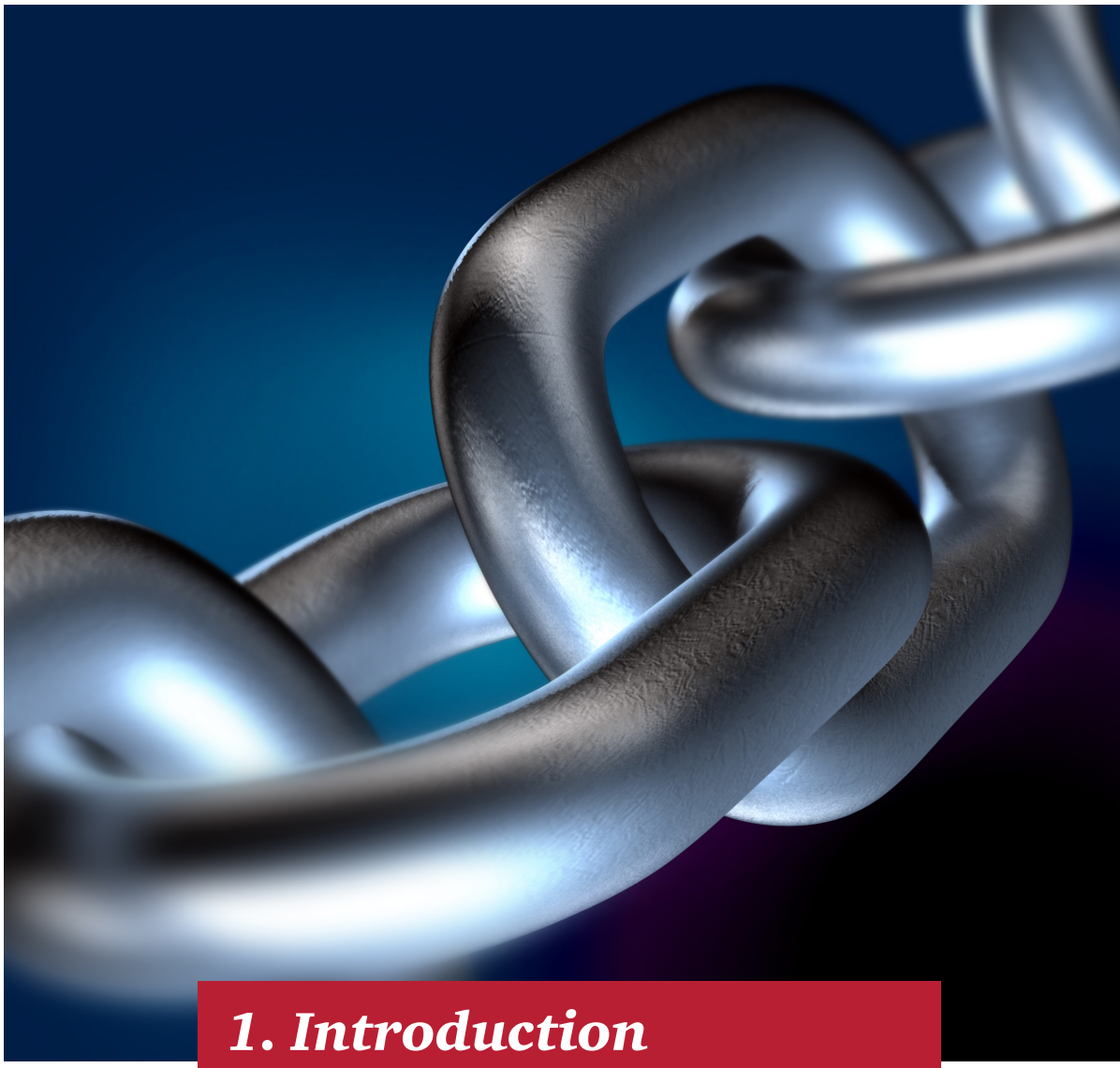
Blockchain and its application in Financial Services

PwC
Woluwe Garden
Woluwedal 18
1932 St-Stevens-Woluwe

Marc Sel
marc.sel@be.pwc.com

Marleen Mouton
marleen.mouton@be.pwc.com



1. Introduction

This article provides an introduction to the concepts of what is commonly referred to as "blockchain". The functionality offered by a blockchain is introduced, and its functioning is described. Subsequently blockchain-based solutions are discussed from a legal perspective. Finally, regulatory aspects of blockchain-based application in the financial sector are addressed.

This article was presented at the ISSE 2016 Conference (Paris, 15-16 November 2016), organised by EEMA.

2. Blockchain in a nutshell

2.1. Purpose

A blockchain consists of a set of protected information blocks chained sequentially to one-another. Together they form a ledger, distributed over the participating nodes. These nodes are computing platforms that interact with the end users. The terms blockchain and distributed ledger are commonly used as synonyms. The purpose of the ledger is to share information amongst all parties that access it via an application. Access to this ledger in terms of reading and writing may be unrestricted ('permissionless'), or restricted ('permissionbased'). The shared information is protected against modification, meaning that any alteration would be easily and immediately detectable. For that reason, once information is recorded on the blockchain, it is considered immutable because it is so strongly protected.

2.2. Building blocks

The main building blocks of a blockchain system are its data structure, i.e. the blockchain, and its nodes, where the logic and computations take place. Nodes exist in two types, full function nodes and partial nodes. Each full function node maintains a complete copy of the blockchain, is capable of committing transactions to it, and participates in extending the chain. All full function nodes are equivalent in terms of functionality, and are connected in a peer-to-peer network. This means there is no hierarchy amongst the nodes, and all nodes are able to communicate with one another. A partial node is equally connected to the network in a peer-to-peer fashion, but does not contain a full copy of the blockchain. It needs the services of a full function node to commit transactions, and it does not participate in extending the chain.

A blockchain starts from its genesis block, and new blocks are appended periodically. Each block records executed transactions. The nodes collaborate to connect the blocks into a blockchain, creating a ledger that cannot be changed backwardly without redoing a proof-of-work.

2.3. Functioning and security functions

Each block contains two types of information. The first type is application-specific information ('payload') that records transactions or smart contracts. These consist of a combination of data and code executable by the nodes. The second type is internal information that secures the block and specifies how it is chained to another. Blocks get automatically propagated across the network, verified and linked via hash[1] values.

The main protection mechanisms are the following. The first protection mechanism is linking each block with its predecessor in a way that is computationally hard to undo. This is achieved by the combination of two techniques. The first technique is the use of a hash tree. This means that a hash is calculated for each block, which includes the hash value of the previous block. This is done for each new block created, with the exception of the first block (the 'genesis' block), which has no predecessor. The second technique is the inclusion of a special number in each block, the block's 'nonce'. Insertion of the right nonce allows to calculate a specific hash value over the entire block. Such a nonce is computationally hard to calculate, therefore it is referred to as a 'proof-of-work'. When the correct nonce is inserted in the location reserved, calculating the hash function over the block will yield a specific hash value, i.e. one that starts with a specified number of zeroes. Since the nonce is hard to calculate, replacing a block by another one would mean redoing the nonce computations of all blocks that were subsequently linked to it. With the current state of algorithms and computing power, it is generally believed to be infeasible after extending the chain with approximately six blocks.

[1] A hash function is a mathematical one-way function that converts an input string of arbitrary length in an output string of fixed length, e.g. 128 or 160 bits. One-way means given the output, it is mathematically infeasible to derive the input. Other requirements imposed on hash functions include the impossibility for collisions (different inputs that convert to the same output) and the impossibility to find a second pre-image (given the output, it is mathematically infeasible to find a second input that would convert to the same output)

The second protection is the peer-to-peer built-in consensus mechanism. A majority of nodes need to agree about the next block that extends the chain. There is no central point of control that can be compromised. A blockchain system functions without a central trusted entity, in a peer-to-peer mode, where all nodes are equal. There is no trust between the nodes, so they need to rely on a consensus mechanism to confirm the transactions. The consensus mechanism is based on a verification by every node that the received information complies with a set of rules, and by a verification of the nonce (the 'proof -of-work'). The rules verify that the proposed transaction complies with the application functionality. This is application-specific. For example in the case of a virtual currency it is verified that the payer has ownership over the coins he wants to spend.

Such ownership is demonstrated by a signature using the private key of a Public Key Infrastructure (PKI) key pair. The verification of the 'proof-of-work' demonstrates that a node has invested the required computational power to participate in the extension of the chain.

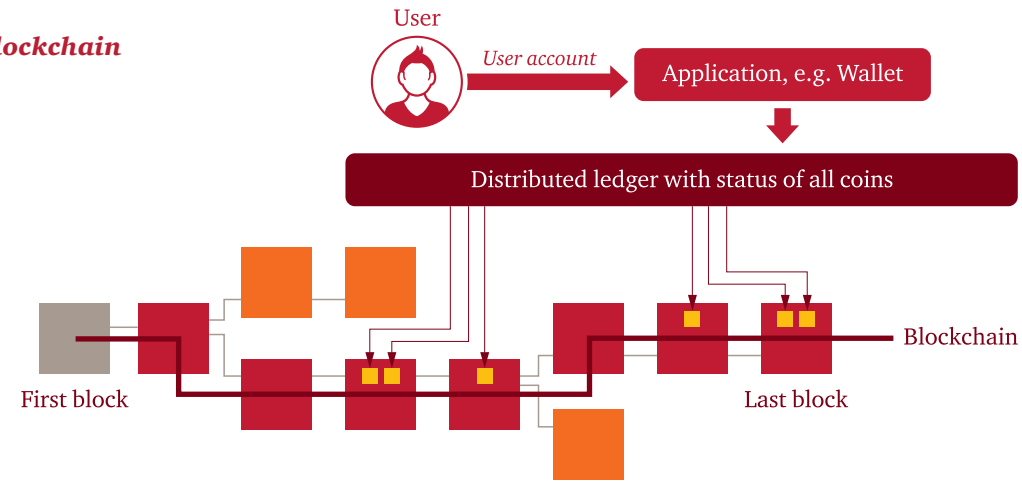
If two nodes would broadcast different versions of the next block at the same time, some nodes may receive one or the other first. Each node would work on the first block received, but save the other branch in case it becomes longer. The tie will be broken when the next nonce is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.

While these two protection mechanisms are inherent to each blockchain, the third protection mechanism is optional. It stems from the fact that blockchains come in two different flavours: permission-less and permissioned. The public, bitcoin-like systems, where every node can participate (read, add entries or extend the blockchain by finalising a candidate block with the correct nonce) are denoted as permission-less. On the other hand, permissioned blockchains allow only a limited set of known and accepted nodes to process the transactions and extend the chain. As this type of chain is typically set by know and consenting organizations with assumed level of trust, the consensus mechanism can be based on a less intensive computational process. Such permissioned blockchain function is based on the self-interest of the participants and they do not need to prove each other they invested sufficient amount of computational power in confirming the transactions.

2.4. Basic applications – virtual coins

Virtual coins are a popular family of applications build on blockchain. A coin consists of the combination of data (representing value) and code (rules on how to spend the value). Figure 1 illustrates the main components of a coin system such as bitcoin (a virtual currency) or namecoin (a repository where DNS-names and their corresponding IP address are stored).

Figure 1 – Coins on a blockchain



Legend Genesis block · Orphaned block · Main block · Blockchain · Coin

2.4.1. Making a payment

An end user installs a wallet application and generates an account and an address to interact with the blockchain. He initially pays using a traditional payment method to receive his first coins at that address. Once these are received, he can create his own payment transactions from the wallet. Such a transaction contains data and code. The data identifies payer, payee and amount. The code defines in a script language how to unlock the value the payer wants to transfer to the payee, and how to lock the value subsequently to the payee. Performing the transaction requires interaction with a full function node to execute the script code. Upon successful execution, the transaction output is broadcast to peer nodes, which relay the output to further peers.

2.4.2. Mining

Upon reception, nodes insert the transaction output they received in the payload of their new candidate block. In the payload there is room for this output, and there are two reserved locations. One location is reserved to be filled in by the nonce, the other one can be filled by a value that represents the creation and allocation of a benefit. All full function nodes insert the benefit value of their choice (typically a transaction that makes a payment to them self) and start 'mining', i.e. searching the nonce that when combined with the rest of the information, yields a valid hash value. This searching is also referred to as the proof-of-work.

The first node to find a hash value that meets the specified condition broadcasts the newly completed block to all other nodes, to verify it. This new block contains the benefit value for the miner that was the first to successfully find the required nonce. If this new block is successfully verified by the network, the originating miner sees his efforts rewarded by the benefit and the results included in the payload of the new block are available in all full function nodes. The successful miner created value for itself, which can be used in future transactions. A competing miner may broadcast his block just after the first miner, and also link his block to the blockchain. However, the nodes will notice the time difference and his block will become an orphan block.

Partial nodes do not mine, and may store the entire blockchain, or only parts thereof, i.e. those blocks that contain transactions relevant to them. Partial nodes can interact with end users, but they are dependent upon full function nodes to commit transactions to the blockchain. A wallet can be implemented on a mobile devices as partial node, maintaining only information about the coins its owner can spend. The mobile device would not have to store the full blockchain, but would still be able to offer wallet functionality to its user. Making or receiving payments would however require the wallet on the partial node to interact with a full function node.

For more information about cryptocoins, the seminal article by Nakamoto[2] is suggested. Today there are a significant number of competing coins available, and on-line reporting[3] is available via different channels.

2.5. Advanced applications – smart contracts

The possibilities of the mechanism explained in the preceding section can be extended into smart contracts. The underlying idea for those is to make a breach of a contract expensive (e.g. vending machine dispatches a drink in exchange for cash, 'breaking' the machine is more expensive than supplying the cash). A smart contract is a contract capable of automatically enforcing itself between individual participants, without the involvement of a third party.

Smart contracts define rules and consequences, as traditional legal documents do. Furthermore they take information as in input and perform the specified actions as a result.

They contain a combination of data and code. Rather than being coded in a dedicated cryptocurrency script language, smart contracts are written in a richer programming language such as Solidity. A contract layout consists of:

Contracts are created by a function called the constructor. Upon execution of the contract's constructor it gets inserted into the blockchain. When the relevant event happens, a blockchain transaction is sent to that address and the smart contract is executed. The execution typically consumes some cryptocurrency value.

Today the most popular implementation of smart contracts is probably Ethereum[4], a public blockchain-based platform. Each node runs the Ethereum Virtual Machine (EVM), which can execute peer-to-peer contracts using a cryptocurrency called ether. It was proposed in 2013 by Vitalik Buterin, and its development was funded by an online crowd sale during July–August 2014. The Ethereum platform was officially launched at July 30, 2015 and is now a significant development ground for smart contract applications.

Contract contractname

Variables
(the data part, where 'public' variables maintain the state)

[Events]
(optionally, a list of events the contract listens for)

Functions
(the code part)

Constructor
(the part of the code that creates the contract on the blockchain)

Other functions
(other application logic)

[2] https://bitcoin.org/bitcoin.pdf

[3] http://coinmarketcap.com

[4] https://www.ethereum.org

2.6. Blockchain applications and trust model

2.6.1. Dapps - applications deployed on a blockchain

Applications built on blockchain are called *dapps* (distributed applications). As a blockchain is essentially a public ledger of transactions it can be used to develop cryptocurrencies and distributed applications where ordering of transactions is important. This includes trading in financial instruments, records of almost any type (loans, mortgages, land titles, business registries, ...), contracts, signatures, wills, degrees, certifications, patents, trademarks, licences, proof of authorship and related. Permissioned blockchains are attractive for the regulated industries, where the nodes need to comply with the regulatory rules.

In September 2016, there were 299 *dapps* based on Ethereum in various states of maturity available[5]. They cover green energy consumption tokens, lotteries, digital asset management, and many more topics.

2.6.2. Trust in the blockchain

Trust is a concept that is hard to define. In the context of this article, it is defined as an attitude of a trustor that influences his future decisions regarding a trustee. It is based on past behaviour and assumed future engagements of the trustee, combined with the degree of control the trustor or another party holds over the trustee (if any).

Regarding trust, following observations can be made. Dieter Gollmann stated that trust is bad for security[6]. Rather than trust, one should rely on evidence. However, when using ICT solutions, the evidence they provide is hard to verify. Also, *dapps* are dependent on cryptographic functions and keys, so using a *dapp* requires trusting cryptography. While the use of cryptography became commonplace, key management remains challenging (e.g. a user may lose his private key, which in the case of a blockchain leads to losing access to digital assets). Furthermore, Piotr Cofta[7] argued that we do not need trust, but confidence. He formulates it as confidence = trust + control, where control expresses what is enforceable. If we follow this line of thinking, it needs to be considered that control is exercised in a *dapp* in a way which is very different from a traditional application. The main source of this difference is the built-in consensus model: whether a transaction is recorded on the ledger requires the majority of the nodes to accept it. This means that computing power rules and is used to define a shared truth.

The security of blockchain based applications presents itself as attractive. Integrity is provided via a hash tree, and is verifiable to all participants. Confidentiality is facilitated through the use of pseudonyms (which are actually public keys). However, what is published on the blockchain is publicly visible, so it may be required to encrypt selective data elements, or operate a permissioned blockchain where you can limit access to.

Availability is inherently strong since a *dapp* is built on a peer-to-peer architecture, which provides replication of the blockchain to all participating nodes.

Nevertheless, following observations are in order. A decision to accept a block and hence the validity of its transactions is based on consensus of the majority of the nodes. Since we deal with pseudonyms it is not transparent what the majority is composed of. There are no guarantees that a single party (or multiple colluding parties) does not operate a majority of nodes, and hence controls the consensus. Furthermore, the system code is open source code that can be scrutinised, and the content of the blockchain is publicly visible as well. But it has been demonstrated that code despites exposure and multiple reviews may still contain weaknesses. The largest *dapp* created on Ethereum so far is the Distributed Autonomous Organisation (DAO). It organised a token sale in May 2016, and collected a value of approximately 14 % of all existing ether, corresponding to roughly 150 million USD. The DAO got hacked in June 2016. Today it is still not clear how much money the attacker will finally be able to extract, but according to the information currently announced by the DAO's curators, this is in the order of magnitude of tens of millions of USD.

Finally, the people managing the code are humans, and are subject to legislation. Legislation in a global context can be qualified as complex, and the controls exercised over humans in the context of *dapps* cannot easily be made transparent.

[5] http://dapps.ethercasts.com/

[6] 'Why Trust is Bad for Security' - doi:10.1016/j.entcs.2005.09.044

[7] 'Trust, Complexity and Control: Confidence in a Convergent World', ISBN 978-0-470-06130-5

3. Financial services
The Blockchain-train has left the station

The financial services industry is currently shifting in a higher gear when it comes to using Distributed Ledger Technology (hereafter DLT or the technology).

3.1. The current situation

It is well known and recognized in the financial industry that there are many possible benefits[8] to be taken from the technology and together we are also steadily establishing a general idea of how it all works. At the same time, there are reasons to be hesitant to implement such revolutionary technology in an industry that heavily relies on the trust of the general public. The fact that the industry is heavily regulated and the presence of deposit guarantee schemes have helped maintaining said trust so far. But how are the regulators dealing with the many changes that are currently happening in the industry?

To picture the current DLT landscape it is worth mentioning that just recently four of the world's biggest banks have announced to team up and develop a new form of digital cash that could become a new industry standard to clear and settle financial trades over DLT[9]. There is also the R3CEV consortium[10], which has taken up the task to build a next generation of global financial services technology.

Through the use of a so-called private distributed ledger, there is only a limited amount of participants that have access to the recorded data. It is now shown in practice that there is a way to construct a DLT that provides the necessary discretion and privacy, but simultaneously has the option to flag transactions on a real-time basis for the regulators to see and monitor. In such an environment there is a high level of privacy, and at the same time, regulators can keep an eye on possible illegal activity and help maintain the financial stability in general.

In addition, there is the Ripple[11] protocol that would solve the scalability problem[12] Bitcoin has been struggling with. This scalability problem would be one of the major issues for financial institutions where hundreds of thousands of transactions are processed every day. This would require an enormous computing power assuming the same type of DLT used by Bitcoin is applied. As a consequence there would be additional energy requirements that may ultimately level out any of the cost reductions that were achieved over the currently used technology infrastructure. The Ripple protocol offers a solution that should be well considered for future projects.

To conclude the discussion of the current situation, we would like to mention cybersecurity, which has become a major concern in the financial industry. Hackers have been trying vigorously to exploit weak spots or flaws in the underlying code of DLT-projects and digital currency exchanges[13]. In June 2016 hackers had found such weak spot in the Decentralized Autonomous Organization ***(DAO)***[14], more specifically in the way smart contracts[15] were executed on this Ethereum based platform[16]. Cybersecurity is therefore a top-priority for DLT-projects and the regulators.

---

[8] If the technology is adopted in the day-to-day operations of financial institutions, there is a high possibility this will result in faster, cheaper and automated processing of financial transactions, defence against fraudulent activity and improved

[9] https://www.ft.com/content/1a962c16-6952-11e6-ae5b-a7cc5dd5a28c

[10] R3CEV is a consortium that establishes a partnership with over 50 of the leading financial institutions. Including: Barclays, Commonwealth Bank of Australia, Goldman Sachs, JP Morgan, State Street, UBS, Bank of America, Deutsche Bank, HSBC, BNP Paribas … and which has developed "Corda", a platform designed to achieve a global database that records the state of deals and obligations between institutions and people. Ultimately, the goal is to eliminate much of the manual, time consuming effort currently required to keep disparate ledgers synchronised with each other. www.r3cev.com

[11] Ripple is a company that has designed a protocol similar to Bitcoin for routing payments and settling funds. Designed to simplify interbank payments at the infrastructure level. Ripple currently has end users in the financial industry, including banks, governments and clearinghouses.

[12] The current way Bitcoin operates, it has to deal with bandwidth limitations and enormous energy needs. It is very limited in the amount of transactions it can handle per second compared to for example the processing capacity of VISA. The set of problems are being looked at and several proposals have been made but what the solution will look like is to be seen.

[13] For example: Mt. Gox or Bitfinex. Both digital currency exchanges that were attacked by hackers.

[14] Essentially an investment fund that was built on top of the Ethereum blockchain. Ethereum is a decentralized platform with its own unique type of blockchain that runs smart contracts (See footnote 8) and uses "Ether" as a digital currency. (https://www.ethereum.org/)

[15] Computer programs that can execute the terms of a contract and transfer value between parties.

[16] The hacking resulted in the theft of multiple millions of dollars' worth of digital currency. It has to be noted however that there was no breach in the DLT itself but in DAO's smart contract-code, enabling the hackers to withdraw money from the investment pool.

3.2. A regulatory point of view

Regulators have initially monitored many of these initiatives and there are examples where enforcement actions were taken against projects that were clearly in breach of the current legal framework[17]. After the initial wait-and-see stance, regulators have become convinced of the possibilities of the technology since it has the ability to achieve a more accurate way of reporting and increase regulatory efficiency. DLT could offer the regulators access to a vast amount of records and ultimately alter the way the industry is regulated. It has already shown that this has the ability to reveal money-laundering schemes or potentially discover unauthorized[18] international tax avoidance in a quicker way[19].

This increased interest in the technology by the regulators was noticeable by the amount of reports and guidance that were published in short succession. For example, the European Securities and Markets Authority ***(ESMA)*** has recently closed off a period for a call for evidence on investments using virtual currencies or DLT and the European Banking Authority ***(EBA)*** has set up a task force to investigate DLT implications. These and others actions are to be welcomed and show of some appreciated well-willingness from the regulators' side. In addition, the EBA has also expressed its positive opinion on bringing virtual currencies under the fourth Anti-Money Laundering Directive[20].

In addition to the growing number of publications and on-going research, there are now regulators actively facilitating DLT projects. For example, the State of New York is offering a 'BitLicense' which allows businesses to conduct virtual currency activities on a DLT-infrastructure[21]. In the UK, the Financial Conduct Authority ***(FCA)*** has set up a regulatory sandbox[22] to provide innovative initiatives with a so-called 'safe space', i.e. businesses can test their products and services in a way they do not have to worry about regulatory constraints or be afraid of legal action taken against unauthorized activities. Similar to the UK, the Australian government is taking a leading role in providing start-ups with facilities to further develop their activities with assistance from for example the Australian Securities and Investments Commission ***(ASIC)***. Adding to that, the Reserve Bank of Australia ***(RBA)*** is developing their 'New Payments Platform' ***(NPP)*** by implementing DLT. This will provide, amongst others, real-time payments and 24/7 availability[23].

The existence of these 'safe spaces' however uncover the fact that DLT initiatives have not yet found their definite place within the current legal framework and legislative changes will be necessary to provide the financial industry with legal certainty in their activities.

3.3. The regulators as conductors for innovation?

With the offering of new payment systems coming soon in Europe due to the implementation of the Payment Services Directive 2[24], it might be an excellent time for the industry and regulators to cooperate. Setting up a comprehensive set of guidelines and standards for the industry to adopt a DLT that can slowly but steadily change the underlying technological infrastructure and answer the regulatory challenges. It has been noted in the Committee on Economic and Monetary Affairs ***(CEMA)*** report[25] that the existing body of EU legislations would be a good fit to implement such new provisions[26].

This could lead to a combination of both imposed regulation and, to a certain extent, self-regulation. Resulting in a bespoke legal framework that offers legal certainties and where there is room left for the financial institutions to continue the development of their best practices[27].

To conclude, it will be very interesting to monitor any further developments from the EU and the US regulators' side. The question remains whether there will be a transatlantic regulatory cooperation possible. Or, will there be no breakthrough at all in the coming years and will the financial industry divert to a different track and adopt an alternative to DLT?

---

[17] By FinCEN against Ripple for example, for not adhering to AML regulation, https://www.fincen.gov/news_room/nr/pdf/20150505.pdf

[18] OKCoin; http://fintechist.com/okcoin-guilty-money-laundering-conducting-business-illegally/

[19] Think of the BEPS Action plans by the Organisation for Economic Cooperation and Development (OECD) to address perceived flaws in international tax rules. For regulators to approve DLT initiatives there will have to be identification measures implemented in the offered service. This is realisable due to adaptability of the technology and can be foreseen by the financial service providers. For example, we are referring to payment service providers based on DLT such as Circle. There are many user identification measures that have to be met before transactions can be initiated by the service users. (https://www.circle.com/en-gb/legal/intl-user-agreement).

[20] http://europa.eu/rapid/press-release_IP-16-2380_en.htm.

[21] http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf

[22] https://www.the-fca.org.uk/firms/project-innovate-innovation-hub/regulatory-sandbox

[23] http://fintech.treasury.gov.au/australian-regulators-engagement-with-the-fintech-industry/

[24] http://ec.europa.eu/finance/payments/framework/index_en.htm

[25] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A8-2016-0168+0+DOC+PDF+V0//EN

[26] For example the EMIR, CSDR, SFD, MiFID, UCITS, AIFMD and the newly drafted PSD2.

[27] We have seen a similar regulatory treatment for crowdfunding; which has led to many successful initiatives.