US DIGITAL ASSET ANTI-MONEY LAUNDERING ACT:

How proposed US crypto-asset ban would support banking sector's monopoly and harm civil society through financial exclusion

OPEN DIALOGUE

22 January 2024

The Open Dialogue Foundation (ODF) was established in Poland in 2009 on the initiative of Ukrainian student and civic activist Lyudmyla Kozlovska (who currently serves as President of the Foundation). Since its founding, statutory objectives of the Foundation include the protection of human rights, democracy and the rule of law in the post-Soviet area. In July 2017 the area of interest of the Foundation was expanded due to the rapidly deteriorating situation in Poland and other EU member states affected by illiberal policies implemented by their populist governments. The Foundation has its permanent representations in Brussels, Warsaw and Kyiv.

ODF coordinates the efforts of the Building True Change Coalition (BTC Coalition) composed of human rights defenders, political activists, Bitcoin entrepreneurs, and industry experts. The BTC Coalition aims to: (1) combat the abuse of Anti-Money Laundering / Countering the Financing of Terrorism (AML/CFT) within the wider range of transnational repression mechanisms; (2) promote financial inclusion in non-democratic and developing countries; (3) promote Bitcoin and stablecoins as tools to support human rights efforts and provide humanitarian aid worldwide; and (4) educate on the role of Bitcoin mining as an instrument to facilitate the adoption of renewable energy sources.[1]

This Submission has been prepared by Lyudmyla Kozlovska and Bota Jardemalie. The Testimonials included within it are attributed to the individuals as described therein.

Website: https://odfoundation.eu/ ; e-mail: lyudmylakozlovska@odfoundation.eu

Twitter: @ODFoundation

Project Manager:

Lyudmyla Kozlovska (the Open Dialogue Foundation): lyudmylakozlovska@odfoundation.eu

Copyright: The Open Dialogue Foundation, January 2024

OPEN DIALOGUE

[1] https://en.odfoundation.eu/projects-and-campaigns/combating-financial-exclusion-and-work-of-btc-coalition/

TABLE OF CONTENTS:

KEY NOTES....4

FINCEN PROPOSAL 2023-0016A (FINCEN–2023–0016): KEY ISSUES....6

THE RISKS OF A ZERO-RISK APPROACH: HOW FATF'S AML COMPLIANCE FINANCIALLY EXCLUDES CIVIL SOCIETY....7

ODF'S EXPERIENCE WITH DE-RISKING....8

CRYPTO-ASSETS AS A BANK OF LAST RESORT: THE ROLE OF BITCOIN AND STABLECOINS IN SUPPORTING CIVIL SOCIETY AMID FINANCIAL REPRESSION....9

VOICES OF CIVIL SOCIETY: TESTIMONIES FROM AROUND THE WORLD....12

RECOMMENDATIONS....17

ANNEX 1: FALSE POSITIVES IN AML/CFT COMPLIANCE: THEIR NATURE AND CONSEQUENCES....19

ANNEX 2 TO JOINT SUBMISSION OF THE CIVIL SOCIETY COALITION:....23

TESTIMONIAL OF OBI NWOSU 26

TESTIMONIAL OF LYUDMYLA KOZLOVSKA 29

TESTIMONIAL OF JAROSLAV LIKHACHEVSKY.... 34

TESTIMONIAL OF ANNA CHEKHOVICH.... 36

TESTIMONIAL OF FADI ELSALAMEEN 40

TESTIMONIAL OF JESÚS GONZÁLEZ 43

TESTIMONIAL OF BOTA JARDEMALIE 45

TESTIMONIAL OF JORGE JRAISSATI 48

TESTIMONIAL OF ROYA MAHBOUB 49

TESTIMONIAL OF SUBA CHURCHILL 50

TESTIMONIAL OF TETIANA PECHONCHYK.... 53

TESTIMONIAL OF MICHAEL CHOBANIAN.... 56

KEY NOTES

- The USA, as a pioneer in combating anti-money laundering/countering the financing of terrorism (AML/CFT) — having introduced the Bank Secrecy Act (BSA) in 1970[2] — and as one of the founding members of the Financial Action Task Force (FATF), sets standards for global financial policy to comply with AML/CFT rules;
- This submission presents the unintended consequences of enacting the now-processed Digital Asset Anti-Money Laundering Act[3] (DAAMLA), which potentially leads to financial exclusion of ordinary law-abiding citizens, civil society organizations (NGOs), political refugees, diaspora communities and other vulnerable to political persecution in the form of transnational repression as well as various marginalized groups of society;
- In commonly shared view of industry experts and civil society representatives, the DAAMLA constitutes rather an expression of years-long prejudices and misconceptions by its primary sponsor, Sen. Elizabeth Warren than a genuine contribution to combating financial crime; **Sen. Warren's crusade has been joined by the largest US banks**[4, 5] seeing the cryptocurrency sector outside their control[6] as a significant threat;
- The DAAMLA appears to lack a basic understanding of the nature of crypto-assets and blockchain infrastructure, devising provisions that would subject technology providers and users (such as millions of individual Bitcoin miners) **to enormous overreporting, resulting in the law being effectively unenforceable or paralyzing/shutting down the entire independent crypto-assets market in the US**;[7]
- Extending the BSA to technology providers (inc. even software developers) and practically all users of blockchain networks on which crypto-assets are based, as planned by the DAMMLA, would be against the fundamental principles of the BSA[8] (and other currently applicable laws). They subject financial institutions to specific obligations and reporting requirements (such as KYC and SAR procedures), but do not require individual users and technology providers to do so. The very logic of seeing as financial institutions defies elementary common sense. The devised provisions would be akin to requiring i.e. all Wi-Fi networks providers/administrators to identify, continuously spy on and report on their users;
- Subjecting self-hosted wallets infrastructure providers and their users to such regulations would go against the very nature of peer-to-peer transactions, which do not involve any financial

[2] https://www.irs.gov/businesses/small-businesses-self-employed/bank-secrecy-act
[3] https://www.warren.senate.gov/newsroom/press-releases/warren-expands-coalition-of-banking-committee-support-for-bill-cracking-down-on-cryptos-use-in-money-laundering-drug-trafficking-sanctions-evasion
[4] https://cointelegraph.com/news/elizabeth-warren-surveillance-legislation-help-big-banks
[5] https://cointelegraph.com/news/anti-crypto-bill-elizabeth-warren-american-bankers-association
[6] https://www.thestreet.com/crypto/innovation/proposing-a-government-ban-on-crypto-jpmorgan-ceo-fights-the-inevitable
At the heart of the debate was Dimon's surprising advocacy for a U.S. ban on crypto, a stance seemingly supported by Senator Warren. Chizhik, however, suggested that Dimon's comments were more strategic than literal, considering JPMorgan's investment in its own blockchain platform, Onyx.
[7] https://blockworks.co/news/senators-crypto-miners-validators-aml
[8] https://www.coincenter.org/how-i-learned-to-stop-worrying-and-love-unhosted-wallets/

intermediaries, blockchain transactions, and result in effectively banning them, stifling innovation and seriously infringing on the constitutional rights and freedoms of the individual;[9]

- As the US is debating the proposed law, discussing the adoption of stronger anti-money laundering/financing of terrorism regime concerning so-called digital assets, the interests of ordinary people and NGOs, relying on self-hosted wallets as the most secure instrument, are hardly taken into account;
- Bitcoin and stablecoins stored and transferred through self-hosted wallets, have provided pro-democracy activists with an important tool to avoid two main problems: de-banking (forced exclusion from the financial system) and autocratic governments' control over financial institutions;
- Due to already-existing regulations, there are significant impediments affecting customers, in particular certain categories of them. Nowadays, the practice of "de-risking" has been adopted by financial institutions worldwide (incl. the US, UK and EU) in order to comply with the strict recommendations of the FATF on AML/CFT laws.[10] De-risking leads, among other consequences, to banks terminating business relations with individuals and organizations targeted by smear campaigns or politically motivated legal assistance requests. This has proven to be a simple yet powerful tool of transnational repression for authoritarian governments and other illiberal regimes aiming to paralyze the activities of their opponents;
- One of the consequences of this abuse is the financial exclusion and undue deprivation of property (asset freezing). Moreover, transnational legal assistance frameworks allow malicious governments to access sensitive information, including banking data. As some US Senators intend to expand the scope of existing regulatory framework and "to close existing loopholes**," it is essential that these efforts should not infringe upon the rights of law-abiding customers, including those seeking refuge from or opposing authoritarian regimes;**
- Facing these challenges, the oppressed and marginalized have adopted crypto-assets, namely Bitcoin and stablecoins, as a so-called "bank of last resort," enabling them to combat ever-increasing financial repression. In many areas of the world, this has become a way to help people pay for necessities outside of official channels, deliver financial support and effectively finance humanitarian/emergency aid;[11]
- Self-hosted wallets, which are targeted by DAAMLA that seeks their effective elimination), are commonly used for this purpose, and the privacy they provide ensures the security and safety of both donors and beneficiaries.

[9] https://www.coincenter.org/the-digital-asset-anti-money-laundering-act-is-an-opportunistic-unconstitutional-assault-on-cryptocurrency-self-custody-developers-and-node-operators/
[10] https://www.fatf-gafi.org/en/topics/fatf-recommendations.html
[11] https://www.financialinclusion.tech/

FINCEN PROPOSAL 2023-0016A (FINCEN–2023–0016): KEY ISSUES

with regard to the Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern by the Financial Crimes Enforcement Network (FinCEN)[12]

- Convertible Virtual Currency mixing (CVC mixing) is a technology integrated into some popular cryptocurrency payment processors (gateways), providing services to digital asset holders. Like any technology or device, this technology can be used for legitimate purposes, as well as illicit activities.
- Such payments are necessary to convert crypto-currencies into fiat currencies and link them with the traditional financial system to cover daily-life expenses: most transactions carried out using them are legitimate[13, 14] (while the legitimate crypto usage is estimated at 99,85% overall)[15] and some calculations regarding terrorism financing via CVC mixing recently may be significantly exaggerated.[16, 17] Thus, subjecting CVC mixing to extreme scrutiny, overreporting, and recordkeeping, as intended by the FinCEN proposal, would massively violate individuals' rights and constitute a kind of a preventive measure reaching too far;[18]
- As noted even by FinCEN itself, there are fully legitimate purposes for the application of these technologies. From the perspective of asylum-seekers, dissidents, human rights defenders, and all those associated with them who are at the risk of political persecution, these technologies are a vital instrument supporting their lives and activities, usually against the interests of oppressive authorities;[19]
- **Contrary to the belief and assumption made in the FinCEN proposal, combating illicit financial activities should not take precedence over the rights of millions of lawful crypto-currency users. Their safety and privacy should be genuinely, not only declaratively, taken into account. These rights cannot be sacrificed merely to facilitate the task of law enforcement authorities**;
- According to the US Constitution and international law, the government not entitled to arbitrarily exceed its powers at the expense of individual rights and freedoms, including data protection and the right to dispose of one's own funds[20], and subject citizens (and foreigners alike) to permanent, indiscriminate preventive surveillance;

---

[12] https://www.regulations.gov/document/FINCEN-2023-0016-0001

[13] https://www.linkedin.com/pulse/what-legitimate-use-cases-using-mixer-tara-annison/

[14] https://www.chainalysis.com/blog/crypto-mixers/
A small percentage of crypto mixer users are cybercriminals. (…) In July, we found that almost 10% of all cryptocurrencies held by illicit entities have been laundered through a mixer in 2022.

[15] https://finance.yahoo.com/news/only-0-15-total-crypto-174206641.html
A recent report by Chainalysis has revealed that the legitimate usage of cryptocurrencies far outweighs their illegal use. The report pointed out that only 0.15% of the total cryptocurrency transaction volume last year was for illicit activities.

[16] https://www.wired.com/story/us-treasury-crypto-mixer-hamas/
Cryptocurrency tracing firm Chainalysis, which frequently works with government and law enforcement customers, went so far as to publish a blog post yesterday cautioning against mistaken analyses that overestimate the role of cryptocurrency in financing entities like Hamas and the Palestinian Islamic Jihad.

[17] https://www.chainalysis.com/blog/cryptocurrency-terrorism-financing-accuracy-check/

[18] https://egodeath.capital/blog/fincen-may-be-violating-your-rights-bitcoin#fincen-questions

[19] https://bravenewcoin.com/insights/why-bitcoin-mixers-are-a-double-edged-sword-for-anti-money-laundering

[20] https://www.wired.com/story/us-treasury-crypto-mixer-hamas/
The new rules, if adopted following a 90-day period of public comment and debate, would potentially represent the broadest restrictions imposed yet on the mixing services and could make it far harder for cryptocurrency holders to put their money through the services before cashing it out at a US cryptocurrency exchange, or even at a foreign exchange that accepts US customers.

- Given the available data, most transactions that constitute money laundering or other types of financial crime occur within the traditional financial system. Therefore, targeting CVC mixing seems misguided and more of an attempt to increase regulatory control over citizens rather than a genuine law enforcement effort. For instance, the circumvention of sanctions imposed by the US and its allies on Russia, to a large extent, is done through the traditional financial system,[21] using third countries such as China, Turkey or Kazakhstan;[22]
- Also, as noted in the Wall Street Journal article: "*FinCEN's proposal could have a chilling effect by further associating certain crypto activities with terrorist financing and money laundering, according to Alex Zerden, a former FinCEN official who founded financial technology and risk advisory firm Capitol Peak Strategies."*[23]
- Since targeting CVC mixing means targeting crypto-currency payment processors and sending shockwaves through the entire crypto industry, the proposed rulemaking, if it comes into force, would represent a significant regulatory blow not only to citizens' rights, but also to the US new technology sector, stifling blockchain-based innovation and hitting its competitive position globally, much to the delight of world's autocrats.

THE RISKS OF A ZERO-RISK APPROACH: HOW FATF'S AML COMPLIANCE FINANCIALLY EXCLUDES CIVIL SOCIETY

Banks and other financial institutions, including cryptocurrency exchanges, are required to adhere to *"fit and proper"* standards when following FATF's Recommendations and adopted on their basis regulations globally, often applying a zero-risk approach to new clients. However, *"propriety"* is a loosely defined term. To assess the risk level of a customer, these institutions use automated systems that examine an individual or an organization's online media coverage. This process presents an opportunity for an illiberal government to completely expel a civil society organization from the banking system, not only domestically but also internationally. The only requirement is to generate negative coverage across different media outlets in several languages, prompting financial institutions to flag and refuse a customer. As a result, politically-exposed organizations or individuals can become victims of the so-called **false positives** in AML compliance, which disproportionately affects low-profit customers ***(Annex 1).***

Financial institutions prioritize customers based on their value, with ordinary individuals having relatively low value and non-profits having an even lower value.

Financial institutions use data from data providers like Refinitiv and Dun & Bradstreet as part of their Know Your Customer (KYC) and AML compliance processes. When data providers detect negative coverage, it most likely leads to the rejection of a potential customer's application or termination of the existing relationship. This decision is made regardless of whether the negative coverage is part of an orchestrated smear campaign, as financial institutions tend to adopt a zero-risk approach, even at the expense of organizations that work for democracy and the benefit of people in need, such as providing humanitarian aid. The situation can become more drastic when an autocratic government, exerting full control over its law enforcement agencies, fabricates politically motivated criminal charges against its opponents, perverting, at the end of the day, the Western justice system. When a Western bank receives

[21] https://en.odfoundation.eu/a/570712,everything-for-the-front-everything-for-victory-how-tokayev-helps-putin-while-fooling-ukraine-and-the-west/#6-tokayev-is-lobbying-the-usa-the-eu-and-ukraine-to-lift-anti-russian-sanctions
[22] https://en.odfoundation.eu/a/684240,russias-decade-long-war-against-ukraine-how-to-accelerate-ukrainian-victory/
[23] https://www.wsj.com/articles/u-s-targets-crypto-mixers-over-money-laundering-risks-e431def

a formal request for information from a law enforcement or judicial body of a country in which it operates, which itself received the request from a third country, it raises a red flag automatically in relation to the person or entity in question. This situation can have significant consequences, including an account closure or the rejection of the customer's application, further harming civil society organizations and politically-exposed individuals.

Clearly, such investigations tend to create sensational news, which further increases the number of negative results indexed by search engines and business intelligence firms. Regime propaganda eagerly exploits this. The news is quickly transmitted to banks, auditors, and even real estate companies or landlords, allowing subservient propagandists and prosecutors of illiberal regimes to hurt those who are affected.

Therefore, corruption is not the only method that can be effectively employed in the service of malign foreign actors to expand their influence within a Western democracy, this situation with misuse of AML/CFT regulations creates a mockery of the principle of mutual trust between states. Once again, the West is played by its enemies, often with the assistance of leading law and advisory firms.

The practice of illiberal regimes excluding their opponents from the financial system currently suffers from a lack of public awareness, which further exacerbates the abuse of legal cooperation mechanisms. ODF became a victim of the misuse of FATF Recommendations, which resulted in negative consequences for ODF's AML bank compliance. This occurred due to politically motivated public attacks and abuse of mutual legal requests, including mechanisms of the Schengen Information System, by the illiberal regimes that also tried obtaining banking data of ODF and its associates. As a result of the misuse of AML compliance, ODF and its associates became considered high-risk clients by banks and subsequently faced financial exclusion and account closures.

The FATF Recommendations are drafted with an accusatory bias for NPOs/NGOs. However, there is no substantiated statistical data to support this practice. Moreover, this approach is consistent with the rhetoric of authoritarian and undemocratic states, which inherently categorise and treat NGOs as entities that not only create threats to national security but are also involved in money laundering and terrorist financing. This further reduces civic spaces.

ODF'S EXPERIENCE WITH DE-RISKING

For over a decade, ODF has been exposing numerous instances of EU, bilateral, and international legal cooperation mechanisms enabling transnational repression. Since 2017, ODF has been subjected to significant abuse of inter-state mechanisms. In 2017, ODF took a stand in defence of the rule of law in Poland, which was met with a legal harassment and disinformation campaigns conducted by the Law and Justice government alongside the Kazakhstani and then-Moldovan regimes that ODF had criticised. Moreover, the Law and Justice government orchestrated numerous attempts at shutting down or paralysing ODF by organising smear campaigns against the foundation in Poland and within international institutions, including the European Parliament, the Parliamentary Assembly of the Council of Europe, and the OSCE Parliamentary Assembly.

ODF has been successful in nearly all court disputes with the Polish authorities, including several libel cases. Although some proceedings launched by ODF against the authorities are still pending, all allegations against the organization have been proven false. Despite ODF's successes in court, raising a compliance red flag is much easier than removing it. Unfortunately, a persistently damaged reputation can take years to heal, and the current legal framework does not offer any remedies to restore the bank accounts of the

NGO and its associates whose accounts have been closed in Belgium.[24] Based on its own experiences, ODF understands the need to raise public awareness regarding the practice of cutting opponents of illiberal regimes from the financial system.

CRYPTO-ASSETS AS A BANK OF LAST RESORT: THE ROLE OF BITCOIN AND STABLECOINS IN SUPPORTING CIVIL SOCIETY AMID FINANCIAL REPRESSION

In May 2023, a G7 Finance Ministers and Central Bank Governors Meeting announced in its communiqué[25] about the need for the "effective monitoring, regulation and oversight are critical to addressing financial stability and integrity risks posed by crypto-asset activities and markets, while supporting responsible innovation." The G7 manifested its commitment to implement an "effective regulatory and supervisory frameworks for crypto-asset activities and markets as well as stablecoin arrangements, which are consistent with the FSB's recommendations and standards and guidance established by SSBs." While the G7 presented crypto-assets as "a financial stability and integrity risk," it has yet to address the growing problem of financial exclusion and the abuse of AML/CFT laws for transnational repression against activists and opponents. They also have not acknowledged how peer-to-peer transactions and Bitcoin self-hosted wallets have become the only tool available for human rights activists in illiberal countries.

The problem of authoritarian governments exerting control over financial institutions is evident: assets are at risk of being seized at any time, jeopardizing the survival of NGOs. Additionally, this situation enables security and fiscal services to exploit FATF recommendations to monitor the funding sources of watchdog organizations, providing authorities with information that can be used to intimidate and persecute these NGOs politically.

In various authoritarian regimes, financial systems are increasingly being weaponized against dissenters, posing a significant threat to human rights and personal security. Governments in countries like Russia[26], Turkey[27], Kazakhstan[28, 29], Belarus[30], Venezuela, Afghanistan[31], and Iran[32] exert control over financial institutions, leading to asset seizures and surveillance of opposition and human rights groups. This situation compels people and opposition movements to turn to alternative means like Bitcoin for financial transactions and support, evading government oversight and safeguarding their assets and personal freedoms.

In Palestine, rampant corruption forces people out of official banks to protect their hard-earned savings, while banking data is used to target the opposition.[33, 34]

A significant example of de-risking relates to the situation with Ukrainian and pro-Ukrainian NGOs and volunteer initiatives that fundraise to provide humanitarian aid to soldiers and refugees. In February 2022, following the Russian attack on Ukraine, the Ukrainian society and the state encountered two critical challenges that the traditional banking system could not adequately address. First, banks and other

[24] https://www.politico.eu/newsletter/eu-confidential/politico-eu-confidential-tv-star-to-run-slovenia-banned-from-schengen-summer-time-feedback-overload/
[25] https://www.consilium.europa.eu/media/64307/g7-communique-20230513.pdf
[26] https://www.reuters.com/article/us-russia-politics-navalny/russia-freezes-bank-accounts-linked-to-opposition-politician-navalny-idUSKCN1UY1ER
[27] https://stockholmcf.org/erdogans-long-arm-deutsche-bank-closes-accounts-of-erdogan-opponents-without-giving-any-reason/
[28] https://www.hrw.org/news/2021/07/07/kazakhstan-crackdown-government-critics
[29] https://en.odfoundation.eu/a/32928,oppositionist-therefore-extremist/
[30] https://www.theguardian.com/world/2020/nov/13/belarus-tells-banks-seize-money-raised-help-protesters-lukashenko
[31] https://bitcoinmagazine.com/culture/bitcoin-financial-freedom-in-afghanistan
[32] https://www.iranintl.com/en/202212067151
[33] https://www.haaretz.com/2015-06-23/ty-article/former-pm-of-palestine-accused-of-money-laundering/0000017f-e3ec-d7b2-a77f-e3efbc930000
[34] https://pace.coe.int/en/files/31623/html

financial institutions were temporarily paralysed, causing payments from and to Ukraine to be delayed or get stuck *"in transit"* for several weeks. This was a critical time when life-saving equipment, drones, and other supplies were urgently needed. Second, crowdfunding platforms' accounts and bank accounts of organizations supporting Ukraine financially and through in-kind donations were massively suspended. GoFundMe, Patreon, Wise (formerly TransferWise), and regular banks closed the accounts of numerous organizations around the world, often without explanation or citing internal rules that exclude transactions associated with *"armaments, military goods, and services."*[35, 36]

In each of the aforementioned situations, crypto assets have served as a bank of last resort for those who otherwise would have been unable to protect their funds or make money transfers. This has allowed many to keep their savings safe from the hands of corrupt governments, local dictators, and political police. Privacy and ease of use have been crucial in making cryptocurrencies viable tools for civil society, enabling NGOs to continue providing crucial support.

We do believe it is a crucial time to address the use of Bitcoin by civil society. Members of the European Parliament, members of the parliaments across the Council of Europe and the OSCE region have considered our recommendations:

- In April 2023, European Parliament adopted a „REPORT on the proposal for a regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing". Report includes:
  a) Provisions for "banks of last resort": legitimate credit and financial institutions shall provide measures to prevent unwarranted de-risking, ensuring non-discrimination and financial inclusion for customers, including those associated with higher-risk categories such as refugees, human rights defenders, individual users of crypto-assets, NGOs, and their representatives and associates.
  b) Establishment of additional security measures for processing special categories of personal data and personal data related to criminal convictions and offences.
  c) Prevention of the prohibition of self-hosted cryptocurrency wallets being provided and stored by crypto-asset service providers, as they are used for legitimate purposes such as humanitarian fundraising or fund custody.
  d) Setting exceptions for certain crowdfunding providers and introducing more flexible criteria for risk assessment.
  e) Providing clarity on additional sources of information used to determine risk, which should be reliable and credible. This includes information from civil society organizations, the media, and commercial entities, such as risk reports. [37]
- In January 2023, 29 members of the Parliamentary Assembly of the Council of Europe (PACE), representing 14 countries, submitted a motion for resolution concerning the misuse of legal cooperation and AML/CFT laws.[38] The motion called to ensure protection against both transnational crime and the protection of privacy and human rights. Notably, this was the first time that European legislators acknowledged the role of crypto assets, such as Bitcoin and stablecoins, as tools for facilitating the work of civil society initiatives and the delivery of humanitarian aid.
- During the June session in 2023, the PACE discussed and adopted a resolution, which stressed the "*misuse on politically motivated grounds of interstate legal co-operation mechanisms such as anti-*

[35] https://ain.ua/2022/08/09/wise-zablokuvav-rahunky-fondiv-yaki-dopomagaly-ukrayini/
[36] https://vctr.media/ua/ne-takyj-j-idealnyj-chomu-ukrayinczi-vzhe-skarzhatsya-na-paypal-132476/
[37] https://www.europarl.europa.eu/doceo/document/A-9-2023-0151_EN.html#_section6
[38] https://pace.coe.int/en/files/31622/html

money laundering and anti-terror financing measures may result in violations of the right to a fair trial (…) This may in turn lead to financial exclusion of targeted individuals and NGOs and effectively prevent them from conducting their human rights activities and participating in economic and social life."[39]

- In July 2023, the Parliamentary Assembly of the Organization for Security and Cooperation in Europe (OSCE PA) adopted our amendment to the so-called Vancouver Declaration, which calls its 57 member states to "*ensure that Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) mechanisms are not used as tools of transnational repression to stifle dissent or target human rights defenders, anti-corruption campaigners, exiled dissidents, and diaspora communities, taking into account the potential unintended consequences of prevention-focused AML/CFT regulations and their side effects, including the potential for increased financial exclusion and further malicious exploitation of strict AML/CFT and related provisions, and further urges them to reflect in relevant regulations the use of crypto-assets, such as bitcoin and stablecoins, to defend human rights and to provide humanitarian aid.*"[40] Furthermore, we greatly appreciate the adoption by the Members of the OSCE PA a Resolution specifically on the role of national parliaments in enhancing the participation of civil society in parliamentary and decision-making processes.
- In October 2023, members of the PACE submitted a motion for resolution acknowledging the concerns raised by the United Nations Special Rapporteur on counter-terrorism and human rights, Fionnuala Ní Aoláin.[41] She stressed that 69 % of relevant Human Rights Committee recommendations focused on the abuse of counter-terrorism surveillance practices against civil society, as well as the need to define transnational repression and analyse/reflect in the relevant regulation what role bitcoin and stablecoins play in that case.[42]
- The recent public consultation on the FATF Best Practice Paper to Combat the Abuse of NPOs faced significant challenges. Despite being conducted in a tight timeframe, it took years to start public consultation discussions about FATF's recommendations' negative consequences.[43] This situation highlights the need for NGOs to be provided with more time and resources to address regulatory issues that significantly impact their operations and existence. Moreover, the consultation should not be limited to addressing only terrorism financing (TF) abuses but should also encompass concerns related to money laundering (ML) abuse. The AML/CFT legal frameworks are usually based on the same legislative foundations, and the issues related to AML are often more prevalent than those related to TF. Therefore, the entire study and its specific recommendations should comprehensively cover both TF and ML concerns.

We hope that an open dialogue between civil society and US regulators, particularly FinCEN on how FATF recommendations and transnational legal cooperation can be enhanced will ensure protection against transnational crime while safeguarding privacy and human rights. Furthermore, it should be reflected in relevant regulations how peer-to-peer transactions and Bitcoin self-hosted wallets have become the only tool available to human rights activists in illiberal countries.

[39] https://pace.coe.int/en/files/32999/html
[40] https://www.oscepa.org/en/documents/annual-sessions/2023-vancouver/declaration-29/4744-vancouver-declaration-eng/file_
[41] https://defendcivicspace.com/wp-content/uploads/2023/06/SRCT_GlobalStudy.pdf
[42] https://pace.coe.int/en/files/33081/html
[43] https://www.fatf-gafi.org/en/publications/Fatfrecommendations/FATF-BPP-Combat-Abuse-NPOs-Public-Consultation.html

VOICES OF CIVIL SOCIETY: TESTIMONIES FROM AROUND THE WORLD

Full texts of the testimonies are available in **Annex 2** to this Paper.

1. **Testimonial of Jaroslav Likhachevsky (Belarus, currently resides in the Netherlands), co-founder of the New Belarus platform and Bysol Foundation, director of the AI company Deepdee from Belarus:** "There are two serious problems with banks in the EU Member States for the Belarusians in exile: (1) they face difficulties opening/holding accounts in the EU and CoE Member States, and (2) they cannot use the banking system to deliver financial support to activists in Belarus due to the danger and ineffectiveness of the traditional bank transfers to authoritarian regimes. Ales Bialiatski, a current political prisoner in Belarus and 2022 Nobel Prize recipient, was arrested under tax evasion charges in 2011. The Belarusian regime has abused FATF recommendations on AML/CFT preventive measures to gain access to financial records from Lithuania and Poland as evidence. Now, regimes like Belarus use FATF recommendations on AML allegations as a pretext to collect financial information from Western democracies.[44] Therefore, the team has developed a safe and secure solution to provide financial support for local activists and organizations using crypto assets, which also allows them to build their own institutions and services in parallel. The team uses Bitcoin and stablecoins to deliver humanitarian aid to Belarus and support pro-democratic and anti-Russian activists on the ground. The team's future plans include building Digital Belarus, as a prototype for the future Belarusian Democratic state, with democratic institutions, including taxation and representation, using crypto assets like Bitcoin and stablecoins to maintain privacy and security, and to ensure they are not de-platformed or de-banked due to the upcoming Anti-Money Laundering regulation. In parallel, the Ministry of Interior of Belarus announced the development of a regulation to ban cryptocurrency peer-to-peer transactions between individuals, allegedly to combat criminal transactions.[45]

   On 29 August 2023, Alexander Lukashenko signed a decree on measures to counteract unauthorized payment transactions that should give law enforcement agencies of Belarus unorganised access to the financial information of Belarusian residents. This law will become another tool for political repressions in Belarus."

2. **Testimonial of Anna Chekhovich, financial director of Alexei Navalny's Anti-Corruption Foundation (FBK) (Russia, currently resides in Lithuania):** "The Anti-Corruption Foundation (ACF), founded by Alexei Navalny, has been collecting donations in cryptocurrency since 2016 due to the unsafe nature of collecting only fiat donations, with the Russian banking system being fully controlled by the regime. Since the ACF's recognition as an extremist organization in 2021, the organization was forced to leave Russia, and most have moved to EU countries, where they registered legal entities to continue their activities. However, the founders of the Future Russia Foundation, formerly the ACF, have been facing problems in opening a simple bank account due to banks' AML compliance, and their bank accounts get closed without any explanation. Western banks treat Russians in exile as potential money launderers, and their transactions are often treated as suspicious. This leads to living without bank accounts which is impossible in the modern world. At some point, humanitarian aid was only possible through cryptocurrency, but European banks refused to conduct transactions related to cryptocurrency, making it impossible to buy cryptocurrency directly from the fund's accounts. Paysera payment system closed the organization's account after attempting to buy Bitcoin.

   Now the EU has banned all crypto transactions with Russia within the framework of new sanctions against Russia, making it absolutely impossible for the foundation to financially support activists who are fighting the regime while in Russia. These new restrictions will not play a significant role in the fight against sanctions circumvention, but will cause enormous damage to the activities of activists

[44] https://news.zerkalo.io/economics/47760.html?c
[45] https://t.me/police_minsk/12242

and human rights organizations working with Russia. It will not stop Russian corrupt officials, but it will have a significant impact on the Russian opposition movement, and the founders of the Future Russia Foundation call for a solution that will not hinder humanitarian aid and will not put recipients of funds in Russia at risk."

3. **Testimonial of Ismail Mesut Sezgin, Turkish opposition political commentator and research assistant at Regent's Park College, and self-employed business (Turkey, currently resides/citizen of the UK):** The case of transnational repressions in Turkey shows how authoritarian regimes can abuse international institutions and regulations to destroy lives of those who speak up against them, even if they are in the EU and other democracies. Mesut Sezgin, who wrote his Ph.D. at Leed Beckett University on the Hizmet Movement, spoke publicly and published YouTube videos about the failed coup attempt in Turkey. His Twitter and YouTube accounts were blocked by Turkish authorities, and Patreon account was also blocked in Turkey. In 2021, Mesut Sezgin was enlisted as a member of *"Fethullahist Terrorist Organization"* by the Turkish government, causing financial assets to be frozen and seized internationally without due process. The financial blacklist caused problems, destroying his financial situation and business. Even in the UK, financial institutions started treating him as if he were a terrorist.

   This situation is not unique, as people in Turkey designated as *"terrorists"* and blacklisted cannot send or receive money from or to their families and friends in Turkey. Even providing financial support can be used as evidence of being a member of a terrorist organization, and some people in Turkey have been banned from banking. This creates a dire situation for families of political prisoners and blacklisted activists, as any financial support from European countries or other democracies is impossible. The western financial institutions following broad wording of the recommendations of FATF on AML/CFT preventive measures also treat them as terrorists, smugglers, and money launderers.

4. **Testimony of Jorge Jraissati (Venezuelan, currently residing in Spain), Director of Alumni for Liberty, an international network of young freedom activists with over 10,000 members from 139 countries:** "Authoritarian regimes and illiberal governments have been weaponizing the international banking system as a tool for domestic and transnational repression. In response to this development, our activists have turned Bitcoin into their "bank of last resort." Our organization has used Bitcoin to finance its activities in over fifty countries, and we currently pay 29 staff members through this cryptocurrency. In autocratic countries, our activists have reported that their bank accounts were either closed or weaponized. We have also documented cases of activists in exile who have been deprived of the right to have financial services, as they are targeted with disinformation campaigns and fabricated criminal allegations, which trigger de-risking mechanisms in bank compliance. This means that requirements originally established to adhere to AML/CFT laws are harming human rights defenders even at the very heart of the European Union. Similarly, several transnational legal assistance frameworks are allowing malicious governments to access sensitive information of their opponents abroad (including their banking data), jeopardising their safety. For these reasons, regulators and civil society have to work together to build mechanisms to prevent the unintended consequences of FATF standards and instruments to protect the financial rights of all law-abiding citizens."

5. **Testimonial of Fadi Elsalameen, a prominent critic of corruption in the Palestinian Authority's government led by Mahmoud Abbas), an adjunct senior fellow at the American Security Project and the Bitcoin Policy Institute in the US (Palestine, currently U.S. citizen):** Fadi Elsalameen, who has been exposing human rights violations and corruption in Palestine for over a decade, presents on two issues: (1) how the Palestinian Authority's complete control over the banking system has been weaponized to harass dissidents and anyone who exposes abuse of humanitarian aid or financial

assistance, and (2) how Bitcoin has become a solution to protect activists against corrupt regimes and connects communities in Israel and Palestine through Bitcoin transactions. Elsalameen personally experienced the Palestinian Authority's abuse of anti-money laundering regulations and anti-terrorism laws when his accounts were frozen by Bank of Palestine in 2021, which then leaked his personal information to a newspaper owned by the terrorist organization Hezbollah. The leak was intended to incite violent attacks against him, which later led to Palestinian security forces shooting at his house with live bullets in March 2021.

The European Parliament's latest resolution on Palestine calls for transparent elections, an end to repression of dissent, and accountability for human rights violations. Civil society in Palestine has welcomed this resolution, but is still facing the high cost of corruption under the regime of Mahmoud Abbas. The European Union and Council of Europe must take action in the following ways: (1) exclude the Palestinian Interior Ministry and security services from European Union financial assistance until effective measures are taken to stop torture, hold those responsible accountable, and release political prisoners; (2) ensure that AML/CFT regulations are not abused by the PA to harass dissidents; and (3) prevent the abuse of AML/CFT regulations through mutual legal assistance to silence opponents abroad.

6. **Testimonial of Obi Nwosu, former CEO of a regulated Bitcoin exchange Coinfloor (UK, Portugal):** "While KYC procedures and risk-based approaches are necessary to prevent money laundering and terrorist financing, they can inadvertently lead to de-banking and de-platforming of high-risk customers. The *"travel rule"* developed by FATF recommendations requires sharing of customer information, which can be used by dictatorial regimes to target recipients of funds. The *"tipping off"* rule prevents financial institutions from disclosing the reasoning behind their risk-based approach rules to their customers, due to concerns of money laundering and terrorist financing. However, this can lead to unintended consequences for individuals who are targeted with false information or adverse media, particularly those living under dictatorships and authoritarian regimes. These individuals may be off-boarded or de-platformed without explanation, leaving them with no recourse. The *"fitness and propriety"* standards can lead to a risk-averse culture, and discrepancies in anti-money laundering and terrorist financing rules are often not spoken about due to fear of regulators. Financial institutions are facing a complex challenge when it comes to providing services to members of civil society, activists, human rights defenders, and NGOs, as they are often considered high-risk customers. In some cases, these requirements can result in one being de-banked or de-platformed, leaving them no other option but to turn to cryptocurrencies such as Bitcoin and stablecoins. Therefore, two provisions should be put in place: (1) enabling members of civil society to seek recourse if they have been de-banked or de-platformed and (2) allowing them to use services like Bitcoin and stablecoins without being de-platformed or de-banked purely because they use these services.

7. **Testimonial of Jesús González, a computer engineer and representative of the Venezuelan opposition (Venezuela, currently resides in Spain):** Jesús González has been opposing the dictatorship of Chavez and Maduro for over 15 years and has been a member of the Interim Government of Venezuela since 2019. The opposition aimed to use the frozen Venezuelan funds in the US to provide financial aid to activists, opposition members, and social programs in Venezuela. With the help of the US government, they successfully implemented a program called "*Heroes de la Salud*" in 2020 during the pandemic. The program converted designated US funds into stablecoins and transferred them to over 68,000 health workers in Venezuela through a direct and secure platform to avoid reprisals of Maduro's regime. The program was replicated with frozen funds and digital platforms for all areas of the Interim Government, allowing them to continue operating without putting their personal security at risk. The mechanism helps overcome obstacles imposed by the authoritarian state-controlled

financial system. However, human rights defenders and opposition members, like Leopoldo López, well-known pro-democracy activist and Sakharov prize laureate, face bank compliance problems in the EU, with many of their colleagues unable to even open a bank account due to banks de-risking and closing their accounts or freezing their payments following broad wording of the FATF recommendations on AML/CFT preventive measures.

8. **Testimonial of Bota Jardemalie, a licensed attorney in the State of New York and a human rights defender (Kazakhstan, political asylum in Belgium):** Bota Jardemalie was granted political asylum in Belgium due to the extraordinary risks she faced in the form of reprisals by Kazakhstan against her for her legal work against the regime. The Council of Bars and Law Societies of Europe (CCBE) recognises Jardemalie as "lawyer in danger."

   Despite Jardemalie's political asylum, she remained in danger even in Belgium. At Kazakhstan's request, in 2013 INTERPOL published a Red Notice to arrest Jardemalie on fabricated charges of alleged embezzlement of BTA Bank in Kazakhstan, that was later INTERPOL cancelled this Red Notice for non-compliance with the rules against political abuses of INTERPOL. Kazakhstan's regime twice tried to extradite Jardemalie from Belgium unsuccessfully, with false AML allegations. Belgium refused those extradition requests.

   After their attempts at extraditing Jardemalie and physically harassing her failed, in 2016, a proxy for the Kazakhstani regime, BTA Bank, filed a criminal complaint against Jardemalie in Belgium, accusing her of money laundering on Belgium soil. The Chamber du Conseil of the Tribunal of the First Instance of Brussels dismissed the criminal investigation against Jardemalie and ordered the complainer to pay Jardemalie €15000 in procedural compensation and €5000 more, *ex aequo et bono*, as compensation for the temerarious and vexatious procedure. This case is an example of SLAPP - Strategic Lawsuit Against Public Participation, another tool of transnational repression, with abuse of AML laws.

   In parallel, Jardemalie has been a target of a very aggressive smear PR campaign in 5 languages online, sponsored by the Kazakh regime. As a result of negative PR, she started experiencing problems with banking: banks in Belgium closed her bank accounts without any explanation, considering as a high-risk client, and refused to open her a bank account. She also was blocked from making Western Union transfers. She fell victim to the misuse of AML bank compliance as a result of politically motivated public attacks, and subsequently faced financial exclusion and account closures.

9. **Testimonial of Roya Mahboub, a serial entrepreneur and one of the first female CEOs in her home country, Afghanistan (Afghanistan, currently residing in the US)**: "Bitcoin allowed the organization to overcome physical and social obstacles in paying Afghan women. With a simple transaction, Bitcoin could instantly appear in a woman's digital wallet, without interference from men. My team has trained over 17,000 young women in coding, digital skills, and entrepreneurship, and has built dozens of internet classrooms and mobile computer labs across Afghanistan. We tried to develop practical skills and foster self-reliance among women, breaking down traditional cultural barriers that limit them to domestic duties.

   Since August 2021, bank and wire services like Western Union, MoneyGram have run out of paper currency and have cut off services, leaving one-third of Afghans struggling with food insecurity and 50-70% with unstable housing situations. Websites like GoFundMe have been blocked from fundraising efforts for "compliance" reasons. Bitcoin has provided a crucial financial lifeline for many during these difficult times, who stay in the country and continue working behind closed doors."

10. **Testimonial of Suba Churchill, executive director of the Kenya National Civil Society Centre and chairperson of the Horn of Africa Civil Society Forum (Kenya):** "I am a member of Kenya's Universal Peer Review (UPR) process, and I can at best describe the National Risk Assessment on Money Laundering and Terrorism Financing for Kenya as a farce. First, the entire process in my view, has

always been shrouded in unnecessary secrecy, and is approached by the concerned Kenyan authorities as (1) an investigation into an already established crime (2) in which the Not-for-Profit sector is presumed guilty until proven innocent despite the country's constitutional provision of presumption of innocence until one is proved guilty by a court of competent jurisdiction Second, consultation of NPOs has been done remotely, and without their knowledge of what one is being drawn into. I can testify on my own and other NGOs' experience that Kenya's state security agencies are engaged in harassment of non-governmental organizations but claim that this was consultation on FATF standards."

11. **Testimonial of Michael Chobanian, President of the Blockchain Association of Ukraine and a founder of the first cryptocurrency exchange in Ukraine, KUNA.io (Ukraine): "**From the invasion's first moment, we at KUNA decided to act swiftly to help our army and the people who suffered most due to these horrific events. In collaboration with the Ministry of Digital Transformation and the Ministry of Defense, our team launched the official Crypto Fund of Ukraine to solicit cryptocurrency donations. The majority of funding comes through crypto assets such as Bitcoin and Ethereum, where AML technologies (e.g. Chainalysis, Crystal Blockchain) have been successfully implemented. All crypto that we received and converted was analysed for illegal activity. These solicited funds are used to purchase much needed medical supplies, military equipment, and humanitarian aid here in Ukraine. As of July 2023, the Fund has collected more than $60 million dollars in donations, while in total Ukraine has raised more than $225 million in crypto donations since February 2022.[46]

    As CEO of the first crypto exchange in Ukraine, we provided advice and education to various financial and intelligence institutions in Ukraine, such as the Ministry of Digital Transformation of Ukraine, the National Bank, and the Secret Service/Police, on how to use cryptocurrency to counter terrorist financing and reduce money laundering.

    Also important to mention that since 2020, representatives of the authoritarian regimes in Belarus and Russia have tried to obtain personal information on their opponents, accusing them of funding extremism and money laundering.[47] In the case of Belarus, it is the BYSOL Foundation. This is a fund that helps financially those who were fired for protesting or were victims of repression by the Belarusian government.[48] Unlike our colleagues from the Chinese platforms, we refused to hand over information about our users due to politically motivated requests. We believe it is important that such deterrent elements are also reflected in the regulation of democratic countries, in the EU, the USA[49], UK and Ukraine."

12. **Testimonial of Tetiana Pechonchyk, head of the Board of the Human Rights Center ZMINA, (Ukraine):** "In Ukraine, the implementation of the FATF Recommendations negatively affects the operations of NGOs and has led to financial exclusion of NGOs. For example, in November-December 2021, banks blocked the accounts of two reputable Ukrainian civil society organizations - the Institute of Mass Information and the Civil Network OPORA.[50] However, two months later, the full-scale invasion of Ukraine by the Russian Federation began, and the requirement to submit the ultimate beneficial owners for civil society organizations was postponed until the end of martial law in the country. In other words, the problem was postponed but not solved, as this trend will resume after the war ends. In addition, inspections can be applied during martial law to those NGOs that have managed to submit their ultimate beneficial owners data.

[46] https://crystalblockchain.com/articles/crypto-regulations/ukraine-receives-over-224m-in-crypto-donations/
[47] https://reform.by/169292-kriptobirzha-otkazalas-vydavat-kgk-dannye-po-operacijam-fonda-bysol
[48] https://bysol.org/en/bs/
[49] https://www.banking.senate.gov/imo/media/doc/Chobanian%20Testimony%203-17-22.pdf
[50] https://zmina.info/articles/chomu-banky-blokuyut-rahunky-gromadskyh-organizaczij-i-chy-mozhna-z-czym-shhos-zrobyty/

The regulatory measures introduced in Ukraine, ostensibly aimed at preventing money laundering and terrorist financing, have inadvertently led to unnecessary overregulation and operational impediments for NGOs. While the intention to align with international standards and protect against financial crimes is commendable, the hurried and unclear implementation of these regulations has created significant challenges. The lack of precise definitions for ultimate beneficial owner (UBOs) in NGOs and the absence of accessible guidance and practical submission options have hindered compliance efforts, rendering it virtually impossible for many entities.

The postponement of deadlines and the ongoing debate over the Methodology for determining UBOs underscores the flaws in the regulatory framework. These issues, compounded by the impact of external events such as the Russian invasion, further demonstrate the need for a more balanced and effective approach to AML/CFT regulations that genuinely serves their intended purpose without placing undue burdens on civil society organizations.

Our key recommendation to FATF is to involve civil society in the regulatory process to avoid such consequences and financial exclusion. We advocate that NGOs should be removed from the list of entities obliged to report UBOs, both in the Law and in the Methodology. Should NGOs remain on the list, a proper communication mechanism must be established among the National Bank of Ukraine, other banks, and NGOs to prevent the blocking of banking services for NGOs."

The problem of the unclear definition of the ultimate beneficial owners for NGOs in the regulation appears not only in Ukraine. ODF has similar experience in Poland: the Polish regulations, to which local NGOs are subject to since 2022, in a manner similar to corporate entities, do not clearly specify who UBOs are in their cases. As the corporate governance of NGOs may be significantly different from that of companies, in many cases it is not possible to apply the provisions by way of direct analogy.

Practically, the understanding of the law in banks may vary and change. Sometimes, a bank, following its internal guidelines, may assume an NGO's founders as its sole UBOs. Another bank - or the same bank after changing the guidelines or compliance officers in charge - may require all members of supervisory and/or management bodies to be recognised as such. When the bank detects an inconsistency between the required statement made by the organization and the Central Register of Beneficial Owners (CRBR), it may suspend or close the NGO's account and notify the authorities of the alleged violation of the law.

Importantly, the aforementioned statement must strictly correspond to the bank's guidelines, otherwise the organization's banking contracts may be at risk of termination (even if the NGO, following its actual and current corporate governance model, identifies its UBOs differently, including more broadly). This creates both practical and legal issues, as in order to fully comply with the law, the NGO is obliged to make its own interpretation of the applicable provisions and provide the data of its "actual" UBOs in the filing with the CRBR.

RECOMMENDATIONS

1. Ensure regulatory approach which allows to use Convertible Virtual Currency mixing (CVC mixing), peer to peer Bitcoin and stablecoin transactions, use of self-hosted wallets, as tools for protection against transnational repressions, safeguarding privacy and human rights, and facilitation the work of civil society initiatives and the delivery of humanitarian aid;

2. Facilitate adoption of the S.831 - Transnational Repression Policy Act[51] to stop abuses of means of international cooperation by authoritarian regimes, including AML/CFT regulations.
3. Following the EU regulatory practice and OSCE PA Vancouver Declaration recommendations, ensure that legitimate credit and financial institutions shall provide measures to prevent unwarranted de-risking, ensuring non-discrimination and financial inclusion for customers, including those associated with higher-risk categories such as refugees, human rights defenders, individual users of crypto-assets, NGOs, and their representatives and associates;
4. Establish of additional security measures for protection against weaponization of personal banking and crypto-assets services providers data by authoritarian regimes.
5. Set exceptions for certain crowdfunding providers that use self-hosted cryptocurrency wallets for legitimate purposes such as humanitarian fundraising and introducing more flexible criteria for risk assessment.
6. Provide clarity on additional sources of information used to determine risk, which should be reliable and credible. This includes information from civil society organizations, the media, and commercial entities, such as risk reports.
7. Conduct public hearings to ensure inclusion of the positions of all interested parties, including human rights defenders, civil society representatives, software developers and crypto-assets investors. Ensure that FinCEN and US FATF representatives conduct regularly consultation addressing terrorism financing and money laundering abuses.
8. Continue open and regular engagement with all interested parties, including human rights defenders, civil society representatives, software developers, crypto-assets services providers and crypto-assets investors **to respect their position** as to the Digital Asset Anti-Money Laundering Act[52], and for other purposes, introduced Ms. WARREN (for herself, Mr. MARSHALL, Mr. MANCHIN, and Mr. GRAHAM).[53]

[51] https://www.congress.gov/bill/118th-congress/senate-bill/831/titles?s=1&r=15
[52] https://www.warren.senate.gov/newsroom/press-releases/warren-expands-coalition-of-banking-committee-support-for-bill-cracking-down-on-cryptos-use-in-money-laundering-drug-trafficking-sanctions-evasion
[53] https://www.warren.senate.gov/imo/media/doc/Digital%20Asset%20Anti-Money%20Laundering%20Act%20of%202023.pdf

Annex 1: False positives in AML/CFT compliance: their nature and consequences

General definition: **legitimate transactions flagged as suspicious by financial compliance systems** (e.g. banks, cryptocurrency exchanges, crowdfunding platforms). They can occur *accidentally* or be the result of *malicious (targeted)* actions against the person or entity in question by undermining their reputation. Upon further review, if carried out diligently (taking into account the sources of information in question), nothing suspicious would be found.

As indicted in the research paper published by the Italian Economic Journal (May 2022), apart from the detriment of the interests of law-abiding customers, they lead to ***Excessive and useless reporting****, known as the "crying wolf effect" (Takats 2011), is a crucial shortcoming that any anti-money laundering (AML) design aims to address and fix. The "crying wolf effect" harms the informational value of reports that banks and other professionals are obliged to file to comply with AML regulations.*[54]

Type	Description	How it works (examples)	Case study
Random	Unusual commercial transactions	Transfers for not provided services or undelivered goods, despite previous arrangements, are returned to the sender	Priorité Energie, which helps low-income families in Paris to insulate their homes under a government initiative, had its funds frozen and was told by Revolut that it would no longer offer services to the company. After Priorité transferred money to one of its suppliers in Czechia, he supplier was unable to deliver the goods and returned the money (the situation was reported in 2020).
Random	Crowdfunding and other fundraising actions	Regular cash deposits (as result of fundraising/charity actions - money collected to boxes during charity events) or bank transfers flagged as suspicious activity due to their frequency, varying/unusual transaction amounts or their form (cash). It may also stem from associations with specific, flag-raising context and keywords (support for Ukraine's military, body armours, helmets etc.)	Open Dialogue Foundation, other pro-Ukraine individuals and initiatives collecting funds and donating to the Ukrainian military or war-related humanitarian causes

[54] https://link.springer.com/article/10.1007/s40797-022-00195-2

Malicious	Smear campaign - fake news or overall negative publicity in the media/social media (even indirect - related to actual or perceived associates)	Politically motivated press and social media attacks accusing the customer of criminal activity, bogus commercial interests, links to sanctioned countries etc. carried out by non-democratic (e.g. Kazakhstan) and hybrid regimes as well as Western companies acting on their behalf to influence journalists and business intelligence firms (e.g. Refinitiv, Dun & Bradstreet)	Retaliatory attacks on Open Dialogue Foundation for criticism of human rights and rule of law violations in Kazakhstan, in Plahotniuc's Moldova and Poland since 2017; the same *modus operandi* in the cases of Kazakh, Belarusian, Russian and Turkish activists in exile
Malicious	Political prosecution by home or third countries and legal assistance requests	Dubious, politically motivated criminal investigations into alleged fraud, money laundering, extremism, terrorism, espionage etc. publicised in the media or transmitted to local law enforcement via mutual, European or bilateral legal assistance frameworks requesting banking data under a pretext of seeking evidence. Once a bank is approached by police or prosecutor's office with a request to disclose information on a person/entity in question, it flags the customer as highly suspicious and, subsequently, the bank terminates the customer's accounts	Retaliatory attacks on Open Dialogue Foundation for criticism of human rights and rule of law violations in Kazakhstan, in Plahotniuc's Moldova and Poland, included legal assistance requests from Poland (as European Investigative Orders) and from Moldova to Belgian authorities in 2019-2022;the same *modus operandi* in the cases of Kazakh, Belarusian, Russian and Turkish activists in exile

Malicious	Arbitrary designation as security threat	Secret opinions issued by special/security/intelligence services labeling customers as security threat for obscure reasons, which leads to their data being included in the national and European (Schengen Information System) databases of undesirable persons for political purposes - if publicised by e.g., the spokesperson of special services, they result in red flags at financial institutions. Also, as a part of politically motivated persecution, security and law enforcement services from different countries may exchange information concerning the customers and, request banking data flagging the customer. In the process of fulfilling this request, the bank may flag the customer as suspicious and trigger AML/CFT monitoring procedures.	Lyudmyla Kozlovska and Open Dialogue Foundation controversially labelled as security threat by rule-of-law rogue Poland in 2018 Ismail Sezgil, an exiled Turkish opposition political commentator had his accounts blocked and funds frozen in the UK and EU when Turkey's government published his data on the list of the Fethullahist Terrorist Organisation (FETO) alleged members. Kazakhstan, Belarus, Russia also abuse accusations of extremism, being a threat to the national security with the same pattern of targeting the activists in exile and those associated with them. The details are in the testimonials.
Random	Legitimate transactions involving high-risk country flagged as suspicious, based solely on their location or customers' countries of origin or customers'name s	Geographic location of the transaction serve as the only indication of suspicious transaction, without considering the actual transactional activity (e.g. support for opposition movements or family members)	Navalny's Foundation, Interim Government of Venezuela, BYSOL Foundation supporting anti-corruption and opposition activities, as well as supporting politically persecuted persons and their families in Russia and Belarus. Migrants and refugees from sanctioned countries or occupied territories (Donbas, Crimea)

Random	Use of crypto-assets	Donations received by an NGO from anonymous donors via its self-hosted wallet are transferred to the NGO's account on the cryptocurrency exchange - donors' anonymity raises compliance flags. Transfers from accounts on cryptocurrency exchanges to bank accounts deemed high-risk by banks due to the very use of crypto-assets, despite their intended purpose (donations for legitimate purposes), and difficulty of identifiying each donor.	Open Dialogue Foundation and emergency donations for Ukraine's support, Navalny's Foundation, Interim Government of Venezuela, BYSOL Foundation

Annex 2 to Joint submission of the civil society coalition:

Tools to prevent abuse of FATF anti-money laundering/financing of terrorism rules and address transnational repression

Testimonial of Obi Nwosu, *former CEO of Coinfloor, a regulated bitcoin exchange in the UK and Europe. Mr. Nwosu advocated for and worked with regulators, including the House of Commons Treasury Committee. He also advised the Metropolitan police, the Bank of England, HM Revenue & Customs, and the intelligence services in the UK. Coinfloor worked closely with regulatory advisors across Europe. Mr. Nwosu will explain the reason why civil society and politically-persecuted groups have been unintentionally marginalised because of the way the existing AML/CFT regulations and directives work within the UK and in the EU.* ***Page 20***

Testimonial of Lyudmyla Kozlovska, *president of the Open Dialogue Foundation (ODF) and a human rights defender from Ukraine. ODF is known for its support for Ukraine during the Maidan Revolution, its response to Russian aggression in 2014, and its advocacy campaigns to protect political prisoners. ODF has been campaigning for the Rule of Law in Poland since 2017, winning several libel cases against top government officials and other court disputes with the country's increasingly oppressive authorities. Despite the enforced, transnational persecution with SIS II mechanisms and disconnection from the banking system (following the abuse of AML/CFT laws and state-sponsored smear campaign), ODF has managed to operate and raise emergency funds for Ukraine through the use of crypto-assets like Bitcoin and Tether. Ms. Kozlovska advocates for EU regulators to provide remedies and prevent misuse of AML/CFT laws and support civil society activists using Bitcoin and stablecoins to address financial exclusion, political oppression and the delivery of humanitarian aid.* ***Page 23***

Testimonial of Jaroslav Likhachevsky, *co-founder of the New Belarus platform and Bysol Foundation and director of AI company Deepdee from Belarus. Mr. Likhachevsky is creating a Digital State for Belarus, outside of the reach of the Lukashenko's regime. In particular, Bitcoin and Tether stablecoinsare used to deliver humanitarian aid in Belarus by the Belarusian civil society and opposition to avoid mass arrests and political persecution.* ***Page 28***

Testimonial of Anna Chekhovich, *financial director of Alexei Navalny's Anti-Corruption Foundation (FBK) from Russia. Targeted by Putin's regime, the foundation has gradually lost access to financial institutions. FBK has been using Bitcoin since 2015 to help overcome financial repression. At that time, the Russian government began blocking the bank accounts of various foundations, even those very loosely connected to the FBK. Mr. Navalny and his family have also had their personal accounts frozen along with many people who worked on the FBK team. Bitcoin has given them a financial tool away from the reach of Putin's regime.* ***Page 30***

Testimonial of Ismail Mesut Sezgin, *Turkish opposition political commentator and research assistant at Regent's Park College, and self-employed business owner in the UK. Mr. Sezgin became a victim of abuse of AML/CFT mechanisms in 2021 in Turkey when he was listed by the authorities among the FETO members and his assets were frozen. It has severely affected his relations with financial institutions in European countries as well.* ***Page 32***

Testimonial of Fadi Elsalameen, *a prominent critic of corruption in the Palestinian Authority's government led by Mahmoud Abbas), an adjunct senior fellow at the American Security Project and the Bitcoin Policy Institute in the US. In 2021, the Bank of Palestine disclosed Fadi Elsalameen's financial records after Palestinian Authority fabricated a criminal case against him, accusing Mr. Elsalameen of money laundering, threatening national security in response to Mr. Elsalameen's anti-corruption investigations, exposing him and people associated with Mr. Elsalameen to retaliation, including an assassination*

attempt. To protect himself from total surveillance and harassment by corrupt Palestinian intelligence agencies, Mr. Elsalameen uses Bitcoin for his anti-corruption investigations. ***Page 34***

Testimonial of Jesús González, *a computer engineer and representative of the Venezuelan opposition, will share his experiences of allocating Venezuelan frozen funds in the United States via stablecoins under the "Heroes de la salud" project to more than 60,000 workers in the health sector during the Covid-19 pandemic. Many members of the Interim Government of Venezuela are subject to de-risking in EU countries because of trumped-up accusations by the Maduro regime, as well as their use of stablecoins for humanitarian aid.* ***Page 37***

Testimonial of Bota Jardemalie, *a Harvard Law graduate, is a licensed attorney in the State of New York and a human rights defender from Kazakhstan. For years, she has defended the Kazakh opposition, political activists, human rights defenders, victims of torture, and advocates for human rights, democracy, and the fight against corruption. In 2013, Bota Jardemalie was granted political asylum in Belgium due to the extraordinary risks she faced in the form of reprisals by Kazakhstan against her for her legal work that opposed the regime. The Council of Bars and Law Societies of Europe (CCBE) recognises Jardemalie as "lawyer in danger.* ***Page 39***

Testimonial of Jorge Jraissati, *the Director of Alumni for Liberty, an international network of young freedom activists with over 10,000 members from 139 countries. Its members include elected officials, think tank directors, journalists, academics, and other leaders committed to forming a global pro-liberty coalition. His initiatives include international advocacy, grassroots activism, policy proposals, training programs, research projects, and humanitarian efforts. Jorge is also an economist and a researcher at IESE Business School for the Center for Public Leadership and Government.* ***Page 42***

Testimonial of Roya Mahboub, *Roya has a D.Sc. Honorary Doctor of Science of Engineering from McMaster University, and she is a Fellow of Executive Education from Stanford University. Roya is a serial entrepreneur and one of the first female CEOs in her home country, Afghanistan. She is a CEO of the Digital Citizen Fund that focuses on digital literacy to bridge the gap between education and the job markets, and a founding leader of The NewNow, a group of rising global leaders tackling global challenges. Roya is also the founder and coach of the world-renowned Afghan Girls Robotics Team.* ***Page 43***

Testimonial of Suba Churchill, *executive director of the Kenya National Civil Society Centre and chairperson of the Horn of Africa Civil Society Forum, which is a regional African network of civil society organisations that is working together to monitor and expand civic space in the countries in which the Forum operates.* ***Page 44***

Testimonial of Tetiana Pechonchyk, *head of the Board of the Human Rights Center ZMINA, an organization that protects the freedom of expression, freedom of assembly and association, countering discrimination, preventing torture and ill-treatment, fighting impunity, supporting human rights defenders and social activists in Ukraine (including occupied Crimea) as well as protecting thoseaffected by the armed conflict in Ukraine. In May 2022, ZMINA received the OSCE Democracy Defender Award "for outstanding contribution to promoting and protecting fundamental freedoms and human rights in both non-government and government-controlled territories in Ukraine".* ***Page 47***

Testimonial of Michael Chobanian, *President of the Blockchain Association of Ukraine and a founder of the first cryptocurrency exchange in Ukraine, KUNA.io. Chobanian is an external adviser to Ukraine's Deputy Prime Minister and Minister for Digital Transformation of Ukraine, Mykhailo Fedorov. Since the start of Russia's full-scale war against Ukraine, Michael Chobanyan has launched a Crypto Fund for Ukraine to help the Armed Forces which has raised over $100 million of donations. At the request of the Ministry of Digital Transformation, Chobanyan helped the Government of Ukraine to create and manage state cryptocurrency wallets for donations in Kuna Exchange. Since 2020, representatives of authoritarian regimes of Belarus and Russia have been trying to obtain personal information about their opponents from*

the Kuna Exchange through abuse of AML/CFT laws, accusing their opponents of financing extremism and money laundering. Unlike Chinese platforms, Kuna Exchange refused to disclose information about its users due to politically motivated requests. Chobanyan therefore advocates that the regulation of democratic countries, in the EU, the US and Ukraine, should reflect preventive measures against abuses in AML/CFT regulation. ***Page 50***

Testimonial of Obi Nwosu, *former CEO of Coinfloor, a regulated bitcoin exchange in the UK and Europe. Mr. Nwosu advocated for and worked with regulators, including the House of Commons Treasury Committee. He also advised the Metropolitan police, the Bank of England, HM Revenue & Customs, and the intelligence services in the UK. Coinfloor worked closely with regulatory advisors across Europe. Mr. Nwosu will describe the reason why civil society and politically-persecuted groups were unintentionally marginalised because of the way the existing AML/CFT regulations and directives work within the UK and in the EU.*

My name is Obi Nwosu. From 2013 to 2021, I was the CEO of a UK-based Bitcoin exchange, Coinfloor, which had over 70% market share in the UK at one point. I was also the CEO of one of the first regulated Bitcoin exchanges in mainland Europe. During my tenure, we provided advice and education to various financial and intelligence institutions in the UK, such as the FCA, the Bank of England, and the Metropolitan Police, on how to use cryptocurrency to counter terrorist financing and reduce money laundering.

As someone with significant experience in both the cryptocurrency and regulated financial services industries, I want to emphasise that regulated financial institutions are committed to preventing terrorist financing and money laundering, as well as supporting human rights defenders and members of civil society. However, the current AML/CTF regulations often force them to inadvertently exclude, de-bank, or de-platform members of civil society.

This happens for four main reasons:

- The *"Know Your Customer"* (KYC) and *"risk-based approach"* to client onboarding
- The *"Travel rule"*
- The *"Tipping off"* rule
- The *"fitness and proprietary"* standards

I'll explain how and why this occurs below and make recommendations on what can be done to avoid this.

1. KYC, which stands for *"know your customer,"* is a process that financial institutions must carry out to verify the identity of their clients. The process is necessary because it helps institutions to identify and prevent the use of financial services by terrorists and money launderers.

While the KYC process is essential, it can be challenging for financial institutions to carry out the related risk-based approach without excluding innocent users. This approach requires institutions to assess the risk level of each new customer and determine if they are likely to engage in terrorist financing or money laundering. The assessment is often subjective, and there is no set formula to follow.

One of the major challenges faced by financial institutions is false information being spread about their clients, particularly those opposing, or targeted by, dictators and dictatorial regimes. This misinformation is often spread at a low cost through media channels and picked up by automated systems designed to check for adverse media about customers.

When negative news is flagged, financial institutions are required to spend time and money translating and fact-checking the information to decide whether to onboard the customer or not. This process can be time-consuming and costly, making it challenging for institutions to onboard the customers targeted by these regimes. In some cases, financial institutions may choose to de-bank or de-platform the customer instead of onboarding them, as it may be the more cost-effective solution.

In summary, while KYC is necessary, the related risk-based approach can be challenging for financial institutions. False information being spread about clients, particularly those opposing dictators and

dictatorial regimes, adds to the difficulty of the KYC process. Financial institutions must balance the cost of onboarding a new customer with the potential risk they may pose to their business.

2. The travel rule is a regulation that requires financial institutions, including those in the cryptocurrency space, to share KYC (know your customer) information with other financial institutions when their customers transfer funds. This is meant to prevent money laundering and terrorist financing by allowing the movement of funds to be traced through the global financial system. However, in countries where dictatorships exist, the banking sector is often captured by the regime. Therefore, any shared information with banks in those countries can be used and abused by those regimes. If an organisation, such as a human rights defender group, raises money in the West to help people living under a dictatorship, transferring that money through the banking system would reveal the organisation's bank details, which can put the recipients of the money in grave danger, as they may be monitored, imprisoned, tortured, or killed. The travel rule prevents members of civil society from using the banking system to safely send money to recipients living in countries under dictatorships or totalitarian regimes, which represents more than half the people on the planet. Even if a sending bank chose not to provide the information, it would not help because the non-compliance would stand out and potentially put the recipients at risk.

3. Tipping off refers to the requirements of financial institutions and their compliance departments, customer service departments, senior leadership team, and anyone who interfaces with customers to not explain or share their risk based approach rules and thresholds with affected customers. The reason why you would want to do this is clear from a money laundering/terrorist financing perspective.

If you were to explain the logic by which you decided to off-board a customer, then a group of money launderers or terrorist financiers could work out the logic you use to game the system so that they can always circumvent your controls by staying within the limits, rendering the risk based approach impotent. The problem with this is that dictatorships and authoritarian regimes know this. They know that if they keep spreading adverse media about someone, they will be off-boarded, and that when they are off-boarded or de-platformed, they will have no recourse. The financial institution is not able to explain the logic that they used to off-board them because that would be an example of tipping off, which would go against financial services regulation.

The problem here is that if you have been off-boarded incorrectly, complaining does not help. Part of the risk-based approach is often whether or not people are very forceful in how they deal with customer service agents. This is often suggested as a criterion financial institutions should take into account when deciding whether to onboard a customer. A customer who is often forceful with the customer service department, complains or pushes too much can be further identified as a high risk for money laundering. So not only do you have no recourse, but if you try to complain, that makes it even less likely that you will get an account or service.

4. As a former industry professional with nearly a decade of experience, I can attest to the importance of the fitness and propriety requirements in the regulated financial services industry. Fitness ensures that professionals know the law and regulation and that they are able to identify and act upon suspicious activity for the protection of customers and to reduce the risk of terrorist financing. However, the punishment for not behaving in a fit and proper manner can be extreme, including being stripped of your title and being unable to practise in the industry again. Propriety is also a subjective measure, which can lead to a risk-averse culture and a higher level of customers being off-boarded. Industry professionals are often silent about discrepancies or exploitable elements within anti-money laundering and terrorist financing rules due to fear of any potential negative impact on their careers. As a former industry professional, I feel it is important to speak up about these discrepancies when my former industry colleagues can not.

In summary:

Financial institutions are facing a complex challenge when it comes to providing services to members of civil society, activists, human rights defenders, and NGOs. In order to comply with regulations and protect against financial crime, institutions must implement KYC (know your customer) procedures and a risk-based approach to identify and mitigate risk and not *"tip off"* highlighted clients about their internal risk thresholds. They may also be required to screen for adverse media, and comply with the *"travel rule"* which mandates the sharing of certain customer information between financial institutions during transactions.

However, for some individuals and organisations seeking to be clients of these financial institutions, these requirements can result in being de-banked or de-platformed, with no recourse or allies within the industry to speak out against unfair treatment. This not only affects them, but also the thousands or even millions of people they support and represent, particularly those in marginalised parts of society or in other parts of the world who rely on them for financial support and aid.

As a result, these individuals turn to cryptocurrencies like Bitcoin and stablecoins as a last resort when they have no other banking options or cannot trust other banking options. They use these cryptocurrencies to send money to their loved ones, colleagues, or the people they are trying to help in destination countries without them being targeted by dictatorial regimes. The recipients can then convert the cryptocurrencies back into local currency and use them to further their objectives, such as getting food, water, and medicine or mounting a defence against the sitting dictatorships.

To address this issue, we requests two things:

Firstly, provisions should be put in place to enable members of civil society to seek recourse if they have been de-banked or de-platformed. This should be mandated by the government, and potentially a third-party ombudsman could be appointed to determine the reasons for the banks' actions and whether the person can be replatformed. This needs to be government mandated as the financial services institution has no financial incentive to do this otherwise and every incentive - both financial and regulatory - not to.

Secondly, members of civil society should be allowed to use services like Bitcoin and stablecoins and not be de-platformed or de-banked purely because they use these services. This is because these services act as the bank of last resort when there are few or no other banking services available and even with the first provision, the travel rule still precludes the use of the banking system in many cases.

Testimonial of Lyudmyla Kozlovska, *president of the Open Dialogue Foundation (ODF) and a human rights defender from Ukraine. ODF is known for its support for Ukraine during the Maidan Revolution, its response to Russian aggression in 2014, and its advocacy campaigns to protect political prisoners. ODF has been campaigning for the Rule of Law in Poland since 2017, winning several libel cases against top government officials and other court disputes with the country's increasingly oppressive authorities. Despite the enforced transnational persecution with SIS II mechanisms and disconnection from the banking system (following the abuse of AML/CFT laws and state-sponsored smear campaign), ODF has managed to operate and raise emergency funds for Ukraine through the use of crypto-assets like Bitcoin and Tether. Ms. Kozlovska advocates for EU regulators to provide remedies and prevent misuse of AML/CFT laws and support civil society activists using Bitcoin and stablecoins to address financial exclusion, political oppression and the delivery of humanitarian aid.*

ODF is a human rights NGO that was established in 2009 in Poland and has been headquartered in Brussels since 2018. ODF is known for its support for Ukraine during the Maidan Revolution[55], its response to Russian aggression in 2014[56], and its advocacy campaigns to protect political prisoners[57] and refugees.[58] Following the full-scale Russian invasion of Ukraine in 2022, ODF (via its Polish branch) launched a humanitarian aid delivery programme to provide protective equipment and other necessary resources to Ukraine's soldiers and refugees, having as of September 2023 delivered €8.31 million worth of aid.[59]

In 2017, ODF took a stance in defence of the rule of law in Poland. This was met with a campaign of legal harassment and disinformation, conducted by the Law and Justice government, alongside the Kazakhstani and then-Moldovan regimes that ODF had criticised. The Law and Justice government orchestrated numerous attempts to shut down or paralyse ODF and organised a smear PR campaign against ODF in Poland and within international institutions such as the European Parliament, the Parliamentary Assembly of the Council of Europe or the OSCE Parliamentary Assembly.[60]

In 2018, the Law and Justice government in Poland declared Lyudmyla Kozlovska a threat to national security based on a classified report by special services and subsequently banned her from entering Poland, abusing the Schengen Information System (SIS) as a tool for political persecution.[61, 62] In 2018, the Moldovan authorities, controlled by oligarch Vladimir Plahotniuc, accused Lyudmyla Kozlovska of financing the Moldovan opposition, of money laundering and of being a threat to national security.[63]

Both regimes have explored other existing mechanisms of international, European and bilateral legal cooperation that enabled transnational repression. Requests for international legal assistance were submitted to Belgian authorities by Poland and Moldova to obtain information, including banking data on ODF and members of its management.

In October 2022, the Parliamentary Assembly of the Council of Europe (PACE) passed a resolution urging to pay particular attention to *"alerts entered by States found in systematic breach of the rule of law"* and to "*make sure that the data in SIS are not entered for political reasons".*[64] This was part of the significant progress which has been made condemning the political misuse of SIS, the abuse of INTERPOL notices and politically motivated extradition requests.[65]

[55] https://en.odfoundation.eu/projects-and-campaigns/support-for-the-revolution-of-dignity-maidan/
[56] https://en.odfoundation.eu/a/4896,70-helmets-got-into-the-hands-of-donbas-and-aidar-battalions/
[57] https://en.odfoundation.eu/?s=&s_ph=political%20prisoners&s_tag[]=707
[58] https://en.odfoundation.eu/?s=&s_ph=refugees&s_tag[]=375
[59] https://en.odfoundation.eu/a/713785,summary-of-humanitarian-aid-to-ukraine-for-the-period-24-02-2022-30-09-2023/
[60] https://en.odfoundation.eu/a/9096,law-and-justices-campaign-against-the-open-dialogue-foundation/
[61] https://en.odfoundation.eu/a/8984,the-lyudmyla-kozlovska-case-timeline-updated/
[62] https://www.politico.eu/newsletter/eu-confidential/politico-eu-confidential-tv-star-to-run-slovenia-banned-from-schengen-summer-time-feedback-overload/
[63] https://en.odfoundation.eu/a/541007,moldova-dismisses-the-report-slandering-kozlovska-and-krameks-open-dialogue-foundation/
[64] https://pace.coe.int/en/files/31339/html%23S.embed_link-K.C-B.1-L.1.zw
[65] http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=28303&lang=en

ODF has won virtually all court disputes with the Polish authorities, including several libel cases (some proceedings launched by ODF against the authorities are still pending), and all the allegations against ODF have been proven false.[66, 67] These allegations have also been debunked by investigative reports in the press and via multiple analyses of the Foundation itself.[68] Also, the Supreme Administrative Court in Warsaw ruled that Lyudmyla Kozlovska's entry ban and subsequent expulsion from Poland, and temporarily, from the EU was arbitrary and unjustified, as the supposed evidence collected by the Polish security services *"does not warrant the conclusion that Kozlovska poses a threat to state security"*.[69]

However, despite this, financial institutions have started to view ODF as a high-risk client since around 2019. As a result, ODF's bank accounts in Belgium were closed, and the attacks on ODF also led to the closure of personal accounts and termination of all contracts of its executives (Lyudmyla Kozlovska, Bartosz Kramek, and Martin Mycielski) in Belgium and the UK, and in the case of Martin Mycielski to being placed on a permanent blacklist with BNP Paribas Fortis and KBC banks (as informed by them when trying to re-open accounts).

Fake news and published allegations against ODF and its executives, including accusations of money laundering and security threats, have influenced business intelligence agencies and tools such as Refinitiv and Dun & Bradstreet services. In 2018, a Refinitiv World-Check Risk Intelligence (Refinitiv) report was produced (and later updated) consisting of propaganda pieces from Moldova and Poland, which included an investigation against Lyudmyla Kozlovska in Moldova and a fake Russian passport allegedly owned by her. (See Annex 2 hereto)

Although the investigation of the prosecution in Moldova was closed as politically-motivated in 2020[70] after the democratic opposition took power in the country, just as the country's so-called parliamentary report into ODF was withdrawn in early 2023,[71,72] the banking system still considers the allegations to be true.

In the years 2019-2021, two Belgian banks, KBC and BNP Paribas Fortis, terminated the contracts with ODF and placed it on their blacklists, while virtually all other banks in Belgium (ING, Belfius, Beobank, Crelan, Keytrade, Argenta, AXA, Aion) rejected its application. Additionally, personal accounts of ODF's associates were closed by KBC, BNP Paribas Fortis and ING, while KBC and BNP Paribas Fortis also closed accounts of an affiliated company, KL Solutions SRL (owned by Lyudmyla Kozlovska and Bartosz Kramek). In 2020, the personal accounts of Lyudmyla Kozlovska, Bartosz Kramek, two other ODF associates and the corporate account of KL Solutions, were all closed by the UK-based Revolut. None of the banks provided reasons for these decisions, as they are not required to do so.

In 2022, the money transfer platform Wise closed ODF's account, presumably due to ODF's activities in support of Ukraine, which raised concerns about associations with the military conflict there.

Since then, ODF has been unable to open an account with other Belgian or foreign banks (having applied in banks in Poland, Estonia and Malta), effectively rendering ODF de-banked. Despite ODF's efforts to find legal remedy (as reported below), no effective solution has been found in Belgium.

[66] https://en.odfoundation.eu/a/336905,court-maciej-wasik-must-apologize-to-the-open-dialogue-foundation/
[67] https://en.odfoundation.eu/a/9523,20-lawsuits-filed-against-law-and-justice-interim-measure-against-tvp/
[68] https://en.odfoundation.eu/?s=&s_ph=fake%20news&s_tag[]=1364
[69] https://en.odfoundation.eu/a/478849,pis-once-again-lost-to-the-president-of-the-open-dialogue-foundation-the-supreme-administrative-court-overturned-the-verdict-of-the-neo-judges-in-her-case/
[70] https://en.odfoundation.eu/a/31239,moldova-has-closed-the-political-investigation-against-lyudmyla-kozlovska/
[71] https://www.parlament.md/ProcesulLegislativ/Proiectedeactelegislative/tabid/61/LegislativId/6331/language/en-US/Default.aspx
[72] https://en.odfoundation.eu/a/541007,moldova-dismisses-the-report-slandering-kozlovska-and-krameks-open-dialogue-foundation/

According to the European Banking Authority (EBA), the practice of de-banking as the result of de-risking higher-risk clients runs contrary to the provisions of Directive 2015/849 of 20 May 2015 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing.[73]

Detailed information on the timeline for de-banking ODF in Belgium can be found in the annex below.

ANNEX 1

Timeline of ODF's de-banking in Belgium

On 30 August 2021, BNP confirmed the termination of the business relationship with ODF and explained that it did not wish to disclose or discuss its customer acceptance policy and that its decisions were purely discretionary.

On 10 September 2021, BNP informed Ms. Kozlovska of the unilateral closure of her account in accordance with Article 14 of the General Terms and Conditions of BNP Paribas Fortis Bank.

On 23 September 2021, the directors of ODF wrote to the **International Cooperation Unit of the Brussels Public Prosecutor's Office** to inform them of their fear of being targeted by legal assistance requests on Belgian soil by the Polish authorities.

On 28 September 2021, ODF filed a complaint **with the Financial Ombudsman's office** concerning its debanking. The complaint referred to the possible political nature of the prosecution in Poland and the fact that unilateral account closure may constitute a practice contrary to the purpose of Directive 2015/849.

On 29 September 2021, one of ODF's board members, Martin Mycielski, filed a similar complaint regarding the closure of his personal accounts.

On 29 September 2021, ODF asked BNP to grant it **access to the basic banking service** provided for in Article VII.59/4 § 1 of the Economic Law Code as the legal conditions for access to such a service are met. Indeed, ODF did not appear to be able to find a banking institution willing to give it access to basic banking services (ING refused to open an account on 23 November 2018; KBC unilaterally decided to close the bank account in January 2021, while BNP terminated its contract on 10 August 2021). Following this last closure, ODF applied to every other bank offering services to non-corporate clients in Belgium, including Belfius, Beobank, Crelan, Keytrade, Argenta, AXA and Aion, but was informed that it would not be possible to open an account with any of them.

On 1 October 2021, **the Financial Ombudsman** declared ODF's complaint inadmissible, as it was a dispute between legal entities, and it was not competent to deal with it (having a mandate to interfere only when an individual is concerned). On the same day, the Ombudsman acknowledged receipt of Martin Mycielski's complaint and put it under review.

On 5 October 2021, BNP informed Bartosz Kramek of the unilateral closure of his account in accordance with Article 14 of the Bank's General Terms and Conditions.

On 15 October 2021, ODF reminded BNP Bank that under Article VII.59/4. § 3 of the Code of Economic Law, a refusal to provide basic banking services to a company must be explicitly and adequately justified in writing without delay and at the latest within ten working days of receipt of the request. In the absence of a response within this legal deadline, ODF requests BNP to open this basic service promptly.

[73] https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2022/Opinion%20on%20de-risking%20%28EBA-Op-2022-01%29/1025705/EBA%20Opinion%20and%20annexed%20report%20on%20de-risking.pdf

On 18 October 2021, the Financial Ombudsman issued an opinion on a complaint filed personally by one of ODF's executives, stating that he is not authorised to make a decision on the closure of ODF's current account. The Ombudsman acknowledged that ODF had applied for access to the basic banking service for companies, which was established in the law of 8 November 2020, but has yet to be fully implemented due to the absence of implementing acts. Given this legal gap, the Ombudsman requested that the bank extend the notice period until the legislation on basic banking services becomes fully effective. However, the bank only agreed to extend the notice period until 9 November 2021 and did not respond to the Ombudsman's proposal.

Regarding the personal accounts of board members, the Ombudsman's role was limited to verifying the terms and conditions prescribed by Article 14 of BNP's General Terms and Conditions. The Ombudsman confirmed that these procedures had been complied with. However, the Ombudsman understands ODF's point of view, supported by the nearly simultaneous closure of multiple accounts, but acknowledged that he does not have the authority to compel the banks to provide reasons for their decisions, which would enable him to take a position on the matter.

On 19 October 2021, **BNP notified ODF of its refusal to provide a basic banking service**. The bank explained that it had not responded earlier to the request for access to the basic service because of the ongoing proceedings with the Ombudsman. BNP then explains that its policy is not to offer such a service unless it is obliged to do so by designation pursuant to Article VII.59/4. § 3 of the Economic Law Code.

Faced with the impossibility of establishing a dialogue with BNP, the Ombudsman's inability to obtain acceptance of a temporary solution for maintaining access to banking services, and the subsequent refusals of other banks, **ODF filed a lawsuit against BNP** in November 2021.

On 18 November 2021 **AXA Bank in Belgium refused to open bank accounts to ODF** *"after examination of the request by AXA's head office"* and because *"the AXA Bank "Client acceptance policy" committee does not wish to enter into a client relationship"* with ODF: *"The decision to refuse a person, an organisation or a company is decided unilaterally by the head office of AXA and is irrevocable; there is no appeal against this possible and our agency (branch) has no say in this. The headquarters of AXA does not motivate this decision and therefore does not explain it"*. In prior months, similar refusals with even less information were received in writing or by phone from Belfius, Beobank, Crelan, Keytrade, Argenta and Aion banks.

On 3 February 2022 **the Brussels Court rejected ODF's lawsuit against BNP,** as it did not find sufficient grounds to regard it as *"emergency"* (which is one of the established conditions to involve the court) and considered actions taken by ODF to find an alternative to the closed account as non-exhaustive. Also, concerning the basic bank service, the courts considered the law as not yet applicable. Despite being fully deprived of access to a bank account and being financially excluded, ODF was ordered by a court to pay compensation to BNP in the amount of 1,560 euros.

ANNEX 2

In 2018, Refinitiv World-Check Risk Intelligence database produced this highly inaccurate report (it was updated in 2020), consisting of propaganda pieces from Moldova and Poland, which included a politically motivated investigation against Lyudmyla Kozlovska in Moldova and fake Russian and Moldova passports allegedly owned by her. World-Check Risk Intelligence has been used and trusted by the world's biggest companies for over two decades. Below are screenshots from World-Check Risk Intelligence:

EXTERNAL SOURCES	http://krs.infoveriti.pl/Fundacja,Otwarty,Dialog,Warszawa,Zarzad,KRS,0000353754.html http://krs.infoveriti.pl/Silk,Road,Biuro,Analiz,I,Informacji,Warszawa,Zarzad,KRS,0000416937.html http://www.canal2.md/news/presedintele-fundatiei-open-dialog-ludmila-kozlovska-a-fost-citata-la-procuratura-pentru-combaterea-criminalitatii-organizate-si-cauze-speciale_99452.html http://www.parlament.md/LinkClick.aspx?fileticket=BL60U7TezNI%3d&tabid=86&mid=488&language=ro-RO http://www.realitatea.md/ludmila-kozlovska--citata-de-pccocs-pe-un-dosar-de-spalare-de-bani-si-spionaj--doc-_88648.html https://deschide.md/ro/stiri/politic/39733/EXCLUSIV--Raportul-integral-al-comisiei-%E2%80%9EOpen-Dialog%E2%80%9D-inclusiv-paginile-SECRETE.htm https://ekrs.ms.gov.pl/krsrdf/krs/wyszukiwaniepodmiotu.podmiotdaneszczegolowe/RP/0000416937 https://en.odfoundation.eu/team/lyudmyla-kozlovska https://media.publika.md/md/other/201812/049e013c-dd6f-4e56-9234-77a6da9c477b_09888400.pdf https://odfoundation.eu/zespol https://www.publika.md/kozlovska-citata-la-pccocs-presedinta-fundatiei-open-dialog-va-fi-audiata-pe-27-decembrie_3029306.html https://www.zdg.md/stiri/politic/pccocs-a-incetat-urmarirea-penala-pe-numele-sefei-fondului-open-dialog-ludmila-kozlovzka/
LAST WORLD-CHECK UPDATE DATE	2020-05-13 11:26
ENTERED	2018-12-24

UID	[redacted]
VERSIONCREATEDDATE	2020-05-13 11:26
LAST NAME	KOZLOWSKA
FIRST NAME	Ludmila
ALIASES	KOZLOVSKA,Ludmila;KOZLOVSKA,Lyudmyla
LOW QUALITY ALIASES	
NATIVE ALIASES	
ALTERNATIVE SPELLING	
CATEGORY	INDIVIDUAL
TITLE	
SUB-CATEGORY	
POSITION	
AGE	
AGE DATE (AS OF DATE)	
DOB	1985/03/17
PLACE OF BIRTH	Sevastopol,Ukraine
DECEASED	
PASSPORTS	
IDENTIFICATION NUMBER	{PL-PESEL}850317[redacted]
LOCATIONS	~ Chisinau, Chisinau ~ MOLDOVA;~ Warsaw, Masovia ~ POLAND
CITIZENSHIPS	RUSSIAN FEDERATION;MOLDOVA;UKRAINE
E/I	F
LINKED TO INDIVIDUAL	
COMPANIES NAMES	Fundacja Otwarty Dialog;Silk Road Biuro Analiz i Informacji Sp z oo
FURTHER INFORMATION	[BIOGRAPHY] Deputy President of the Management Board of Silk Road Biuro Analiz i Informacji Sp z oo (Oct 2015 -). President of the Management Board of Fundacja Otwarty Dialog (Apr 2013 -). [IDENTIFICATION] ID no: PESEL 850317[redacted] Multiple Russian Federation/Moldovan/Ukrainian citizenship`s (reported Nov 2018). [REPORTS] Dec 2018 - reportedly under investigation by the Prosecutor Office for Combating Organised Crime and Special Causes (PCCOCS) on suspicions of alleged involvement in money laundering and espionage. Apr 2019 - no further information reported.
KEYWORDS	

Testimonial of Jaroslav Likhachevsky, *co-founder of the New Belarus platform, Bysol Foundation and director of AI company Deepdee from Belarus. Mr. Likhachevsky is creating a Digital State for Belarus, outside of the reach of the Lukashenko regime. In particular, Bitcoin and tether stablecoins are used to deliver humanitarian aid in Belarus by the Belarusian civil society and opposition to avoid mass arrests and political persecution.*

Our team is working on the Digital Belarus platform. In collaboration with the Belarusian pro-democratic movement led by Sviatlana Tsikhanouskaya, we have taken on the mission of creating a Belarusian economy in exile, with the next goal of establishing a democratic government in Belarus. Bitcoin and Tether stablecoins, in particular, are used to deliver humanitarian aid to Belarus and support pro-democratic and anti-Russian activists on the ground. Digital Belarus is a platform that helps to build horizontal connections and find sponsors for: an initiative, a foundation, or an individual to support. During this time, the platform has seen the emergence of fundraisers for campaigns and initiatives and personal fundraisers for those affected by the regime.

2020 for Belarusians was a year of rigged elections and enormous repressions by the Lukashenko regime. Thousands of people were detained, tortured, and beaten within the first days after election day, and hundreds of thousands of people lost their jobs due to their political activism.

Our response to the repercussions was solidarity - to support people willing to have a free and democratic country. That is how BySol started back in August 2020. During 2020 alone, about 4500 activists and initiatives on the ground were provided with financial support in the total amount of 2,934,719 EUR, 100% crowdfunded by Belarusian society itself.

We have two serious problems with banks in the EU member states:

First, our activists can only open bank accounts in Belarus or once leaving to exile, they are experiencing difficulties opening/holding accounts in the EU and CoE member states. There is no clear explanation how to prevent it - AML compliance is a black box that we cannot open. This problem was presented in the 2022 PACE Motion for Resolution entitled *"Addressing the specific challenges faced by the Belarusians in exile."*

Second, we cannot use the banking system to deliver financial support to activists in the country. The traditional way, via bank transfer, became dangerous and ineffective for civil societies in authoritarian regimes.

In November 2020, an incident with ByHelp (a partner organisation to Belarus Solidarity fund, based in the UK) occurred: the regime seized more than 500 000 EUR of support for thousands of activists in Belarus. This seizure of financial support happened because ByHelp used the banking system of Belarus which is controlled by the regime. The worst was that the regime received a list of every recipient of financial aid from ByHelp. Hundreds of activists were arrested, beaten, charged, and even sentenced. Everything that the regime was doing was done under the pretext of fighting against extremism, terrorism, and money laundering.

I would like to remind about the 2011 case of Ales Bialiatski, the current political prisoner in Belarus and the recipient of the Nobel Prize in 2022. In 2011, the regime in Belarus arrested Bialiatski under charges of tax evasion. The indictment was made possible by financial records released by prosecutors in Lithuania and Poland. Nowadays, regimes like Belarusian still collect financial information from Western democracies, using AML allegations as a pretext.

So, we, the Digital Belarus team, developed a solution to provide financial support, based on crypto assets. It was a safe and reliable way to support activists without the involvement of controlled financial institutions.

Throughout the whole activity period, BySol and Digital Belarus collaborated with various EU & US-based institutions. Recently the Federal Ministry of Finance of Germany showed interest in a crypto-based approach to delivering financial support. They needed to come into sight together with the SWIFT ban in Russia in order to be able to continue the implementation of the *"Holocaust Survivor Program"*.

Described above cases are showing that crypto-based mechanisms are a safe and secure solution to provide financial support for local activists, and organisations within territories controlled by authoritarian and totalitarian regimes.

Digital Belarus: Shipping of funds to Belarus is a small part of our current tasks. At the moment we are launching the Digital Belarus platform. Which is aimed to be a prototype for the future Belarusian Democratic state. At a certain point, the most important civil institutes (such as healthcare, education, and judiciary) started to fall apart under the Lukashenko regime. The only way for us to keep going was to build our own institute and services in parallel. The same, we have no other choice, but to build a parallel economy.

For example, in 2021 (COVID-19 pandemic year), the regime fired hundreds of medical doctors because of their civil position, with no chance to get a new job in healthcare in Belarus. We have built the telemedicine platform to enable online consultations for patients in Belarus, hiring the same doctors, who have been recently fired. The service is registered as an EU entity. We need to process cross-border payments: (1) Salaries to doctors from the EU to Belarus, (2) Payments from the patients to the platform. None of them are safe from being revealed by the regime if we use the traditional banking system. The only tool to provide privacy and security is crypto assets.

The next plans are to build democratic institutions, including taxation and representation. So, the people of Belarus could elect and finance their leaders and representatives (as Office of Svietlata Tsikhanouskaya). At the same time, Lukashenko's regime is considering the financing of civil and democratic initiatives as financing extremists or even terrorist organisations. That's why privacy and security are our top priorities.

In parallel, the Ministry of Interior of Belarus announced the development of a regulation to ban cryptocurrency peer-to-peer transactions between individuals, allegedly to combat criminal transactions.[74]

Similarly, under the pretext of "fighting fraud," on 29 August 2023, Alexander Lukashenko signed a decree on measures to counteract unauthorised payment transactions. This decree, which should be effective in six months - by 1 March 2024, will give law enforcement agencies of Belarus unorganised access to the financial information of Belarusian residents. Lukashenko's decree provides that "the provision of information about incidents from the automated incident processing system to law enforcement agencies of Belarus ... is not a violation of banking secrecy. Processing of personal data contained in the information on incidents shall be carried out without the consent of the individual."[75] Unfortunately, this law will become another tool for political repressions in Belarus.

To conclude: it is important for us to be able to use crypto assets in the EU like Bitcoin and stablecoins and not be de-platformed or de-banked due to the upcoming AML regulation.

[74] https://t.me/police_minsk/12242
[75] https://news.zerkalo.io/economics/47760.html?c

Testimonial of Anna Chekhovich, *financial director of Alexei Navalny's Anti-Corruption Foundation (FBK) from Russia. Targeted by Putin's regime, the foundation has gradually lost access to financial institutions. FBK has been using Bitcoin since 2015 to help overcome financial repression. At that time, the Russian government began blocking the bank accounts of various foundations, even those very loosely connected to the FBK. Mr. Navalny and his family have also had their personal accounts frozen as did many people who worked on the FBK team. Bitcoin has given them a financial tool away from the reach of Putin's regime.*

Since 2017, I have been working as its CFO. The Anti-Corruption Foundation is an organisation founded by Alexei Navalny. As many of you know, Alexei Navalny is now tortured in a Russian prison, he is constantly held in a freezing punitive detention cell in inhumane conditions, deprived of access to much needed medical help.

For years, Mr. Navalny's foundation and its staff have been persecuted in Russia. Since 2016, the ACF had been collecting a part of the donations in cryptocurrency. It was already clear at that time that collecting only fiat donations was unsafe for both the foundation and some donors, since the Russian banking system was fully controlled by the regime.

In 2021, after Alexei Navalny's arrest, the ACF was recognized as an extremist organisation, and was forced to leave Russia. Over 500 journalists and 70 human rights organisations and media outlets were forced to leave Russia as well. Most of these organisations have moved to EU countries, where they registered legal entities to continue their activities.

We, activists, were forced to leave Russia because of all the politically motivated allegations that we faced there. Most of those who left, like me, are not known to the international community. One of the serious problems that we face: we cannot open a simple bank account because of banks' AML compliance, or our bank accounts get closed without any explanation. Western banks treat us as potential money launderers, our transactions are treated as suspicious. We have to live without bank accounts which is impossible nowadays. The bank compliance process is not transparent and we cannot appeal or change banks' decisions. For example, in Georgia, banks close bank accounts to the Russians without any explanation, or sometimes, for a donation to the Ukrainian military (*ВСУ*).

Today, the Anti-Corruption Foundation is registered in Lithuania as NGO Future Russia Foundation. In addition to working on major opposition and anti-corruption projects, the foundation has to financially support political prisoners: Alexei Navalny, Lilia Chanysheva, and many others. The ACF covers lawyers' fees, and supports our activists in Russia. All payments are targeted, averaging no more than 500 euros.

Although all founders of the Future Russia Foundation are EU citizens, for a long time it could not even open an account, just because it has the word "Russia" in its name. More than 15 banks refused to open accounts for our NGO. In the end, we were able to open bank accounts, but the foundation cannot make any payments towards Russia through the banking system because the country is under sanctions. Even if it were possible to make such payments, it would put any recipient of funds in Russia at risk in the absence of proper protection against requests from third countries for such information.

Humanitarian aid is now only possible through cryptocurrency transfers, which remain uncontrolled and invisible to the Russian authorities. But today, the vast majority of European banks refuse to conduct transactions related to cryptocurrency. Over the last year we failed to find a bank that would allow us to buy cryptocurrency directly from the fund's accounts. Paysera payment system closed our account after an attempt to buy BTC.

The EU has banned all crypto-asset wallets, accounts, or custody services providing crypto payments of Russians within the framework of new sanctions against Russia. All crypto payments from Russians to European wallet providers are forbidden now. It means that NGOs like ours as well as human rights

defenders cannot support politically persecuted people in Russia. We have completely lost the ability of using European trustworthy crypto exchange services.

Thus, it has become absolutely impossible for the foundation to financially support activists who, risking their freedom and lives, are fighting the regime while in Russia. Most human rights organisations that have left the country have also encountered this problem.

Most initiatives to regulate cryptocurrencies in the EU refer to the misuse of money. Among other things, the use of cryptocurrency by Russian officials as a way to circumvent sanctions is mentioned. Russia circumvents sanctions in other ways, using countries that are friendly to it, and meanwhile, having been deprived of assistance from human rights organisations and NGOs, the opposition potential inside the country is declining at a colossal rate.

Regulations and restrictions on crypto-transactions will not play a significant role in the fight against sanctions circumvention, but they will cause enormous damage to the activities of activists and human rights organisations. This will not stop the officials, but it will have a significant impact on opposition movements.

Testimonial of Ismail Mesut Sezgin, *Turkish opposition political commentator and research assistant at Regent's Park College, and self-employed business owner in the UK. Mr. Sezgin became a victim of abuse of AML/CFT mechanisms in 2021 in Turkey when he was listed by the authorities among the FETO members and his assets were frozen. It has severely affected his relations with financial institutions in European countries as well.*

I believe that my case is a good example of transnational repressions and how regimes like one in Turkey can destroy lives of those who dare to speak up against them. At the end of the day, authoritarian regimes can reach even those who are in the EU and other democracies like the UK by abusing existing international institutions and regulations.

First problems with the government of Turkey I experienced back in 2016, after a failed coup attempt in Turkey. Although I lived in the UK, I wrote my Ph.D. at Leed Beckett University on the Hizmet Movement. So, naturally, after the coup, I wrote publicly and spoke about it on numerous occasions on this very crucial topic. I published YouTube videos[76] on understanding how the coup attempt was unfolded and what was happening in Turkey. I even was invited to BBC HardTalk[77] to talk about this very topic.

Obviously, it backfired. First in Turkey. Shortly, my YouTube channel as well as Twitter account were blocked by Turkish authorities. New accounts which I had opened to circumvent being blocked were also blocked shortly after they gained momentum. Patreon is a membership platform that provides business tools for content creators to run a subscription service and get financial support from their audiences. My Patreon account was also blocked in Turkey.

There have been credible reports that Turkey misuse the Interpol by reporting its dissidents' passports as stolen to disrupt their movements and potentially to get them deported back to Turkey. For this reason, I stopped travelling internationally even within the European Union's border, which was the legal advice I received at the time. I have not travelled until I received my UK Passport.

However, the worst was yet to come.

On 21 December 2021, Turkey's President Recep Tayyip Erdogan issued a presidential decree in which I was enlisted as a member of what the Turkish government define as *"Fethullahist Terrorist Organisation"* (FETO).[78] To fight any dissent, the regime in Turkey routinely labels innocent people as terrorists. As a result, my assets in Turkey were frozen and seized and my name was put in a financial blacklist internationally without any due process.

The decree has had a detrimental effect on my business and has caused immense stress. Every financial institution, even in the West, in the UK, started treating me as if I were a terrorist. The fact that my name has been added to a Turkish terror list destroyed by financial situation, and subsequently, my business and my well-being.

Every credit agency company relies on such lists in assessing a person's financial credibility. In November 2021, the Wise blocked the business account I created for the Centre for Hizmet Studies in the UK as soon as I opened. I provided them with the documents they requested and answered their questions, but they did not respond positively nor explained the reason for blocking the account. The compliance was not engaging in any discussion, nor giving me any chance to appeal their decision. And the same situation persisted.

In January, 2022 the Western Union started flagging by transactions both business and personal. Despite the fact that I again provided the documents they requested; my account was blocked. I, therefore, can

[76] https://youtu.be/vIsErcnaDD0
[77] https://youtu.be/lga89dtI6pU
[78] The decree, which was published in the Official Gazette of the Republic of Turkey, issue 31699, and can be viewed at https://www.resmigazete.gov.tr/eskiler/2021/12/20211224.pdf, page 63 for the decision, and page 68, line 34 for my name.

no longer be able to send or receive money for business or personal via Western Union. My regular business banking choice in the UK, the Barclays Bank has started asking additional, not typical questions with respect to my every ordinary business transaction, causing unreasonable delays in banking services, which negatively affected my business.

In September 2022, I made a lease application for a car but the application was held up. The leasing company did not even respond to my enquiries. The same month, I had a meeting with the TSB Bank to enquire about a possible mortgage. The mortgage expert said she would look into my case in the light of the notes in my report but admitted that it would be very difficult to process a successful application in my case. So, right now, I cannot continue with my studies, work as a self-employed entrepreneur, and have access to regular financial products as a loan or a mortgage.

I have to add that the situation is even worse for those who are in Turkey. Any financial support from European countries/other democracies is impossible for families of political prisoners and blacklisted activists in Turkey. People that the Turkish government has designated us as *"terrorists"* and put on a blacklist cannot send or receive money from or to their families and friends in Turkey. This is exacerbated by the fact that some people in Turkey have also been banned from banking in Turkey. More importantly, any financial interactions whether it is for business or providing financial support with those the Turkish government accuses of being a member of a terror organisation can and are being used as an evidence in itself of being a member of such organisation. Most recently, around 750 people were arrested in December 2022 on the grounds of providing help and financial support for family members of the jailed in Turkey. The operation was carried out by the Anti-Smuggling and Organized Crime Department (KOM), the Counterterrorism Bureau (TEM) and the Cybercrime Department in coordination with the Security General Directorate's intelligence unit and the Financial Crimes Investigation Board (MASAK). Those people did not commit any financial crimes, but they are treated as terrorists, smugglers and money launderers. And the western financial institutions treat them as such as well.

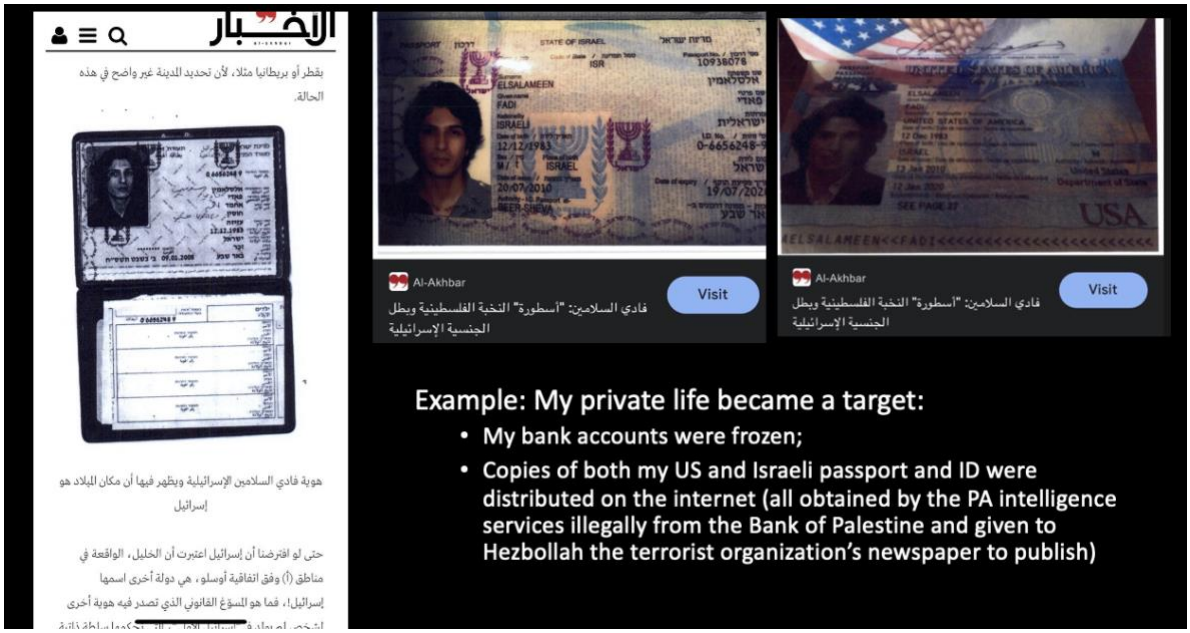
Testimonial of Fadi Elsalameen, *a prominent critic of corruption in the Palestinian Authority's government led by Mahmoud Abbas), an adjunct senior fellow at the American Security Project and the Bitcoin Policy Institute in the US. In 2021, the Bank of Palestine disclosed Fadi Elsalameen's financial records after Palestinian Authority fabricated a criminal case against him, accusing Mr. Elsalameen of money laundering, threatening national security in response to Mr. Elsalameen's anti-corruption investigations, exposing him and people associated with Mr. Elsalameen to retaliation, including an assassination attempt.*

To protect himself from total surveillance and harassment by corrupt Palestinian intelligence agencies, Mr. Elsalameen uses Bitcoin for his anti-corruption investigations.

Since 2009 I've been exposing human rights violations and corruption in Palestine, highlighting these issues in the US Congress and Senate, the US government and in social media. During my presentation I would like to bring your attention to 2 issues:

1. How the Palestinian security services weaponised banking to harass all forms of dissent and eliminate anyone who exposes the abuse of humanitarian aid or financial assistance from the EU and the US.
2. How Bitcoin has become a solution against abuses of corrupt regimes and connects communities in Israel and Palestine through Bitcoin transactions.

For the last 8 years the Palestinian Authority has obtained *de facto* complete control over the local banking system. As a result, the access to banking to journalists, critics and dissidents through the abuse of anti-money laundering regulations (AMLR) and anti-terrorism laws: this is just the tip of an iceberg made of physical violence, intimidation and even murder. I experienced it personally when in 2021 Bank of Palestine together with the Palestinian Intelligence Service froze my accounts and leaked my US and Israeli passport copies, home address, and detailed banking transactions to Al Akhbar newspaper, which is owned by the terrorist organisation Hezbollah.



The leak was intended to cast a shadow on me as a U.S. agent, thus deliberately sanctioning violent attacks against my life.[79, 80] I would like to draw your attention to the video which shows how it works in practice. The video documents P.A. security forces shot at my house with live bullets in March 2021 when I was visiting my family. We collected 60 live bullets shot to our house.[81] The PA never opened an investigation, and my sources inside Abbas office told me it was carried out by Majed Faraj men, the head of Palestinian Intelligence Service and with his orders.[82]

State Department officials including deputy assistant secretary for Israeli-Palestinian affairs Hady Amr subsequently raised the threats with Palestinian officials and stressed that the U.S. was concerned by the situation. Even after the State Department registered a complaint, the Palestinian Authority refused to condemn the death threat or call it off.

In order to protect myself from this kind of attacks and in a safe way support other anti-corruption activists in Palestine I'm using Bitcoin.

The political killing of Nizar Banat, a well-known anti-corruption critic of the Palestinian Authority, is yet another example. Nizar Banat was a candidate in the parliamentary election of the Palestinian legislative council had experienced all possible forms of political persecution: smear campaigns, surveillance through banking and financial institutions, torture, fabricated accusations.[83] Nizar Banat had already been arbitrarily arrested more than eight times for his critical comments on social media. After multiple attempts on his life, on the night of June 24th, 2021, Nizar Banat was politically killed by Palestinian Security Services.

It happened right after he called on the EU to freeze financial aid because of its misuse by the Abbas government and for its violations of human rights and fundamental freedoms. I would like to show a video of how he was arbitrarily arrested and tortured to death in the detention facility by 14 agents.

The EU representative, Heads of Mission of Canada, Norway and Switzerland issued a statement in agreement with the heads of the EU missions in Jerusalem and Ramallah calling for an immediate investigation into the murder of Banat through an independent body and in a fully transparent manner and bringing those responsible for his death to justice. In August 2022 UN Committee against Torture called for justice and expressed regrets that the P.A. has so far failed to ensure accountability for Nizar Banat's death. What did P.A.? In June 2022 president Abbas gave order to military court to release the 14 officers initially charged with Banat's death under the pretext of "the sanitary protection measures implemented during the COVID-19 pandemic".[84]

As Amnesty International[85], Human Rights Watch[86], independent media and Palestinian human rights activists have observed, none of those responsible for the political killing have been brought to justice. Instead - members of the Banat family, our lawyer and peaceful protesters are being prosecuted in fabricated criminal cases for calling on the EU, the US and the International Criminal Court to conduct an independent investigation and bring justice. P.A. are preventing the holding of a memorial ceremony for Nizar Banat in Hebron and preventing the family and friends from visiting his grave on 24 June 2022.

The European Parliament, in its latest resolution on Palestine in December 2022, called for transparent elections, an end to the repression of dissent, and accountability for human rights violations. Civil society

[79] https://casetext.com/case/elsalameen-v-bank-of-palestine-plc
[80] https://al-akhbar.com/Palestine/214280
[81] https://www.youtube.com/watch?v=oTCbgyFrOiM
[82] https://youtu.be/oTCbgyFrOiM
[83] https://www.youtube.com/watch?v=SvFDgfM_Y3g
[84] https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CAT%2FC%2FPSE%2FCO%2F1&Lang=en
[85] https://www.amnesty.org/en/latest/news/2022/06/palestine-authorities-have-failed-to-ensure-accountability-for-the-killing-of-nizar-banat/
[86] https://www.hrw.org/news/2022/06/30/palestine-impunity-arbitrary-arrests-torture

in Palestine welcomes this resolution while paying a very high price for the corruption of the regime of Mahmoud Abbas.

As the largest donor to Palestine and an influential actor, the European Union and CoE have a role to play: in particular, it needs:

1. to exclude of the Palestinian Interior Ministry and security services from European Union financial assistance until effective steps are taken to stop torture, hold liable those responsible for them, including the culprits of the assassination of Nizar Banat and release political prisoners;
2. to make sure that anti-money laundering and countering terrorism regulations (AML/CFT) are not abused by the Palestinian Authority to harass dissidents and crack down on civil society, demand from the Abbas government to release frozen assets of its critics;
3. prevent the abuse of AML/CFT regulations through mutual legal assistance to silence opponents abroad.

Testimonial of Jesús González, *a computer engineer and representative of the Venezuelan opposition, will share their experiences of allocating Venezuelan frozen funds in the United States via stablecoins under the "Heroes de la salud" project to more than 60,000 workers in the health sector during the Covid-19 pandemic. Many members of the Interim Government of Venezuela are subject to de-risking in EU countries because of trumped-up accusations by the Maduro regime, as well as their use of stablecoins for humanitarian aid.*

"I have been an opponent of the dictatorship of Chavez and Maduro for at least the last 15 years. Since 2019, I am also a member of the Interim Government of Venezuela headed by president Juan Guaido. Our Interim Government is recognized as legitimate by the international community.

The Venezuelan opposition wanted to use the Venezuela funds frozen in the US to provide direct financial help to activists, members of the opposition as well as to finance important social programs in Venezuela. We have managed to do it with the full support of the US government.

In 2020, during the pandemic, we implemented a program "Heroes de la Salud" that allowed us to convert designated US funds into stablecoins and via a direct fund transfer platform sent them to over 68 thousand health workers in Venezuela. How did we do it?

First, we needed to deal with the regulatory issues in the US. As I said, we agreed with the US government to use some funds of Venezuela frozen by the United States to help health workers, nurses and doctors. We had to comply with a number of legal and institutional requirements in order to obtain an OFAC licence for the use of the funds as we had proposed.

Second, we needed to find a way to transfer money to Venezuela. The banking system in Venezuela is controlled by the dictatorship. So, we needed to find a direct, decentralised, and secure mechanism to transfer money directly to the health workers. It was important to protect the identity of the beneficiaries of the program in order to avoid the regime's reprisals against them. We identified a US registered fiat-stablecoins payment platform. The platform used a P2P (peer-to-peer) decentralised payment model. We created a website that we linked to the payment platform. All beneficiaries of our program needed to go to the website and register in order to be qualified for the program. They had to register and submit required documents to prove the work they performed. We did the registration and verification of the beneficiaries of the program according to the parameters developed together with the US government.

Third, the information about the program and the website for the registration we circulated mainly via direct mass emails to email addresses on our mailing lists that we had prepared in advance.

So, through this program, we allocated approximately 20 million USD in stablecoins to over 68 thousand health workers. Each participant in our program received the equivalent of 100 USD in three equal tranches that they could withdraw in local currency if necessary.

We worked hand in hand with the United States government to implement this program, and after successfully completing it, we replicated the payment mechanism with frozen funds via digital platforms and stablecoins to all areas of the Interim Government. That allowed us to continue operating to fight for freedom of our country without putting our personal security at risk. Currently, around 20,000 monthly secure payments have been made through this mechanism in Venezuela, both for the benefit of interim government officials and for NGO and civil society initiatives. The mechanism works and is scalable. We have used it for many other programs, financed not only by the US government but also by European governments, such as Germany.

This mechanism also allows us to overcome some obstacles that have been imposed on us by the international financial system just for being defenders of human rights and freedom.

As human rights defenders and members of the opposition, like Leopoldo López, well-known pro-democracy activist and Sakharov prize laureate, we routinely face problems with bank compliance in the EU. Many of my colleagues from Venezuela cannot even open a bank account in the EU as the banks do not want to deal with them. The banks prefer to de-risk and close our accounts and/or freeze our payments. I am relatively lucky, because in addition to the Venezuelan passport, I am a holder of Spanish citizenship. So, I am still can have a bank account in Spain, although I regularly have compliance problems with my bank."

Testimonial of Bota Jardemalie (Kazakhstan, political asylum in Belgium): *Bota Jardemalie, a Harvard Law graduate, is a licensed attorney in the State of New York and a human rights defender from Kazakhstan. For years, she had defended the Kazakh opposition, political activists, human rights defenders and victims of torture, advocates for human rights, democracy, and the fight against corruption. In 2013, Bota Jardemalie was granted political asylum in Belgium due to the extraordinary risks she faced in the form of reprisals by Kazakhstan against her for her legal work against the regime.*

The Council of Bars and Law Societies of Europe (CCBE) recognises Jardemalie as "lawyer in danger."[87, 88, 89]

I have been persecuted by my country Kazakhstan for years for my legal work in support of political victims of the Kazakhstan regime. I provided counsel and support to members of the democratic opposition, political activists and independent media of Kazakhstan.

Despite my political asylum, I remained in danger even in Belgium. At Kazakhstan's request, in 2013 INTERPOL published a Red Notice to arrest me on fabricated charges of alleged embezzlement of BTA Bank in Kazakhstan. Later INTERPOL cancelled this Red Notice for non-compliance with the rules against political abuses of INTERPOL. Kazakhstan's regime twice tried to extradite me from Belgium unsuccessfully. Belgium refused those extradition requests.

Kazakhstan has been trying very hard to stop me from doing my work. In late 2014, I received a credible threat that I was in danger and, I quote, "the Kazakhs hired people to either kidnap you or turn you into a vegetable." The Belgian federal police launched an investigation of a criminal conspiracy targeting me. Three individuals, two former agents of the STASI (the East German secret police) and a Russian national, came under scrutiny by the Belgian federal police for criminal conspiracy, forgeries and use of forged documents, use of false identity, and impersonation of agents of public authority, all of these alleged crimes committed in order to locate and/or to kidnap me.[90] On 29 November 2019 those individuals were sentenced by the Brussels Criminal Court.[91]

After their attempts at extraditing me and physically harassing me failed, in 2016, a proxy for the Kazakhstani regime, BTA Bank, filed a criminal complaint against me in Belgium, accusing me of money laundering on Belgium soil. The Federal prosecutor dismissed (*non-lieu*) the case ("*Il n'existe aucune charge contre Botagoz Jardemalie*''). However, Kazakhstan's agent, backed by the unlimited resources of an oil-rich state, persisted in appealing the decisions of the Instruction Judge and the Federal Prosecutor, continuously demanding further investigative steps to be taken against me. It took six years of relentless legal harassment by Kazakhstan's proxy until April 25, 2023, when the Chamber du Conseil of the Tribunal of the First Instance of Brussels completely dismissed the criminal investigation against me. The Tribunal also ordered BTA Bank to compensate me with €15,000 in procedural compensation and an additional €5,000 *ex aequo et bono*, as recompense for the temerarious and vexatious procedure. This case serves as a clear example of the abuse of AML regulations and illustrates a form of SLAPP—Strategic Lawsuit Against Public Participation, another tool of transnational repression.

Using allegations in money laundering as a pretext, Kazakhstan made at least three mutual legal (MLA) assistance requests to Belgium to receive all my banking information, all my electronic devices, and my professional legal files. These requests have been some "fishing expedition" – attempts to obtain my

[87] https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/HUMAN_RIGHTS_LETTERS/Kazakhstan_-_Kazakhstan/2018/EN_HRL_20180423_Kazakhstan_Concerns-over-lawyer-Botagoz-Jardemalie.pdf
[88] https://www.lawsocieties.eu/news/avocats-en-danger/6000558.article
[89] https://protect-lawyers.org/en/item/botagoz-jardemalie-3/
[90] https://www.lepoint.fr/societe/barbouzerie-kidnapping-piratage-l-incroyable-histoire-de-l-homme-le-plus-traque-d-europe-16-11-2021-2452171_23.php
[91] https://www.lesoir.be/263653/article/2019-11-29/trois-barbouzes-condamnes-pour-lespionnage-de-la-refugiee-kazakhe-bota

professional files as lawyer and human rights defender.[92] Two Belgian banks provided behind my back all my banking information, including account transactions and my personal identification, to the regime that persecuted me for years, without my knowledge or consent.

As a result, the regime tried to use this information to track my movements, monitor my financial activity, and wanted to use it as evidence against me in a fabricated criminal case. This personal information was shared without my knowledge or consent, putting me in danger and compromising my rights as a political refugee.

In April 2018 the Minister of Justice of Belgium accepted one of the mutual legal assistance requests filed by Kazakhstan, without carrying out proper verification required under the law, failing to protect a refugee and to respect the rights of a lawyer and the legal profession. At the request of the Kazakh authorities, on October 1, 2019, the Belgian police, accompanied by two unidentified Kazakh officers, searched my Brussels apartment.[93] My professional documents and computer equipment were seized. At the time of the execution of this MLA request, no judicial remedy in Belgium was available to me to enable me to protect my fundamental rights and prevent further violation of those, who I was helping, including Kazakh political activists, journalists and victims of torture.[94] However, on 13 January 2022, the Constitutional Court of Belgium in its judgement 1/2022[95] upheld my position, ruling that, despite the absence of a right explicitly provided for by the law, the remedy should exist for someone in my position when the request for mutual legal assistance comes from a non-EU Member state, and it was necessary to provide me a right of appeal in Belgium in order to be able to challenge the legitimacy of the mutual assistance in criminal matters requested by Kazakhstan. (Constitutional Court, judgement 1/2022)

In parallel, for years, I have been a target of a very aggressive smear PR campaign in 5 languages online, sponsored by the Kazakh regime. As a result of negative PR, I started experiencing problems with banking: banks in Belgium closed my bank accounts without any explanation and refused to open her a bank account. I also was blocked from making a Western Union transfers.

Having been unsuccessful in neutralising me as a lawyer and human rights defender whether by having me arrested, extradited or kidnapped, in November 2017, Kazakhstan arrested my older brother, Iskander Yerimbetov, who still lived in Kazakhstan.[96] He was arrested based on false allegations in money laundering of funds allegedly stolen from BTA Bank. His arrest was therefore both a reprisal against me for my work, and a means of pressuring me to cease advising victims of the regime. When arrested, officers of the Secret service of Kazakhstan demanded that my brother persuade me, his younger sister, to return to Kazakhstan. My brother refused to cooperate.[97] He was severely tortured[98, 99] and sentenced for 7 years.[100] His case was recognized as politically motivated by international institutions and organisations that demanded his immediate release.[101, 102, 103, 104] On December 7, 2018, the United Nations Working Group on Arbitrary Detention (UN WGAD) concluded that my brother was detained in violation of international law and urged his immediate and unconditional release.[105] My brother was

[92] https://pace.coe.int/en/files/30051/html
[93] https://parismatch.be/actualites/politique/332927/lincroyable-traque-dune-dissendente-kazakhe-exilee-en-belgique
[94] https://www.fidh.org/en/issues/human-rights-defenders/belgium-kazakhstan-judicial-harassment-against-ms-botagoz-jardemalie
[95] https://www.const-court.be/public/f/2022/2022-001f.pdf
[96] http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=24490&lang=en
[97] https://pace.coe.int/en/files/25176/html
[98] https://www.hrw.org/news/2018/02/15/kazakhstan-businessman-alleges-torture
[99] https://pace.coe.int/en/files/30207/html
[100] https://www.nhc.no/en/kazakhstan-must-release-iskander-yerimbetov-and-co-defendants/
[101] https://www.osce.org/permanent-council/403400
[102] https://www.europarl.europa.eu/doceo/document/TA-8-2019-0203_EN.pdf?redirect
[103] https://www.rubio.senate.gov/public/_cache/files/9b633465-8854-445f-a677-69a7f628505f/7DC6415F07E32C5C0BF1D3273EBBB27F.07-29-19-bipartisan-letter-on-kazakhstan-political-prisoner.pdf
[104] http://semantic-pace.net/tools/pdf.aspx?doc=aHR0cDovL2Fzc2VtYmx5LmNvZS5pbnQvbncveG1sL1hSZWYvWDJILURXLWV4dHIuYXNwP2ZpbGVpZD0yODIzNyZsYW5nPUVO&xsl=aHR0cDovL3NlbWFudGljcGFjZS5uZXQvWHNsdC9QZGYvWFJlZi1XRC1BVC1YTUwyUERGLnhzbA==&xsltparams=ZmlsZWlkPTI4MjM3
[105] https://www.ohchr.org/sites/default/files/Documents/Issues/Detention/Opinions/Session83/A_HRC_WGAD_2018_67.pdf

released in December 2019. In 2020, he and his family received humanitarian visas from Switzerland, and in 2021, they were granted political asylum in Switzerland.

My case illustrates the abuse of AML laws as well as international cooperation mechanisms and banking information by authoritarian regimes to persecute individuals who stand up against them. It is a clear example of how far such regimes will go even in the EU to silence their critics. I believe that this case serves as a reminder that we must remain vigilant in protecting the rights of refugees and defending against the misuse of international legal instruments.

Testimonial of Jorge Jraissati, *the Director of Alumni for Liberty, an international network of young freedom activists with over 10,000 members from 139 countries. Its members include elected officials, think tank directors, journalists, academics, and other leaders committed to forming a global pro-liberty coalition. His initiatives include international advocacy, grassroots activism, policy proposals, training programs, research projects, and humanitarian efforts. Jorge is also an economist and a researcher at IESE Business School for the Center for Public Leadership and Government. His articles can be found in publications like Economic Affairs, the Brookings Institution, and Foreign Policy. He has been a guest speaker at institutions like the European Parliament, forums like the Copenhagen Democracy Summit, and universities like Cambridge and Harvard.*

The use of Bitcoin as a tool to overcome financial and political oppression:

As director of Alumni For Liberty (an international network of young leaders with over 10,000 members from 139 countries), I would like to discuss and work on addressing the problem of financial exclusion and abuse of Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) regulations.

In essence, we have identified that authoritarian regimes and illiberal governments have been abusing FATF recommendations, weaponizing the international banking system as a tool for domestic and transnational repression.

As these states abuse their power, our activists have turned to Bitcoin as their "bank of last resort." Between Alumni For Liberty and our umbrella organization (Students For Liberty), we have used Bitcoin to finance activities in over fifty countries, and we currently have 29 staff members who receive their payments through Bitcoin.

For instance, in authoritarian countries like Venezuela and Myanmar and illiberal democracies like Bolivia and Hungary, many of our activists reported that their bank accounts were used by regimes to create false political claims, disinformation, and legal accusations against them. We have also documented sixty cases where grassroots leaders reported the termination of their bank accounts for political reasons. Similarly, activists of our organization from fifteen countries (such as Venezuela, Uganda, Nigeria, Ghana, Belarus, Russia, Burundi, Rwanda, Chad, Bangladesh, Lebanon, Sudan, Pakistan, Myanmar, and Tanzania) have reported using bitcoin as their bank of last resort as protection from political repression because of the abuse of the FATF recommendations that shape AML/CFT laws.

An even more worrisome situation lies in the fact that financial exclusion for political reasons is not limited to authoritarian contexts. The public seems to think that activists in exile are safe from financial exclusion. However, many human right defenders currently living in democratic countries are deprived of the right to have financial services. This happens as activists are often the target of disinformation campaigns and fabricated criminal allegations, which trigger de-risking mechanisms in bank compliance.

This means that bank compliance requirements that were originally established to adhere with AML/CFT laws end up harming human rights defenders even at the very heart of the European Union and several democratic countries, violating the right to financial services. In fact, this problem goes beyond the termination of their accounts. Currently, there are several transnational legal assistance frameworks that allow malicious governments to access sensitive information of their opponents abroad, including their banking data. This practice can endanger even the physical safety of these citizens.

For these reasons, we have to address this issue. It is frustrating to see authoritarian regimes developing tools for transnational repression based on the FATF standards and Recommendations, such as FATF recommendation 8 on non-profit organisations. Since Germany is one of the key members of the Financial Action Task Force, what we propose is to create spaces for dialogue between regulators and civil society. This cooperation will enable us to build mechanisms to prevent the unintended consequences of the FATF standards, as well as instruments to protect the financial rights of all law-abiding citizens.

Testimonial of Roya Mahboub, *Roya has a D.Sc. Honorary Doctor of Science of Engineering from McMaster University, and she is a Fellow of Executive Education from Stanford University. Roya is a serial entrepreneur and one of the first female CEOs in her home country, Afghanistan. She is a CEO of the Digital Citizen Fund that focuses on digital literacy to bridge the gap between education and the job markets, and a founding leader of The NewNow, a group of rising global leaders tackling global challenges. Roya is also the founder and coach of the world-renowned Afghan Girls Robotics Team. Roya has received several awards including Time's 100 Most Influential People in 2013, the 2014 Tribeca Disruptive Innovation Award, The 2015 Advancement of Gender Equality through Education Award, Young Leader of World Economic Forum, 2018 Wonder Women 2018, and 2019 Education Award Winner, and the prestigious Presidential Leadership Scholarship.*

In 2013, I founded Women's Annex, a digital platform that allowed women in Afghanistan to earn money by publishing their content. However, the platform faced challenges due to the inability to pay women-contributors directly, as many lacked bank accounts and money had to be deposited into the account of a male relative. A man – that male relative - could easily take the money for himself and nothing could be done about it.

At first, we paid Women's Annex's employees and contributors in cash. The problem was that the women wanted to send the money to family and pay vendors in different parts of the country. They used the hawala system, an 8th-century money transfer process that relied on brokers and a web of trusted intermediaries. This ancient platform was dated, slow, and reliable for women, many of whom already had Nokia cellphones and had started to create and use their own Facebook accounts. Sometimes the money did not make it through the hawala system, and it was hard to verify that the whole amount reached the recipient. So, I researched the idea of mobile money. As it turned out, cellphone-based payment systems like M-PESA, which worked so well in Kenya, never took off in Afghanistan. PayPal was still not available because of U.S. sanctions.

To overcome this obstacle, my team implemented a crypto payment system using Bitcoin and stablecoins, which allowed our women to receive payments directly to their digital wallets, without interference from male relatives. Bitcoin and stablecoins allowed the organization to overcome physical and social obstacles in paying Afghan women. With a simple transaction, Bitcoin and stablecoins could instantly appear in a woman's digital wallet, without interference from men.

Later, with my Digital Citizen Fund, I began to increase Afghan women's technological and financial literacy**,** particularly with the use of crypto assets such as Bitcoin and stablecoins to enable financial inclusion and privacy. My team has trained over 17,000 young women in coding, digital skills, and entrepreneurship, and has built dozens of internet classrooms and mobile computer labs across Afghanistan. We tried to develop practical skills and foster self-reliance among women, breaking down traditional cultural barriers that limit them to domestic duties.

Since August 2021, bank and wire services like Western Union, MoneyGram have run out of paper currency and have cut off services, leaving one-third of Afghans struggling with food insecurity and 50-70% with unstable housing situations. Websites like GoFundMe have been blocked from fundraising efforts for "compliance" reasons. Bitcoin and stablecoins have provided a crucial financial lifeline for many during these difficult times, who stay in the country and continue working behind closed doors. So, while the Taliban could crush local businesses or shut down financial modernization plans, they cannot stop Bitcoin. My team in the US continues helping many young women — including some of the stars of Afghanistan's female youth robotics team Afghan Girls Robotics Team that have not left Afghanistan.

Testimonial of Suba Churchill, *executive director of the Kenya National Civil Society Centre and chairperson of the Horn of Africa Civil Society Forum, which is a regional African network of civil society organisations that is working together to monitor and expand civic space in the countries in which the Forum operates:*

I am a member of Kenya's Universal Peer Review (UPR) process, and I can at best describe the National Risk Assessment on Money Laundering and Terrorism Financing for Kenya as a farce.

Besides, I am also an active member of the Kenya NPO Coalition on FATF, a coalition of Kenyan NPOs that has been creating awareness of the FATF and its processes, including Risk Assessments and Mutual Evaluation Review since 2019.

In December 2014, the Non-Governmental Organizations Coordination Board deregistered 510 organisations under its regulation, 15 of them accused of links to terrorism[106]. Some of them were even linked by the regulatory authority to the 1998 twin bombings of the US embassies in Kenya and neighbouring Tanzania while the others were deregistered for failure to file annual returns as required under the law.

On April 7, 2015, the government published in the official government gazette a list comprising 86 individuals and entities, including two human rights organisations namely, Muslims for Human Rights (MUHURI) and Haki Africa for what it claimed that the affected individuals and organisations supported terrorism[107].

In their defence, Haki Africa and MUHURI accused the government of targeting them for their important work documenting human rights violations committed by the security forces, including against individuals especially youth suspected of engaging in terrorism.

The court later absolved the two human rights organisations as indeed most of the 86 organisations that had been falsely accused of supporting terrorism.

The gazette notice gave the listed entities and individuals one day's notice to demonstrate to the authorities "why they should not be declared as a 'specified entity'''.

Being declared a "specified entity" has wider implications beyond bank account freezes. Under the Prevention of Terrorism Act (POTA) of 2012, "specified entities" are equated with "terrorist groups." Membership in a terrorist group is punishable by up to 30 years' imprisonment.

According to international standards regarding counterterrorism measures, governments should ensure a transparent listing and delisting process, based on clear criteria, with an appropriate, explicit, and uniformly applied standard of evidence, as well as an effective, accessible, and independent mechanism of review for the individuals and entities concerned.

The POTA does not provide a mechanism for appealing the decision of the committee, which may violate both the Kenyan constitution and international law. Article 47 of Kenya's 2010 constitution provides for fair administrative action that is expeditious, efficient, lawful, reasonable, and procedurally fair. International law prohibits the imposition of government sanctions without adequate due process.

The Kenya NPO Coalition on FATF was initiated by the Kenya National Civil Society Centre and Muslims for Human Rights to mitigate some of these excesses of the State.

[106] https://www.bbc.com/news/world-africa-30494259
[107] https://www.hrw.org/news/2015/04/12/kenya-ensure-due-process-terrorism-list

Consultation of NPOs has been done remotely, and **without their knowledge of what one is being drawn into**. I would like to use my own example to show how **Kenya's state security agencies are engaged in harassment of non-governmental organisations but claim that this was consultation on FATF standards**.

The entire process of **the National Risk Assessment for Kenya on Money Laundering and Terrorism Financing** in my view, has always been **shrouded in unnecessary secrecy**, and is approached by the concerned Kenyan authorities as (1) an investigation into an already established crime (2) in which the Not-for-Profit sector is presumed guilty until proven innocent despite the country's constitutional provision of presumption of innocence until one is proved guilty by a court of competent jurisdiction.

In 2021 I was ambushed by a former colleague at the university who now works with one of Kenya's State security agencies. I was strolling along the beach after a day-long workshop in my capacity as a member of Kenya's UPR process at the Travellers Beach Hotel and Club when I bumped into this former college-mate who happened to have been at the nearby Whitesands Hotel. Suddenly, he seemed unusually happy that we were meeting again after a long while. He invited me to join him and his colleagues at the poolside of their hotel. Very quickly, our conversation with him and his colleagues degenerated into what tended more towards **an interrogation ensued**.

Judging from the manner in which one of his colleagues was writing down every word I uttered almost verbatim, it was clear that they were extracting extremely valuable intelligence and important information from me.

After we finished, I went to my hotel and called my former college-mate to ask why we had had this type of strange official conversation at the pool with his colleagues and why one of them had been taking notes of everything I had said. He declined to explain, adding that it was a sensitive matter we could discuss in-person later.

Later we met again over coffee. He explained in a rather low tone what their mission at the Whitesands Hotel had been all about. **They had been at the hotel for three weeks conducting the National Risk Assessment for Kenya on Money Laundering and Terrorism Financing, and had been at a loss how they would "get some insights from the civil society on the matter"!**

Rather than to have a process that assists the Government and its competent authorities to assign responsibilities for combating money laundering, terrorism financing and proliferation financing (ML/TF/PF) to the relevant line ministries/government agencies on the basis of the identified risks and vulnerabilities, the Kenyan authorities organised interrogations of civil society activists at the poolside!

I later learned that Muslims for Human Rights and Haki Africa were interrogated in the same way.

The way the Kenyan authorities conducted the National Risk Assessment has not assisted in prioritising and allocating anti-money laundering and combating financing of terrorism (AML/CFT) resources efficiently to ensure that a larger proportion of resources are allocated to areas that present higher ML/TF risks.

In fact Kenyan authorities did not contribute to the institutional risk assessments for anti-money laundering and countering the financing of terrorism (AML/CFT). These assessments are intended to support reporting institutions, such as financial institutions and designated non-financial businesses and professions, in evaluating the effectiveness of their internal controls for AML/CFT, including the implementation of a risk-based approach. They did not prepare Kenya for its 2nd Round of Mutual Evaluation by the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG) that was ongoing at the time, where strong focus was placed on the general understanding of the ML/TF risks facing the country and the application of a risk-based approach to mitigate the identified risks.

Shocked at the revelation, the Kenya National Civil Society Centre (KNCSC) and the Civil Society Reference Group (CSRG) teamed up with Muslims for Human Rights (MUHURI) in 2021 in a process that culminated into a shadow report titled: **Civil Society Perspectives on Kenya's National Risk Assessment and Mutual Evaluation Review Processes**.

Testimonial of Tetiana Pechonchyk, *head of the Board of the Human Rights Center ZMINA, an organization that protects freedom of expression, freedom of assembly and association, countering discrimination, preventing torture and ill-treatment, fighting impunity, supporting human rights defenders and social activists in Ukraine, including occupied Crimea, as well as protecting persons affected by the armed conflict in Ukraine. In May 2022, ZMINA received the OSCE Democracy Defender Award "for outstanding contribution to promoting and protecting fundamental freedoms and human rights in both non-government and government-controlled territories in Ukraine".*

- In Ukraine, the implementation of the FATF Recommendations negatively affects the operations of the NGOs and has led to financial exclusion of NGOs. For example, in November-December 2021, banks blocked the accounts of two reputable Ukrainian civil society organisations: the Institute of Mass Information and the Civil Network OPORA.[108] However, two months later, the full-scale invasion of Ukraine by the Russian Federation began, and the requirement to submit the ultimate beneficial owners for civil society organisations was postponed until the end of martial law in the country. In other words, the problem was postponed but not solved, as this trend will resume after the war ends. In addition, inspections can be applied during martial law to those NGOs that have managed to submit their ultimate beneficial owners data.
- The regulatory measures introduced in Ukraine, ostensibly aimed at preventing money laundering and terrorist financing, have inadvertently led to unnecessary overregulation and operational impediments for NGOs. While the intention to align with international standards and protect against financial crimes is commendable, the hurried and unclear implementation of these regulations has created significant challenges. The lack of precise definitions for ultimate beneficial owner (UBOs) in NGOs and the absence of accessible guidance and practical submission options have hindered compliance efforts, rendering them virtually impossible for many entities.
- The postponement of deadlines and ongoing debate over the Methodology for determining UBOs underscores the flaws in the regulatory framework. These issues, compounded by the impact of external events such as the Russian invasion, further demonstrate the need for a more balanced and effective approach to AML/CFT regulations that genuinely serves their intended purpose without placingundue burdens on civil society.
- Our key recommendation to FATF is to involve civil society in the regulatory process to avoid such consequences and financial exclusion. We advocate that NGOs should be removed from the list of entities obliged to report UBOs, both in the Law and in the Methodology. Should NGOs remain on the list, a proper communication mechanism must be established among the National Bank of Ukraine, other banks, and NGOs to prevent the blocking of banking services for NGOs.

In December 2019, Ukraine adopted a new Law of Ukraine "On Preventing and Combating Money Laundering, Financing of Terrorism and Financing the Proliferation of Weapons of Mass Destruction" (hereinafter - the Law).

This Law was adopted to align with the recommendations of the Financial Action Task Force (FATF), as well as Directive 2015/849/EC of the European Parliament and of the Council "On preventing the use of the financial system for money laundering and terrorist financing," which was issued on May 20, 2015. The law is aimed at protecting the rights and legitimate interests of citizens, society and the state, ensuring national security by defining the legal mechanism for preventing and combating money laundering, financing of terrorism and proliferation of weapons of mass destruction.

[108] https://zmina.info/articles/chomu-banky-blokuyut-rahunky-gromadskyh-organizaczij-i-chy-mozhna-z-czym-shhos-zrobyty/

The new law requires most legal entities, including public organisations and charitable associations, to register information about their ultimate beneficial owner (UBO) and ownership structure in the Unified State Register of Legal Entities, Physical Entrepreneurs and Public Formations (Unified State Register).

The vagueness of the Law in defining what is a UBO of non-governmental organisations (NGOs) has caused difficulty. At the same time, the relevant authorities did not provide an official clarification on how to fill out relevant forms and submit documents, which in practice led to refusals to enter information on NGOs or incorrect information being entered into the Unified State Register.

The situation was further aggravated with extremely short deadlines for submitting information on UBOs, the inability to submit such information online or by mail, long queues at Administrative Services Centers and state registrars, and the impossibility to make an appointment to submit the relevant documents.

At the same time, the failure to submit or late submission of information on UBOs or its absence or documents to confirm information on UBOs of a legal entity is subject to a fine of UAH 17,000 to 51,000, which, according to Article 166-11 of the Code of Administrative Offences, must be paid by the managers of the legal entity.

In fact, NGOs and other legal entities were put in a situation, in which the fulfilment of legal requirements was obviously impossible and blocked by the state.

The situation was further complicated by an insufficient information campaign and the fact that most NGOs were unaware of the need to submit data on UBOs.

Given these problems and the practical absence of UBOs for public organisations, more than 200 NGOs issued a statement calling on the Verkhovna Rada of Ukraine to exclude public associations with legal entity status and charitable organisations from the list of legal entities that have to submit information on UBOs.[109]

However, on October 8, 2021, the Verkhovna Rada passed Bill No. 5807 and postponed only for 9 months (until July 2022) the deadline for Ukrainian companies and NGOs to submit information on UBO.

The full-scale Russian invasion of Ukraine that began on February 24, 2022, suspended for some time the process of submission of UBOs information by legal entities[110], in particular NGOs.

It was only in June 2023 that the Ministry of Finance of Ukraine started to develop a methodology for determining a UBO of a legal entity (hereinafter - the Methodology), which should establish clearer criteria as to which legal entities have a UBO and who should be considered a UBO. After reading a draft Methodology, NGO experts criticised most of its provisions, and some have been continuing to oppose the definition of NGO managers as UBOs for NGOs and advocating for their exclusion from the Law.

On October 3, 2023, Government Resolution No. 1011 came into force, approving the Methodology for determining UBOs. Paragraphs 33-39 contain criteria for determining UBOs of a non-profit organisation - legal entity. The Methodology contains mostly all the shortcomings mentioned by members of civil society in their criticism of the criticism of UBOs for NGOs and charitable organisations, in particular:

- The requirement to file information on UBOs for NGOs and charitable organisations is an unwarranted interference with freedom of association,
- NGOs work for public rather than private interests; their benefit is directed to the public,
- NGOs generally do not aim to make a profit,

[109] https://zmina.ua/statements/zayava-shhodo-vyznachennya-ta-derzhavnoyi-reyestracziyi-kinczevyh-beneficziarnyh-vlasnykiv-gromadskyh-organizaczij/

[110] At the same time, political parties, trade unions, employers' organisations and their associations, creative unions, lawyers' associations, condominiums, chambers of commerce and industry, religious organisations, state and local self-government bodies, state and communal enterprises, institutions and organisations were exempted from submitting information on UBO. A three-month deadline was set for the submission of information on UBO, which began on July 11 and expired on October 11, 2021.

- the most important decisions (on election of governing bodies, disposition of property, approval of amendments to the charter) in NGOs and charitable organisations are made jointly - by the general meeting of all members of the organisation. Each of these members has influence on the decisions and it is impossible to speak about the belonging of property to one or several persons, as the property belongs to the organisation.

On September 6, 2022, the Law was supplemented by paragraph 4 of the transitional provisions. According to the Law, legal entities that have not reported their UBOs must provide the information to the Government within three months after the termination or lifting of martial law.

According to the same paragraph on transitional provisions, organisations that submitted such information earlier must analyse their charters, determine whether there are individuals in the organisation who can dispose of the organisation's property and finances or their shares, form governing bodies and determine the organisation's activities. Thereafter, NGOs that have previously reported UBO information must update the data in accordance with the new Methodology within six months, until April 3, 2024.
NGOs that reported UBOs earlier may face problems in their operations. The Ministry of Justice of Ukraine approved Order No. 2542/5, according to which from December 1, 2023 banks, as primary financial monitoring entities, are obliged to verify information on UBOs and ownership structure of the NGOs in the Unified State Register and compare the information with actual financial operations of the NGO. If banks identify discrepancies, they are obliged to notify the Ministry of Justice.

Since the Methodology provides a broad framework for determining of UBOs in NGOs and charitable organisations, it will allow banks to broadly interpret what constitutes "discrepancies" in determining of UBO and the ownership structure of organisations and their financial transactions. The Ministry of Justice will be able to require NGOs to make changes to their UBOs and ownership structure in the Unified State Register, and banks will be able to block transactions on accounts of the NGOs until the "elimination of discrepancies" in accordance with the law and the National Bank of Ukraine Board Resolution No. 65 of 19.05.2020.

NGO representatives argue that from December 1, 2023, problems in banking services and banks' reporting to the Ministry of Justice of allegedly false information in the Unified State Register could begin even for NGOs that have not yet reported their UBOs.

The regulatory measures introduced in Ukraine, ostensibly aimed at preventing money laundering and terrorist financing, have inadvertently led to unnecessary overregulation and operational impediments for NGOs. While the intention to align with international standards and protect against financial crimes is commendable, the hurried and unclear implementation of these regulations has created significant challenges. The lack of precise definitions for UBOs in NGOs and the absence of accessible guidance and practical submission options have hindered compliance efforts, rendering it virtually impossible for many entities. The postponement of deadlines and ongoing debate over the Methodology for determining UBOs underscore the flaws in the regulatory framework. These issues, compounded by the impact of external events such as the Russian invasion, further demonstrate the need for a more balanced and effective approach to AML/CFT regulations that genuinely serves their intended purpose without placing undue burdens on civil society organisations.

Our organisation, ZMINA Human Rights Center, believes that the current version of the Law results in undue overregulation that negatively affects the operations of the NGOs. We advocate that NGOs should be removed from the list of entities obliged to report UBOs, both in the Law and in the Methodology.

Testimonial of Michael Chobanian, President of the Blockchain Association of Ukraine and a founder of the first cryptocurrency exchange in Ukraine, KUNA.io. Chobanian is an external adviser to Ukraine's Deputy Prime Minister and Minister for Digital Transformation of Ukraine, Mykhailo Fedorov. Since the start of Russia's full-scale war against Ukraine, Michael Chobanyan has launched a Crypto Fund for Ukraine to help the Armed Forces which has raised over $100 million of donations. At the request of the Ministry of Digital Transformation, Chobanyan helped the Government of Ukraine to create and manage state cryptocurrency wallets for donations in Kuna Exchange. Since 2020, representatives of authoritarian regimes of Belarus and Russia have been trying to obtain personal information about their opponents from the Kuna Exchange through abuse of AML/CFT laws, accusing their opponents of financing extremism and money laundering. Unlike Chinese platforms, Kuna Exchange refused to disclose information about its users due to politically motivated requests. Chobanyan therefore advocates that the regulation of democratic countries, in the EU, the US and Ukraine, should reflect preventive measures against abuses in AML/CFT regulation.

My name is Michael Chobanian, and I am a Ukrainian fintech entrepreneur and crypto enthusiast. In 2014, I founded KUNA — Eastern Europe's first Bitcoin agency which has since transformed into a full-fledged cryptocurrency exchange with more than 450 thousand users worldwide.

On February 24th, the Russian Federation attacked my homeland with a full-scale war. Thousands of civilians have been killed and hundreds of homes have been destroyed. By the Ministry of Finance's accounts, the damage from the Russian invasion has already amounted to $500 billion dollars—and the number rises daily.

From the invasion's first moment, we at KUNA decided to act swiftly to help our army and the people who suffered most due to these horrific events. In collaboration with the Ministry of Digital Transformation and the Ministry of Defense, our team launched the official Crypto Fund of Ukraine to solicit cryptocurrency donations. The majority of funding comes through crypto assets such as Bitcoin and Ethereum, where AML technologies (e.g. Chainalysis, Crystal Blockchain) have been successfully implemented. All crypto that we received and converted was analysed for illegal activity. These solicited funds are used to purchase much needed medical supplies, military equipment, and humanitarian aid here in Ukraine.

As of July 2023, the Fund has collected more than $60 million dollars in donations, while in total Ukraine has raised more than $225 million in crypto donations since February 2022.[111]

One of our top priorities throughout this fundraise was to ensure the transparency of the donation process. While KUNA is providing the technological platform for crypto donations, the Ukrainian government - specifically, the Ministries of Digital Transformation and Defense have ultimate control of the funds and it is they who are responsible for the fund's distribution. KUNA is serving a strictly technical and organisational role in the fundraising process and coin management - crypto banking.

As CEO of the first crypto exchange in Ukraine, we provided advice and education to various financial and intelligence institutions in Ukraine, such as the Ministry of Digital Transformation of Ukraine, the National Bank, and the Secret Service/Police, on how to use cryptocurrency to counter terrorist financing and reduce money laundering.

Also important to mention that since 2020, representatives of the authoritarian regimes in Belarus and Russia have tried to obtain personal information on their opponents, accusing them of funding extremism and money laundering.[112] In the case of Belarus, it is the BYSOL Foundation. This is a fund that helps

[111] https://crystalblockchain.com/articles/crypto-regulations/ukraine-receives-over-224m-in-crypto-donations/
[112] https://reform.by/169292-kriptobirzha-otkazalas-vydavat-kgk-dannye-po-operacijam-fonda-bysol

financially those who were fired for protesting or were victims of repression by the Belarusian government.[113]

Unlike our colleagues from the Chinese platforms, we refused to hand over information about our users due to politically motivated requests. We believe it is important that such deterrent elements are also reflected in the regulation of democratic countries, in the EU, the USA[114], UK and Ukraine.

Regarding the regulation of the crypto assets providers – we see that traditional banks do not want to provide services to crypto companies because of their perception of increased regulatory risk associated with the crypto industry. Generally, it does not matter for banks whether a crypto company has a licence or not. In the existing climate, onboarding crypto companies as clients requires banks to invest in additional compliance measures to meet regulatory requirements. Banks are unwilling to bear these additional compliance costs and instead prefer to avoid dealing with crypto-related businesses altogether. Traditional banks may also perceive a reputational risk in associating with crypto companies. There have been a lot of misconceptions as to the use of crypto and lots of negative publicity. Thus, banks do not have client relationships with crypto companies.

As a result of these challenges, crypto companies are forced to turn to financial intermediaries, such as CheckOut and Clear Junction, which work with banks on their behalf. These intermediaries charge fees for their services, increasing the operational costs for crypto companies. This ultimately puts them at a competitive disadvantage compared to businesses in other industries that can easily access traditional banking services.

In conclusion, the difficulty faced by crypto companies in opening bank accounts with traditional financial institutions is a significant problem that hampers their growth and competitiveness. This issue highlights the need for greater cooperation between the crypto industry and the banking sector, as well as the development of more effective regulatory frameworks to address the concerns of both parties.

[113] https://bysol.org/en/bs/
[114] https://www.banking.senate.gov/imo/media/doc/Chobanian%20Testimony%203-17-22.pdf