USING LEGAL ENTITY IDENTIFIER (LEI) ON BLOCKCHAIN FOR REDUCING MONEY LAUNDERING RISKS AT FINANCIAL INSTITUTIONS

Makhmud Makhmudov,
Master student, Estonian Entrepreneurship University of Applied Sciences Mainor, Enterprise Strategic Management
E-mail: *m.efendi@leipapa.com*

Abstract

The increasing use of blockchain technology nowadays can play a key role in using the decentralized network as a standard database for the unified and secured registry, through which financial institutions can conduct a relevant customer due to diligence measures and business transactions by verifying organizations' Legal Entity Identifier (LEI) codes, self-sovereign identifiers managed by the Global Legal Entity Identifier Foundation (GLEIF). With proper implementation, this solution can be applied to blockchain networks, offering the additional advantage of quality control and detailed business analysis. Thus, by giving financial institutions the benefit of interacting with legal entities that have proved their reputation and, therefore, by reducing the money laundering risk at financial institutions, blockchain technologies now could reach global standardization and acceptance by financial institutions worldwide.

Keywords: *LEI, blockchain, anti-money laundering, risk assessment, risk management.*

Introduction

Money laundering and terrorist financing can do harm to the stability of a financial system, and negatively affect the reliability of banks and other financial institutions, such as security firms and insurance companies. Money laundering activity has been associated with several cases related to bank failures around the globe, including the closures of the European Union Bank, Riggs Bank, Danske Bank AS etc. Such cases indicate that the risk of money laundering has been implemented at the financial institutions mentioned above and the overall risk of involving financial institutions in such transactions is high.

As money laundering and terrorist financing threaten financial and non-financial institutions and societies, the challenge, and the necessity to develop technologies in order to prevent and detect financial crime intensifies. The key features and main tools for solving this problem are, respectively, the knowledge (awareness) of the financial institutions' employees and the information technologies. This paper proposes to consider the risks of money laundering and terrorist financing arising during the establishment of relationships between financial institutions and prospective clients and during the conduction of due diligence measures with the existing clients. The author believes that internal control mechanisms at financial institutions should be constantly developed to identify the risks associated with the legalization of criminal proceedings and ensure the economic security of a particular financial institution. The purpose of this research is to propose using a global registry of legal entities (LEI index) through which financial institutions can conduct relevant diligence and business transactions, thereby reducing the risk of money laundering at financial institutions, by verifying the Legal Entity Identifier (LEI) codes, self-sovereign identifiers managed by the Global Legal Entity Identifier Foundation (GLEIF), a Swiss-based organization that coordinates the management of the global LEI system under the oversight of the Legal Entity Identifier Regulatory Oversight Committee (LEI ROC). Currently, an LEI index has a number of shortcomings caused by the peculiarities of its implementation, which, as a result, may lead to the conclusion that it is unsuitable for operation within the framework of financial institutions. It is crucial to have an LEI index developed in a way to provide its security and reliability, performance, data relevance, and the auditable and immutable history of all changes made. Therefore, the author proposes to develop an LEI index on a decentralized platform in order to meet the requirements necessary to use an LEI index

https://doi.org/10.17770/acj.v1i93.6733

as a reliable source and to avoid the impossibility of obtaining up-to-date information when requested by financial institutions.

To achieve this objective, it is necessary to solve the following tasks:

- analyze legal acts and recommendations in this area;
- identify the risk types and the risk factors of financial institutions in the field of Anti Money Laundering and Counter-Terrorism Financing (AML/CFT) when carrying out due diligence measures;
- determine the role of LEI to reduce the risk of money laundering and terrorist financing and the significance of its implementation on a decentralized platform.

The author used the provisions and conclusions on solving the problems of risk management in the field of combating money laundering and terrorism financing specified in the Guidelines of the Association of Certified Anti-Money Laundering Specialists (ACAMS), the Guidelines of the Estonian Financial Supervision Authority for the theoretical and methodological basis of the research. The nature of the tasks set and a systematic approach to their solution determined the use of the following research methods in the work: analysis, synthesis, generalization, and other general scientific methods. The author used the provisions of legislative acts and recommendations from authorities, sources presented on the Internet, and research results of the author as the information basis of the study.

Legal acts and recommendations

We live in the age of international control over money laundering and terrorist financing tightening. Through several money laundering typologies exercises, the Financial Action Task Force (FATF), an intergovernmental body formed in 1989, demonstrated that money laundering can be achieved through virtually every medium, financial institution, or business.[1] A key element of FATF's efforts is its detailed list of appropriate standards for countries to implement. These measures are set out in the 40 FATF Recommendations adopted by the FATF plenary in February 2012, with the last revision made in October 2021, which provides a complete set of countermeasures against money laundering and terrorist financing, covering (among others) the identification of risks and development of appropriate policies and the transparency of legal persons and arrangements, combined with international cooperation.

At the June 2012 Los Cabos Summit[2], the G20 Leaders endorsed the Financial Stability Board (FSB) report "A Global Legal Entity Identifier for Financial Markets"[3] and encouraged "global adoption of the LEI to support authorities and market participants in identifying and managing financial risks"[4]. A more detailed definition of LEI will be described below.

The activity of financial institutions is one of the main in global economics and is the most sensitive to external changes. The establishment and maintenance of an effective AML/CFT program is an obligatory part of any financial institution's charter to operate. As stated in (1) § 14 of the Estonian Money Laundering and Terrorist Financing Prevention Act: "The obliged entity establishes rules of procedure that allow for effective mitigation and management of, inter alia, risks relating to money laundering and terrorist financing".[5] Moreover, in accordance with the 10th FATF recommendation, CDD measures to be taken as "identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information", as well as "identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner, such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements, this should include financial institutions understanding the ownership and control structure of the customer".

The risk-based approach is one of the main recommendations of the FATF. The approach is based on risk identification, as stated above, and assessing the risk of money laundering at a financial institution, which helps to determine the level of the client's risk, and helps to identify clients with a high risk of money laundering. The risk-based approach makes it possible to prevent the use of a financial institution for the purpose of money laundering.

Risk factors of financial institutions

In accordance with § 13 of Estonian Money Laundering and Terrorist Financing Prevention Act: "For the purpose of identification, assessment, and analysis of risks of money laundering and terrorist financing related to their activities, obliged entities prepare a risk assessment, taking account of at least the following risk categories:

1) risks relating to customers;
2) risks relating to countries, geographic areas or jurisdictions;
3) risks relating to products, services or transactions;
4) risk relating to communication, mediation or products, services, transactions or delivery channels between the obliged entity and customers".

Based on the information from Basel Committee on Banking Surepvision[6] and according to recommendations from Estonian Financial Inspection[7], in the context of AML/CFT, the business units (e.g., front office of financial institutions, customer facing activity) are the first line of defense in charge of identifying, assessing, and controlling the risks of their business. They should know and carry out the policies and procedures and be allotted sufficient resources to do this effectively. The second line of defense includes the chief officer in charge of AML/CFT, the compliance function but also human resources or technology. The third line of defense is ensured by the internal audit function.

Table 1: The real sample of risk rating tool used by financial institutions

Risk factor	Type	Risk level	Risk value	Weight
Customer type	Private company limited by shares	High risk	8	0.1
Customer industry	Financial services - regulated	Low risk	3	0.15
Customer relationship	New client, recent incorporated >1y, no previous bank account	High risk	10	0.1
Customer jurisdiction	UK	Medium risk	4.6	0.2
UBO jurisdiction	UK	Medium risk	4.6	0.25
Monthly turnover	500 00 € <	High risk	7	0.2
Total				1
	Total:	Medium Risk	**5.72**	initial risk rating

Source: Composed by the author based on the data provided by financial institution

Thus, financial institutions must implement their risk rating tool according to the appropriate risk-appetite and use it while identifying clients and conducting due diligence measures. The sample risk rating tool is presented in Table 1.

According to GLEIF research (2018), "in order to accurately identify client organizations with the most up-to-date data, financial institutions tend to use a variety of different identifiers for cross-checks. In average they use 4 different identifiers internally, but about a third say they use 5 or more identifiers". GLEIF also warns in their research that "financial institutions use multiple identifiers for cross-checking. But this creates confusion because the same ID may be associated with multiple entities (49%), and different IDs can relate to the same entity (47%). Only two thirds of financial institutions believe they hold accurate client information. Less than a third of clients can be relied on to report material changes to their legal entity, so the burden remains with the institution to conduct regular reviews". These facts show the real challenges the financial institutions facing while interacting with their clients, and it is necessary to pay special attention to this, since they are factors preventing the normal work of responsible employees when using a risk-based approach to reduce the financial institution's risk of use for the purpose of money laundering.

What is a LEI

The LEI system was developed by the 2012 Group of Twenty (G20) in response to the inability of financial institutions to identify legal entities uniquely, so that their financial transactions in different national jurisdictions could be fully tracked. LEI ROC currently is a coalition of financial regulators and central banks across the globe and is encouraging the expansion of the LEI.

According to GLEIF, the LEI is a 20-character, alpha-numeric code based on the ISO 17442 standard developed by the International Organization for Standardization (ISO). It connects to key reference information that enables clear and unique identification of legal entities participating in financial transactions.[8]

Picture 1: The meaning of the digits in the LEI code

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
LOU IDENTIFIER Prefix used to ensure uniqueness among codes from LOUs				ENTITY IDENTIFIER Entity-specific part of the code generated and assigned by the LOUs according to transparent, sound and robust allocation policies														VERIFICATION ID Two checks digits as described in the ISO 17442 standard	
2	1	3	8	0	0	8	L	Q	A	H	Z	J	R	B	A	1	V	8	8

Source: https://docs.leipapa.com

The LEI code specifies the minimum reference data, which must be supplied for each LEI, such as the official name of the legal entity as recorded in the official registers, the registered address of that legal entity, the country of formation, the codes for the representation of names of countries and their subdivisions.[9] The information stating the date of the first LEI assignment, the date of last update of the LEI information, and the date of expiry (when applicable) is also stored in the global database. Moreover, each LEI contains information about an entity's ownership structure (direct and ultimate parent entities) and therefore answers the questions of "who is who" and "'who owns whom"[10] for each particular entity. Every single LEI code is unique, and it shall be issued only once for a specific legal entity and the same LEI code cannot be issued to another legal entity. The LEI code does not replace the registry code (registration number of the entity) of the commercial register, which is still used to identify a legal entity.

LEI codes associate legal entities with key information, which allows them participating in global financial markets to be clearly and uniquely identified and are already used to identify the parties to EMIR derivative instruments transactions and due to the application of implementing regulation EU/2017/105, no other alternative codes can be used when providing notification of transactions made with derivative instruments starting from the 1st of November 2017. Moreover, LEI codes are used for reporting as of the 3rd of January 2018. Pursuant to the MiFIR and MiFID II[11] regulation, transaction reports shall, among other things, also be used for investigating market abuse.[12]

In simple words, LEI code is a uniform way of keeping track of legal entities around the world. LEI codes are global and have no borders at all for relevant and trusted identification of entities. Looking in that way, the publicly available LEI data pool can be regarded as a global directory, the registry which may greatly enhance transparency at the global marketplace. Such information is important for compliance departments of financial institutions and anti-money laundering specialists while conducting due diligence measures as part of KYC procedures, especially in such cases where foreign legal entities have the complicated and opaque structures of ownership.

The management of the LEI system is coordinated and supported by GLEIF, while registrations and data storage are performed by Local Operating Units (LOUs), which, in turn, use a branched structure of Registration Agents (RAs) that receive applications from legal entities for the registration of LEI codes, checking the data, processing legal documents, sending applications to the relevant LOU for further issuance of the LEI code. GLEIF invokes that "financial services businesses can save

time, gain greater transparency, and work in a more streamlined fashion by adopting an LEI for each client organization".[13]

GLEIF research (2018) explores the challenges that the banking sector faces when it comes to onboarding new client organizations, with a view to investigating, in particular, the implications of Know-Your-Customer (KYC) requirements. Financial institutes operate in multiple jurisdictions and therefore need a global standard such as LEI system, which offers various businesses a unified approach to identifying legal entities and has the potential to take the complexity out of business transactions.[14]

Why to use blockchain

As stated above, GLEIF coordinates the management of the global LEI system and maintains a registry called as the Global LEI Index. However, a centralized service or a management body maintaining a registry can be considered as a single point of failure for the whole system. Moreover, currently there are several sources, within which LEI data is stored. When a legal entity is registered or provided an update with a LOU, there is often a waiting period, that can take up to several hours before the updated information appears on various search tools online. Given that the very nature of the LEI is that it is a digital product, all the data is stored online between separate entities, and the information may not match between them, and may be inconsistent across search tools.

The data quality concerns associated with lapsed LEIs were specified and summarized in the LEI ROC progress report (2018)[15], pointing out the risks that the second LEI identifier could be issued to the same legal entity (if for instance, a name change was not timely recorded), confusion about the surviving LEI in case of mergers, difficulties in reconciling LEI data with other databases (e.g. different addresses), lack of management of challenges to LEI data by third parties (as LOUs cannot generally update a record without the agreement of the entity). Another concern is that data enhancements are not implemented for lapsed LEIs, for instance, the collection of relationship data, which is progressively rolled out.[16] Such concerns and potential vulnerabilities are crucial for registries such as Global LEI Index, where information about legal entities must be relevant and verified, as well as access all the time without interruptions since financial institutions' representatives should get validated information while performing AML checks of their clients.

One approach to address this is to use a Distributed Ledger Technology (DLT) more commonly known as blockchain technology, an emerging technology for secure, decentralized, and transactional data sharing across a large network of untrusted participants without relying on a central trusted authority to record and validate transactions. Blockchain technology produces a structure of data with inherent security qualities. It is based on the principles of cryptography, decentralization, and consensus, which ensure trust in transactions.[17]

Blockchain has three levels of security:

- Blockchain is a distributed network that allows storing data in an unchanged form transparently.
- Blockchain stores information in a chain of blocks, where each contains information about the previous one (the hash value).
- Information in the blockchain is protected using mathematical algorithms.

Centralization is the primary difference between the registry built on blockchain and implemented with a regular database. While all records secured on a regular database are centralized, each participant on a blockchain has a secured copy of all records and all changes. Thus, each user can view the provenance of the data, and if there's an inconsistency, blockchain technology will immediately identify and correct any unreliable information, since each participant maintains a copy of the records. The widespread adoption of blockchain technology these days to ensure that any number of centralized databases are not compromised, gives enough arguments to decide on the appropriateness of using blockchain for the Global LEI Index registry. It is also stated by GLEIF, that integration of LEI into solutions based on digital certificates and blockchain technology, will allow anyone to easily connect all records associated with an organization and identify "who owns whom".[18]

Blockchain "by design" is a reliable and distributed platform to share data and services securely. Instead of, as now, centralizing the data in one database, it will be distributed automatically to interconnected nodes, owned by the participating operational units. This provides a robust defense against attack. The blockchain technology will update Global LEI Index in ~~a~~ real-time with quality data and reflect relevant information as they change over time while maintaining an auditable and immutable history. Any changes made on one system will be logged and updated on the others in a real time and due to its interconnected network and data protocols, there are no single points of failure nor a single authority that controls the system. These features make blockchain the ideal technology for Global LEI Index and as a blockchain-agnostic innovator, GLEIF continues to implement their Digital Verifiable Credential (DVC) proof-of-concept on both public (Ethereum) and private (Hyperledger Indy) blockchains.[19]

Conclusion

After analyzing legal acts and recommendations in the field of AML/CFT, the author has concluded that financial institutions have to establish internal rules and procedures allowing effective mitigation and risk management of relating to money laundering and terrorist financing. Customer due diligence measures should be conducted as identifying customers and verifying their identity with the use of reliable and independent source documents. The risk-based approach is one of the main recommendations of the FATF, which is based on the risk identification and assessing the risk of money laundering at a financial institution, which helps to determine the risk level of clients and identify clients with a high-risk of money laundering. Financial institutions are obliged to prepare a risk assessment, considering at least risks relating to customers, risks relating to countries, geographic areas or jurisdictions, and risks relating to products, services or transactions. Moreover, financial institutions must implement their risk rating tool according to the appropriate risk-appetite and use it while identifying clients and conducting due diligence measures.

Since there are several challenges that financial institutions face while interacting with their clients related to the data relevancy and accuracy, the author proposes the using of the Legal Entity Identifier (LEI) system that was developed by the 2012 Group of Twenty (G20) for reducing money laundering risks. Since each LEI code contains information about an entity's ownership structure (direct and ultimate parent entities) and the reference data, such as the registered address of that legal entity, the country of formation etc., it can be used as a way of keeping track of legal entities around the world and the publicly available LEI data pool can be regarded as a global directory, which may greatly enhance transparency in the global marketplace. However, a LEI registry implemented on a centralized database faces several challenges, such as the time lagging, security, and accuracy issues, which is crucial for such registries where information about legal entities must be relevant and verified.

The author considered a solution to implement LEI registry with use of Distributed Ledger Technology (DLT). Such solution will provide the highest level of security, real time updates and will make available the whole history of updates and transactions for each LEI code. The first approach of implementation of the solution mentioned herein is in the stage of development by GLEIF contractors on both public (Ethereum) and private (Hyperledger Indy) blockchains.

References

[1] Association of Certified Anti-Money Laundering Specialists (ACAMS) (2019). Study Guide CAMS certification exam. P.1.

[2] G20 Los Cabos Mexico (2012). P.7-8. G20 Leaders Declaration. https://www.fsb.org/wp-content/uploads/g20_leaders_declaration_los_cabos_2012.pdf (request date 15.12.2021.).

[3] Financial Stability Board (FSB). (2012). A Global Legal Entity Identifier for Financial Markets. https://www.fsb.org/wp-content/uploads/r_120608.pdf (request date 15.12.2021.).

[4] Financial Stability Board (FSB) (2019). Press Release. P.1. https://www.fsb.org/wp-content/uploads/R280519-2.pdf (request date 18.12.2021.).

[5] Riigi Teataja (2022). Money Laundering and Terrorist Financing Prevention Act. https://www.riigiteataja.ee/en/eli/ee/517112017003/consolide/current (request date 03.01.2022.).

[6] Basel Committee on Banking Supervision (2020). Sound management of risks related to money laundering and financing of terrorism. P.5. https://www.bis.org/bcbs/publ/d505.pdf (request date 04.01.2022.).
[7] Finantsinspektsiooni juhendid. Krediidi- ja finantseerimisasutuste organisatsiooniline lahend ning ennetavad meetmed rahapesu ja terrorismi rahastamise tõkestamiseks. (2018). https://www.fi.ee/sites/default/files/2018-11/FI_AML_Soovituslik_juhend.pdf (request date 28.12.2021.).
[8] Global Legal Entity Identifier Foundation (GLEIF). https://www.gleif.org/en/about-lei/introducing-the-legal-entity-identifier-lei (request date 03.01.2022.).
[9] Global Legal Entity Identifier Foundation (GLEIF). https://www.gleif.org/en/lei-data/access-and-use-lei-data/level-1-data-who-is-who (request date 03.01.2022.).
[10] Global Legal Entity Identifier Foundation (GLEIF). https://www.gleif.org/en/about-lei/introducing-the-legal-entity-identifier-lei (request date 03.01.2022.).
[11] European Securities and Markets Authority (ESMA). (2018). https://www.esma.europa.eu/policy-rules/mifid-ii-and-mifir (request date 04.01.2022.).
[12] European Securities and Markets Authority (ESMA). (2017). https://www.esma.europa.eu/sites/default/files/library/esma70-145-238_lei_briefing_note.pdf (request date 04.01.2022.).
[13] Global Legal Entity Identifier Foundation (GLEIF). LEI in KYC: A New Future for Legal Entity Identification. https://www.gleif.org/en/lei-solutions/lei-in-kyc-a-new-future-for-legal-entity-identification (request date 04.01.2022.).
[14] Global Legal Entity Identifier Foundation (GLEIF). (2018). Know Your Customer (KYC): The Challenges Faced by the Banking Sector When Onboarding New Client Organizations. Research Findings. https://www.gleif.org/content/3-lei-solutions/6-lei-in-kyc-a-new-future-for-legal-entity-identification/gleif-research-findings_challenges-onboarding-client-organizations-in-banking-sector_v1.0-final.pdf (request date 05.01.2022.).
[15] Legal Entity Identifier Regulatory Oversight Committee (LEI ROC). (2018). The Global LEI System and regulatory uses of the LEI. P. 9. https://www.leiroc.org/publications/gls/roc_20180502-1.pdf (request date 08.01.2022.).
[16] Financial Stability Board (FSB). (2019). Thematic Review on Implementation of the Legal Entity Identifier. https://www.fsb.org/wp-content/uploads/P280519-2.pdf (request date 08.01.2022.).
[17] IBM. Basic Blockchain Security. https://www.ibm.com/topics/blockchain-security (request date 10.01.2022.).
[18] Global Legal Entity Identifier Foundation (GLEIF). LEI in KYC: A New Future for Legal Entity Identification. https://www.gleif.org/en/lei-solutions/lei-in-kyc-a-new-future-for-legal-entity-identification (request date 04.01.2022.).
[19] McKenna, K., Piechocki, M. (2020). Grafting Blockchains into Enterprise Businesses - The LEI and Digital Verifiable Credentials [Video]. https://www.youtube.com/watch?v=59pPG_srJmQ&t=708s (request date 12.01.2022.).

Anotācija

Blokķēdes tehnoloģijas izmantošanas pieaugumam mūsdienās var būt būtiska nozīme, lai pielietotu decentralizētu tīklu kā standarta datubāzi vienotai un aizsargātai reģistrācijai, caur kuru finanšu iestādes var veikt attiecīgu klientu uzticamības un biznesa darījumu pārbaudi, analizējot LEI kodu – suverēnu identifikatoru, ko pārvalda Globālais juridisko personu identifikatoru fonds (GLEIF – *Global Legal Entity Identifier Foundation*). Veicot pareizu identifikatora ieviešanu, šo risinājumu var izmantot blokķēdes tīklos, piedāvājot kvalitātes kontroles un detalizētas biznesa analīzes papildu priekšrocības – finanšu iestādēm iespēju sadarboties ar juridiskām personām, kuras ir pierādījušas savu nevainojamu reputāciju, tādējādi samazinot naudas atmazgāšanas risku finanšu iestādēs.

Autors secina, ka blokķēdes tehnoloģija šobrīd varētu sasniegt globālu standartizāciju un akceptu no finanšu iestāžu puses visā pasaulē.