateways between the DLT and the outside world.

For example, participants of the DLT arrangement who want to receive 'real assets' in exchange for 'non-native assets' (IOUs) received within the DLT arrangement must transfer their IOUs to the gateway (the trusted entity) by selling their IOUs to the trusted entity (the gateway). The trusted entity keeps the received IOUs and, via a system outside the DLT arrangement, transfers 'real assets' of equivalent value to the IOUs to the seller of the IOUs.

Theoretically, any trusted entity or group of trusted entities participating in a DLT arrangement could provide a gateway to other payments, clearing and settlement systems. The quality of the IOUs used within the DLT depends to a large extent on the standing of the issuers of the IOUs, their organisational efficiency, and the structure of the exchange market between the IOUs and the 'real asset' (eg central bank money).

This is reminiscent of the situation described by Tommaso Pado-Schioppa in his classic paper 'Clearing and settlement of securities — a European perspective'.[41] In the field of securities settlement, 'omnibus accounts' are a familiar concept, with 'American depository receipts' (ADRs) being a prime example. ADRs are traded in the USA but represent a specific number of shares in foreign countries, which would be too difficult to trade, clear and settle in their home countries.

If central banks are not ready to offer an efficient method to provide central bank money as a high-quality settlement asset, this opens the door for other market participants to provide efficient 'substitutes' that can be applied via DLT. However, this may entail the kind of risk in clearing and settlement arrangements that central banks and supervisors have historically sought to avoid as a result of previous quantum leaps in technology, such as improved means of electronic communication.

GETTING ACQUAINTED WITH DECENTRALISED CONSENSUS

Core 'real-time gross settlement' services can be offered on centralised and distributed ledger platforms. Traditional (interoperable) payments, clearing and settlement systems have a single central entity, which runs a centralised ledger (or the 'golden copy' of the logical ledger, which can, technically, be distributed to mirrored replicas). All participants trust the centralised ledger. In a perfect world, what the trusted central entity declares to be the new status is considered by all participants of the payments, clearing or settlement network to be the truth. It is the consensus of all participants that the trusted central entity updates the 'golden copy' of the ledger correctly.

The trusted entity could be a central bank or another authority, which confirms the correct status of the ledger with its official 'rubber stamp'. For traditional bankers, born and raised with such an understanding, it is not easy to accept that consensus does not necessarily depend on such a 'trusted' entity and that the blockchain in a distributed

'public' ledger system — such as Bitcoin — is a 'trustless' or 'permissionless' system (ie a peer-to-peer system between unidentified participants).

Distributed 'public' ledger systems can reach consensus without a 'rubber stamp' from a trusted central party. DLT uses consensus algorithms to prioritise ('time-stamp') one valid transfer after another, so that only one transfer is accepted and others are ultimately rejected (avoidance of 'double-spending').

The consensus model used in Bitcoin is called 'proof of work', which is based on the idea that any special access to a network comes at a price.[42] Specific members of the network — so-called miners who stay in competition with each other to 'win the game'[43] — have an economic interest in maintaining the trustworthiness of the network. The miner, who is selected probabilistically to act as a 'neutral referee' for the next block in the chain, earns an incentive for his or her contribution to the 'game'. Economically, all players benefit more from cooperating than manipulating. In the end, a newly verified block is chained to the existing blocks so 'strongly' by cryptography hash-algorithms, that the 'blockchain' is considered an (almost) immutable transaction log (journal of the sequence of transactions).

Due the nature of extended networks, two miners may create a new block in parallel but with different transactions (eg for Bitcoin, the probability is about 1.7 per cent[44]). Where two different versions of the blockchain exist in parallel for a certain period of time, such situations are known as 'forges'. A rule has been created so that, in the event of a forge, only the transactions in the longer blockchain will continue to be considered verified and valid. All transactions in the shorter branch will be reversed or dropped.

The longer a transaction is considered settled by the systems' participants, the higher the likelihood that the transaction has really reached finality. This approach to finality will be unfamiliar to the majority of current bankers, who have been brought up to define an unambiguous and transparent moment of finality. If settlement finality becomes a probabilistic (called 'eventual consistency') function, traditional definitions and legal consequences of settlement finality may no longer be applicable.

RESTRICTING FUNCTIONALITY AMONG NETWORK MEMBERS

For a distributed ledger, proposed transactions and subsequent positions are broadcast to all participants, who maintain a copy of the ledger which is ultimately accepted as the new version of the ledger. In fully decentralised arrangements, not a single function is exclusively executed by just one member of the network. In such 'permissionless' or 'open' DLT systems, all members of the network are entitled to read the full blockchain of transactions from the very beginning.

There are, however, alternatives to permissionless and open networks. These alternatives are 'closed' or 'permissioned' systems. Participants in these networks are identified and permitted *ex ante* (by some 'central' mechanism) and can be differentiated by the functions they are permitted to perform. There may be participants who can only send and receive assets. Others have (exclusive) rights to validate transactions. A third group (eg supervisors) have the right to read only.

Such 'permissioned' DLT systems are currently the focus of discussion and proof-of-concepts in the banking industry. They do not need the complex and resource-intensive 'proof-of-work' consensus mechanism of 'permissionless' DLT systems, and can be understood as a hybrid between the original blockchain toolbox of technical components and central control or, respectively, governance. This is a bridge for the use of DLT, which has the potential to be a trigger for

the next quantum leap in designing trading, payment, clearing and settlement platforms, as indicated by Yves Mersch, among others.

CONCLUSIONS

Inspired by the 'reality check' for blockchain technology provided by the real-world case of Bitcoin, different banks, consortia and central banks are experimenting with DLT to improve existing systems and build new platforms, changing traditional process and business-logics to explore new business cases.

For payments, clearing and settlement platforms in particular, the applicability of central bank money will be a key success factor for the breakthrough of DLT: without the link to central bank money, finality will always be outside the blockchain.

However, the new process and business logic, which is enabled by DLT may cause uncertainties compared with traditional setups. Central banks, oversight and supervisory authorities are aware of several of these challenges, eg in the areas of legal risks, governance, operational security and data protection or control of data by the data subject (including the 'right to be forgotten').

Although more research and discussion is needed, this journey really could 'radically alter the financial ecosystem as we know it'.[45] All members of the banking industry — from central banks to providers of critical financial market infrastructures — should continue to work on those 'discovery' projects started already, to gain better understanding and experience of how DLT works. Cross-functional groups of experts from banks or central banks (eg information technology, operations, market infrastructure and legal) need these experiences to better evaluate the pros and cons of the new process designs. Such knowhow is essential in order to find sound solutions for the challenges the new processes and business models will bring.[46]

How central banks interpret their mandate evolves over time. Twenty years ago, central banks limited their responsibility in operational systems to large-value payments systems. Now, they provide delivery-versus-payment mechanisms for securities settlement systems (eg TARGET2-Securities), provide services to mobilise collateral and foster the establishment of near real-time retail payments systems. Today, their role includes acting as a catalyst for change, and the journey of the blockchain is a special example, which — at the end — could further expand the scope of central banks' mandate. Central bankers may be assigned tasks that will improve attractiveness of their currency by providing efficient settlement solutions to apply central bank money on new international trading, clearing and settlement platforms built on DLT.

There is even the potential risk that without sufficient and efficient interfaces between emerging new trading, clearing and settlement platforms, which to a large extent apply to DLT and the provision of central bank money, other market participants will provide substitutes for central bank money (eg IOU arrangements). These alternative methods for settling against assets other than central bank money could see a return to higher-risk situations (eg of extensive netting or extensive settling in commercial bank money), such as arose previously during the phase of massive automation and extensive use of electronic communication but which now seem to be under control.

The new technology of DLT must not come as entirely permissionless open systems. Within 'hybrid' permissioned systems, certain functions (from notary functions to system access) could be kept centralised and under the control of central banks. Network participation could be limited to entities with specific licences. In other words, different network members should be restricted to different functions. In the final analysis, DLT is a toolbox (see Table 1), which must be used with a deep understanding of the structure of financial systems and the roles

and responsibilities of all participants, whether banks, central banks or third parties.

References and Notes

(1) Deutsche Bundesbank/Eurosystem (n.d.) 'Payment systems/tasks and services', available at: www.bundesbank.de/Redaktion/EN/Standardartikel/Tasks/Payment_systems/payment_systems.html (accessed 19th May, 2017).

(2) Mersch, Y. (2017) 'Developing Europe's payment landscape', paper presented at Bundesbank's Payment and Securities Settlement Symposium, Frankfurt am Main, 18th May.

(3) Hendry, S. (2016) 'The Bank of Canada's blockchain experiment', paper presented at the Chicago Payments Symposium, 13th October.

(4) Mersch, Y. (2016) 'Distributed ledger technology: role and relevance of the ECB', paper presented at the 22nd Handelsblatt Annual Conference Banken-Technologie, Frankfurt, 6th December, available at: www.ecb.europa.eu/press/key/date/2016/html/sp161206.en.html (accessed 15th December, 2016).

(5) Ali, R., Barrdear, J., Clews, R. and Southgate, J. (2014) 'Innovations in payment technologies and the emergence of digital currencies', *Bank of England, Quarterly Bulletin*, Vol. 54, No. 3, pp. 262–275.

(6) Williamson, O.E. (1979) 'Transaction-cost economics: the governance of contractual relations', *Journal of Law and Economics,* Vol. 22, No. 2, pp. 233–261.

(7) Pinna A. and Ruttenberg W. (2016) 'Distributed ledger technologies in securities post-trading: revolution or evolution?', Occasional Paper No. 172, European Central Bank, April, 2016; www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf (accessed 4th May, 2017).

(8) Akkoyunlu, E.A., Ekanadham, K. and Huber, R.V. (1975) 'Some constraints and trade-offs in the design of network communications', in 'Proceedings of the Fifth ACM Symposium on Operating Systems Principles, Austin, TX, 19th–21st November', ACM, New York, NY, pp. 67–74.

(9) Lamport, L., Shostak, R. and Pease, M. (1982) 'The Byzantine generals problem', *ACM Transactions on Programming Languages and Systems*, Vol. 4, No. 3, pp. 382–401.

(10) Fischer, M. J., Lynch, N. A. and Paterson, M. S. (1985) 'Impossibility of distributed consensus with one faulty process', *Journal of the Association for Computing Machinery*, Vol. 32, No. 2, pp. 374–382.

(11) Haber, S. and Stornetta, W.S. (1991) 'How to time-stamp a digital document', *Journal of Cryptology*, Vol. 3, No. 2, pp. 99–111.

(12) Dwork, D. und Naor, M. (1992) 'Pricing via processing or combatting junk mail', in Brickell, E.F. (ed.) 'Advances in Cryptology — CRYPTO '92', *Lecture Notes in Computer Science*, Vol. 740, pp. 139–147.

(13) Parnas, D.L. (1994) 'Software aging', in 'Proceedings of the 16th International Conference on Software Engineering, Sorrento, 16th–21st May', IEEE Computer Society Press, Los Alamitos, CA, pp. 279–287.

(14) Brewer, E. (2000) 'Towards robust distributed systems', in 'Proceedings of the 19th Annual ACM Symposium, Principles of Distributed Computing, Portland, OR, 16th–19th July', pp. 7–10.

(15) National Institute of Standards and Technology (2001) 'Secure Hash Algorithm 2', in: 'Security Requirements for Cryptographic Modules', Federal Information Processing Standards Publication 140-2, NIST, Gaithersburg, Md.

(16) Osipkov, I., Vasserman, E.Y., Hopper, N. and Kim, Y. (2007) 'Combating double-spending using cooperative P2P systems', paper presented at the 27th International Conference on Distributed Computing Systems, Toronto, 25th–27th June.

(17) Hoepman, J.H. (2008) 'Distributed double spending prevention', paper presented at the 15th International Workshop on Security Protocols, *Lecture Notes in Computer Science*, No. 5964, pp. 152–165.

(18) Committee on Payment and Settlement Systems, Technical Committee of the International Organization of Securities Commissions (2012) 'Principles for Financial Market Infrastructures', Bank for International Settlements, Basel.

(19) Central bank money is a liability of a central bank. Commercial bank money is a liability of a commercial bank. Credit risk in a settlement process arises when counterparties have the potential to default on their obligations. Liquidity risk arises in settlement if participants are unable to transfer readily the assets they owe. Compared with central bank money (as a liability), Bitcoins are 'tokens' and a Bitcoin transaction is a record of the right to claim an unspent token for a new transaction.

(20) Mills, D., Wang, K., Malone, B., Ravi, A., Marquardt, J., Chen, C., Badev, A., Brezinski, T., Fahy, L., Liao, K., Kargenian, V., Ellithorpe, M., Ng, W. and Baird, M. (2016) 'Distributed Ledger Technology in Payments, Clearing and Settlement', Finance and Economics Discussion Series 2016-095, Division of Research & Statistics and Monetary Affairs, Federal Reserve Board, Washington, DC.

(21) Federal Reserve, Board of Governors (2016) 'Policy on Payment System Risk', 23rd September, available at: www.federalreserve.gov/paymentsystems/files/psr_policy.pdf (accessed 6th May, 2017).

(22) Committee on Payment and Settlement Systems of the Central Banks of the Group of Ten Countries (1992) 'Delivery versus Payment in Security Settlement Systems', Bank for International Settlements, Basel.

(23) On 6th April, 2017, CLS Group announced an automated payment netting service - CLSNet - for foreign exchange (FX) trades that are settling outside the CLS settlement service by using DLT: 'Participants will be able to submit FX instructions

for spot, tom/next day, forwards, non-deliverable forwards (NDFs), swaps and same-day trades for more than 140 currencies. They will be able submit FX instructions through traditional SWIFT channels or distributed ledger technology (DLT)'. See: CLS (n.d.) 'CLSNet', available at: www.cls-group.com/ProdServ/Pages/CLSNet.aspx (accessed 8th May, 2017).

(24) Committee on Payment and Settlement Systems of the Central Banks of the Group of Ten Countries (1996) 'Settlement Risk in Foreign Exchange Transactions', Bank for International Settlement, Basel.

(25) Galati G. (2002) 'Settlement risk in foreign exchange markets and CLS Bank', *BIS Quarterly Review*, December, pp. 55–66.

(26) Padoa-Schioppa, T. (2001) 'Clearing and settlement of securities: a central bank money perspective', paper presented at the Deutsche Bundesbank Symposium, 'Payment and Securities Settlement Systems in Germany against the Background of European and International Developments', Frankfurt, 5th September, *BIS Review*, Vol. 81, pp. 1–7.

(27) European Central Bank (2016) 'The international role of the euro, interim report', available at: www.ecb.europa.eu/pub/pdf/other/euro-international-role-201606.en.pdf (accessed 29th May, 2017).

(28) Broadbent, B. (2016) 'Central banks and digital currencies', paper presented at the London School of Economics, 2nd March.

(29) Barrdear, J. and Kumhof, M. (2016) 'The macroeconomics of central bank issued digital currencies', Staff Working Paper No. 605, Bank of England, 18th July, available at: www.bankofengland.co.uk/research/Pages/workingpapers/2016/swp605.aspx (accessed 29th July, 2016).

(30) Skingsley, C. (2016) 'Should the Riksbank issue e-krona?', 16th November, available at: www.riksbank.se/en/Press-and-published/Speeches/2016/Skingsley-Should-the-Riksbank-issue-e-krona/ (accessed 29th May, 2017).

(31) Andolfatto, D. (2015) 'Should the Fed issue its own Bitcoin?', paper presented at 'P2P Financial Systems 2015', conference organised by Goethe University Frankfurt, Deutsche Bundesbank and UCL, Frankfurt, 29th–30th January.

(32) Chapman, J., Garratt, R., Hendry, S., McCormack, A., and McMahon, W. (2017) 'Project Jasper: Are Distributed Wholesale Payment Systems Feasible Yet?', available at: http://www.bankofcanada.ca/wp-content/uploads/2017/05/fsr-june-2017-chapman.pdf (accessed 4th June, 2017).

(33) Garratt, R. (2017) 'CAD-coin versus Fedcoin', 14th April, available at: www.r3cev.com/s/cad-coin-versus.pdf (accessed 4th May, 2017).

(34) Deutschen Bundesbank and Deutschen Börse Group (2016) 'Gemeinsamer Blockchain-Prototyp von Deutscher Bundesbank und Deutscher Börse', press release, 28th November, available at: www.bundesbank.de/Redaktion/DE/Pressemitteilungen/BBK/2016/2016_11_28_blockchain_prototyp.html (accessed 15th December, 2016).

(35) Deutsche Börse Group (2017) 'Deutsche Börse presents blockchain concept for risk-free cash transfer', press release, 23rd January, available at: http://deutsche-boerse.com/dbg-en/media-relations/press-releases/Deutsche-Boerse-presents-blockchain-concept-for-risk-free-cash-transfer/2883236 (accessed 4th March, 2017).

(36) Bank of Japan (2016) 'ECB and the Bank of Japan launch a joint research project on distributed ledger technology', available at: www.boj.or.jp/en/announcements/release_2016/rel161207a.htm/ (accessed 4th May, 2017).

(37) Monetary Authority of Singapore (2017) 'MAS working with industry to apply distributed ledger technology in securities settlement and cross border payments', 9th March, available at: www.mas.gov.sg/News-and-Publications/Media-Releases/2017/MAS-working-with-industry-to-apply-Distributed-Ledger-Technology.aspx (accessed 14th March, 2017).

(38) Chan, K.C. (2017) 'Gov't developing fintech', paper presented at Internet Economy Summit, 10th April, available at: www.news.gov.hk/en/record/html/2017/04/20170410_113015.shtml (accessed 14th April, 2017).

(39) EconoTimes (2017) 'Bank of Korea, R3 consortium to carry out blockchain project', available at: www.econotimes.com/Exclusive-Bank-of-Korea-R3-consortium-to-carry-out-blockchain-project-549053 (accessed 14th March, 2017).

(40) Reuters (2016) 'UBS leads team of banks working on blockchain settlement system', 24th August, available at: www.reuters.com/article/us-banks-blockchain-ubs-idUSKCN10Z147 (accessed 4th May, 2017).

(41) Padoa-Schioppa, ref. 26 above.

(42) Dwork and Naor, ref. 12 above.

(43) Milkau, U., Neumann, F. and Bott, J. (2016) 'Development of distributed ledger technology and a first operational risk assessment', *CAPCO Journal of Financial Transformation*, Vol. 44, pp. 20–30.

(44) Decker, C. and Wattenhofer, R. (2013) 'Information propagation in the Bitcoin network', paper presented at the 13th IEEE International Conference on P2P Computing, 18th–21st July, Toulouse.

(45) Thiele, C.-L. (2017) 'Industry dialogue on "distributed ledger technology — potential benefits and risks"', paper presented at the G20 Conference 'Digitising Finance, Financial Inclusion and Financial Literacy', Wiesbaden, 26th January.

(46) Another problem is the situation, which was experienced by 'The Decentralized Autonomous Organization' (DAO). An unknown participant hacked the DAO blockchain by using a bug in the software of a 'smart contract' and transferred a large amount from DAO's address to a separate address. The (philosophical) question arose whether obviously illegitimate transactions should be retained in order to preserve the inalterability of common ledger. Just reversing the action — especially if reversal is initiated or executed by a central entity — would violate the core principle of decentralised consensus.