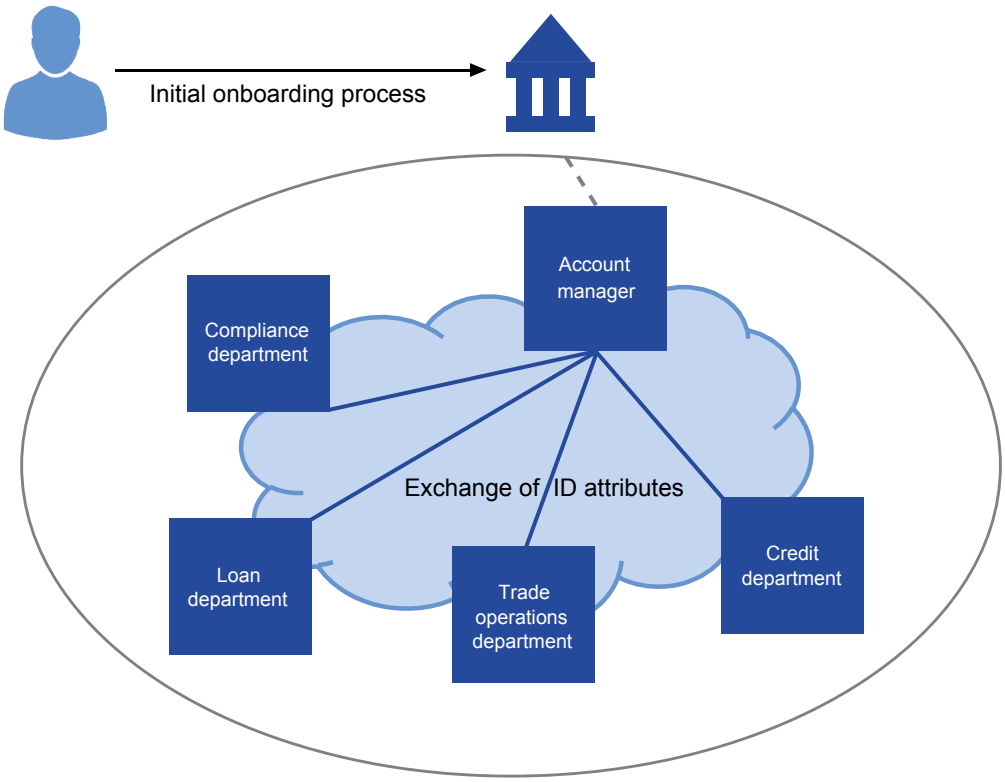
ABE EBA

EURO BANKING ASSOCIATION



Security and identity challenges in cryptotechnologies

Information Paper

EBA Cryptotechnologies Working Group

September 2017

CONTENTS

Introduction **4**

Distributed ledger technology (DLT) characteristics **5**
- Permissioned ledgers and limiting access 5
- Privacy of information 5
- Immutability of data 6
- Participating nodes on the ledger 6

Third party provider (TPP) authorisation and consent management **7**
- A uniform view of all authorised (TPPs) for banks 8
- Customer consent management using DLT 9
- Benefits and practical considerations for consent management 10

Exchange of know your customer (KYC) information within banks and with subsidiaries **11**
- Distributed identity attributed management within banks 12
- Distributing identity attributes between banks and their subsidiaries 12
- Benefits and practical considerations for KYC management 14

Looking ahead **15**

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

FIGURES AND PICTURES

Figure 1: Managing third party provider authorisation for European banks 7
Figure 2: Distributed consent management ledger 9
Figure 3: Distributed identity attribute management 11
Figure 4: Exchange of ID attributes with subsidiaries 13

INTRODUCTION

Data security is of paramount importance in financial services. The secure storage and exchange of information is one of the key services banks offer their customers. As end user demands evolve and new regulations such as the second Payment Services Directive (PSD2) mandate more open exchange of data, financial institutions have been exploring the possible roles of cryptotechnologies[1] in this changing environment. While rules regarding access, speed, and participation are changing, ensuring the integrity and security of financial data will continue to be a necessity.

The focus of this report is on how cryptotechnologies can maintain or improve data security and integrity while opening new opportunities for financial institutions. Cryptotechnologies can help financial institutions to both enable regulatory compliance and improve service to end users while lowering costs and providing future flexibility as payments and financial services continue to evolve. While the full value of cryptotechnologies will come with widespread usage, many banks today are pursuing an incremental approach to adoption. This approach involves an assessment of how cryptotechnologies interact with legacy systems to determine where distributed ledger technology (DLT) fits in an institution's technology stack. The use of cryptotechnologies can occur within a single organisation, an entire payments community, cross-domain, or even across borders.

Through numerous group discussions and demos from banks and software providers, the Euro Banking Association's Cryptotechnologies Working Group has analysed how cryptotechnologies may help achieve higher efficiencies by improving speed, accessibility, and operability to facilitate new services in an environment marked by new commercial and regulatory developments regarding access and control of data. Two use cases were examined, covering third-party authorisation (both from a bank and customer perspective) as well as know your customer (KYC) and due diligence processes. Financial institutions are already exploring the use of the technology in these areas, and have been developing fit-for-purpose DLT solutions. The challenge for financial institutions in adopting cryptotechnologies will be in re-thinking their implications on existing IT and business processes while maintaining flexibility and adaptability for future needs.

This report will begin with an explanation of the characteristics of evolving DLT solutions. It will then examine two use cases related to third-party consent management and sharing of KYC attributes within and between organisations, including the benefits and challenges associated with each use case. It will end with a look ahead at how financial institutions can benefit from increased industry adoption of cryptotechnologies.

[1] Cryptotechnologies are also referred to as distributed ledger technology or DLT. The term "blockchain" will not be used in this report, as it is a specific type of distributed ledger and the focus of this report is on the technology in general.

DISTRIBUTED LEDGER TECHNOLOGY (DLT) CHARACTERISTICS

Previous reports of the cryptotechnologies working group[2] have identified four key aspects shared by various cryptotechnology solutions:

- A shared, uniform ledger that is replicated among all participants over a network of interconnected computers;
- Security and accuracy of the ledger is ensured through cryptographic methods;
- Control of the ledger is decentralised among network participants (no single central authority);
- Once verified, transactions on the ledger are fixed and indisputable.

Cryptotechnologies were initially designed to ensure finality and transparency of transactions across a distributed network. These core features were not developed with legacy bank processes and financial regulations in mind. With an increasing number of financial institutions actively exploring the use of cryptotechnologies, there have been several important developments in DLT solutions designed to help the technology adapt to the business, legal, and regulatory realities of financial organisations. Financial institutions using cryptotechnologies today must make determinations on a few additional key aspects that can affect data security.

Permissioned ledgers and limiting access

Early implementations of cryptotechnologies, such as Bitcoin, were unpermissioned (and continue to be so), meaning that any party can join the network and verify transactions. In the traditional, highly regulated payment infrastructure business, on the other hand, access to messaging and payment networks is always permissioned. This is not expected to change with the use of cryptotechnologies. Permissioned ledgers allow more control over who has access to the ledger and which role is assigned to each participant. Today, central authorities such as national central banks or other market infrastructure providers play the role of maintaining and verifying ledgers, but with DLT, this role can be divided over multiple entities in the network. However, having unauthorised entities involved in verifying new transactions would be too risky for financial institutions and their customers. Thus, while control can be decentralised, it will still have to be exercised by authorised parties. When using cryptotechnologies, all entities involved in verifying new ledgers must therefore be authorised.

Authorisation to view information on the DLT ledger will also be controlled. Initiatives such as Multichain[3], Ripple Connect[4], and Hyperledger Fabric[5] all offer permissioned access to view ledgers, ensuring that all nodes can be identified and are authorised to access information on the ledger. These entities can then be given permission to access information on a need-to-know basis. Permissioned access to the ledger will be vital for creating the trust needed for institutions to exchange information between organisations and across borders. These layers of access ensure that all participants in a ledger meet certain standards for verifying information and/or accessing information, helping maintain data security in the network.

Privacy of information

While cryptotechnology solutions employ various methods to ensure confidentiality for participants on the ledger as data is shared across the network (e.g. by using pseudonyms for each party sending

[2] "Applying cryptotechnologies to trade finance," May 2016. https://www.abe-eba.eu/downloads/knowledge-and-research/EBA_May2016_eAPWG_Applying_cryptotechnologies_to_Trade_Finance.pdf
"Cryptotechnologies in international payments," March 2017. https://www.abe-eba.eu/downloads/thought-leadership/EBA-Cryptotechnologies-in-international-payments-March-2017.pdf

[3] https://www.multichain.com [4] https://ripple.com [5] https://www.hyperledger.org/projects/fabric

and receiving information), the amount of information shared on the ledger does leave open the possibility of reverse engineering transactions to determine which banks or bank customers are directly involved in a transaction. This has understandably led to concerns among institutions for whom confidentiality is paramount. To combat this, some cryptotechnology initiatives have developed private ledgers that ensure that information exchanged as part of a transaction is only visible to the parties involved in that transaction. The Corda platform by R3[6] is a prominent example of a private ledger developed with involvement from leading banks around the world. The ability to exchange information privately on a cryptotechnology platform may be a key enabler of widespread adoption going forward and allow experimentation without the risk of disclosing sensitive information of any kind.

Banks using DLT must determine which information is most suited to be exchanged internally or externally using cryptotechnologies. For more sensitive information, participants should choose which information is kept on-ledger (using DLT) and which information is stored off-ledger (using traditional systems like databases or data warehouses). This will necessarily involve an analysis of whether the cost of segregating data between ledgers outweighs the cost-savings and increased efficiency that can come from using cryptotechnologies.

Immutability of data

Financial services data is always subject to change, particularly data related to a customer's identity. Financial institutions thus need to be able to amend or withdraw data as information evolves or regulation (or a user) demands. In other words, certain data needs to be revocable. The need for revocability was not a key concern in the first generation of cryptotechnologies. Banks have worked together to develop new solutions to this problem by using private channels within a cryptotechnology solution or by holding sensitive data off-ledger and using a distributed ledger to exchange specific attributes. These developments seek to overcome concerns related to commercial sensitivity of data.[7] When determining how to use cryptotechnologies, financial institutions must consider data immutability to select the use cases and approaches that are most appropriate for a distributed ledger solution.

Participating nodes on the ledger

Determining which entities can participate as nodes on a cryptotechnology ledger will be a key issue for banks. A ledger used internally by a bank may be made up of individual nodes that represent entire departments, or individuals within specific departments. Ledgers used across organisations (for instance, between a bank and its domestic or foreign subsidiaries) may see each node representing an entire organisation, departments within each organisation, or individual employees. Banks need to determine which actors or entities need direct access to the ledger to ensure proper representation and avoid bottlenecks while protecting access to sensitive customer data.

As new regulations such as the General Data Protection Regulation (GDPR)[8] open up space for end users to control their own data, it is possible that consumers and businesses could eventually represent nodes on a cryptotechnology ledger. This is unlikely to occur in the near future, but banks should start thinking about possible implications, such as how to enable enhanced user control without opening up access to a distributed ledger directly, e.g. via Application Programming Interfaces (APIs).

[6] https://www.r3.com and https://www.corda.net

[7] Scalability is an additional concern in this space. The more data stored on the ledger, the bigger each copy of the ledger will be as it is shared among all nodes. Having some data stored privately or off-ledger means that each copy of the ledger held by all nodes will be smaller, thus increasing overall scalability.

[8] http://www.eugdpr.org

THIRD PARTY PROVIDER (TPP) AUTHORISATION AND CONSENT MANAGEMENT

With new regulations such as the revised Payment Services Directive (PSD2) and the GDPR due to become applicable in 2018, European banks and third parties will need to undergo a shift in how they manage consent for financial services. Banks will be required to provide access to payment accounts upon their customers' request while having to ensure at the same time that end users and third parties are properly authorised and permissioned to access data. This will require a change in business practices that will be aided by the widespread adoption of technologies such as APIs. Cryptotechnologies also hold the potential to help banks comply with these new regulations while preparing for a future where the controlled sharing of data and value within and between organisations is facilitated on a large scale.

Cryptotechnologies can enable enhanced consent management in two ways: by giving European banks an up-to-the-second, unified view of all authorised third party providers in Europe and by giving end users control over which entities they have authorised to access their bank account information. Each of these solutions addresses a different side of the same problem by ensuring that third party access to bank account data is authorised and that end users retain control of their bank account data.

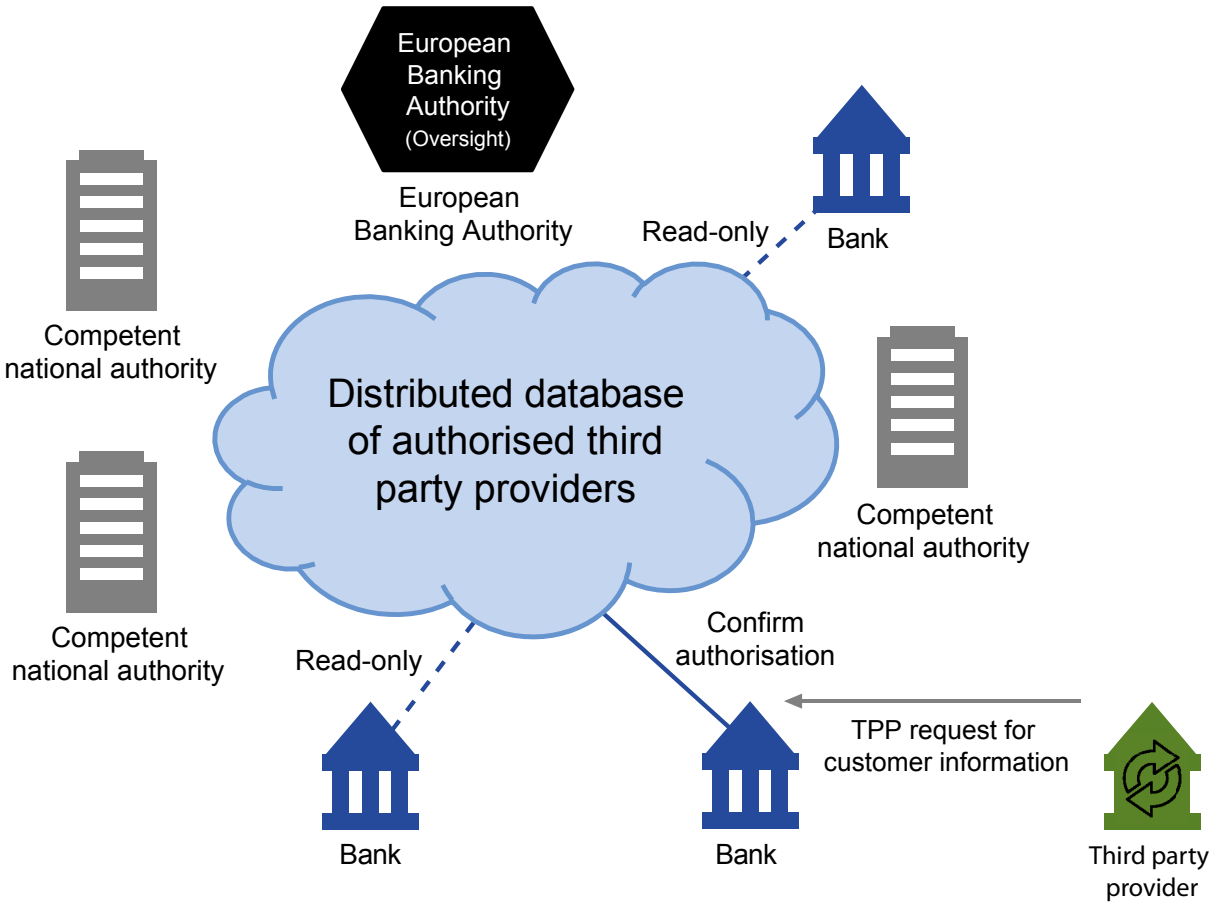


Figure 1: *Managing third party provider authorisation for European banks*

A uniform view of all authorised TPPs for banks

The bank side of consent management involves providing a list of all authorised third party providers to every bank in Europe. This would allow European banks to instantly check to see if a third party requesting access to a customer's bank account data is authorised to access that data under the PSD2. In theory, cryptotechnology solutions are not necessary for performing the task of consistently updating a ledger of authorised entities that can be used by banks throughout Europe. Indeed, the European Banking Authority released a consultation paper in July 2017 proposing "a technological solution that will support both manual insertion and automated transmission of information by competent authorities (CAs) to the European Banking Authority (EBA)."[9] But in practice, having a single central authority update a ledger entails several issues, including:

- Determining which entity updates the ledger;
- Whether a single entity is needed for all of Europe of if authorisation is coordinated between national authorities;
- Ensuring that all banks across Europe have a uniform copy of the authorisation ledger that can be updated in real time and that experiences little downtime in availability (the automated solution outlined in the EBA Consultation Paper discusses updating information from national CAs on a D+1 basis);
- Avoiding errors and omissions that can occur when banks manually check a routing table for information.

Using DLT to manage and check data on authorised third party providers could enable a more efficient, cost-effective, and reliable authorisation process.

A cryptotechnology authorisation ledger would ensure that all European banks would have a shared, single view of all authorised third party providers in Europe. Under the PSD2, the European Banking Authority is mandated to establish and maintain a central register of third party providers as authorised by CAs in EU member states. European banks will rely on this register to verify that third party providers (both Payment Initiation Service Providers (PISPs) and Account Information Service Providers (AISPs)) are entitled to provide payment services to end users under the PSD2. With so many participants involved in updating, managing, and using the register, the use of DLT could enable greater speed and efficiency, with lower cost and a lower risk of unauthorised access to bank account information. With a distributed register for third party providers, all national CAs could instantly update the ledger under rules set by the EBA authority without the need for manual interventions. This includes a record of a TPP's authorisation under the PSD2 as well as a record of exactly when a TPP loses that authorisation for any reason. European banks could then have read-only access to this ledger to verify any TPP requesting bank account information of one of the bank's customers. Once the entity is verified as being an authorised TPP under the PSD2, it would only have to provide proof of a customer mandate to receive specified access to customer information. Should a TPP lose its authorisation for any reason, the automated verification using cryptotechnologies could also void all existing consent given to the TPP from end users.

Banks will need to update internal IT and business processes to accommodate this, but this process is already under way with the development of APIs and the move to faster payments. Scalability concerns would not be an issue as banks would merely be accessing the crypto register to verify the data stored on the ledger; they would not need to add data or transactions to the ledger itself. The implementation of PSD2 will necessitate deeper coordination between

[9] https://www.eba.europa.eu/documents/10180/1911083/Consultation+Paper+on+the+draft+RTS+and+ITS+on+the+EBA+Register+under+PSD2+%28EBA-CP-2017-12%29.pdf

banks throughout Europe and a harmonised process for authorising third party providers to access customer data. DLT can play an important role in this process by enabling banks to instantly check third party authorisation and ensure that unauthorised entities do not gain access to sensitive bank account information.

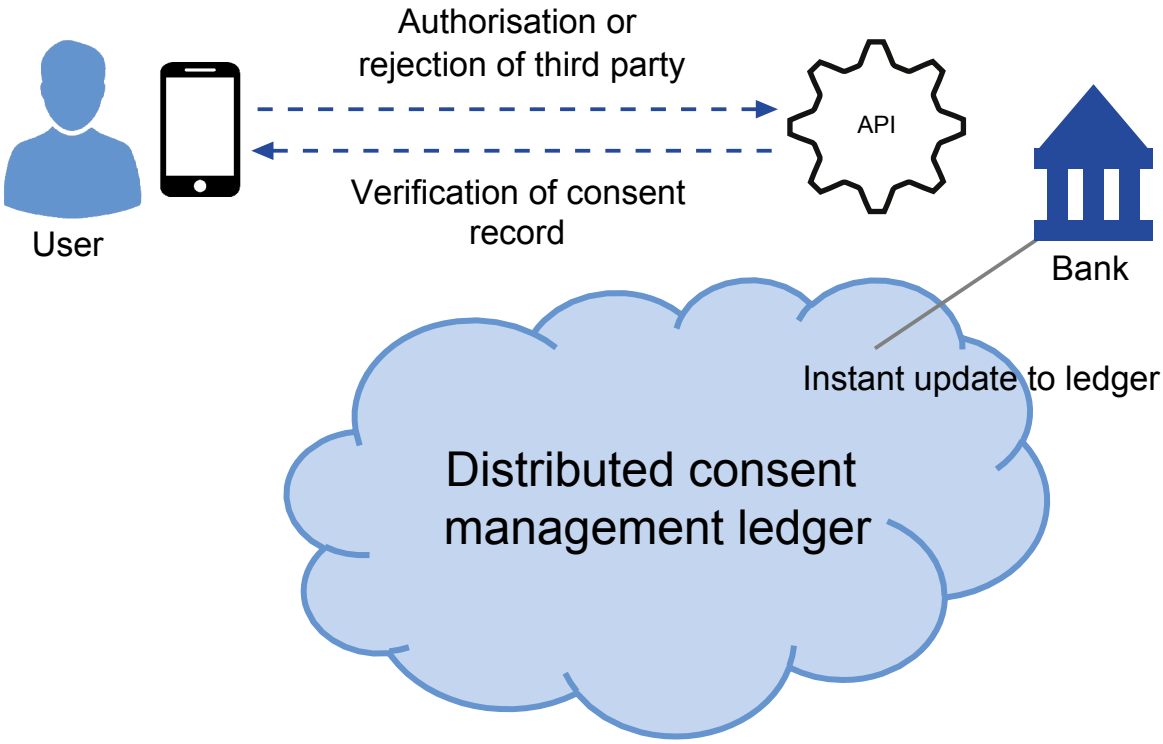


Figure 2: *Distributed consent management ledger*

Customer consent management using DLT

Cryptotechnologies can also enable enhanced control of third party provider authorisation for end users. This is particularly vital considering the PSD2, which will become applicable throughout Europe in January 2018. Under the PSD2, consumers and businesses will be able to authorise third parties to access their bank account data for information or payment initiation services. This use case will also have relevance to the GDPR, which will apply from 25th May 2018 on. The GDPR will also require explicit consent from end users for the processing or sharing of certain customer data, as well as a "right to be forgotten." In the near term, consumers and businesses may not be given full control to manage all of their digital data across numerous platforms as direct participants in a DLT ledger. Banks will have to ease this complexity by providing their customers with interfaces to help control and manage data, and a fully auditable record of which entities have been given consent to access bank account data could be a key enabler of regulatory compliance and an improved customer experience.

Currently, many banks lack comprehensive and well-integrated end user consent management systems. Cryptotechnologies can provide the needed technology for developing such systems. Being greenfield implementations, cryptotechnologies offer a compelling case for implementing consent management systems, with integration to legacy systems and processes occurring via APIs. A cryptotechnology ledger can give a bank a single, unified view of which permissions their customers have given to various third parties or divisions within the bank without the need to store sensitive data itself on the ledger.

Bank customers may not have direct access to a cryptotechnology ledger, and banks will play a crucial role in providing straight-forward and user-friendly interfaces to enable advanced functionality for end users. Users could either give or withdraw consent for third parties to access their bank account data via a front-end app on a mobile phone or online. Banks would receive these requests via APIs and then immediately (and immutably) store the record of consent on the DLT ledger. Once consent is revoked, the record on the ledger would be instantly updated to reflect this. Any future disputes could easily be resolved by reviewing the record of consent on the ledger, and users could verify their information on the ledger via the interface provided by their bank. The only information stored on the ledger would be the record of consent given to each third party; the end user's bank account information would be stored off-ledger at the bank as it is done today. End users would be able to review this record online or via a mobile app, giving them added control and security of their data even when using multiple third-party apps or bank products.

The use of DLT for customer-facing consent management would help comply with regulations such as the PSD2 and the GDPR while also providing a frictionless experience for bank customers. Permissioned ledgers help minimise scalability concerns, and occasional updates to the record of consent do not represent a high volume of transactions. The concern about immutability of data on a ledger would not be relevant because no private customer information is stored on the ledger, only a record of when consent is given and taken away. In fact, the immutability of this data would be a positive aspect due to the ability to fully audit an entire history of customer authorisations.

Benefits and practical considerations for consent management

Benefits of cryptotechnologies for consent management

- Greater speed and efficiency in ensuring TPP authorisation and customer consent;
- Improved customer experience through enhanced control over third-party access to data;
- Aids compliance with regulations such as the PSD2 and GDPR;
- Instant identification of authorised TPPs increases efficiency and lowers risk of fraud or error;
- Increased transparency due to fully auditable record of all entities that have been authorised under PSD2 or given access by customers to bank account information.

Practical considerations and challenges

- Determine where cryptotechnologies fit in IT stack and update business and data governance processes accordingly;
- Analyse costs of segregating data between ledgers;
- Develop interfaces allowing customers to interact with DLT ledger and use APIs to automate this process;
- Determine which entities are represented as nodes on ledger and what type of access each participant should have (read-only, verify new ledgers, etc.).

EXCHANGE OF KNOW YOUR CUSTOMER (KYC) INFORMATION WITHIN BANKS AND WITH SUBSIDIARIES

The complexity and redundancy involved in KYC processes today is a big driver of cost for banks and their customers. As was explored in the March 2017 report "Cryptotechnologies in international payments"[10] published by the Euro Banking Association's Cryptotechnologies Working Group, DLT offers huge opportunities to lower cost in the complex value chain of international payments. But cryptotechnologies also offer banks a way to rationalise their internal onboarding processes and complex records of identity for a single customer. Further benefits could be achieved by opening access to identity information between a bank and its own subsidiaries. Cryptotechnologies can provide a single internal source of truth on a customer's identity, which could help reduce the time it takes to onboard clients and avoid potential complexities and errors that result from a fragmented information onboarding process.

There are two aspects of KYC that banks must consider: Customer due diligence related to onboarding a client and the anti-money laundering (AML) screening of a payment itself. This use case will deal with the former. By facilitating secure access to KYC information between multiple parties within banks or banks and their subsidiaries, DLT can reduce costs and onboarding time. It can also provide opportunities for banks and their subsidiaries to offer products tailored to the needs of their customers with few redundant processes.

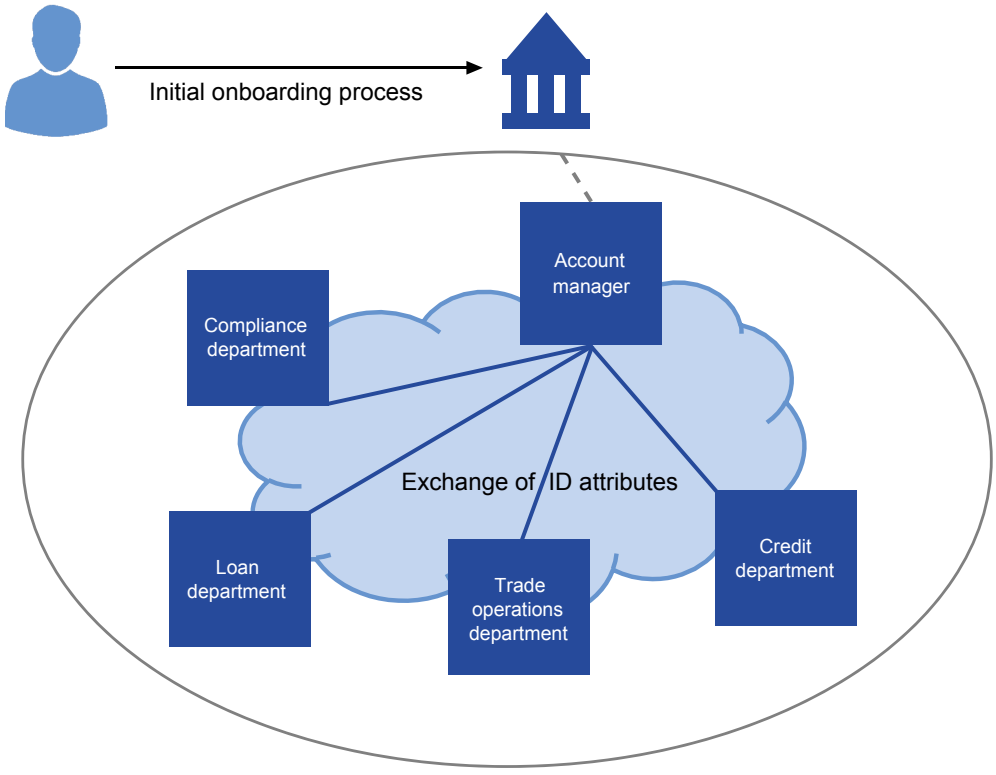


Figure 3: *Distributed identity attribute management*

[10] https://www.abe-eba.eu/downloads/thought-leadership/EBA-Cryptotechnologies-in-international-payments-March-2017.pdf

Distributed identity attributed management within banks

The sharing of customer KYC information within banks can be a very fragmented process (if it happens at all) that is marked by redundant procedures across various divisions. Frequently, a customer must re-submit identity information or documentation when applying to use a new product or service with their bank. The difficulty for banks sharing information internally is a result of highly paper-based processes and a build-up of internal siloes between divisions after bank mergers. With a highly paper-based onboarding process and the complexity of communication between siloes, it is often easier for the bank to perform redundant onboarding processes with existing customers than to re-work internal processes to enable the fast and open exchange of customer information. Many bank customers do not understand why they are required to re-submit information that has already been shared with the bank, which leads to a poor customer experience.

Cryptotechnologies can help facilitate the re-use of customer data within banks. KYC and onboarding processes would remain largely the same, but the storing and exchange of this data would be much more efficient, secure, and faster. After a division within a bank onboards a customer, the KYC information obtained could be stored on a backend system used within the bank. The account manager could then use this information to build a customer's identity that consists of the attributes obtained in the onboarding process and supplemented with additional information as the customer makes transactions. When a customer requests a product or service from another division within the bank, that division can call on the customer's internal identity profile to request access to attributes needed for the additional service. These attributes would then be exchanged internally via DLT, enabling that division to provide the service to the customer without asking for any additional information (or, if additional information is needed, the customer only needs to provide specific information instead of re-submitting prior documentation). There would be no need to share entire documents – only the specific attributes needed for the request would be shared within bank divisions.

Distributing identity attributes between banks and their subsidiaries

This principle could be expanded beyond the (local) confines of a bank as well. Some bank customers, particularly corporates, do business in many jurisdictions. Banks with subsidiaries in multiple markets often leverage their size to attract corporate customers with diverse needs for payments and other financial services. The fact that subsidiaries are often located in separate jurisdictions means that corporates need to go through entirely new onboarding processes each time they use a product or service from a local subsidiary. Despite being the same bank, or a subsidiary providing ancillary services necessary for global commerce (such as insurance), corporate customers still have to go through the complex process of providing necessary documentation and KYC information. Banks can leverage DLT to allow for a more seamless customer experience across jurisdictions while maintaining security of information and compliance with regulations in multiple markets.

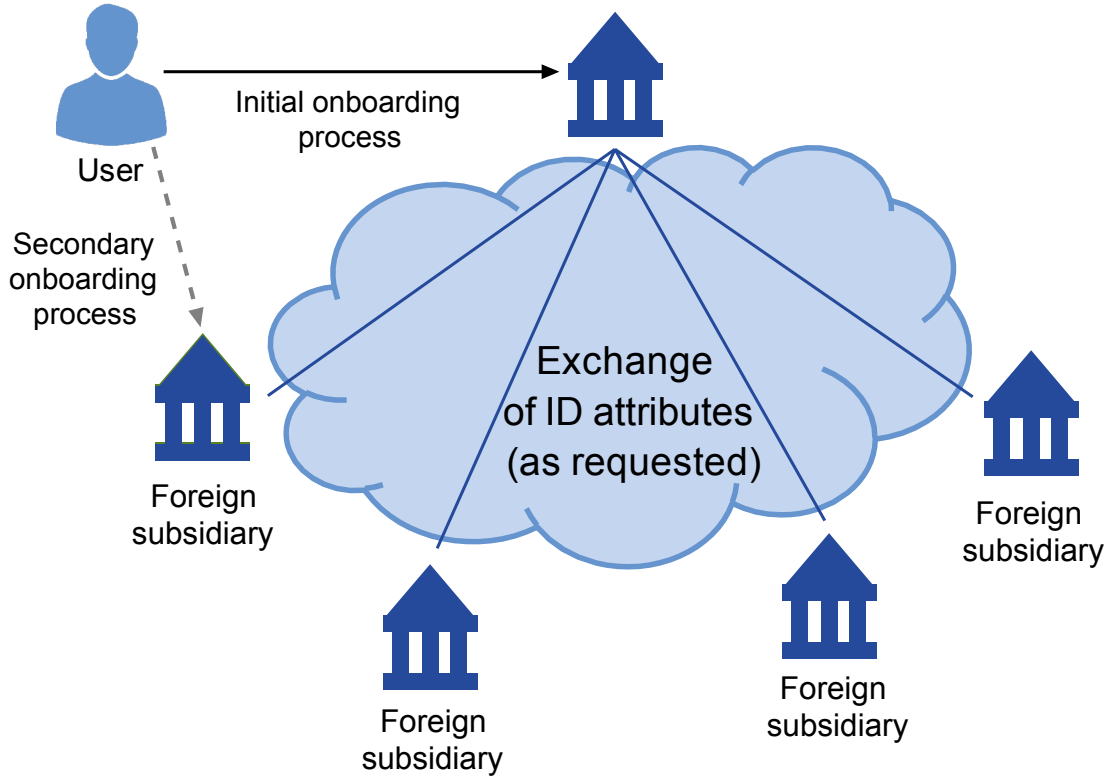


Figure 4: *Exchange of ID attributes with subsidiaries*

In the cross-border space, banks will have to ensure that the exchange of identity attributes across jurisdictions does not compromise compliance with local laws and regulations. Banks may consider using smart contracts to ensure that only valid and legal identity attributes are shared with subsidiaries abroad. Any restrictions on sharing an attribute or piece of data in any jurisdiction can be embedded in the smart contract code to ensure that banks comply with local regulations without the need to rely solely on manual processes. In some jurisdictions, the use of smart contracts may not be enough. Countries such as the Netherlands currently mandate that the entity that onboards a customer remains liable for conducting KYC checks accurately. As regulations such as the GDPR seek to give users more control over their data and technology makes the concept of self-sovereign electronic identity feasible, these regulations may need to be revisited to ensure that they are fit for purpose.

The absence of a global identifier in correspondent banking is a major hurdle for banks today. Although cryptotechnologies can enhance efficiency and speed while enabling the secure exchange of identity attributes (as opposed to full ID documents), the banking industry still needs to harmonise various approaches to legal identifiers and determine whether existing initiatives such as Legal Entity Identifier (LEI) are adequate or whether additional solutions are needed. The lack of a global market practice for exchanging KYC information is another challenge to sharing identity attributes across borders. Different markets require different information for customer onboarding and screening. The higher due diligence requirements needed in correspondent banking mean that any cryptotechnology solution aimed at exchanging KYC information will have to account for requirements in different jurisdictions and maintain flexibility to deal with regulatory changes as they occur.

Benefits and practical considerations for KYC management

Benefits of cryptotechnologies for KYC management:

- Increased efficiency in exchanging information between bank departments and between banks and their subsidiaries;
- Maintaining data security and compliance with regulations allows banks to shift focus to improving customer experience and attracting new users;
- Having information that is machine-readable can reduce error rates and improve speed;
- Potential for cross-selling of products to consumers and businesses based on identity profile.

Practical considerations and challenges:

- Lack of global market practice for exchanging KYC information and absence of global identifier for financial services will continue to be hurdle in correspondent banking;
- Data protection laws in some jurisdictions prohibit the exchange of certain data between institutions
  - Analyse which jurisdictions are most attractive for DLT solutions;
- Need to ensure revocability of data in line with data protection requirements.

LOOKING AHEAD

The use cases examined in this report can help banks as they deal with evolving customer demands and new regulations calling for faster information exchange and greater transparency in financial services. An incremental approach to DLT adoption gives banks the opportunity to assess how the technology interacts with existing internal systems and interbank networks and to examine new use cases that can increase efficiency, lower costs, enable new products and improve service for their customers. As some members of the EBA's Cryptotechnologies Working Group have reported, internal proofs of concept with cryptotechnologies have also helped trigger a wider conversation about the role their organisations play in providing payment services to their customers and where they fit in the payments value chain going forward. This fundamental assessment of the role of banks is vital at a time when new industry players are entering payments and new regulations demand that banks re-think their role as a one-stop shop for payments and banking services.

While the gradual adoption of cryptotechnologies can bring tangible benefits to banks and other players in the short-term, the full benefits of DLT will not be unlocked until the technology is used by a wide variety of financial industry stakeholders. Industry collaboration will be key. Banks should work closely with other financial institutions and regulators to explore the effects cryptotechnologies have on data security, processing efficiency, regulatory compliance, and customer experience. Cryptotechnologies can help open up new horizons on how to explore solutions to existing problems. As DLT adoption evolves from internal use cases to include multiple organisations in multiple jurisdictions, financial industry stakeholders and their customers will experience the full value of transparency, speed, and efficiency without the need to compromise on data security and regulatory compliance.

ABE EBA
EURO BANKING ASSOCIATION

Contact details

For any additional information, please contact:

Daniel Szmukler
Director
d.szmukler@abe-eba.eu

Euro Banking Association (EBA)
40 rue de Courcelles
F - 75008 Paris
TVA (VAT) n°: FR 12337899694

Layout

www.quadratpunkt.de

Illustrations

Euro Banking Association
and Lipis Advisors