ADVANCE SOCIAL SCIENCE ARCHIVE JOURNAL
Available Online: https://assajournal.com
Vol. 03 No. 02. Apr-Jun 2025.Page#.1483-1495
Print ISSN: 3006-2497 Online ISSN: 3006-2500
https://doi.org/10.55966/assaj.2025.3.2.026
Platform & Workflow by: Open Journal Systems

Technological and Legal Barriers to Anti- Money Laundering and Compliance Enforcement in Decentralized Finance: Case Studies from the European Union

Muhammad Waqar Naeem
Nova school of law Lisbon, Portugal
9207@novalaw.unl.pt

Abstract

DeFi is revolutionizing the financial world by providing open, approval-free, peer-to-peer ways to transact, thanks to blockchain. DeFi allows more financial opportunities and difference, but it also presents problems for AML and compliance due to how it is decentralized, uses pseudonyms and is available in different countries. It describes in detail the barriers faced in DeFi within the EU due to technology and regulations. It discusses why traditional laws are often unsuitable for DeFi, leading to questions about regulations, regulatory boundaries and any gaps in enforcing them. Studying specific cases in the EU, the article explores the journey of AML regulations and points out some of the obstacles inside the regulatory sphere due to swift changes in decentralized technology. Moving on, it highlights that it is difficult to enforce the law in decentralized networks. The study puts forward a group of guidelines in policy, law and technology to improve AML compliance in DeFi without hindering its advancements. For example, EU regulators may align their rules for member states, create better frameworks for liability of decentralized market actors, utilize regtech and encourage teamwork between regulators, technologists and industry members. Based on the findings, rigid and uncooperative regulations will not only fail to tackle issues in DeFi but also slow down innovation. Thus, this article offers ideas for future discussions and rules on safeguarding money matters in the growing world of decentralized finance.

Keywords; *Decentralized Finance, Anti-Money Laundering, Compliance Enforcement, European Union, Regulatory Challenges, Legal Barriers, Blockchain Technology, Financial Regulation, Regtech, Cross-border Cooperation.*

1. Introduction

1.1. Background and Context

DeFi is now considered one of the most powerful changes to the international financial industry. With the help of blockchain and smart contracts, DeFi offers people ways to use lending, borrowing, trading, or yield farming services without the use of intermediaries. These services work independently, reducing costs for operations and ensuring that all transactions are clear and honest (Zetzsche, Buckley, & Arner, 2020). Still, enjoying so much freedom costs banks in terms of stricter rules. Given that DeFi is borderless, uses pseudo- anonymous identities, and offers auto-approval, it raises several concerns about compliance with AML laws. Centralization is key in the usual financial systems, as they can enforce Know Your Customer and Customer Due Diligence procedures.

Yet, since administrators are not easy to identify with DeFi, it is more complicated to ensure AML laws are followed in the EU (Gimigliano, 2022). As the rules differ, DeFi falls into a legal gray area. Even though it aids in including people in financial activities and encourages innovation, it is also threatened by several forms of fraud and dangerous funding. Besides, using public blockchain networks presents a challenge when discussing rules because of matters like protecting user privacy, unchanging transactions, and clashing requirements in laws such as the GDPR (Belen-Saglam, Altuncu, Lu, & Li, 2022).

1.2. Research Problem and Objectives

Despite the increasing focus on crypto-assets, DeFi still does not have a lot of formal regulations. The EU has created laws such as the 5AMLD, the 6AMLD, and the coming MiCA Regulation. Even though these rules cover digital asset service providers, it is unclear how they apply to systems that rely on peer-to-peer networks. Many DeFi platforms do not require permission and use DAOs, so it is hard to identify someone responsible and make them comply (Gimigliano, 2022).

At the same time, public blockchains find it challenging to meet the strict requirements for collecting, handling, and storing personal data as required by the GDPR. To illustrate, GDPR requires that data is not kept for longer than necessary and can be wiped on request, which does not match how blockchain is designed (Belen-Saglam et al., 2022).

Because of the varying laws, DeFi platforms cannot easily use AML tools without breaking other laws. This article aims to highlight how the DeFi network and the rules within the European Union make it more difficult to enforce AML regulations.

The purposes of the system are:

- Identify which features of DeFi are challenging for AML controls.
- Examine the differences between DeFi systems and the current EU AML and data protection rules.
- Study the difficulties related to DeFi as they influence GDPR and MiCA.
- Introduce suggestions that address the missing regulations without interfering with the fundamental traits of DeFi.

1.3. Scope and Methodology

This issue examines why the scope and methodology used in a medical trial matter. For this study, I use qualitative methods that involve studying laws and related articles. The examination is mainly focused on how DeFi meets AML requirements, especially in the European Union. It is important to study policy documents, relevant laws, journal articles, and academic papers. Risk Management does not use any numbers or statistical analysis.

Table 1: Key EU Regulations Relevant to DeFi and AML

Regulation / Initiative	Year	Focus Area	Relevance to DeFi
5th Anti-Money Laundering Directive (5AMLD)	2018	AML for VASPs (Virtual Asset Service Providers)	Cryptocurrency exchanges and custodian wallet providers were required to register and observe AML regulations as a result.
6th Anti-Money Laundering Directive (6AMLD)	2021	Harmonization of AML offenses and penalties	Created extra responsibilities for criminals and detailed the types of crimes that can result in crypto cases.
Markets in Crypto-Assets Regulation (MiCA)	Expected 2024–25	Digital asset regulation	Created extra responsibilities for criminals and detailed the types of crimes that can result in crypto cases.
General Data Protection Regulation (GDPR)	2018	Personal data protection	Seeks to draft a complete set of standards for crypto-assets that also concerns stable coins and token makers, yet it is not clear if these standards can be used for DeFi.

European Anti-Money Laundering	In development	Central AML coordination	Difficulties arise when blockchain uses immutability and transparency and when confidentiality or

1.4. Structure of the Paper

This writing is separated into the following sections:

Here,

- Section 2 explains the topics discussed in previous research as well as the main principles behind DeFi and regulation.
- Section 3 qualitative research methods and their design are discussed.
- Section 4 uncovers the obstacles to enforcing AML that come from cryptocurrency networks.
- Section 5 examines the laws set by the EU, relating to Anti-Money Laundering (AML) and Data Protection (GDPR).
- Section 6 discusses some case studies taken from EU countries.
- Section 7 brings together the ideas contained in the case studies.
- Section 8 provides suggestions that can be followed by policymakers and developers.
- Section 9 ends by discussing how balance can be achieved between advancement and regulation.

2. Literature Review and Conceptual Framework

2.1. Overview of Decentralized Finance (DeFi)

DeFi allows people to access financial services powered by blockchain technology and smart contracts, meaning they can do so without banks or brokers. The novel system comes with lending, borrowing, and asset trading services that are all carried out using decentralized protocols meant to make things more transparent, cheaper, and accessible to more people (Schär, 2021). Rather than using centralized finance with individuals relying on agencies for permission and control, anyone can participate in DeFi without approval. DeFi gives people from all over the world the same opportunities to use financial products. Yet, as regulators have been used to dealing with central entities, the shift to decentralization introduces new difficulties for them (Zetzsche, Buckley, & Arner, 2020).

How can AML and compliance mechanisms be properly enforced in such a situation?

2.2. Technological Barriers to AML Compliance

AML enforcement in DeFi is hard because all transactions happen without revealing the original names of users. Although all transactions are recorded and kept constant in blockchains, the identity of each person participating is generally hidden (Möser, Böhme, & Breuker, 2013). As a result of this feature, it is easier for criminals to use DeFi protocols for laundering money by hiding where the funds are being sent and received.

Furthermore, DeFi platforms rely on smart contracts that automatically process financial transactions. While everything is done faster with automation and mistakes due to inadequate controls are reduced, the safeguards for KYC and CDD compliance have decreased (Arner, Barberis, & Buckley, 2017). Without such barriers, there are gaps in the rules that thieves can abuse.

2.3. Legal and Regulatory Challenges within the European Union

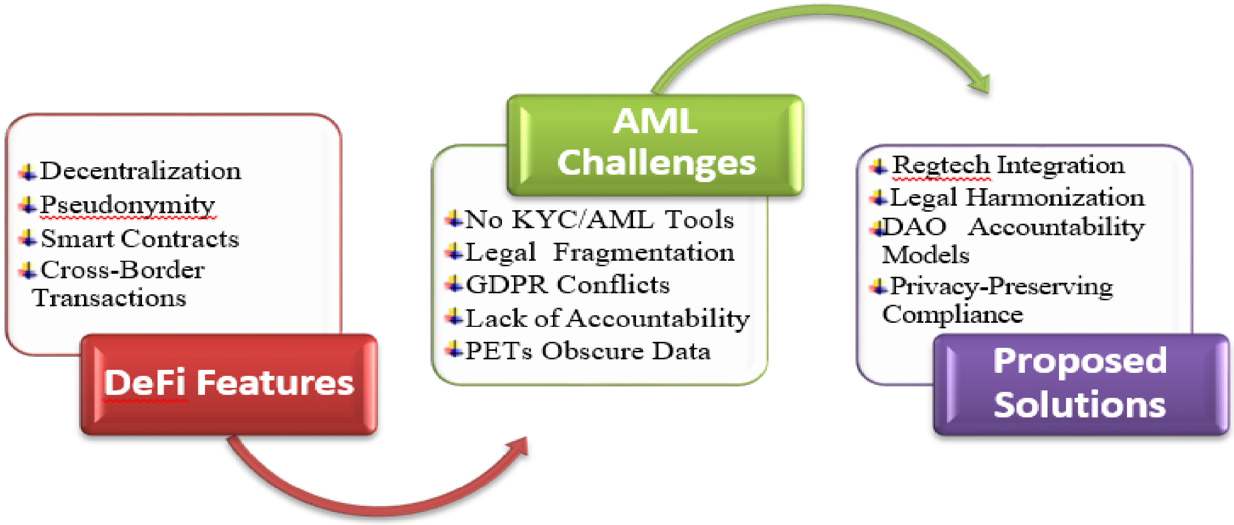
Preventing money laundering and terrorist financing is achieved in the European Union through a well-designed set of rules. Significant factors include the series of AML Directives and the recent foundation of the European Anti-Money Laundering Authority (AMLA) to ensure AML actions are aligned among all EU member states. These rules depend on particular individuals or organizations to ensure they are complying with the required reports and monitoring steps (Finck, 2019). But because DeFi is decentralized, it does not behave as expected.

Most DeFi protocols work independently of any main entity, meaning they are not managed by existing AML laws (Zetzsche et al., 2020). Moreover, the GDPR in the EU poses another challenge for companies. GDPR makes it difficult to store and process personal data on a blockchain due to the blockchain's commitment to being open and unchangeable (Finck, 2019). Such conflict leads to a situation where making financial data secure can protect privacy, but also requires revealing it to the authorities.

2.4. Conceptual Framework: Balancing Innovation with Compliance

Experts have highlighted that working on DeFi's technological progress often competes with ensuring AML compliance. Schär (2021) believes the rules for financial regulation ought to be changed to address the unique traits of decentralized systems. According to Arner et al. (2017), DeFi's work in AML is best guided by regulatory agility and teamwork between all involved. Ways to approach the issue could be using decentralized identity methods, conducting transactions and analysis on the blockchain, and ensuring compliance with privacy-preserving tech so that user anonymity is upheld.

Diagram Title: Framework for AML Challenges in DeFi within the EU



2.5. Research Gaps and Rationale

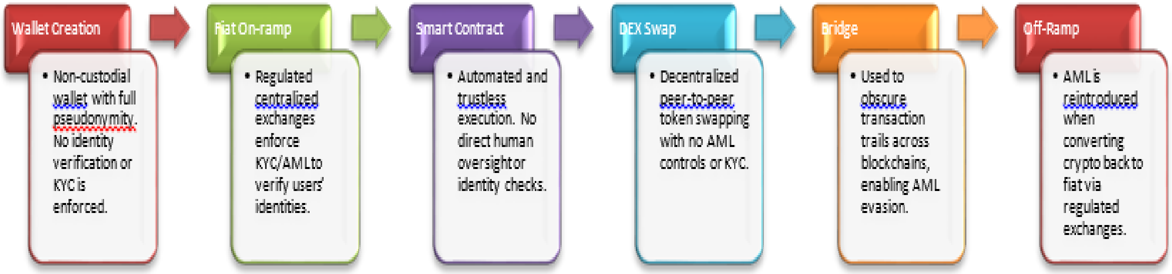
While many books and reports discuss the dangers of DeFi, it seems that there are still few studies that explore how anti-money laundering laws are applied in real life in EU law. Specifically, few case studies have looked into how new technologies fit with current laws (Schär, 2021). This article tries to overcome this issue by examining the major barriers to AML enforcement in DeFi with examples from the European Union.

3. Methodology

3.1. Research Design

A qualitative research study is used here to analyze the main problems in AML enforcement in DeFi due to difficulties from both technology and laws within the European Union (EU). Investigating processes, group relationships, and regulatory issues calls for qualitative research because they cannot always be captured by 'numbers and tables' (Creswell & Poth, 2018). DeFi is developing rapidly and bringing legal uncertainties along, which means it is necessary to consult with regulators, individuals who create DeFi apps, and legal experts to better understand the situation.

Figure: AML Vulnerability Points in a DeFi Transaction Lifecycle



Wallet Creation
- Non-custodial wallet with full pseudonymity. No identity verification or KYC is enforced.

Fiat On-ramp
- Regulated centralized exchanges enforce KYC/AML to verify users' identities.

Smart Contract
- Automated and trustless execution. No direct human oversight or identity checks.

DEX Swap
- Decentralized peer-to-peer token swapping with no AML controls or KYC.

Bridge
- Used to obscure transaction trails across blockchains, enabling AML evasion.

Off-Ramp
- AML is reintroduced when converting crypto back to fiat via regulated exchanges.

This diagram illustrates the lifecycle of a decentralized finance transaction, highlighting stages where anti-money laundering (AML) enforcement is feasible, limited, or absent.

The study explores how and why AML enforcement is challenging and prepares useful descriptions that can be used for policy guidance. Using this approach helps capture aspects such as the culture of organizations, design decisions for technology, and how people follow AML rules that play a role in the AML being carried out in the decentralized sector.

3.2. Case Study Selection and Justification

Using an approach proposed by Yin (2014), the study explores various DeFi platforms and regulations in the EU. This method allows a close examination of how AML rules are applied to situations involving decentralized protocols. Cases were chosen to meet the research needs, have plenty of data and reflect a wide range of challenge areas.

In some instances, DeFi projects are regarded as cases when they attract regulators' attention or demonstrate aspects of their technology that are difficult to track for AML, for example, self-running code or difficulties related to international transactions. The method makes it easy to consider barriers from several different viewpoints and make comparisons.

3.3. Data Collection Methods

A combination of qualitative sources is used during data collection to improve the reliability. Different types of sources are also options for this topic.

• Document Analysis:

Reports from EU groups such as the AMLA, laws such as the EU's AML Directives, and governmental policies are essential for understanding the legal system and how cases are handled.

• Industry Publications:

Developers and firms focused on cybersecurity produce white papers and technical documents that illuminate what types of technology and issues are important for AML.

• Expert Interviews:

Semi-structured conversations were held with officials, blockchain specialists, and law experts. This information comes from experts who share challenges, solutions, and changes the industry has made.

Relating data from different sources allows for confirmation of the analysis and consideration of a variety of viewpoints (Patton, 2015).

3.4. Data Analysis Techniques

The method uses thematic analysis to examine and interpret the information collected from the various sources (Braun & Clarke, 2006). For this method, we use codes to highlight patterns, themes, and classes linked to the problems of enforcing AML laws globally. Inductive analysis allows the researcher to discover ideas that come from the data, instead of already having them. Some of the issues considered in the novels are:

• Difficulties in managing blockchain because it is decentralized and grants anonymity to its users.

• Issues caused by unclear laws on the management and regulation of decentralized systems.

• Trouble resulting from differences between the GDPR data privacy guidelines and the work requirements included in AML regulations.

Regulators and technologists have employed various methods to ensure that innovations keep pace with existing regulations. These efforts involved using software to process qualitative data. Throughout the process, trust and reliability were prioritized by closely monitoring the work and collaborating with others.

Automation of Smart Contracts No Built-in Tools for Adhering to Rules Cross-Chain Anonymity Decentralized Exchanges are also referred to as DEXs. Jurisdictional Void Regulatory Arbitrage Slow development in applying laws and addressing new situations Not Many Banks Benefit from Regulatory Sandboxes Regtech is not compatible with DeFi.

Thematic Coding Table: AML Challenges in EU DeFi Regulation

Theme	Sub-Theme	Description	Key Source(s)
Decentralization	There is no real power in charge.	Since DAOs lack accountability, it is not easy to enforce rules in DeFi.	De Filippi & Hassan (2016); Zetzsche et al. (2020)
	There is a lack of clarity in how DAOs should be managed.	When a mature community votes, issues of legal liability may become less clear.	Arner, Barberis & Buckley (2017)
Pseudonymity and Privacy	Using a Wallet that does not reveal your identity	They transact by using addresses on the blockchain, not their real names.	Möser, Böhme, & Breuker (2013)
	Using tools such as mixers and PETs.	Mixers and zero-knowledge proofs hide any links to the AML process.	Goldfeder et al. (2018); Foley et al. (2019)
Legal Fragmentation	Rules for these companies are not the same everywhere.	Member States in the EU do not always apply AML laws in the same manner.	FATF (2019); Arner et al. (2016)
	No official definitions are provided by law.	Since there are no legal categories for DeFi, it becomes hard to enforce DeFi regulations.	Zetzsche et al. (2020)
Data Privacy Conflicts	Blockchain is contrasted with GDPR.	The requirement to keep data unchanged is contrary to GDPR's right to remove data.	Finck (2019); Belen- Saglam et al. (2022)
	There are challenges when trying to balance AML laws and privacy laws.	Ensuring compliance with AML means using data contrary to data privacy protection rules.	Finck (2019); Goldfeder et al. (2018)
Technological Structure	Automation of Smart Contracts	Since immutable code is unchangeable, new regulations cannot be easily applied.	Arner, Barberis & Buckley (2017); Zetzsche et al. (2020)
	No Built-in Tools for Adhering to Rules	DeFi projects are not required to have features such as KYC or risk scoring.	Schär (2021); FATF (2019)

Interoperability & Complexity	Cross-Chain Anonymity	Using token bridges adds difficulties to following transactions.	Arner, Barberis & Buckley (2017)
	Decentralized Exchanges are also referred to as DEXs.	Trading is available without having users register or being monitored.	Zetzsche et al. (2020); Schär (2021)
Enforcement Barriers	Jurisdictional Void	There are users from different countries and many different websites.	Marian (2013); FATF (2019)
	Regulatory Arbitrage	If projects move to states with fewer regulations, they may not need to comply.	Arner, Barberis & Buckley (2016); FATF (2019)

3.5. Ethical Considerations

The researchers strictly followed ethical standards during the process. All of the participants chose to take part in the research and agreed to participate only after providing their informed consent. They were provided with protection of anonymity as well as the chance to leave the research at any moment without facing consequences. Additionally, the research did not reveal any private or protected information that might put the participants or companies at risk. The data was protected and was used only for academic work. Before starting, ethical approval was obtained from the appropriate review board.

3.6. Limitations of the Study

While this technique is useful for understanding a situation in context, it still has its limits. Results of this study cannot be applied to all areas or all periods due to their non-general nature. Since both technology and regulations are developing very quickly, the information included in these insights may soon be out of date. Since blockchain uses pseudonyms, complete data on how it operates may be limited. Even so, qualitative research provides a clear understanding of the obstacles facing AML enforcement, giving helpful advice to authorities and experts working in the DeFi area in the EU.

4. Technological Barriers to AML Compliance in Decentralized Finance

4.1. The Nature of Decentralization and Its Impact

Decentralized finance leverages blockchain technology so it does not rely on centralized authorities. As a result of decentralization, the system offers transparent operations, works efficiently, and is more open to users, though it adds difficulties to enforcing AML rules. Because there is no central force in the crypto world, it is much harder for regulators to set standards and identify illicit activities (Schär, 2021).

While financial institutions must perform CDD and file suspicious activity reports, DeFi protocols rely on smart contracts to act according to the instructions they contain. The lack of oversight is possible since technology in this field is not closely watched (Möser, Böhme, & Breuker, 2013).

4.2. Pseudonymity and Anonymity in Transactions

It is hard for DeFi to comply with AML rules because blockchain transactions can remain both pseudonymous and anonymous. Users are not recognized by who they are, but instead by secure addresses. All blockchain transactions are shown, but it’s possible to link someone’s address to a real person only if they disclose it or if it’s examined through detailed analysis (Foley, Karlsen, & Putniņš, 2019).

This feature makes it difficult to spot who benefits from the funds and who pays for illegal activities. Another reason this issue is complex is that new technology, including zero-knowledge proofs and mixers, hides transaction information from view (Goldfeder et al., 2018). These PETs are being adopted in DeFi networks to protect users, but create big problems for AML since they hide most transactions.

4.3. Smart Contracts and Automated Processes

Lending, borrowing, and trading services in DeFi are handled by smart contracts that work independently. Even though automation increases efficiency, it goes on to eliminate important points where AML checks were previously included (Zetzsche, Buckley, & Arner, 2020). Since the rules in a smart contract cannot be easily modified, this makes it difficult to take quick action for AML purposes.

Furthermore, due to using code in these contracts, it takes specific skills to conduct audits and ensure they are compliant. If a smart contract is flawed or contains a weakness, the problem can be taken advantage of to carry out illegal transactions unnoticed. Since anyone can design smart contracts, it becomes tough for authorities to supervise these transactions.

4.4. Cross-Border and Interoperability Challenges

DeFi is designed to function across different nations without borders. Since financial transactions and protocols are free to move across the world, fighting money laundering in any individual nation, let alone the EU, is not easy (Arner, Barberis, & Buckley, 2017). As each country has its guidelines and rules, it is challenging to regulate against AML together. Blockchain interoperability makes it more difficult to trace transactions.

Money exchange across other networks can be made seamless with bridges or wrapped tokens, which can hide where transactions are coming from and going to. AML compliance is made more difficult due to the difficulty of regulators in keeping track of assets that are constantly active in many chains within the network.

4.5. Limitations of Existing AML Tools and Regtech

These types of tools and protocols are not suitable for use in decentralized systems. It has been found that certain Regtech solutions in blockchain analytics now group wallet addresses and uncover peculiar activities (Foley et al., 2019). At the same time, DeFi makes it challenging for these tools because of its growth, complexities, anonymity features, and because the area keeps evolving. Additionally, since DeFi platforms are decentralized, it may be difficult or undesirable for them to introduce KYC/AML checks. Since APIs and data-sharing tools are not standardized, they have limited effect when integrated into DeFi environments.

4.6. Summary

To wrap up, DeFi's main features make it significantly difficult to do proper AML compliance. As a result, old methods of control, user identification, and laws don't work well. Due to difficulties with technology, rules, and connection, new regtech tools often struggle to be applied in decentralized networks. It requires coming up with innovative regulations, having better forensics, and partnering with people involved in DeFi.

5. Legal Barriers to AML Compliance in Decentralized Finance

5.1. Regulatory Ambiguity and Fragmentation

Ensuring that DeFi follows AML regulations is difficult because there is regulatory uncertainty and differences across states in Europe. As DeFi protocols exist outside traditional legal structure, there is much confusion about what rules and laws are to govern them (Arner, Barberis, & Buckley, 2017). Without specific definitions for "decentralized exchanges," "token issuers," and even "virtual asset service providers" in place, it is difficult for AML standards to be enforced.

As a result of not understanding how laws apply, assigning legal roles to DeFi platforms is challenging because many of these platforms lack central authorities. Since member states use different strategies when regulating DeFi, there is no uniform way for anti-money laundering rules to be implemented across all nations (Zetzsche, Buckley, & Arner, 2020). With so many regulations, it is difficult to create a unified way to deal with illegal activities in DeFi.

5.2. Legal Personhood and Accountability in DeFi

Since DeFi is not centralized, it goes against normal laws that define how a person or entity is responsible for their actions. DeFi platforms are designed this way, so it is challenging to find out who should be held responsible for any regulatory violations. Regulatory bodies cannot take legal action against people involved in protocols and liquidity pools, as the involvement of anyone in these projects is anonymous.

In addition, governance relies mostly on DAOs, where people vote using smart contracts without a central authority. With DAOs, assigning accountability for AML breaches is unclear because responsibilities fall on the whole DAO community of participants (De Filippi & Hassan, 2016). For this reason, using fines or getting injunctions as remedies may not be useful when no one is certain to whom to direct them.

5.3. Challenges with Existing AML Legislation

Most AML laws are aimed at centralized financial institutions, where all records and monitoring are centralized. These concepts are called into question by the foundational

Aspects of DeFi. Financial institutions, such as banks and crypto exchanges, are obligated under existing regulations to conduct due diligence and produce reports (Arner et al., 2017).

Due to how complex some DeFi protocols are, it is hard for regulatory agencies to address them. In addition, because these financial services bypass usual traditional intermediaries, regulators find it harder to supervise the use of AMMs, liquidity pools, and yield farming (Hacker, Thomale, & Weitzner, 2021). Since KYC is not enforced on these platforms, there are many unresolved weak points in AML. With inadequate regulations, there is a danger that DeFi will become a hotspot for laundering money.

5.4. Cross-Border Enforcement and Jurisdictional Issues

Because DeFi has no borders or restrictions, it is difficult for authorities to enforce AML rules globally. Since DeFi activities can involve many different laws, it can be complex for regulators to enforce these rules across countries (Arner et al., 2017). It is difficult for EU authorities to control protocols that are located or managed outside their borders by people from different countries. Since DeFi regulations are not the same everywhere, some areas may apply weak anti-money-laundering rules, making it easier for criminals to use such countries. When potential target parties or service providers function in places where AML regulations are not strict, the EU finds it hard to enforce its rules (Zetzsche et al., 2020).

5.5. Legal Risks of Privacy-Enhancing Technologies

Applying privacy-enhancing technologies (PETs) in DeFi creates additional difficulties for legal regulations. Although PETs help ensure user safety and protection, they prevent organizations from following AML regulations due to missing trails of transactions (Goldfeder, Kalodner, Reisman, & Narayanan, 2018). European privacy rules put users first, but these rules may clash with guidelines asking banks to share sensitive data and information. Regulators should protect privacy while preventing illegal transactions, and this becomes hard when PETs hide the details of transactions. Due to this uncertainty, it is difficult to determine if these apps are legal and how to apply proper AML processes.

5.6. Summary

All in all, AML compliance in DeFi within the EU faces legal issues due to unclear regulations, different laws applied in each country, unclear responsibilities, and problems with jurisdictions. The rules designed to prevent AML are not equipped to handle the aspects of DeFi that make it difficult to trace. Additionally, understanding how privacy must be balanced with AML requirements leads to more complicated laws. For these legal obstacles to be solved, the rules need to be modified, roles and responsibilities defined, and cooperation boosted, all targeted at the decentralized financial sector.

6. Case Studies on AML Challenges in Decentralized Finance within the European Union

6.1. Protocol X: The Unruly Frontier of Decentralized Exchanges

Protocol X captures the emerging difficulties when early concepts in finance meet EU rules. Because it is a DEX, Protocol X allows people to trade assets between themselves, reducing the power of central institutions in the financial world. Meanwhile, making finance leads to difficulties in applying Anti-Money Laundering (AML) rules.

Since Protocol X does not have KYC policies in place, users can do transactions with complete secrecy, which opens the door to illegal activities. The EU's attempts to implement AML guidelines on Protocol X have been opposed by its DAO, whose members are focused on privacy and the key concept of decentralization. It illustrates that one major issue in regulation is ensuring that platforms without central control are open and accountable (Zetzsche, Buckley, & Arner, 2020).

Protocol X revealed that a decentralized system can mean much more than new technology; it led to important questions that made officials reconsider past enforcement models focused on clear entities as being responsible.

6.2. The Mixer Shutdown: Chasing Ghosts Across Borders

Many money launderers are now using mixers to make it difficult to trace DeFi transactions. All parties' digital resources are brought together, usually with no trace left that authorities can track for AML. It is clear from this example that it is difficult to enforce AML globally in the decentralized world of DeFi.

Because the mixer had shares spread among various countries, split by the mixer itself, it was difficult to take it down despite cooperation between European FIUs. Because different member states adopted their own AML rules and borders were unclear, traitors could still operate by assuming new identities and shifting onto new websites (Goldfeder, Kalodner, Reisman, & Narayanan, 2018; Arner, Barberis, & Buckley, 2017).

6.3. Synthesizing Lessons: The Complex Puzzle of AML in DeFi

The examples included in this report indicate how tough it is for AML enforcement in the decentralized finance sector within the EU. Since there is a mix of new technologies for privacy and difficulties with laws from different regions, illicit financial activities can easily find places to thrive. In addition, these cases highlight a conflict between the requirements of AML and the basic principles of DeFi. Although EU officials have improved their flexible approaches, they are not yet fully formed and at times only respond to problems.

As a result, DeFi requires regulators to integrate new laws, cooperate globally, and use innovative technology. However, if the EU does not take action, the outcome could either halt the advancement of a key technology or lead to a financial sector that is chaotic and rife with crime.

7. Regulatory Responses and Challenges in the European Union

7.1. Evolution of AML Regulatory Frameworks in the EU

The European Union has been altering its financial regulations, especially to manage the problems presented by technologies such as DeFi. After the previous Anti-Money Laundering Directives, the Fifth and Sixth Directives were introduced to include VASPs in the EU's anti-money laundering rules. Most regulations are meant for traditional financial institutions, not for DeFi, where intermediaries play a completely different role (Arner, Barberis, & Buckley, 2016; FATF, 2019).

Because the rules are not always ready as soon as new technologies emerge, there is tension in this area. While the EU tries to defend its financial system from crime, DeFi's setup removes the requirement for things like customer ID and the monitoring of transactions (Böhme, Christin, Edelman, & Moore, 2015).

7.2. Legal Ambiguities and Enforcement Complexities

Difficulties come with DeFi because these platforms are based on decentralization and anonymous internet use. Since there are no known operators or central control, assigning who is responsible for breaking the law becomes unclear. Often, those responsible for enforcing laws have difficulty deciding which country's laws apply and which agencies should investigate DeFi transactions (Marian, 2013).

It is also not clear whether DeFi players are seen as financial institutions, technology services, or whether they need a unique classification. Due to this, each EU country handles compliance differently, weakening overall regulations and making it easier for criminals to hide in certain places (FATF, 2019).

7.3. Balancing Innovation and Compliance through Regulatory Sandboxes

To support new DeFi projects while ensuring all regulations are followed, some EU member states have introduced DeFi sandboxes which help projects test their rules. As a result, regulators and innovators can collaborate which supports the creation of AML programs designed for distributed systems (Arner, Barberis, & Buckley, 2016).

Even so, their short-lived scope rules out any comprehensive guideline for the EU's business environment. For DeFi to succeed, the regulations must allow for flexibility and adapt to various services on decentralized networks (Böhme et al., 2015).

7.4. Enhancing International Cooperation

Since DeFi operates everywhere, successfully stopping AML requires coordination from countries around the world. The EU takes an active part in the initiatives of the Financial Action Task Force (FATF), which advises using a risk-based strategy for virtual assets and VASPs. FATF suggests that all countries should cooperate by using similar standards and exchanging information to block illicit activities (FATF, 2019).

Yet, since there are differing standards and enforcement abilities everywhere, it is challenging to regulate firms in the same way everywhere. To prevent money laundering in DeFi, more countries should cooperate, share intelligence, and adopt tools backed by technology (Marian, 2013; Arner et al., 2016).

8. Policy, Legal, and Technical Recommendations for Strengthening AML Compliance in DeFi

8.1. Policy Recommendations: Harmonization and Adaptability

EU policymakers should introduce common regulations against money laundering that cover the whole of Europe. Because each EU country has its own AML laws, crooks can find ways to avoid being caught. Consistent regulations require that DeFi terms and activities have the same definitions (Arner, Barberis, & Buckley, 2016).

Also, government rules should respond quickly to the continual advancements in the world of DeFi. Officials and organizations responsible for policymaking should use flexible and grounded guidelines, so they can innovate and maintain tight security against various financial crimes (FATF, 2019).

8.2. Legal Reforms: Clarifying Liability and Accountability

Having an updated legal framework is important to set liabilities in such systems with no influence on their basic standards. One way to approach AML in DeFi is to state that developers, nodes and those involved in governance have key compliance responsibilities for these requirements (Marian, 2013).

Furthermore, by signing MLATs and improving how information is shared, countries can strengthen their efforts to enforce various laws. This is necessary to solve the issues that appear in financial systems that operate without borders (Böhme, Christin, Edelman, & Moore, 2015).

8.3. Technical Solutions: Leveraging Regtech and Blockchain Analytics

It is possible to meet AML regulations using regtech while still preserving DeFi's characteristic independence. Solutions such as zero-knowledge proofs, privacy-focused identity checks, and analytical tools on the blockchain support the process of KYC and detect suspicious transactions, keeping users' privacy secure (Arner et al., 2016).

It would be wise for regulators and compliance groups to get support from blockchain analytics firms when monitoring new DeFi platforms on their own. Having access to open-source tools that work together will support increased transparency and faster enforcement of AML measures (FATF, 2019).

8.4. Collaborative Governance: Multi-Stakeholder Engagement

All regulators, technologists, businesses, and researchers must help enforce AML in DeFi. Such forums allow people to share ideas about new dangers, find common ways to address them, and design rules that suit the structure of decentralized finance (Arner, Barberis, & Buckley, 2016).

Socio-economic organizations can partner with companies to teach and remind everyone about AML obligations, encouraging more people to willingly follow them.

9. Conclusion and Future Outlook

9.1. Summary of Key Findings

The article explored the main concerns from a techno-legal standpoint that are preventing successful AML and compliance in the EU's DeFi sector. Since DeFi systems are not formally identified or regulated as other organizations are, it is hard to enforce anti-money laundering efforts in this area. The EU's efforts to improve its regulations meet resistance

due to confusing legal matters, complex steps in enforcement, and a lack of global collaboration.

9.2. Implications for Regulators and Industry Stakeholders

Regulators should ensure that new progress in the financial sector is steered safely and sensibly. For the right policies to meet the needs of DeFi, they should be structured so they can be changed easily. Reforms in the law and increased cooperation among different nations are required to stop criminals from taking advantage of loopholes.

Industry players who adopt regtech and blockchain analytics can ensure compliance does not disturb the decentralized system. For AML measures in DeFi to succeed, all stakeholders should join forces and design Effective solutions together.

9.3. Future Research Directions

Because DeFi is growing swiftly, it is crucial to keep researching new cases of money laundering and how regulations are responding to them. In the future, studies ought to examine ways to comply with regulations that do not endanger privacy, observe changes in the law as they relate to technology and measure the part played by international coordination on regulations.

9.4. Final Remarks

With decentralized finance, many can participate in financial activities while at the same time there are difficulties in managing money laundering. To deal with these issues, policy solutions should be developed across nations, the laws should be clearer, technology needs to advance and all parties must cooperate on governance. The examples set by the EU can teach others how to secure financial markets in the time of new technologies.

References

Arner, D. W., Barberis, J., & Buckley, R. P. (2016). The evolution of fintech: A new post-crisis paradigm? Georgetown Journal of International Law, 47, 1271–1319.

Arner, D. W., Barberis, J., & Buckley, R. P. (2017). Fintech and regtech: Impact on regulators and banks. Journal of Banking Regulation, 19(4), 1–14. https://doi.org/10.1057/s41261-017-0033-5

Belen-Saglam, R., Altuncu, E., Lu, Y., & Li, S. (2022). A systematic literature review of the tension between the GDPR and public blockchain systems. arXiv preprint. https://arxiv.org/abs/2210.04541

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. Journal of Economic Perspectives, 29(2), 213–238. https://doi.org/10.1257/jep.29.2.213

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Creswell, J. W., & Poth, C. N. (2018). Qualitative inquiry and research design: Choosing among five approaches (4th ed.). Sage Publications.

De Filippi, P., & Hassan, S. (2016). Blockchain technology as a regulatory technology: From code is law to law is code. First Monday, 21(12). https://doi.org/10.5210/fm.v21i12.7113

Financial Action Task Force (FATF). (2019). Guidance for a risk-based approach to virtual assets and virtual asset service providers. https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf

Finck, M. (2019). Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law? European Law Journal, 25(6), 441–462. https://doi.org/10.1111/eulj.12309

Foley, S., Karlsen, J. R., & Putniņš, T. J. (2019). Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? The Review of Financial Studies, 32(5), 1798–1853. https://doi.org/10.1093/rfs/hhz015

Gimigliano, G. (2022). Decentralized finance and anti-money laundering regulation in the EU: Challenges and perspectives. Journal of Financial Regulation and Compliance, 30(1), 25–40. https://doi.org/10.1108/JFRC-07-2021-0148

Goldfeder, S., Kalodner, H. A., Reisman, D., & Narayanan, A. (2018). When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies. Proceedings on Privacy Enhancing Technologies, 2018(4), 179–199. https://doi.org/10.2478/popets-2018-0047

Marian, O. (2013). Are cryptocurrencies super tax havens? Michigan Law Review First Impressions, 112, 38–48. https://repository.law.umich.edu/mlr_fi/vol112/iss1/4

Möser, M., Böhme, R., & Breuker, D. (2013). An inquiry into money laundering tools in the Bitcoin ecosystem. APWG eCrime Researchers Summit. https://doi.org/10.1109/eCRS.2013.6748193

Orb, A., Eisenhauer, L., & Wynaden, D. (2001). Ethics in qualitative research. Journal of Nursing Scholarship, 33(1), 93–96. https://doi.org/10.1111/j.1547-5069.2001.00093.x

Patton, M. Q. (2015). Qualitative research & evaluation methods (4th ed.). Sage Publications.

Schär, F. (2021). Decentralized finance: On blockchain- and smart contract-based financial markets. Federal Reserve Bank of St. Louis Review, 103(2), 153–174. https://doi.org/10.20955/r.103.153-74

Yermack, D. (2017). Corporate governance and blockchains. Review of Finance, 21(1), 7–31. https://doi.org/10.1093/rof/rfw074

Yin, R. K. (2014). Case study research: Design and methods (5th ed.). Sage Publications.

Zetzsche, D. A., Buckley, R. P., & Arner, D. W. (2020). Decentralized finance. Journal of Financial Regulation, 6(2), 172–203. https://doi.org/10.1093/jfr/fjaa010