ABE EBA

EURO BANKING ASSOCIATION

Thought Leadership

CRYPTOTECHNOLOGIES: IMPROVING REGULATORY COMPLIANCE

EBA Cryptotechnologies Working Group

The information contained in this document is provided for information purposes only and should not be construed as professional advice.

This information paper is the result of an analysis carried out by the Euro Banking Association's Cryptotechnologies Working Group.

The Euro Banking Association does not accept any liability whatsoever arising from any alleged consequences or damages arising from the use or application of the information and gives no warranties of any kind in relation to the information provided.

Thought Leadership

CRYPTOTECHNOLOGIES: IMPROVING REGULATORY COMPLIANCE

EBA Cryptotechnologies Working Group

CONTENT

INTRODUCTION

European financial institutions are faced with an ever-evolving set of regulations. Compliance with increasing regulations can involve a significant investment of resources in updating internal processes and systems, which can have the effect of limiting resources spent in other areas that generate revenue. A new subset of FinTechs (known as RegTechs) have begun working with financial institutions to facilitate more efficient and effective compliance processes. RegTechs leverage emerging technologies such as Artificial Intelligence (AI) and machine learning to lower costs, increase speed, and free up resources to enable deeper analysis of data. In addition, RegTech offerings can also help improve overall data quality, which can benefit both financial institutions and their customers. Ultimately, leveraging RegTech to improve compliance processes can enable financial institutions to better serve their clients and remain competitive in the digital economy.

While the use of cryptotechnologies for RegTech is still in its early stages, it holds considerable potential to improve the transparency, automation, speed, and resiliency of compliance processes within and between financial institutions and regulatory authorities. Cryptotechnologies such as distributed ledger technology (DLT) can help reduce manual processes and errors, allowing financial institutions to invest more resources on revenue-generating activities such as product development and innovation. This is particularly important for financial institutions today as margins tighten, and new regulations such as the revised Payment Services Directive (PSD2) and General Data Protection Regulation (GDPR) are already in force. RegTech can also help enhance the work of compliance officers and regulators by allowing them to spend more time analysing data and forecasting risk rather than compiling information from various sources. Regulatory compliance is rarely seen as a competitive space that boosts revenue opportunities for financial institutions. With few concerns about competitive advantage and the industry-wide nature of many compliance challenges, RegTech is an ideal space for banks to collaborate to improve regulatory activities and explore the benefits of cryptotechnology-based RegTech solutions.

This information paper will explore use cases for cryptotechnology-based RegTech solutions that financial institutions can use to improve efficiencies, lower costs, and maintain flexibility to remain competitive in the digital economy. The EBA Cryptotechnologies Working Group, comprised of EBA members from European financial institutions and financial industry stakeholders, has identified the areas of Know Your Customer (KYC) and regulatory reporting as particularly attractive areas for the use of cryptotechnologies in RegTech. This paper will begin with a look at how RegTech targets compliance inefficiencies, followed by an overview of major challenges in regulatory compliance faced by the financial sector today. It will then examine two major use cases related to KYC and regulatory reporting, including an explanation of the potential benefits and practical considerations for the use of cryptotechnologies to aid regulatory compliance. The report will conclude with potential next steps to facilitate industry adoption of cryptotechnology-based RegTech that can benefit both financial institutions and regulatory authorities.

HOW REGTECH TARGETS COMPLIANCE INEFFICIENCIES

At its core, RegTech involves using technological tools to maintain, manage, and analyse a vast amount of data. Financial institutions are custodians of large data sets and with the use of RegTech solutions, the data can be quickly translated and analysed to aid regulatory compliance. RegTech can ensure strengthened data integrity through innovative data collecting methods. RegTech can also help financial institutions to quickly and efficiently conduct complex computations based on large data sets, allowing financial institutions and regulators to grasp business situations to understand and manage potential risks quickly. RegTech's real-time accessibility of data can make customer monitoring easier and onboarding smoother. Using emerging technologies such as machine learning, AI, cryptotechnologies such as distributed ledgers (DLT), and application programming interfaces (APIs) to boost automation can reduce human error and lag time that comes from manual input and processing and enable institutions to quickly retrieve information and analyse patterns in large data sets. Thus, RegTech can help financial institutions lower costs, boost flexibility in monitoring and reporting, and ultimately move towards new business models in an open banking environment.

RegTech offerings utilise various new technologies, with most solutions leveraging multiple technologies such as APIs and cloud computing. While most RegTech solutions do not yet utilise DLT, there has been increased interest in the potential for DLT to improve regulatory compliance in the banking sector. The use of DLT in the RegTech space will necessarily go hand in hand with other technologies such as APIs, cloud computing, machine learning, and AI. DLT has strong potential in ensuring data integrity and confidentiality. When combined with APIs, it can help connect to different systems and ledgers, automating and improving data exchange and collection. Pairing DLT with AI and machine learning can improve and quicken the analysis of complex data sets to identify potential risks and lead to actionable insights that can benefit a financial institution's overall business strategy.

IMPROVING REGTECH WITH CRYPTOTECHNOLOGIES

DLT is a sophisticated data sharing tool with enhanced speed, security, and transparency for participants. Data is shared among participants in real time as soon as data is uploaded to the DLT ledger. Uploading new data to the ledger requires a consensus mechanism among the participants, which ensures trust in the quality of the data. As a single source of truth, DLT solutions enable the secure exchange of data, and form a basis for digital identity in the future. As financial institutions improve KYC processes and rely on more sophisticated data analysis (sometimes referred to as Know Your Data), technologies such as DLT will become integral in enabling speed, transparency, efficiency, and security in regulatory compliance.

As with other RegTech solutions, DLT-based RegTech can help reduce manual processes and errors. DLT can be a platform of valid and reliable information that is updated among all participants in real time, leading to greater data integrity and certainty. This function is especially useful for KYC procedures, Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) checks. DLT enables RegTech solutions that are compliant with regulation by design, meaning that the architecture of the system is designed to be compliant with regulations, allowing system participants (financial institutions or departments of a financial institution) to save time and resources currently spent formatting data and compiling reports.

If regulatory authorities are given read-only access to a DLT-based platform, they can view data that is necessary for regulatory reporting without the need for a bank to manually compile and send reports. This allows regulators to conduct thorough investigations faster and in an efficient manner. In short, sound DLT-based RegTech will enable regulators to actively monitor compliance, facilitating the response to regulatory requests. As such, a DLT-based automated proof of compliance, will enable regulators to spend valuable resources on assessing the soundness of financial institutions and systemic risks, while enabling financial institutions to avoid potential compliance errors as well as related fines and free up resources that can be used for revenue-generating activities.

Any DLT-based RegTech will require a governance model that includes both financial institutions and regulatory bodies. Any data that is shared on a DLT platform has to be legitimate and verifiable. Even if the code of the platform is itself inherently compliant with regulations, the entry points on the ledger may be prone to error or fraud. For example, when data stored on the platform is found to be false, it must be possible to determine by whom, how, and when the faulty data was entered into the system. A sound governance model and accountability are needed to ensure participation. A discussion between the financial industry and regulatory authorities will be key to ensure that rulebooks and scheme rules clarify rights and obligations of using the technology and maintaining trust in the system. Otherwise, DLT-based RegTech remains interesting in theory but impractical in reality.

CURRENT CHALLENGES IN REGULATORY COMPLIANCE

Regulatory compliance is generally seen as a "hygiene factor" for financial institutions: a necessary and valuable activity that supports, but does not directly generate, new revenue. Financial institutions face important challenges in complying with regulations using legacy compliance processes. Evolving sets of regulations make it crucial for financial institutions to develop modern compliance processes. Access to customer data within financial institutions is also hampered by siloes and a lack of transparency, making it difficult to automate regulatory checks and analyse customer data. At the same time, access to and analysis of customer data within financial institutions needs to be carefully balanced out between the necessary transparency, and the required data protection. This section will examine current compliance challenges for financial institutions that RegTech solutions seek to improve.

KYC REQUIREMENTS

KYC compliance is a pre-requisite before a financial institution may offer services to a customer. KYC therefore serves as a foundation of formal financial services. Failure to comply with KYC procedures not only leads to fines and regulatory sanctions, it can also hurt a financial institution's reputation. KYC compliance can have high financial cost. In a 2016 survey, Thomson Reuters interviewed nearly 800 financial institutions worldwide on the impact of KYC regulation and found that financial institutions pay an average of USD 60 million annually on KYC compliance, with some spending up to half a billion US dollars a year.[1] Compliance departments that rely on legacy compliance processes are being challenged to keep up with continuously evolving regulations and a growing volume of transactions. Even within individual financial institutions, KYC processes can be siloed, paper-based, and require major investments in compliance resources and training. Information used for customer onboarding is not always available throughout the financial institution, leading to redundant procedures when a customer requests additional services. Financial institutions operating globally, or at least in more than one jurisdiction, may have to implement different KYC requirements and practices per jurisdiction. In a time where the speed and efficiency of payment processing is increasing, the processing of regulatory checks is still time-consuming.

AML/CTF SCREENING

Compliance with requirements on Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) contributes to the prevention of the financing of criminal activities, the laundering of illegally earned money and the hiding of assets. To do this successfully, financial institutions must collect information about their customers, where transactions originate, and the nature of their financial transactions. AML and CTF screening processes involve significant amounts of data, and legacy processes are not always up to the task of processing huge data sets accurately. Some financial institutions have reported 98% of AML/CTF false positive rates as currently they have to manually check every suspicious activity flagged by their systems.[2] AML/CTF sanctions lists must also be updated and reconciled by multiple parties, which can lead to some parties updating lists at different times and result in information asymmetries given the absence of coordinated actions. The increasing amounts of data used in financial transactions means that the complexity

1 https://www.thomsonreuters.com/en/press-releases/2016/may/thomson-reuters-2016-know-your-customer-surveys.html

2 https://www.ibm.com/blogs/insights-on-business/banking/ibm-and-promontory-looking-for-a-needle-in-a-haystack-with-watson/

of AML/CTF screening will increase as well. Banks will need to compile and analyse growing amounts of data to tackle increasingly sophisticated illicit financial activities. Records of customer data will need to be updated and verified in real time and made widely available within and between financial institutions. The reliability of this information will need to be secured among financial institutions and regulators together. Financial institutions must also ensure continued compliance with data privacy laws such as the General Data Protection Regulation (GDPR) throughout the process. Automation will play a key role in updating AML/CTF checks as the speed and reach of financial services grows.

REGULATORY REPORTING

Since the 2008 financial crisis, financial institutions' reporting requirements and the number of regulatory authorities have increased. Financial institutions operating in Europe are required to report to multiple authorities on different areas in financial services, including liquidity, leverage ratio, and non-performing loans.[3] Reporting cycles vary from daily to yearly, and the process of complying with reporting requirements consumes considerable resources. Having more automated systems, with high degrees of data transparency and integrity, would help financial institutions meet these regulatory needs. Regulatory authorities would also benefit from more transparent data, allowing them to more quickly identify potential systemic risks and ensure efficient and effective supervision for the digital age.

THE EVOLVING REGULATORY LANDSCAPE

As customer expectations and technological advances push the evolution of financial services, regulation has evolved to ensure continued stability and control of potential risks. The implementation of the revised Payment Services Directive (PSD2) and the GDPR in Europe are major advances on this front and have had significant impacts on financial institutions' investment in regulatory compliance and innovation. The PSD2's access to accounts clause has spurred financial institutions to develop improved processes for customer onboarding and data exchange. Touchpoints with customers are expanding and financial institutions have found a need to update business practices and regulatory compliance models. The GDPR increases data privacy and requires a change in business processes from financial institutions and corporates. The GDPR mandates strict requirements of customer consent in the use personal data, the provision of detailed information on data processing, and the right to be forgotten. While compliance with each of these regulations offers major organisational, technical, and business challenges on their own, the need to improve compliance processes in an evolving regulatory environment will enable financial institutions to keep pace with the evolving needs of digital financial services. Keeping up with these changes will require greater automation, increased speed, and improved data integrity.

3 European Central Bank, The ESCB Integrated Reporting Framework (IReF), p. 1, https://www.ecb.europa.eu/pub/pdf/other/ecb.escb_integrated_reporting_framework201804.en.pdf

USE CASES FOR DLT-BASED REGTECH

While the use of cryptotechnologies in the RegTech space is currently not widespread, the technology holds much promise in helping financial institutions adapt to a changing regulatory landscape. While DLT cannot solve every problem, it can serve as a key technology that allows financial institutions to save resources spent on compliance functions and increase investments in revenue generating activities by improving data integrity, enhancing transparency, enabling automation, and increasing auditability. The following section will explore use cases for DLT-based RegTech in the areas of KYC management, sanctions screening, and regulatory reporting and how these use cases can benefit both financial institutions and regulators.

USE CASE: DLT-BASED KYC REGISTRY

Financial institutions are strictly mandated to scrutinise and monitor customers to curb illicit finance and responsibly serve their customers. To fulfil this purpose, financial institutions have to check the identities of their customers, the purposes of transactions, and assess the potential risks. These KYC processes take place during the initial customer onboarding process and are repeated both internally (e.g. when a payment is made, or a customer applies for an additional service such as a loan) and externally (such as when a customer makes a cross-border payment). This leads to cumbersome and redundant actions that drive up cost for financial institutions and can ultimately lead to customer dissatisfaction if they are asked to present KYC documentation multiple times.[4] According to KPMG, "up to 80 percent of the effort associated with KYC is dedicated to information gathering and processing, and only 20 percent to assessing and monitoring that information for critical insights."[5]

Cryptotechnologies such as DLT are one of the potential technologies which may improve these processes and thereby free resources. Core features of DLT such as the immutability of data and instant sharing of data between all nodes can help to build a trustworthy and robust KYC registry where every participant can contribute and benefit. This can help entities that are obliged to carry out KYC procedures evolve and streamline their compliance processes and adopt new business models, ultimately passing these benefits on to customers in the form of lower costs or new services. A DLT-based KYC registry has both internal and external uses that will be explored further in this section.

Internal KYC platform

Financial institutions currently apply lengthy, often cumbersome and costly KYC processes, which are typically paper-based and siloed, i.e. data is typically not shared between different departments. The core problem is twofold: 1) the fragmented storage of customer identification attributes and KYC documentation in different departments within a financial institution, and 2) the difficulty in locating, compiling, and exchanging this information with other departments within the financial institution. As a result, financial institutions often ask their customers to re-submit KYC documentation (e.g. proof of address, identification documents, etc.) when they apply for an additional service such as a loan. This leads to a lengthier approval process, increased cost for financial institutions, redundancies, and ultimately

4 Thomson Reuters 2016 Know Your Customer survey: https://www.thomsonreuters.com/en/press-releases/2016/may/thomson-reuters-2016-know-your-customer-surveys.html

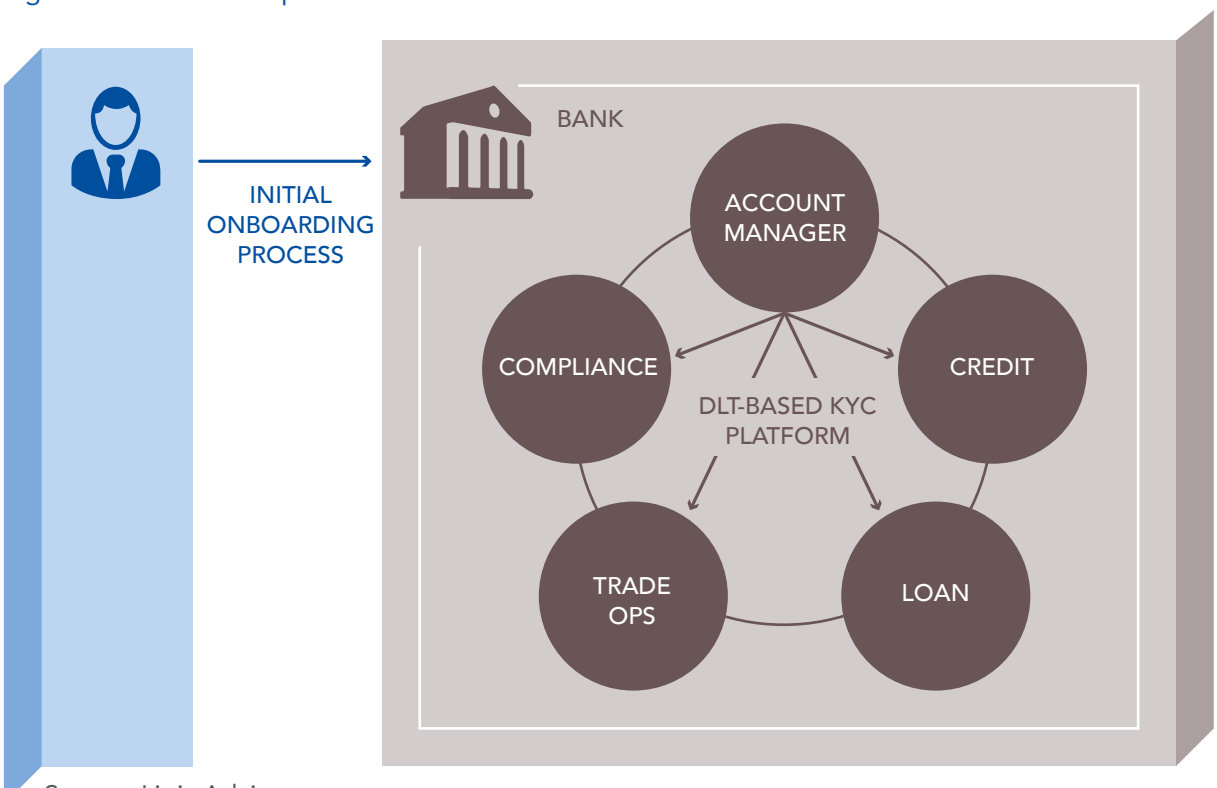
5 KPMG, Could blockchain be the foundation of a viable KYC utility, pg. 2: https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2018/03/kpmg-blockchain-kyc-utility.pdf

to customer dissatisfaction. As the speed of payments and financial services evolves with the introduction of instant payments and open banking, consumers and businesses are unlikely to tolerate such inefficient and costly processes for long.

Financial institutions can immensely benefit from a reliable and robust DLT-based data sharing platform that reduces redundancies in KYC processes without sacrificing compliance with KYC regulations. DLT is a suitable technology as it ensures the integrity and real-time view of data. The simplest form of a potential system is illustrated in Figure 1. A customer submits necessary documents for KYC purposes to an account or branch manager, who subsequently uploads this information on an internal DLT-based platform. This allows for easier exchange of KYC attributes among various departments within the financial institution. Each concerned department has a shared, uniform view of KYC attributes (e.g. name, address, identity number) as needed, resulting in improved data integration, reduced error rates, and improved customer service. Each department would be assigned as a node on the ledger and the information would be verified according to the consensus protocol adopted in the system.

Cryptotechnologies offer a unique approach for an internal KYC platform compared to other technologies such as cloud. A DLT-based platform can enable greater data reliability because the data uploaded onto the platform requires consensus among participant nodes. It also allows each department to independently update a customer's profile each time they obtain additional information from the customer. This updated information is instantly shared and available to all participant

Figure 1: Internal KYC platform



Source: Lipis Advisors

nodes, which enriches customer data across the entire organisation. Even a simple form of DLT application has the potential to improve the entire KYC process and customer experience immensely.

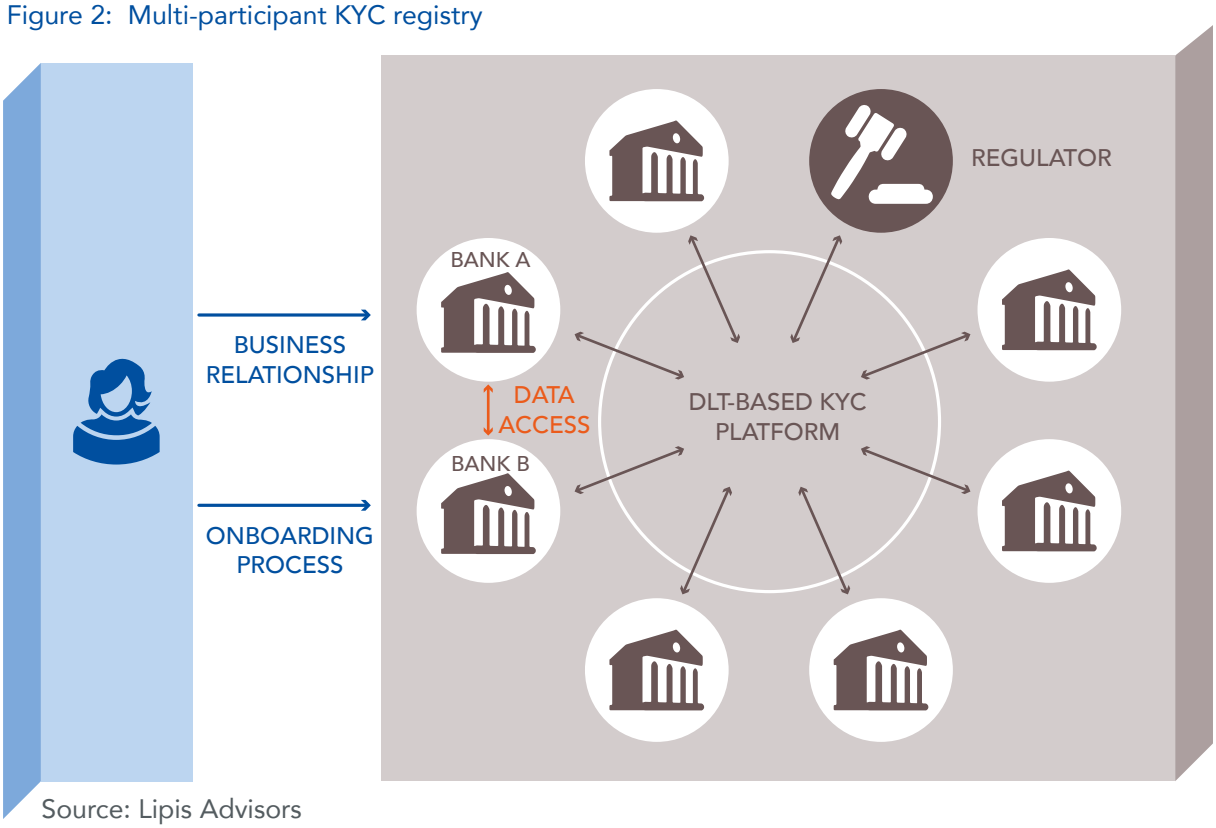
Multi-participant KYC registry

The advantages of DLT for KYC processes are not confined to individual entities that are obliged to carry out KYC checks. A DLT-based multi-participant KYC registry enables all participants on the platform to instantly and securely share customer data in a targeted way both domestically and across borders. This may significantly enhance the process of customer onboarding as a bank can obtain the information about a new customer through the platform, instead of having to ask the customer to re-submit the information. According to a survey conducted by Signicat, one of the leading providers of electronic identity and electronic signature solutions in Europe, more than 50% of customers in Europe abandon their new account applications during the onboarding process.[6] The research also reveals that almost three quarters of Europeans would prefer a fully digital onboarding process. A DLT-based multi-participant KYC registry has the potential to meet these customer needs and at the same time improve customer onboarding and compliance processes for entities that are obliged to carry out KYC checks.

The structure of such a registry is depicted in Figure 2. A customer completes the initial onboarding process with Bank A. When the same customer wants to open an account with Bank B, that bank can use the multi-participant KYC registry to request the necessary information from Bank A. Bank B can then perform any due diligence requirements on the information received from Bank A instead of having to request the same information that the customer already submitted to Bank A. This allows for a quicker onboarding process and better customer service while maintaining compliance with regulations. This process can also be expanded for cross-border use cases, with the DLT registry including rules (e.g. using smart contracts) that ensure regulatory compliance between multiple markets (most

6 Signicat, The Battle to On-board II: The European Perspective on Digital On-boarding for Retail Banks, p.10, https://www.signicat.com/wp-content/whitepapers/signicat-battle-to-onboard-II-v6.pdf

Figure 2: Multi-participant KYC registry



Source: Lipis Advisors

likely on a bilateral basis). Inclusion of regulators as nodes in the multi-participant KYC registry is optional, but it will be important for registry participants to engage with regulators from the outset to demonstrate how the KYC registry can help meet regulatory standards and improve KYC processes industry-wide. If regulators participate in the system, financial institutions can demonstrate their compliance with KYC/AML requirements continuously and avoid the need to compile data and share it with regulators at specific intervals. This will contribute to creating a more trustworthy banking environment, which is beneficial for both financial institutions and regulators.

The inclusion of multiple financial institutions on a DLT-based platform does come with additional challenges. The foremost issue is the need to coordinate and set a proper governance model. Most financial institutions are hesitant to share customer data with other financial institutions, as it would expose their customer base to potential competitors. A DLT-based registry can help avoid these risks by enabling financial institutions to share records of consent or even individual attributes instead of full customer profiles. A proper governance model can also help to ensure that all nodes on the network are registered financial institutions that abide by KYC processes in a manner that is compliant with regulation. Proper governance can help to establish trust among network participants, thereby increasing participation and enabling network effects that enhance the overall benefits of a multi-participant KYC registry. Regulators should also be involved in this process and could play a vital role in fostering cooperation among financial institutions and help to set rules by which the system will

operate. It is important to note that collaborative governance structures and cooperation with regulators does not mean that a single entity controls the registry at a technical level. Rather, it ensures common rules that set the limits for the operation of a decentralised registry used by any professionals subject to AML/CTF obligations at a national or even pan-European level. Lastly, the legal feasibility of relying on a third party's KYC processes would need to be reviewed in each jurisdiction. In Belgium, financial institutions have collaborated on a blockchain-based KYC initiative aimed at simplifying corporate identity management for the entire market.[7] Further successes in other European markets may require similar legal frameworks.

DLT-based KYC benefits

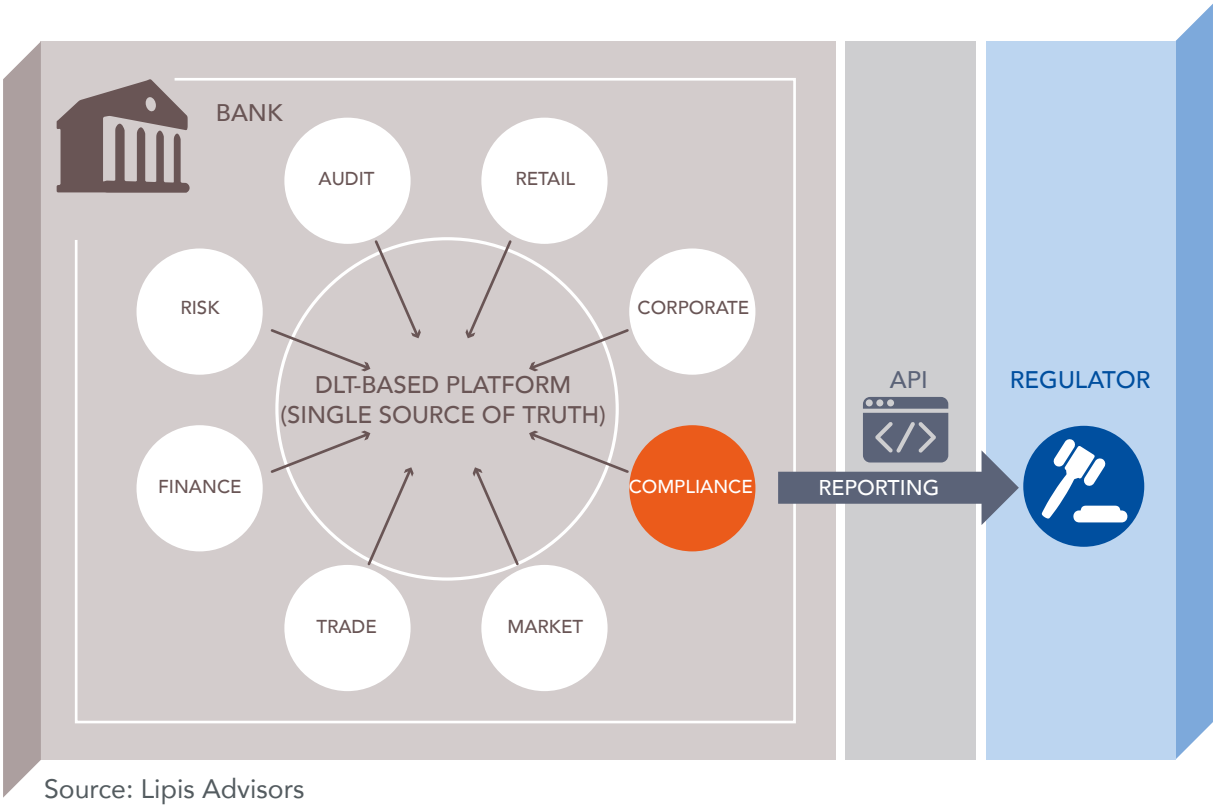
- Increased efficiencies through reduction of redundant KYC checks
- Transparency of information can create a "single source of truth" within a financial institution, helping departments respond to customer requests faster
- Reduced risk of non-compliance with KYC requirements
- Lower cost of regulatory compliance allows financial institutions to pass savings on to customers in the form of lower fees and devote more resources to revenue-generating activities such as product development

DLT-based KYC challenges

- Establishing proper governance structures to ensure that all nodes on the network are regulated financial institutions that comply with KYC regulations. This is also related to ensuring the quality of data uploaded on the network, which come as a precondition for the system to function
- Financial institutions could be reluctant to rely on a third-party actor or platform to aid in KYC compliance, as ultimate liability for KYC compliance rests with the financial institution
- Need for wide participation to ensure network effects. A lack of participation would inhibit the usefulness of the network
- Data privacy and data segmentation. Data shared over the network cannot be commercially sensitive and identifiable personal data must not be shared among all participants without a customer's consent. The use of private ledgers or side chains should be explored
- Review legal feasibility of sharing KYC attributes and relying on third parties to conduct KYC processes on behalf of financial institutions.
- Cost effectiveness has to be high as there are multiple other competing technological solutions to function as a KYC database. Also, legacy systems and multi-jurisdiction data protection regulations may hinder quick and widespread adoption of a DLT-based solution

7 The project has since been managed by Isabel Group, with technology provided by norbloc. https://www.isabelgroup.eu/wp-content/uploads/2018/03/Press-Release-Corporate-KYC-Blockchain-Pilot-EN.pdf

Figure 3: Internal data aggregation system



Source: Lipis Advisors

USE CASE: DLT-BASED REPORTING SYSTEM

Financial institutions are subject to multiple reporting obligations to relevant authorities at various intervals throughout the year. For instance, credit institutions operating within the European Union have to comply with reporting requirements from the European Central Bank and the European Banking Authority on subjects such as balance sheet items (BSI), interest rates (MIR) of monetary financial institutions (MFIs), and the Implementing Technical Standards (ITS). At a national level, financial institutions are also obliged to report to national authorities on balance of payments, international investment positions, etc.[8] Reporting obligations are increasing in terms of volume and complexity, however the methods used by financial institutions to collect and compile data have not evolved accordingly. The result is a highly manual process that leads to many redundancies and overlaps that are prone to errors as well as inconsistencies of data.

Cryptotechnologies can help make these reporting processes more efficient and fault-proof. A reporting system that leverages DLT can enable data to be consolidated on a single platform and verified by participant nodes. The technology also allows financial institutions to control who can view and access the data both internally and externally.

8 European Central Bank, The ESCB Integrated Reporting Framework (IReF), p.1, https://www.ecb.europa.eu/pub/pdf/other/ecb.escb_integrated_reporting_framework201804.en.pdf

This level of automation and control makes a DLT-based reporting system an attractive RegTech solution for financial institutions. Such a system can be used both internally and externally: as an internal data aggregation system and an internal/external "Regulation by Design" model that allows regulators to view information on the platform.

DLT-based internal data aggregation system

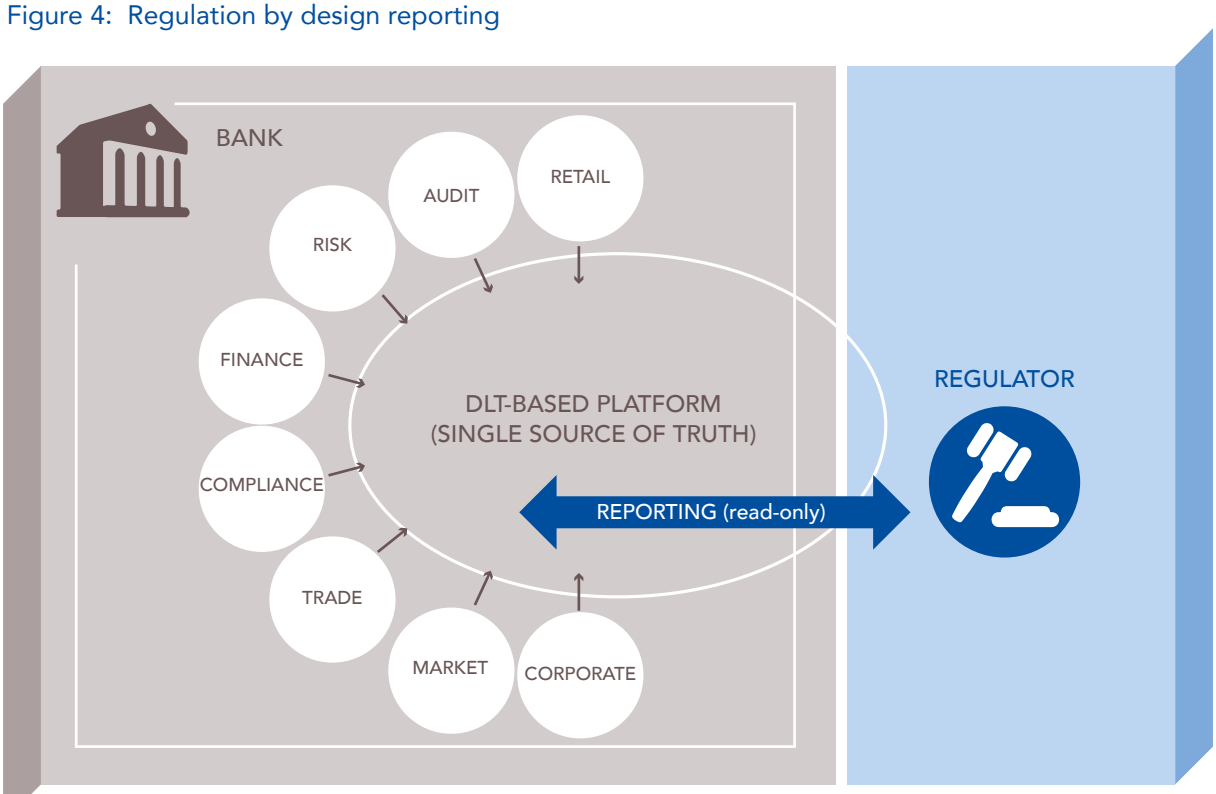
Financial institutions deal with enormous amounts of data and have multiple touchpoints with customers. Each department within a financial institution is highly specialised with regard to their products and roles, and the build-up of legacy technology and business processes has led to situations where different departments have difficulties locating, communicating, and exchanging data with other departments. The result is often that no single department within a financial institution has a comprehensive view of all customer data or data relating to specific customers. In addition, siloed data collection is prone to discrepancies and errors, which creates confusion and can lead to difficulties in complying with certain regulations, which can lead to fines. This is especially true of reporting requirements. If a regulatory report requires information from multiple areas within a financial institution, fragmented data storage as well as lengthy and costly manual reconciliation processes represent an obstacle to regulatory compliance.

The use of DLT can help improve reporting processes for both financial institutions and regulators. Unlike a centralised database, DLT enables multiple parties to store copies of data, which eliminates a single source of failure. This characteristic of DLT is particularly important for financial institutions since they must follow the strictest standard for system robustness. Consensus protocols allow data to be constantly verified, which strengthens data integrity in regulatory reporting. Recent iterations of distributed ledgers (e.g. R3's Corda) allow for different access levels for different nodes in the network. This allows participants to exchange data bilaterally without exposing it to all nodes on the network. This is particularly relevant for data exchanged between a financial institution and a regulatory authority. Compared to other technologies, this allows a DLT-based network to enable more detailed and flexible control over data exchange. The advantages that DLT brings for internal data management and external data exchange make it a suitable technology for a modern regulatory reporting system.

Financial institutions can realise internal improvements using DLT as shown in Figure 3. By establishing a DLT-based data aggregation system, a financial institution can quickly and accurately compile the data needed for regulatory reporting purposes. By leveraging other technologies such as APIs, the financial institution can automatically upload this data into a pre-determined reporting template. The report can then be sent to the regulator using legacy networks.

This DLT-based approach gives financial institutions the flexibility to respond to regulatory reporting requests quickly and efficiently through a verified, single source of truth that can be accessed by all authorised departments within the financial institution. Regulators benefit from more accurate reports and quicker response times, as opposed to requesting additional reports for unclear or incomplete data. More accurate reports and quicker response times give regulators a more comprehensive view of potential risks at an institutional level and among all market players. In turn, financial institutions can devote more

Figure 4: Regulation by design reporting



Source: Lipis Advisors

resources to analysing risks instead of manually compiling data for regulatory reports.

Regulation-by-design reporting

The benefits of DLT for regulatory reporting can be expanded by giving regulatory authorities direct access to a financial institution's DLT network and the ability to view (but not edit) information necessary for regulatory compliance. This allows regulators to monitor compliance continuously while freeing financial institutions from the burden of manual reporting processes. Such a system could be compliant with regulation by design, i.e. the architecture of the network would be compliant with regulations from the outset.

As shown in Figure 4, different departments within a financial institution could upload and verify data on a DLT-based ledger. Instead of taking this data and compiling it into regulatory reports that are then sent to a regulatory authority, the regulator would be given read-only access to the ledger. This would give regulatory authorities the ability to "pull" the necessary data for review at specific intervals or continuously. The financial institution would only need to ensure that the data uploaded to the ledger is accurate and updated at regular intervals. It would remove the need for financial institutions to "prove" compliance by compiling and formatting information into regulatory reports, a time-intensive process today. As long as financial institutions made the necessary information available to regulatory authorities, the authorities

could monitor those financial institutions' regulatory compliance on their own.

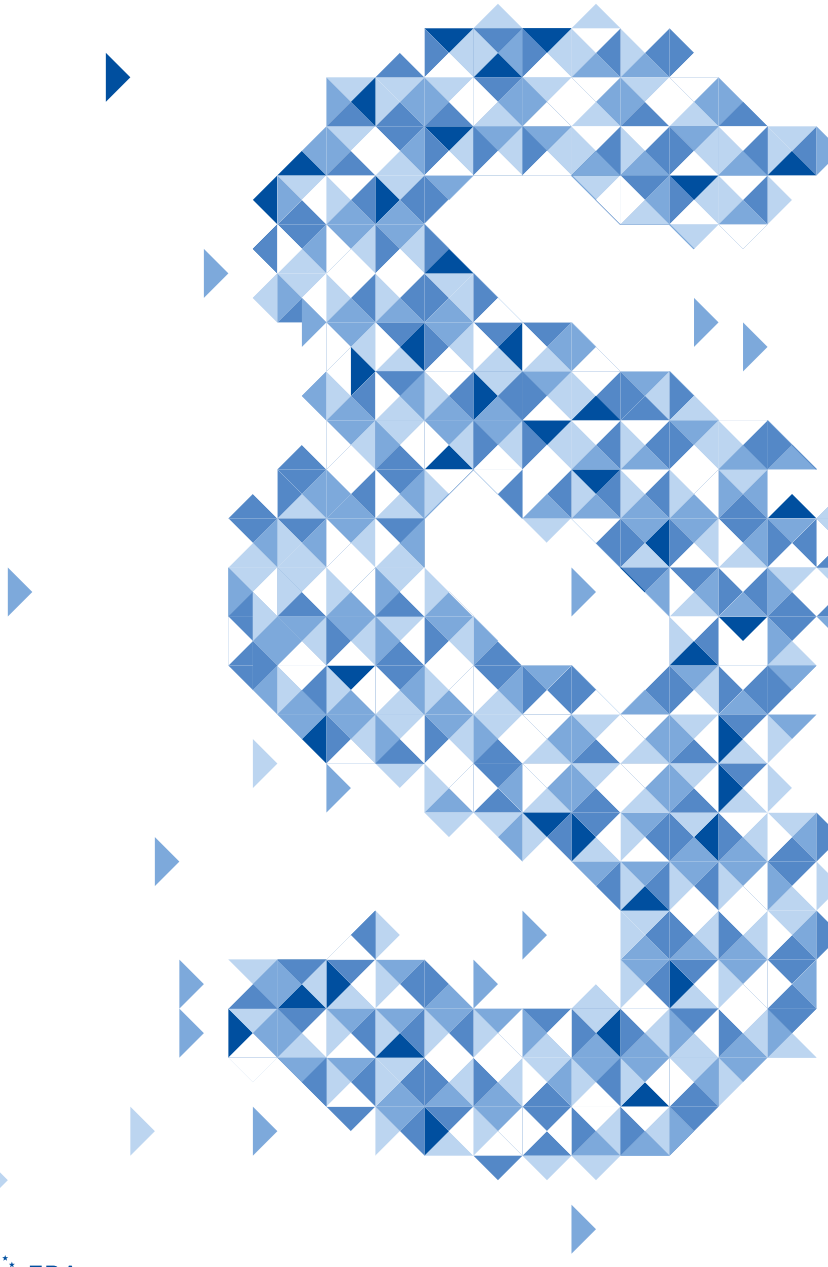
This model of RegTech, often referred to as supervisory technology or SupTech, enables regulators to supervise financial institutions more smoothly and efficiently, while strengthening the overall monitoring process without imposing additional burdens on financial institutions. Compared to the internal data aggregation model, this use case can ultimately enable regulators to access more enriched datasets which can be utilised for a more detailed evaluation of financial institutions. Improved supervisory methods are not only beneficial from the aspect of enriched data and improved procedure, they also enable financial institutions to demonstrate compliance on a rolling basis, with proof of compliance available to regulators at any time.

DLT-based regulatory reporting benefits

- Financial institutions save time and resources currently used on compiling and sending regulatory reports
- Lower cost of regulatory compliance for financial institutions
- Improved resilience of a decentralised platform compared to centralised databases
- Regulators get a more detailed and updated view of financial institutions' activities, allowing them to identify and mitigate potential risks more quickly

DLT-based regulatory reporting challenges

- Ensuring that data on the ledger is appropriate for multiple regulatory authorities, or developing multiple ledgers
- Getting financial institutions to agree to open access to limited data sets for regulatory authorities (while maintaining the confidentiality of commercial and other client data)
- Need for both financial institutions and regulators to institute capability to access DLT-based ledger (overcome obstacles of legacy technology)



CONCLUSION

As financial systems and payment services evolve with the introduction of new functionality, new players, and new access channels, regulatory requirements have necessarily expanded to maintain stability and enable innovation in financial services. The experience of traditional financial institutions has made clear that a modern handling of compliance processes is needed to meet regulatory requirements and stay competitive in the digital economy. RegTech offerings have emerged to help financial institutions to keep up with these evolving requirements. Cryptotechnologies such as DLT offer many potential benefits in the RegTech space. DLT can enable financial institutions to exchange customer information securely and instantly both internally and with other financial institutions. It can also help financial institutions to improve regulatory reporting, and even enable active monitoring by regulatory authorities by providing read-only access to data attributes needed for regulatory purposes. Collaboration between financial institutions and with regulators will be key to enabling DLT platforms both internally and industry-wide, as will the need to integrate with other technologies used in RegTech such as APIs and cloud computing. Data privacy will also be a key challenge when using DLT-based solutions for regulatory compliance, and financial institutions will need to clearly identify and segment data that is shared on a multi-participant DLT ledger. Moreover, both interoperability with legacy systems and cyber security are fundamentally important for the adoption of DLT-based RegTech. Financial institutions can benefit through greater flexibility in meeting compliance requirements, which can help free up resources to focus on revenue-generating activities such as innovation and product development. Ultimately, RegTech solutions can help provide flexibility to financial institutions that will allow them to meet future regulatory challenges and continue to innovate and compete in a safe and secure way.

IMPRINT

Euro Banking Association
40 rue de Courcelles
F-75008 Paris

Contact

association@abe-eba.eu

Graphic design

Bosse und Meinhard, Bonn