Dark Side of Decentralised Finance: A Call for Enhanced AML Regulation Based on Use-Cases of Illicit Activities

Benson, V., Turksen, U. & Adamyk, B

DOI 10.1108/JFRC-04-2023-0065
ISSN 1358-1988

Publisher: Emerald

Dark side of decentralised finance: a call for enhanced AML regulation based on use cases of illicit activities

Vladlena Benson
Aston Business School, Aston University, Birmingham, UK

Umut Turksen
Faculty of Business and Law, Coventry University, Coventry, UK, and

Bogdan Adamyk
Aston Business School, Aston University, Birmingham, UK

Received 25 April 2023
Revised 14 August 2023
Accepted 11 October 2023

Abstract

Purpose – This paper aims to focus on the need for an enhanced anti-money laundering (AML) regulation for decentralised finance (DeFi) to protect the integrity of global financial systems against illicit activities. Research highlights the requirement for a robust regulatory strategy for the fast-paced DeFi evolvement.

Design/methodology/approach – This study used doctrinal legal research by analysing legislation, which involved creating use cases to illustrate different aspects of potential illicit activities via the DeFi ecosystem. Various DeFi applications were assessed for the potential regulatory responses and outcomes.

Findings – This paper offers valuable insight into the regulatory challenges presented by DeFi. This study addresses the blind spots leveraged by criminals afforded by the DeFi's decentralised nature. This paper offers a comprehensive examination of DeFi regulatory challenges based on use-case scenarios and provides recommendations for regulators on how to address them effectively.

Originality/value – This paper proposes measures for regulatory authorities to minimise money laundering risks through new channels such as decentralised exchanges, non-custodial wallets and cross-chain bridges. This study concludes with the future directions for DeFi regulation and AML compliance.

Keywords Decentralised finance, Blockchain, Cryptocurrency, AML regulation, Cross-chain bridge, Non-custodial wallet

Paper type Viewpoint

1. Introduction

Decentralised finance (DeFi) has emerged as a new financial paradigm beyond traditional financial institutions and centralised intermediaries. DeFi offers financial inclusion, elimination of intermediaries and democratic access to financial tools (European Parliament, 2022;

Funding: Research for this paper received funding from the European Union's Horizon 2020 Programme under Grant Agreement 101022004 – TRACE Project – https://trace-illicit-money-flows.eu.

Chao, 2023). Despite its benefits, DeFi presents regulatory challenges that need addressing to ensure financial systems' stability, security and resilience (Priem, 2022; Teichmann and Falker, 2021; Wang, 2022; Durham, 2023).

Criminals actively use FinTech capabilities to launder money obtained illegally and finance criminal activities (Elliptic, 2022). The cryptocurrency sphere has become a petri dish for criminals, as tracking and preventing illicit cryptocurrency transactions is challenging (Jenkinson, 2022).

We have witnessed a rise in anti-money laundering/counter financing of terrorism (AML/CFT) regulation imposing constraints on centralised crypto asset exchanges and the growing adoption of identity verification by virtual asset service providers (Ofoeda, 2022). In response, criminals resorted to unregulated, anonymous alternatives to facilitate illicit transactions. These include DeFi services that do not necessitate creating an account or submitting identity verification, thus presenting a significant risk for AML authorities (Zetzsche *et al.*, 2020).

DeFi is a growing area in the blockchain and cryptocurrency space. It refers to financial applications and services built on top of blockchain technology and operating in a decentralised and trustless form (Sharma, 2021). DeFi enables various financial transactions and activities without intermediaries such as banks or governments.

One of the primary advantages of DeFi is its promotion of financial inclusion, providing individuals and organisations with services previously inaccessible. It can be especially helpful for people in developing countries without access to traditional banking systems. Furthermore, DeFi provides greater transparency over transactions and lower costs than any traditional financial system can offer (Blockworks, 2021).

The World Economic Forum (2021) highlights the benefits of DeFi, as well as its acute challenges, including regulatory gaps, security concerns and scalability limitations.

This paper answers the calls for further research (Ofoeda, 2022; Zetzsche *et al.*, 2020) to explore the regulatory approaches and outcomes for DeFi, by gaining a better understanding of the use cases and surrounding regulatory issues. It seeks to contribute to the ongoing academic and policy debate on DeFi regulation by providing a comprehensive breakdown of key issues, trade-offs and outcomes.

This article presents a comprehensive review of DeFi regulation in the European Union (EU) and worldwide in the context of AML compliance and its future directions – such as exploring cross-chain bridge technologies, which could significantly shape DeFi regulation going forward.

The paper is structured as follows. Section 2 reviews the key literature on DeFi development and regulatory approaches. Section 3 analyses the development of DeFi, its risks and regulatory challenges. Section 4 analyses case studies of the criminal exploitation of DeFi. Section 5 offers practical recommendations for the future DeFi regulatory approach. Section 6 provides the conclusion.

2. Literature review and background to the topic

DeFi operates on blockchain technology in a decentralised, trustless manner, making it difficult for traditional financial regulators to monitor DeFi ecosystem. Thus, the regulatory landscape for DeFi remains in its early stages, with many questions left unanswered. However, during 2021–2022, hundreds of DeFi projects started (Centieiro, 2022), and regulations remains nascent and specific to the DeFi protocol and the jurisdiction concerned (Metelski and Sobieraj, 2022).

Our literature review, based on the analysis of the existing academic, regulatory and industry publications, covers DeFi protocols, articles, reports, legal documents and news releases.

"Decentralized Finance (DeFi) Policy-Maker Toolkit" by the World Economic Forum in 2021 provided an overview of the regulatory challenges facing DeFi, such as how to classify different DeFi products and services and how to apply AML and know-your-customer (KYC) regulations (World Economic Forum, 2021).

Some academics criticised certain aspects of DeFi. Allen (2022), for example, argued that precautionary regulation of DeFi is necessary to limit its growth and that DeFi innovation has limited benefits for society, while not providing new financial products and services (Allen, 2022).

Samoshin highlighted that a regulatory framework can catalyse the mass adoption of DeFi, thus suggesting that direct enforcement of such a framework may not be possible yet (Samoshin, 2022).

On the contrary, Durham (2023) suggested that current blockchain regulation approaches are impractical and would lead to impossible compliance enforcement.

It was suggested that DeFi, instead of flying under the radar of regulation, necessitates regulation to accomplish its fundamental objective of decentralisation (Zetzsche *et al.*, 2020). Moreover, they argue that DeFi presents a chance to create an entirely novel method of developing regulation, known as "embedded regulation".

An in-depth review of the relationship between cryptocurrency and blockchain engineering with law enforcement was made by Courtois *et al.* (2021). The authors reviewed cryptocurrency-related crimes and examined the use and misuse of technology in criminal activities, specifically regarding money laundering and illicit profit generation (Courtois *et al.*, 2021). They showed that many crypto users are amateur investors and that investment scams are the most prevalent form of crypto crime.

From the review of DeFi literature, it is possible to summarise the critical findings and several gaps *inter alia*:

- The regulatory landscape for DeFi is evolving and varies across jurisdictions. Researchers highlight the need for regulators to be agile and flexible in their approach to DeFi regulation, as the industry is rapidly changing.
- Researchers propose specific solutions for addressing the regulatory challenges facing DeFi, including self-regulation by the DeFi industry, the creation of regulatory sandboxes and the use of smart contracts to automate compliance.
- A crucial regulatory issue is whether and how to apply AML and KYC regulations to DeFi.
- Regulators face an additional challenge in classifying different DeFi products and services. Some regulators view DeFi as securities, whereas others have labelled it commodities or digital currencies. This distinction has ramifications for how DeFi is regulated and which regulations apply.
- Most of the research is aimed at studying the experience of highly developed countries in the field of regulation of crypto and the DeFi sphere, which narrows the range of analysis of problems associated with the DeFi sector idiosyncrasies of some emerging market countries.
- There is a need for a more coordinated and consistent global approach to DeFi regulation to ensure that the benefits of DeFi can be fully realised while also protecting consumers and preventing illegal activities.

Overall, the literature review concludes that DeFi is a growing area of interest and has the potential to revolutionise the way we use financial services. DeFi signified a new wave in the crypto market, offering decentralisation, equal access and economic freedom. However, DeFi compliance challenges are complex, rapidly evolving and pose a number of blind spots for regulators.

3. Decentralised finance development

There is no standard definition of DeFi, which on its own presents a research gap. Many researchers view DeFi as an umbrella term for all financial products and services built on public blockchains without involving financial intermediaries (Schär, 2021; Sharma, 2021; Zetzsche *et al.*, 2020). They view DeFi as an alternative to existing financial infrastructure as DeFi imitate many traditional financial transactions and services (such as lending, exchanges, saving, investing, sending remittances and insurance). The key difference is that DeFi transactions are carried out without intermediaries (Adamyk and Benson, 2023). At the heart of DeFi are smart contracts, open protocols, permissionless blockchain and decentralised applications (DApps) (Ojo/Roedl, 2021). Due to the lack of a common definition of DeFi, we suggest that DeFi can be defined as a blockchain-based financial ecosystem within the cryptocurrency space aiming to reshape and enhance traditional financial services through decentralised technologies and smart contracts by eliminating intermediaries and enhancing inclusivity.

The development of DeFi can partly solve the financial inclusion problem because only 69% of adults have bank accounts and access to banking and financial services in the world. Accordingly, 31% of adults (approximately 2 billion people) are excluded from centralised finance (World Bank, 2020). Over 1 billion unbanked adults have mobile phones with internet access, making it easy to receive banking and financial services via DeFi applications (Ofoeda, 2022).

The governance model of DeFi is based on decentralised autonomous Organisations (DAOs) (Wang, 2022). A DAO is a collectively owned, blockchain-governed organisation working towards a shared mission (Ethereum, 2022). DAOs allow any person (usually with a certain number of project tokens) to participate in governance and vote for different decisions. The DAO governance model enabled blockchain transaction evolution – from peer-to-peer to peer-to-network transactions (Wang, 2022).

All DeFi services are created using smart contracts on various blockchains. The peculiarity of DeFi operations is the absence of any national borders and the possibility for almost any person (with internet access and minimal computer knowledge) to download one of many (or several) DeFi crypto wallets for free and start using DeFi products (Adamyk and Benson, 2023).

DeFi has been in active development for about three years – starting in the second half of 2020 (DefiLlama, 2023). The first DeFi project (MakerDAO) was launched in 2015. Projects such as Aave, Compound and Uniswap were launched in 2017–2018. Nevertheless, the volume of DeFi transactions during 2015–2019 was extremely small (DefiLlama, 2023).

DeFi market capitalisation and volumes are tiny in comparison to traditional financial markets. However, the growth potential of the DeFi market is significantly greater than that of traditional finance markets. Even in 2022, a challenging year for global financial markets, the DeFi market demonstrated stability and significant development.

The year 2022 was called "crypto winter" (Archer, 2022), the consequence of which was a significant drop in the value of various DeFi assets, as well as the bankruptcy of many DeFi projects in 2022, such as the crash of Terra (Luna) and their stablecoin UST, Celsius Network, 3 Arrows Capital, Babel Finance, Voyager Digital and BlockFi.

Most DeFi protocols and decentralised applications are built on Ethereum. The Ethereum ecosystem has seen the emergence of several scaling solutions, such as Ethereum 2.0 and

layer two scaling solutions like Optimistic Rollup, which aims to improve the scalability and performance of the network, making it more usable for DeFi applications (Mart and Dempsey, 2021). Most DeFi operations were carried out on the Ethereum blockchain two years ago. Then we have seen the development of thousands of projects on various blockchains, accounting in excess of 100 to date (DefiLlama, 2023).

DeFi is a broad and rapidly evolving field, with a wide range of protocols and applications in its ecosystem. In addition to purchasing and selling various cryptocurrencies via the DeFi market, users can carry out financial operations such as yield farming, crypto staking, margin trading and liquidity mining on different distributed ledger platforms.

3.1 Decentralised finance risks

Implementing DeFi transactions involves risks that cannot be eliminated or transferred, i.e. smart contract risks, volatility risks, liquidity risks, counterparty risks, security and regulatory risks.

None of the users are immune to mistakes. Many DeFi users have little to no prior experience, resulting in a relatively high frequency of errors in such transactions (OECD, 2022). Users of DeFi protocols commonly make a variety of mistakes, including inadequate balance of native network tokens, confusion regarding token approval/unlocking mechanism, mistakenly sending tokens to an incorrect chain, lack of understanding of liquidity pool functioning and investing in tokens without conducting adequate research (1inch Network, 2021).

A significant problem area in DeFi is smart contracts. Smart contract risks refer to potential bugs or errors in a smart contract's code yielding unintended outcomes, such as financial loss. They are one of the primary concerns in DeFi projects because so many rely on smart contracts for proper functioning.

Many projects in DeFi are created quickly without properly auditing their smart contracts. As a result, there is an elevated likelihood of errors in smart contract codes. Fraudsters often use these errors and steal funds. In the first quarter of 2022, over 90% of lost funds in DeFi were related to code exploits and security breaches (Chainalysis, 2022). No code is 100% bug-free and smart contract risks can never be eliminated. However, by implementing these methods, the risk can be minimised, and the likelihood of bugs can be reduced.

To minimise DeFi risks, research and due diligence before investing in any DeFi project or product are essential. It includes comprehending the project's underlying technology and assessing the team behind it. It is also important to use reputable wallets and decentralised exchanges (DEXs) that have undergone security audits and have a good track record.

Almost complete anonymity of DeFi transaction participants makes them vulnerable to cyberattacks, hacks, scams, false and misleading or fraudulent sales. In case of theft of funds, it is impossible to recover the lost funds or prove that theft has taken place. There is no consumer protection or effective law enforcement on the anonymous market.

3.2 Decentralised finance and know-your-customer rules

DeFi is a new and unregulated market. A decentralised market also means that KYC and due diligence procedures are either not carried out at all or are carried out by specific projects voluntarily.

The client of a crypto exchange is usually identified (although there are many cases of registration of accounts on crypto exchanges with fictitious persons). For example, comparison of the possibility of opening an account on a centralised crypto exchange (Binance, Huobi, Kraken, etc.) and a decentralised non-custodial account (Metamask, Trust Wallet, Coinbase Wallet, etc.) reveals that registering accounts on a centralised exchange and opening a DeFi wallet is equally easy. It takes a few minutes. However, there are

differences. Usually, most centralised crypto exchanges (especially those registered in the USA and the EU) will allow you to carry out any operations (funding, withdrawal, trading operations, etc.) only after passing the proper KYC procedure. At the same time, going through the KYC procedure in centralised crypto exchanges often is not much different from the same procedure in banks.

The opposite is the case with DeFi crypto wallet registration. In most cases, no customer identification procedure is applied. To register, a customer only needs to create a password (preferably a complex one) and remember a seed phrase (12–24 random words). Usually, this is enough to create a DeFi wallet and carry out the relevant functions. However, most wallets do not even ask for email verification or other contact details (e.g. mobile phone number or address). A person can create many crypto wallets (the main thing is to remember the passwords and seed phrases, otherwise, access to the funds will be lost entirely). With the help of DEXs [1] or different DeFi lending and borrowing platforms [2], you can carry out almost any operation on the crypto market (Adamyk and Benson, 2023).

It is not easy to track transactions from many unverified DeFi wallets. Of course, one can view all the transactions made by having the wallet address. This information is public. However, it is complicated to prove who exactly carried out these transactions, mainly if criminals use different blockchains, crypto-mixers [3] and/or open new DeFi wallets every time to carry out transactions. Such soft-touch vetting processes are attractive to criminals.

3.3 Decentralised finance regulation: anti-money laundering challenges

Regulatory bodies and central banks in many countries (in particular, in the USA, the EU Member States and the UK) have begun focusing on the DeFi market and those potential negative challenges that DAOs and anonymous DeFi market participants create for governance and oversight.

Several measures have been proposed by the EU Commission to regulate digital assets and prevent their misuse for money laundering and terrorist financing activities (Priem, 2022). These measures include the Sixth Anti-Money Laundering Directive (6AMLD), which requires crypto-asset service providers to register with national authorities, adhere to AML regulations and report suspicious transactions. In addition, the EU has proposed a set of rules known as the Markets in Crypto-Assets (MiCA) Regulation, which seeks to create an oversight framework for crypto assets that includes regulations for issuers, service providers and secondary market participants (European Parliament, 2022).

MiCA ensures crypto-assets' traceability while providing a regulatory framework for digital asset businesses for the first time. This legal document establishes a uniform field of activity and regulates the operations of various players in the cryptocurrency market (crypto exchanges, issuers of crypto assets, virtual assets service providers). The new MiCA regulations are expected to go into effect in 2024, following a final agreement in April 2023. Due to its lengthy legislative process and rapid developments in the virtual and assets market, MiCA still requires reform even though it has not yet taken effect. For instance, its rules do not address some recent innovations like DeFi and non-fungible tokens (NFTs) [4] (Kafteranis and Turksen, 2021).

The decentralised nature of DeFi platforms and a central entity absence pose a potential challenge. The proposed MiCA regulation does not explicitly mention DeFi. However, proposals to indirectly address it by enforcing rules that apply to stablecoins are considered, which are necessary for executing DeFi protocols, and regulating digital asset service providers (Eurofi, 2022).

Regulatory bodies made significant progress in creating a legal framework for regulating transactions with crypto assets for centralised intermediaries (6AMLD, Travel Rules, MiCA rules). There are multiple examples of fines being levied against centralised crypto market

participants. In 2021, the crypto exchange BitMex agreed to pay a $100m fine to settle charges with the Financial Crimes Enforcement Network. BitMex failed to maintain AML controls and procedures and was found to have facilitated over $209m in illegal transactions within darknet markets and unregistered money service businesses (Kyckr, 2021).

European regulators have begun to apply fines to unlicensed crypto exchanges. Binance, the world's largest cryptocurrency exchange, was fined €3.3m by the Dutch Central Bank for providing financial services, maintaining digital wallets and handling cryptocurrency-denominated transactions in the country without authorization. Binance received a fine in April 2022 for failing to register for AML purposes from May 2020 to December 2021, despite being warned multiple times (Couvée, 2022).

It is worth noting that sanctions are mainly applied to those institutions in the crypto assets market that are registered in the USA or the EU. Centralised cryptocurrency exchanges frequently relocate to jurisdictions with less stringent regulatory frameworks, such as the Bahamas, Malta and the Virgin Islands, to exploit lax regulations and maximise profits, potentially at the expense of consumer protection (Chao, 2023). Typically, many big crypto exchanges are registered (re-registered) in countries with liberal crypto market regulation, such as Bahamas (FTX), Seychelles (Huobi, Kucoin, OKX, MEXC), Bermuda (Bittrex), Malta (Crypto.com), Virgin Islands (Bitfinex, BKEX) and Cayman Islands (Binance, BitMart, Latoken) (CryptoCompare, 2023). That is one of the reasons why sanctions for AML/CFT violations are difficult to apply to that cryptocurrency exchanges.

While noting the progress made in regulating centralised crypto markets, we also observe a notable absence: regulations for DeFi transactions still need to consider anonymity and the absence of intermediaries. While all DeFi transactions involving cryptocurrencies are governed by rules applicable to centralised intermediaries, none of these specifics (anonymity and absence of intermediaries) are considered. Because DeFi transactions are usually anonymous, it is pretty challenging to create a legal framework (Adamyk and Benson, 2023) and determine to whom to apply sanctions if the DeFi market projects do not have legal registration.

The regulators are faced with a severe problem – the modern system of regulation (centralised finance) provides for the presence of certain intermediaries whose activities are regulated and who are required to control their clients' transactions. Regulating centralised crypto exchanges followed a similar path, with requirements becoming similar to those applied to banks – particularly regarding AML.

The DeFi market is decentralised and global. Its participants do not interact with any centralised financial institutions. The DeFi ecosystem can rarely interact with traditional finance. At the same time, the participants of the DeFi ecosystem are anonymous. They do not need to identify themselves.

For regulators, the anonymity of transactions is a significant problem. In the case of DeFi transactions, it is practically impossible to block user accounts that have received suspicious funds. For example, if such funds were received because of an exchange (swap) on decentralised platforms (DEXs), the recipient does not know from whom he received the funds. Even if she/he wanted, the account holder could not indicate from whom he received the questionable funds. Accordingly, bringing the recipient to justice is impossible, and there are no legal grounds to block his account.

4. Case studies of criminal exploitation of decentralised finance

Criminals can use DeFi to launder their proceeds of crime by converting them to other assets or obscuring the blockchain transaction history without the need for centralised intermediaries that could attract law enforcement or confiscate their funds.

Due to the interdependency of different DeFi protocols, monitoring and tracing transactions across them can take time and effort. Some DeFi protocols, such as privacy-centric ones, make it difficult for authorities to track and trace transactions. Smart contracts can automate financial processes, making it harder for authorities to detect and prevent money laundering. Furthermore, because DeFi protocols and applications are accessible worldwide, applying AML regulations across different jurisdictions becomes challenging.

Criminals often use multiple DApps, like money laundering methods with traditional financial instruments (Teichmann and Falker, 2021). This is the "layering" step of the money laundering process, adding complexity to transactions to trace illicit funds. Although the transparency of blockchain can enable the tracing of funds through DApps, it can be technically challenging, mainly when multiple intricate DeFi protocols are utilised.

4.1 Methodology

This study used a use-case-based approach, which involved creating hypothetical use cases to illustrate different aspects of potential illicit activities via DeFi ecosystem. The use cases were chosen to represent various DeFi applications and then assessed regarding potential regulatory responses and outcomes.

When considering the potential effects of DeFi regulation, it is essential to consider all stakeholders involved in the ecosystem. These include DeFi users, developers and platforms, regulators and members of the broader financial community. Each group has distinct objectives and incentives; therefore, regulations will impact each group differently.

These use cases were created based on expert opinions, published research and current market trends. They are not exhaustive or prescriptive but provide a basis for exploring potential regulatory outcomes in the DeFi sector.

4.2 Use cases of illicit activities using decentralised finance

The blockchain's transparency allows law enforcement to trace the movement of criminal proceeds from wallet to wallet, making "follow-the-money" a more effective technique than traditional payment methods without transaction records. In many cases, criminals have been caught by tracing their crypto transactions to regulated service providers like exchanges, which are subject to AML regulations and must verify customers' identities, connecting crypto transactions to individuals. The growth of DeFi has made money laundering easier for criminals.

Illicit activities, such as money laundering and fraud, can be used in DeFi in several ways. One potential method is using anonymous or pseudonymous transactions on decentralised platforms, which can make it difficult to trace the origin of funds. In addition, DEXs may be vulnerable to wash trading, front running and other manipulative practices. Furthermore, smart contracts deployed in DeFi could be exploited by hackers to steal funds or used to launder money through complex transaction flows. Illicit actors can also use DeFi platforms to set up Ponzi schemes, where they lure investors with promises of high returns but use the funds from new investors to pay off earlier ones.

Criminals used to convert stolen tokens at centralised exchanges, but regulations now require crypto service providers to verify customers' identities and perform AML checks. DEXs do not impose restrictions or keep records of user identities, making them an attractive option for criminals nowadays. It has driven criminals to DEXs to convert tokens to native assets.

All users must be aware of these risks and take appropriate precautions, such as using reputable DeFi platforms and practising good "security hygiene" when using decentralised applications.

4.3 Use case: money laundering via creating fake initial decentralised exchange offerings

Money laundering through false Initial DEX Offerings (IDO) [5] and fake cryptocurrencies involve using these fraudulent investment opportunities to launder illicit funds and make them appear legitimate.

It is often accomplished by creating a false cryptocurrency or token and promoting it through a fake IDO. Criminals then use these fake investment opportunities to launder money through multiple accounts and transactions, making it difficult to trace its source. To further obscure matters, criminals may create webs of shell companies and offshore accounts to obscure where the cash came from. Eventually, however, this laundered cash may be transferred back into an "official" account, giving the appearance that it came from legal sources.

Money laundering through the fake IDO creation involve the following steps:

(1) A criminal obtains illegal funds through illegal activities like drug trafficking or embezzlement.

(2) The criminal then creates and launches their new cryptocurrency with false details to raise capital from investors.

(3) Criminals use illicit funds to manipulate the price of a new cryptocurrency, giving off the false impression of imminent success for their initial coin offering (ICO).

(4) The criminal then proceeds to sell the newly created cryptocurrency to third-party investors, using the proceeds to launder illicit funds by transforming them into legitimate assets.

(5) Third-party investors may not be aware of criminal activities and mistakenly think they are investing in a legitimate IDO and cryptocurrency, unaware that the funds used to create and promote them were obtained illegally.

(6) Criminals can use the proceeds from selling cryptocurrency to purchase other assets or make further investments, making it difficult for law enforcement agencies (LEAs) to track where the money comes from.

(7) In addition, criminals can create multiple fake IDs and cryptos and sell them to various investors, creating an intricate web of transactions that are difficult to trace.

The cost of creating a smart contract and IDO for a new cryptocurrency can vary greatly depending on several factors, such as the complexity of the smart contract, the platform it is built on (Ethereum, BSC, Polygon, Solana, etc.), and the services needed to launch and market the IDO.

The cost for a simple smart contract and IDO launch can range from several thousand dollars to tens of thousands for more complex projects that include full marketing and promotional services. Many internet platforms provide free tools to create smart contracts. Binance Smart Chain, for instance, provides the Binance Academy development environment (Binance Academy, 2020).

We should mention that the cost is only one of the aspects of creating a successful cryptocurrency and IDO. There are other factors to consider, such as market research, community building and regulatory compliance, which can hugely impact the overall success and cost of the project.

4.4 Use case: hiding tails of illicit money via cross-chain bridges

The integration of blockchains has been a prevalent trend in recent years, with advancements in DEXs and cross-chain bridges significantly reducing the impediments to

the seamless transfer of capital across various crypto assets. However, these technologies have also been exploited for illicit purposes, such as money laundering activities by ransomware groups and hackers. These entities are using DeFi systems to anonymously transfer billions of dollars in crypto, thereby obscuring the illicit nature of their financial flows (Jenkinson, 2022). The lack of identity verification procedures in some DeFi services exacerbates the "cross-chain problem" that affects all virtual asset services. Using DEXs, cross-chain bridges and coin swap services by criminal and high-risk entities has obfuscated more than $4bn worth of illegal cryptocurrency proceeds since 2020 (Elliptic, 2022).

Approximately $1.5bn worth of illicit crypto assets processed by DEXs and cross-chain bridges are associated with entities the USA has sanctioned. A significant portion of this amount, approximately $972m, is attributed to Tornado Cash (Elliptic, 2022). Tornado Cash, the most widely used decentralised mixer on the Ethereum network before being subject to US sanctions, facilitated the laundering of $1.54bn in confirmed illicit funds, with $1.04bn of the total amount stemming from reported thefts (Elliptic, 2022). Other notable sources of illicit sanctioned assets include exchanges such as SUEX, Chatex, Garantex, the dark Web marketplace Hydra and the Lazarus Group, a state-sponsored cyber-hacking group operating out of North Korea (Elliptic, 2022).

Cross-chain bridges are technologically sophisticated applications that facilitate transactions across various blockchain networks. They play a crucial role in enabling the transfer of cryptocurrencies, NFTs and other digital assets between different blockchain networks. With cross-chain bridges, inter-blockchain transactions are possible.

The utilisation of bridges is often observed in conjunction with DEXs, as criminals frequently require inter-blockchain token swapping before conversion on bridges. It can result from the unavailability or high cost of a specific trading pair, making direct chain-hopping unfeasible due to insufficient liquidity.

Once criminal funds are converted to a different token or bridged to a different blockchain, their trail becomes obfuscated. Attempting to trace them across tokens or blockchains demands manual investigation, often proving unfeasible or unsuccessful.

Despite cryptocurrency transactions being recorded on a public ledger (which makes it possible for anyone to trace the movements of coins and tokens), this is a challenge for people who may want to obscure the origin and destination of their transactions for various reasons. One of the latest possibilities to "solve this problem" is to use cross-chain bridges, often used by money launderers to conceal their tracks. In our following use-case example, we will describe the steps involved in hiding the tails of a cryptocurrency transaction using a cross-chain bridge.

Hiding tails of illicit money via cross-chain bridges refers to transferring digital assets from one blockchain to another, intending to hide the origin or destination of the funds. This process typically involves the following steps:

(1) The first step is setting up a wallet on the source blockchain, where the funds will be transferred. This wallet can be set up on a centralised or decentralised exchange, depending on the level of anonymity desired by the user.

(2) Next step – the individual obtains the cryptocurrency assets through illegal means, such as hacking, theft or fraud, to their crypto wallet.

(3) The received crypto assets are converted to cryptocurrencies not directly associated with illegal activity, all within the same blockchain network as usual.

(4) The user transfers their new crypto assets to a non-custodial wallet and trades them through DEXs such as Uniswap, dYdX or Curve Finance. They exchange these funds for another cryptocurrency like Ethereum, BNB or Polygon using

a smart contract, which automatically executes the trade based on market price.

(5) The next step is creating a non-custodial wallet on the destination blockchain. The funds need to be transferred there. Users must have accounts on both networks and possess private keys for logging.

(6) The individual transfers assets to a suitable cross-chain bridge, such as Synapse Bridge, Binance Bridge or Multichain Bridge (Howell, 2023). It may be done through standard cryptocurrency transfer procedures.

(7) After transferring crypto assets to the cross-chain, we need to convert them to another asset. Cryptocurrencies should be exchanged for the native token of the cross-chain bridge, which can then be quickly transferred to another blockchain through this intermediary.

(8) Once a cryptocurrency has been converted to a token, the next step is to transfer it onto another blockchain. It can be done by sending the token directly to someone's wallet on the destination. Verifying and broadcasting this transfer may occur on both networks before automatic conversion to the original cryptocurrency occurs on the destination blockchain.

(9) The next step is confirming the transaction. Waiting for confirmation helps guarantee an irreversible transaction. After these funds have been accessed, they can be used for various purposes like trading or transferring to another network.

(10) The last (desired for criminals) step is incorporating crypto assets into a legitimate banking system. It can be done by exchanging crypto assets for stablecoins or fiat currencies like US$ and depositing the money into a bank account.

Hiding the source of a cryptocurrency transaction can be an intricate process, but it is possible through cross-chain bridges. By following the steps outlined in this example, criminals can obscure the origin and destination of their transactions.

Tracking the tails of crypto via cross-chain bridges is a serious challenge for LEAs. Measures addressing its causes should be implemented to prevent cross-chain money laundering. Firstly, DEXs must increase their transparency and make it simpler for LEAs to monitor and trace funds' movement.

Secondly, it is imperative to bolster the security of DEXs and make it harder for money launderers to exploit them. It can be accomplished with multi-signature wallets, which require multiple users to approve transactions before they go live.

Thirdly, enhancing the interconnection and interoperability between different blockchain networks is essential. Doing so will make it more challenging for money launderers to move funds between chains, as LEAs can track funds' movement between blockchains. To accomplish this goal, standards and protocols that facilitate asset transfers between chains must be created.

5. New decentralised finance regulation approach

DeFi market functions without financial intermediaries and mostly anonymously, and regulatory bodies need to radically change the approach to building a regulatory framework.

The EU's MiCA rules are a progressive document regarding the regulation of the activities of the participants of the centralised crypto market. However, this legal instrument does not consider the DeFi market regulation. It is tricky to unambiguously interpret the

legal norms introduced in the MiCA regarding the prohibition of the issuance of cryptocurrency if the issuer does not have legal status or license (Eurofi, 2022).

For DeFi projects, such norms, most likely, cannot be applied. Most DeFi projects do not have a specific governing body to which MiCA regulations can be applied. Management in most DeFi projects is carried out collectively by small anonymous ownership of governance tokens. There is no such single governing body. Therefore, it is practically impossible to apply the provisions of the MiCA in this case.

However, not all DeFi projects are decentralised. Certain EU regulators have raised doubts regarding the authenticity of the decentralised nature of DeFi platforms, as some are currently operated by a central development team and follow standard governance guidelines in most cases (Eurofi, 2022).

In our opinion, in such a scenario, the owners of significant participation in the DeFi projects will try to veil their significant influence on the management of the project as soon as possible. Their votes will be dispersed among many anonymous holders of management tokens.

5.1 Self-regulatory approach to decentralised finance

Considering all the problematic aspects of DeFi market regulation, it can be opined that promoting voluntary standards for DeFi market participants is one of the first steps. A voluntary regulatory framework for DAOs might be a good approach.

Introducing specific self-regulatory standards for DeFi market participants (DApps developers) is essential. Such standards should be introduced primarily to protect market participants, not for regulatory purposes. For example, standards for capital, standards for integrity and openness of operations, standards for the quality and security of smart contracts and standards in auditing.

There are recent positive examples in the field of centralised crypto exchanges. In particular, after the collapse of the FTX crypto exchange (one of the reasons for the collapse was the use of customer funds to carry out their risky operations, which undermined trust in centralised exchanges and caused the outflow of funds to DeFi wallets), other market participants (Binance, KuCoin, OKX, etc.) independently initiated the creation of reserve funds and disclosed information about the formed level of reserves with the possibility of their control by clients (Malwa, 2022).

DeFi project developers can independently raise the standards of the DeFi market. Developers can independently include in their software programmes the need to undergo KYC and due diligence for their clients and the possibility of checking compliance with AML/CFT requirements.

There are many examples of using the KYC procedure by DeFi platforms. For example, launchpad DeFi platforms DAO Maker, Polkastarter, BSCPad and others have established KYC procedures for all their clients (DAO Maker, 2023). In our opinion, such a step increases participants' trust in their projects and allows these launchpad platforms to reduce the possibility of participating in their projects for illicit activities.

Many DeFi platforms use the services of specialised organisations that conduct the KYC procedure. For example, Blockpass Identity Lab explores ways blockchain technology can protect personal data by providing utilities that include embedded identity, reputation collateral and proof of liveness (Blockpass, 2023).

We suggest that introducing specific standards for the DeFi market will positively affect not only the developers of DeFi programmes but also all market participants. In most cases, a DeFi project will develop better if it conforms to generally accepted industry standards.

Bona fide market participants will not worry that their accounts may be blocked or compromised.

5.2 Loopholes in current decentralised finance regulations

DeFi raises concerns about possible illegal activities. As such, regulators must maintain oversight of the DeFi industry and implement additional regulatory measures in the future to protect consumers and ensure that DeFi is safe and legal.

After conducting our research, we have identified specific loopholes in the current regulation of DeFi in many countries, including the EU, UK and USA. These loopholes include the following:

- Jurisdictional challenges: DeFi and NFTs transactions can take place across borders. It is challenging for regulators to enforce regulations in a cross-border context fully.
- DEXs: The activity of DEXs is not under the oversight of regulators. DEXs are not operated by a central authority, making it difficult for regulators to monitor and regulate them.
- IDOs: Regulators have not issued specific guidance on regulating IDOs. It would likely be subject to the same regulatory framework as ICOs. The nature of IDOs and how they are promoted through decentralised platforms make them challenging to regulate fully.
- Lack of specific regulations: The EU, UK and the USA have not yet established legislation for DeFi and NFTs activities. It may create uncertainty for businesses in this sector and a regulatory gap that bad actors could exploit.
- Lack of custody and insurance: DeFi and NFTs protocols mostly do not have a custodian to hold assets. Some do not have insurance to cover users' assets in case of a hack or other security breaches.

We believe that an essential step in improving the regulation of DeFi should be to develop a complex regulatory framework for Defi. A lack of guidelines and a regulatory framework for DeFi lead to uncertainty for developers, investors and users. The regulatory authorities should establish clear guidelines for DeFi project developers, outlining what is and is not allowed.

DeFi operates on a decentralised basis, and the jurisdictional challenges can make it difficult for regulators to monitor and enforce regulations effectively. For example, most DeFi platforms function in multiple jurisdictions (often globally) with differing regulations. It can exploit the gaps between these jurisdictions to avoid compliance with particular rules. It might also implicate routing transactions via jurisdictions with more lenient regulations or establishing the platform in a jurisdiction with limited supervision of DeFi activities. DeFi platforms could exploit these jurisdictional mismatches by boosting their services to users from tightly regulated countries, technically registered in jurisdictions without regulations. These jurisdictional contrasts can make it difficult for regulators to effectively monitor and enforce regulations, allowing some DeFi platforms to operate in a legal grey area. That is why international co-operation and creating a global regulatory framework for DeFi operation is essential. Regulators should foster international co-operation to ensure that DeFi regulations are consistent across borders and to mitigate cross-border risks.

The regulation of DeFi platforms with many users, such as DEXs and lending platforms, is currently limited. However, the risks to ordinary users of such platforms are significant. Regulators should focus their efforts on key players in DeFi to protect consumers. They

should suggest international licensing rules and a standard registration process for DeFi projects and platforms. Regulators should continuously monitor and evaluate the effectiveness of regulations and adjust as necessary to ensure that they are serving their intended purpose.

There is currently a lack of consumer protection in the DeFi space, and consumers may be at risk of losing their investments or becoming victims of fraud. Regulators should create a dedicated task force to monitor and enforce DeFi regulations. They should guide projects and platforms on how to comply with regulations.

One of the primary important steps is to promote DeFi education and awareness. Governments and regulatory authorities should promote education and awareness about DeFi, to help ensure that consumers are informed and able to make informed decisions about participating in the DeFi ecosystem.

5.3 A proposal for effective decentralised finance regulations

Based on our research, a number of practical recommendations for improving DeFi regulation while providing sufficient space for the sector to grow and innovate are offered.

We believe that an essential step in improving the regulation of DeFi would require a robust regulatory framework for DeFi.

The top developed countries around the world are known for being financial power hubs, with a long-standing tradition of pioneering new financial services. As DeFi continues to grow and DeFi applications and platforms become more commonplace, these nations can position themselves as leaders in regulating this rapidly developing sector.

Our research indicates that the regulatory approach in EU, the UK and the USA towards DeFi is generally technology-neutral, cautious and risk-based. It does not seek to stifle innovation within the sector but instead ensures projects adhere to existing regulations without endangering financial stability or consumers. *n* addition, it's worth noting that regulatory authorities are actively working to establish and enhance a dedicated regulatory framework for DeFi.

That is why we suggest that regulators should take a "balanced approach" to DeFi regulation, balancing the need to support innovation and experimentation in the DeFi ecosystem with the need to mitigate its potential risks and negative impacts. This approach should cover minimum licensing requirements combined with disclosure obligations to ensure transparency regarding the operations and risks of DeFi platforms and their users.

We propose to mandate DeFi platforms (especially DEXs) to incorporate fundamental AML and KYC measures, to prevent the funding of illicit activities and safeguard against money laundering. It should entail providing guidance and assistance to DeFi platforms in the implementation of such measures, and in complying with other regulatory obligations, such as data privacy and consumer protection.

Regulators should create a regulatory sandbox for DeFi and NFT projects, similar to the one the UK Government has for fintech start-ups. It would allow projects to test and refine their products in a controlled environment before launching to the public. DeFi and NFT start-ups can test their platforms and products in the sandbox while receiving guidance and oversight from regulatory experts. The experts can review the project's smart contracts and risk management processes to ensure they align with regulatory standards before full-scale deployment. This proactive evaluation helps identify vulnerabilities that might have gone unnoticed in a real-world launch. DeFi and NFT projects that successfully complete the sandbox phase could enhance market confidence and attract more investors and users. Sandbox can also be a great educational environment for regulators and DeFi teams. As DeFi is an emerging technology, regulators can gain insights into the technology

complexities enabling more informed policymaking. Collaboration between policymakers and DeFi project teams can lead to innovative regulatory approaches needed for the unique decentralised nature of the DeFi ecosystem.

Establishing a precise definition and legal classification of crypto assets is essential. Doing so will create an organised regulatory framework for these assets, providing investors with more protection.

Establishing an equitable tax framework for DeFi will bring transparency to the DeFi participants' taxation and spur growth within the DeFi ecosystem, guaranteeing all stakeholders involved contribute their fair share of taxes.

In the DeFi sector, it is essential to set standards for projects to adhere to, ensuring their reliability and trustworthiness for investors. Protecting consumers from fraud and other misconduct within cryptocurrency is paramount. Although some may view mandatory compliance controls as inconvenient or counter-intuitive to DeFi's philosophy, such measures are crucial and will ultimately benefit the sector.

DeFi requires stringent cybersecurity regulations to shield its users from hacking and other cyberattacks. All entities operating within this sector should take appropriate steps for protection against these risks.

It is worth emphasising that the balanced approach to DeFi regulation should not be viewed as a uniform solution, but rather as a versatile and adaptable framework that can evolve alongside the changing needs and circumstances of the DeFi ecosystem. Regulators must be willing to modify and adapt their approach as the DeFi ecosystem evolves and matures, to ensure that the regulatory framework remains adequate and relevant.

Governments, regulators and the industry are still grappling with how best to assess DeFi's potential and associated risks. Countries such as the EU, UK and USA are working on closing regulatory loopholes related to DeFi. We hope our research and proposals will contribute to creating a comprehensive regulatory framework for DeFi space that considers innovations, consumer protection and AML concerns.

6. Conclusions

The DeFi ecosystem presents a complex challenge for regulators as it operates in a decentralised manner and outside of traditional financial systems. The advent of regulatory initiatives specific to DeFi has recently emerged. However, notable advancements have not been achieved.

This study aimed to provide a use-case-based analysis of potential illicit activities via DeFi protocols and suggest regulatory approaches and outcomes in the DeFi space to minimise the possibility of money laundering and other illicit activities in DeFi. We identified specific gaps in the current regulation of DeFi and proposed measures to minimise the risks of money laundering through new channels such as DEXs, non-custodial wallets and cross-chain bridges.

The study highlights the importance of collaboration between regulators and DeFi stakeholders to achieve a "suit-for-all" ("balanced") regulatory approach. It may involve creating a common understanding of the DeFi ecosystem, its risks and benefits, and the most appropriate regulatory responses. Regulators should focus on promoting transparency and compliance with basic DeFi platform standards. It may include enforcing AML/KYC requirements, minimum licensing standards, open transaction records, disclosure obligations and upholding security protocols. Implementing a "balanced" regulatory approach to DeFi regulation can have numerous advantages for developers and users of the technology, including increased innovation and experimentation opportunities, lower entry barriers for new or smaller platforms and some level of consumer protection for all DeFi

users. This safeguard helps mitigate risks associated with DeFi and provides necessary protection in case of fraud or other negative outcomes.

DeFi regulation is a complex and rapidly evolving area, and the most effective approach to regulation should consider the needs of all stakeholders. DeFi regulation's success will depend on regulators' ability to collaborate with DeFi stakeholders and adapt to the evolving DeFi ecosystem. By prioritising the critical principles of market fairness, financial crime deterrence, safety and stability, regulators and industry stakeholders have the potential to form a productive partnership, fostering the continued growth of the DeFi sector while ensuring consumer protection and effectively mitigating financial crimes.

Notes

1. DEXs are blockchain-based platforms that offer trading and liquidity for digital assets, enabling users to buy and sell cryptocurrencies and other digital assets without needing a centralised intermediary.
2. DeFi lending and borrowing platforms enable users to lend and borrow digital assets with the use of smart contracts, automating the process and eliminating the need for trust in centralised intermediaries.
3. Crypto-mixers are service that blends many users' cryptocurrencies to obfuscate the funds' origins and owners. Cryptocurrency mixers create a complex transaction network that obscures the funds' original sources and owners. This process enhances privacy and makes it difficult to trace the origins of the funds.
4. NFTs represent assets tokenised on a blockchain with distinct codes and metadata separating them from other tokens. NFTs are tradable for money, cryptocurrencies or other NFTs. Their exchange value hinges on market perception and owner assessment.
5. IDO is a decentralised crowdfunding method used by blockchain projects to introduce their native tokens through a DEX. This approach involves raising investment capital from individual investors, facilitated by liquidity pools and smart contracts on a DEX platform. IDOs are an alternative to ICOs, enabling new cryptocurrency projects to launch tokens. In both ICOs and IDOs, participation is open to all, involving providing liquidity to receive tokens in return. IDOs are recognised for their decentralisation, user-friendliness, accessibility and liquidity benefits.

References

1inch Network (2021), "Top 5 most common user mistakes in DeFi", available at: https://blog.1inch.io/top-5-most-common-user-mistakes-in-defi-273001aeafc3 (accessed 7 March 2023).

Adamyk, B. and Benson, V. (2023), "DeFi regulation in the EU: should we act now?", available at: https://trace-illicit-money-flows.eu/defi-regulation-in-the-eu-should-we-act-now/ (accessed 3 February 2023).

Allen, H.J. (2022), "DeFi: Shadow Banking 2.0?", available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4038788 (accessed 23 March 2023).

Archer, C. (2022), "Crypto winter: a simplified precis of 2022", available at: www.ig.com/en-ch/news-and-trade-ideas/crypto-winter–a-simplified-precis-of-2022-221215 (accessed 12 March 2023).

Binance Academy (2020), "An introduction to binance smart chain", available at: https://academy.binance.com/en/articles/an-introduction-to-binance-smart-chain-bsc (accessed 16 March 2023).

Blockpass (2023), "White paper: identity for a connected world. A user centric identity application for regulated industries and the internet of everything", available at: https://storage.googleapis.com/blockpass-website-media/wp-content/uploads/2018/09/Blockpass-Whitepaper-v1.3.3.pdf (accessed 5 March 2023).

Blockworks (2021), "Goldman Sachs: DeFi has its advantages over traditional finance", available at: https://blockworks.co/news/goldman-sachs-defi-has-its-advantages-over-traditional-finance (accessed 7 March 2023).

Centieiro, H. (2022), "Defi ecosystem landscape report", available at: https://capital.hashkey.com/viewerjs-0.5.8/documents/en/capital_insight/HashKey%20Capital%20-%202022%20DeFi%20Ecosystem%20Landscape%20Report.pdf (accessed 2 March 2023).

Chainalysis (2022), "Hackers are stealing more cryptocurrency from DeFi platforms than ever before", available at: https://blog.chainalysis.com/reports/2022-defi-hacks/ (accessed 5 March 2023).

Chao, W. (2023), "Crypto exchange's jurisdiction-shopping: a regulatory problem that requires a global response", *Columbia Journal of Transnational Law*, February, www.jtl.columbia.edu/bulletin-blog/crypto-exchanges-jurisdiction-shopping-a-regulatory-problem-that-requires-a-global-response (accessed 8 March 2023).

Courtois, N.T., Gradon, K.T. and Schmeh, K. (2021), "Crypto currency regulation and law enforcement perspectives", *ArXiv*, doi: 10.48550/arXiv.2109.01047, (accessed 8 March 2023).

Couvée, K. (2022), "Binance lands €3.3 million AML penalty in the Netherlands", available at: www.moneylaundering.com/news/binance-lands-e3-3-million-aml-penalty-in-the-netherlands/? (accessed 8 March 2023).

CryptoCompare (2023), "Compare all bitcoin exchanges, reviews, live streaming bitcoin prices, fees, deposit methods", available at: www.cryptocompare.com/exchanges/#/overview?f2=Centralized (accessed 8 March 2023).

DAO Maker (2023),), "Upcoming crypto projects and IDOs: Dao maker", available at: https://daomaker.com/launchpad (accessed 10 March 2023).

DefiLlama (2023), "Total value locked all chains", available at: https://defillama.com/chains (accessed 10 March 2023).

Durham, J. (2023), "Regulatory sandboxes enable pragmatic blockchain regulation", *Washington Journal of Law, Technology and Arts*, Vol. 18, 1, available at: https://digitalcommons.law.uw.edu/wjlta/vol18/iss1/3 (accessed 28 February 2023).

Elliptic (2022), "The state of cross-chain crime 2022: elliptic", available at: https://hub.elliptic.co/reports/the-state-of-cross-chain-crime-2022/ (accessed 10 February 2023).

Ethereum (2022), "Decentralized autonomous organizations (DAOs)", available at: https://ethereum.org/en/dao/ (accessed 10 February 2023).

Eurofi (2022), "Decentralised finance", available at: www.eurofi.net/current-topics/decentralised-finance/ (accessed 8 March 2023).

European Parliament (2022), "Markets in crypto-assets (MICA)", available at: www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)739221 (accessed 10 February 2023).

Howell, J. (2023), "List of 6 best cross-chain bridges", available at: https://101blockchains.com/best-cross-chain-bridges/ (accessed 1 February 2023).

Jenkinson, G. (2022), "Illicit cross-chain transfers expected to grow to $10B: here's how to prevent them", available at: https://cointelegraph.com/news/illicit-cross-chain-transfers-expected-to-grow-to-10b-here-s-how-to-prevent-them (accessed 1 February 2023).

Kafteranis, D. and Turksen, U. (2021), "Art of money laundering with non-fungible tokens: a myth or reality?", *European Law Enforcement Research Bulletin*, Vol. 22 No. 6, p. 31. https://bulletin.cepol.europa.eu/index.php/bulletin/article/view/531 (accessed 12 February 2023).

Kyckr (2021), "White paper: AML fines report 2021", available at: www.kyckr.com/resourcegated/aml-fines-report-2021 (accessed 29 November 2022).

Malwa, S. (2022), "Crypto exchanges scramble to compile 'proof of reserves' as FTX contagion grips markets", available at: www.coindesk.com/business/2022/11/09/crypto-exchanges-scramble-to-compile-proof-of-reserves-as-ftx-contagion-grips-markets/ (accessed 14 February 2023).

Mart, J. and Dempsey, C. (2021), "Scaling Ethereum and crypto for a billion", available at: www.coinbase.com/blog/scaling-ethereum-crypto-for-a-billion-users (accessed 21 February 2023).

Metelski, D. and Sobieraj, J. (2022), "Decentralized finance (DeFi) projects: a study of key performance indicators in terms of DeFi protocols' valuations", *International Journal of Financial Studies*, Vol. 10 No. 4, p. 108.

OECD (2022), "Why decentralised finance (DeFi) matters and the policy implications", available at: www.oecd.org/daf/fin/financial-markets/Why-Decentralised-Finance-DeFi-Matters-and-the-Policy-Implications.pdf (accessed 16 February 2023).

Ofoeda, I. (2022), "Anti-money laundering regulations and financial inclusion: empirical evidence across the globe", *Journal of Financial Regulation and Compliance*, Vol. 30 No. 5, pp. 646-664.

Ojo/Roedl, M. (2021), "Decentralized finance and regulation: enhancing the role of innovative techniques through regulation", *CIISD Economic Review*, Vol. 5 No. 12, available at: https://mpra.ub.uni-muenchen.de/107717/ (accessed 19 February 2023).

Priem, R. (2022), "A European distributed ledger technology pilot regime for market infrastructures: finding a balance between innovation, investor protection and financial stability", *Journal of Financial Regulation and Compliance*, Vol. 30 No. 3, pp. 371-390.

Samoshin, A. (2022), "Feasibility of regulatory enforcement in decentralized finance", available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4199742 (accessed 26 January 2023).

Schär, F. (2021), "Decentralized finance: on blockchain-and smart contract-based financial markets", Federal Reserve Bank of St. Louis *Review*, Second Quarter, pp. 153-174.

Sharma, R. (2021), "Decentralized finance (defi) definition and use cases", available at: www.investopedia.com/decentralized-finance-defi-5113835 (accessed 13 February 2023).

Teichmann, F.M. and Falker, M.-C. (2021), "Money laundering via underground currency exchange networks", *Journal of Financial Regulation and Compliance*, Vol. 29 No. 1, pp. 1-14.

Wang, A. (2022), "Rethinking the rule and role of law in decentralized finance", *2022 IEEE 24th Conference on Business Informatics (CBI)*, 2022, pp. 118-125, https://ieeexplore.ieee.org/document/9944750, (accessed 21 February 2023).

World Bank (2020), "World development indicators", available at: https://databank.worldbank.org/source/global-financial-inclusion-and-consumer-protection-survey (accessed 1 February 2023).

World Economic Forum (2021), "Decentralized finance (DeFi) policy-maker toolkit. Whitepaper", www3.weforum.org/docs/WEF_DeFi_Policy_Maker_Toolkit_2021.pdf (accessed 1 February 2023).

Zetzsche, D.A., Arner, D.W. and Buckley, R.P. (2020), "Decentralized finance", *Journal of Financial Regulation*, Vol. 6 No. 2, pp. 172-203.

Further reading

Yinliang (2022), "The leading edge? How this wallet allows non-KYC mastercard payments", available at: https://chaindebrief.com/the-leading-edge-how-this-wallet-allows-non-kyc-mastercard-payments/ (accessed 3 February 2023).

Corresponding author

Bogdan Adamyk can be contacted at: b.adamyk@aston.ac.uk