



GLOBAL FINANCIAL INTEGRITY



CYRUS R. VANCE CENTER  
FOR INTERNATIONAL JUSTICE

# THE DIGITAL ASSET ECOSYSTEM IN EL SALVADOR: Challenges and Risks to Countercheck Financial Crime



January 2025

JANUARY 2025

# THE DIGITAL ASSET ECOSYSTEM IN EL SALVADOR: CHALLENGES AND RISKS TO COUNTERCHECK FINANCIAL CRIME

Global Financial Integrity and the  
Cyrus R. Vance Center for International Justice

Copyright ©2024 by Global Financial Integrity®. Some rights reserved. The report is published under a Creative Commons Attribution License. For more information on this license, visit: [creativecommons.org](https://creativecommons.org).

Cover collage by Maria Isabel Gaviria.

# ACKNOWLEDGEMENTS

This report was researched, written and produced by Global Financial Integrity (GFI) and the Cyrus R. Vance Center for International Justice.

## **GLOBAL FINANCIAL INTEGRITY (GFI)**

GFI is a Washington, DC-based think-tank focused on illicit financial flows, corruption, illicit trade, and money laundering. Through high-caliber analyses, fact-based advocacy to promote beneficial ownership, and a cloud-based database to curtail trade fraud, GFI aims to address the harms inflicted by trade misinvoicing, transnational crime, tax evasion, and kleptocracy. By working with partners to increase transparency in the global financial system and promote Trade Integrity, GFI seeks to create a safer and more equitable world.

## **CYRUS R. VANCE CENTER FOR INTERNATIONAL JUSTICE**

The Cyrus R. Vance Center for International Justice of the New York City Bar Association advances global justice by engaging lawyers across borders to support civil society and an ethically active legal profession. The Vance Center is a unique collaboration of international lawyers catalyzing public interest innovation that brings together leading law firms and other partners worldwide to pioneer international justice initiatives and provide pro bono legal representation to social justice NGOs. Through its Institutional Integrity Program, the Vance Center pursues openness and honesty in government, supporting a robust civil society, judicial independence, and integrity.

The Vance Center thanks pro bono law firms involved in researching legislation, regulation, and best practices.

## DISCLAIMER

This report discusses financial crime risks and identifies red flag indicators. It should be noted that the assessment of risks and identification of red flags does not signify that a crime has occurred. There are many legitimate reasons why financial behavior may appear to be unusual; an anomaly does not indicate illicit activity. The mention of specific cases, companies, or countries in this report should not be interpreted as an allegation of wrongdoing; they are included for educational purposes only.

The findings and analysis in this report do not necessarily represent the views of any participating reviewer or organization.

**CONTENTS**

- Acronyms and Terms** ..... 7
- Executive Summary** ..... 9
- Key Concepts and Definitions** ..... 11
- El Salvador Introduction and Background** ..... 14
  
- Chapter I. Legal Framework for the Prevention of Money and Asset Laundering in El Salvador** ..... 24
  - A. Regulatory Framework** ..... 25
    - The Current Law Against Asset and Money Laundering (LAAML) (1998) ..... 26
    - 2023 Special Draft Bill to Prevent, Control, and Penalize Asset Laundering, Terrorist Financing, and the Proliferation of Mass-Destruction Weapons (APL) ..... 27
    - Digital Asset Issuance Law And Reforms: Registration, Regulators, Supervisors and PSAV Enforcement Entities ..... 28
  
  - B. Institutional Framework** ..... 29
    - Financial Investigation Unit (FIU) ..... 29
    - Suspicious Activity Reporting (SAR) ..... 30
    - Customer Due Diligence (CDD) ..... 30
    - Politically Exposed Persons (PEP) ..... 31
    - Beneficial Owners ..... 31
    - Obligated Subjects ..... 32
    - Virtual Asset Service Providers ..... 32
      - (i) Application of AML/CFT Standards ..... 33
      - (ii) Risk Assessment and Focusing on VASP Applicable Policies ..... 36
    - Suspicious Activity Reporting Obligations for BSPs and DASPs ..... 37
    - Beneficial Ownership (BO) and BSPs and DASPs ..... 37
    - The Travel Rule ..... 38
    - Customer Due Diligence and VASP ..... 38

International Cooperation: Inquiries on Digital Assets Services Providers Accounts, Freezing/Seizure, and Assets Recovery.....	39
<b>Chapter 2: Risks of the VA Ecosystem and Financial Crimes</b> .....	40
VA and Financial Crime Risks in El Salvador.....	41
Citizenship by Investment (CBI).....	42
Real-World Assets Tokenization.....	42
Agricultural Products Tokenization.....	43
Debt and Fund Tokenization.....	44
Stablecoin Issuance.....	45
Political Financing.....	46
<b>Chapter 3: VASP and the Data Protection Legal framework in El Salvador</b> .....	48
<b>A. International References</b> .....	49
(i) General Data Protection Regulation (GDPR).....	49
(ii) The Gramm-Leach-Bliley (GLBA) Act.....	50
<b>B. Chivo Wallet: Privacy policy, terms and conditions</b> .....	50
<b>C. Virtual asset wallets</b> .....	52
<b>D. A comparative analysis of virtual asset wallets</b> .....	53
<b>Recommendations</b> .....	54
Recommendations to Counter Financial Crimes.....	54
Recommendations to promote AML/CTF/PF.....	54
Recommendations on Political Financing.....	55
Recommendations on Real-World Asset Tokenization.....	55
Recommendations on Personal Data Protection.....	56

# ACRONYMS AND TERMS

ACRONYMS	DESCRIPTION
<b>AML</b>	Anti-Money Laundering
<b>APL</b>	Anteproyecto Ley Especial Para la Prevención, Control y Sanción del Lavado de Activos, Financiamiento al Terrorismo y de la Proliferación de Armas de Destrucción Masiva de 2023 Draft Bill Special Law for Asset Laundering Prevention, Control, and Enforcement, Financing of Terrorism, and Mass-Destruction Weapon Proliferation of 2023
<b>BCR</b>	Banco Central de reserva Central Reserve Bank
<b>BFAA</b>	Bitcoin Fund Administration Agency
<b>BL</b>	Bitcoin Law
<b>BO</b>	Beneficial Ownership
<b>BSP</b>	Bitcoin Services Provider
<b>BTC</b>	Bitcoin
<b>CBI</b>	Citizenship by investment
<b>CFTC</b>	Commodity Futures Trading Commission
<b>CIPLAFT</b>	Comité Interinstitucional para la prevención, control y represión del lavado de activos y el financiamiento del terrorismo y de la proliferación de armas de destrucción masiva Interinstitutional Commission for the Prevention, Control, and Enforcement of Asset Laundering, Financing of Terrorism, and Mass-Destruction Weapon Proliferation
<b>CRB</b>	Central Reserve Bank
<b>CSAM</b>	Child Sexual Abuse Material
<b>CTF</b>	Combating the Financing of Terrorism
<b>DA</b>	Digital assets
<b>DAT</b>	Distributed Accounting Technology
<b>DDC</b>	Due Diligence Customer
<b>DeFi</b>	Decentralized Finances
<b>DAIL</b>	Digital Assets Issuance Law
<b>DNFBP</b>	Designated Non-Financial Businesses and Professions
<b>CNAD</b>	National Commission of Digital Assets Comisión Nacional de Activos Digitales

<b>DASP</b>	Digital Asset Service Providers
<b>ETH</b>	Ether
<b>FATF</b>	Financial Action Task Force
<b>FGR</b>	Fiscalía General de La República de El Salvador Attorney General's Office
<b>FIU</b>	Financial Intelligence Unit
<b>GAFILAT</b>	Financial Action Task Force of Latin America
<b>GOES</b>	Government Of El Salvador
<b>ICT</b>	Information and Communication Technologies
<b>KYB</b>	Know Your Business
<b>KYC</b>	Know Your Customer
<b>KYT</b>	Know Your Transaction
<b>LAAML</b>	Law Against Asset and Money Laundering
<b>LPP</b>	Ley de Partidos Politicos Law of Political Parties
<b>MDWP</b>	Mass-Destruction Weapon Proliferation
<b>ME</b>	Mutual Evaluation
<b>ML</b>	Money Laundering
<b>NBTCO</b>	National Bitcoin Oficce Oficina Nacional de Bitcoin
<b>OFAC</b>	U.S. Treasury Office for Foreign Asset Control
<b>PEP</b>	Politically Exposed Persons
<b>RID</b>	Relevant Information Document
<b>SEC</b>	Securities and Exchange Commission
<b>SFS</b>	Superintendence of the Financial System
<b>SLACCRO</b>	Special Law Against Cyber Crime and Related Offences
<b>USDT</b>	Tether
<b>TF</b>	Terrorist Financing
<b>VA</b>	Virtual asset
<b>VASP</b>	Virtual Assets Service Provider

# EXECUTIVE SUMMARY

This report examines in detail how El Salvador's virtual asset ecosystem has evolved, providing a broad perspective on technological innovation, financial crime prevention, and data protection in relation to governmental entities' liability. The pioneer adoption of Bitcoin as a legal tender in the country has created a unique and dynamic environment that presents both outstanding opportunities and significant challenges. This report aims to provide a clear assessment of the current state of things, highlighting the advances made.

## I. THE ANTI-MONEY LAUNDERING AND TERRORIST FINANCING LEGAL FRAMEWORK IN EL SALVADOR

El Salvador's legal framework for the prevention of money laundering and terrorist financing (AML/CTF) shows a commitment to align with international standards such as the Financial Action Task Force (FATF) and the Latin American Financial Action Task Force (GAFILAT, as per its initials in Spanish). Additionally, recent legal efforts, including proposed amendments such as the Bill on Prevention of Money Laundering, Terrorist Financing, and the Proliferation of Mass Destruction Weapons are a step forward to strengthening the regulatory framework, even though important reinforcement opportunities remain ahead.

The recent regulatory changes, including reforms to the Law of Digital Asset Issuance, confer full powers to the National Digital Assets Commission CNAD,

as per its initials in Spanish including overseeing Bitcoin service providers (BSPs) and digital asset service providers (DASPs). Meanwhile, this reform incorporates Bitcoin as a part of the digital asset ecosystem. Additionally, the National Digital Assets Commission will be responsible for overseeing all Bitcoin-related activities, as well as authorizing the issuance of digital assets and stablecoins, and overseeing all stakeholders in those issuances.

Importantly, the public sector should promote clear and consistent enforcement of this reform, along with sufficient resources devoted to supervision and research. This will help promote effective international cooperation and inter-agency coordination. Additionally, the collaboration between private and public sectors also provides an opportunity to prevent financial crime.

## II. EMERGING THREATS IN EL SALVADOR'S VIRTUAL ASSETS ECOSYSTEM

El Salvador's virtual asset ecosystem shows potential risks which could be exploited for illegal activities. Some risks mentioned in the report examine various cases of cryptocurrency-related fraud, scams, and money laundering, highlighting vulnerabilities in the adoption of new technologies.

It is worth highlighting that a solid information security infrastructure and data protection protocols are needed to maintain regulatory transparency and supervision, thus preventing consumers from being vulnerable to identity theft, robbery, and other cybercrimes.

Furthermore, emerging technologies, including the

adoption of decentralized finance and the issuance of tokens through smart contracts, have become a key element in fostering investment. However, cyber offenders have also taken advantage of this infrastructure, which makes information security standards necessary to prevent its misuse or exploit its potential vulnerability.

### III. DATA PROTECTION

As of the closing date of this report, El Salvador hadn't yet passed a law specifically safeguarding and regulating data in the context of technological advances, establishing regulatory oversight or mitigating users' privacy risks and financial security. The Law of Public Information Access (LAIP as per its Spanish acronym) provides certain data protection, but it fails to address the comprehensive framework that an evolving digital ecosystem requires.

### IV. RECOMENDATIONS

This report concludes with a set of specific recommendations for El Salvador that may help support the government's ability to effectively prevent and mitigate financial crime. Main recommendations include:

**Strengthen the AML/CTF regulatory framework in El Salvador:** Prioritize integral risk assessments, strengthen oversight of virtual asset service providers, and streamline information exchange mechanisms with international partners.

**Enact a Data Protection Law:** Implement a data protection law incorporating international best practices, ensuring user privacy, robust security

measures, and effective deployment.

**Reinforce information security infrastructure:** Invest in and upgrade national cyber security infrastructure to prevent the use of technology for illegal purposes.

**Enhance transparency and oversight of political financing:** Introduce solid and transparent regulations ruling political parties and campaign financing, with explicit provisions for reporting and verification of donations and transfers made using virtual assets.

**Foster collaboration and education:** Foster collaboration between the main actors in the public and private sectors, thus enhancing information exchange and AML/CTF efforts.

**Invest in public awareness-raising campaigns:** Promote finance literacy and cybersecurity best practices through widespread public awareness-raising campaigns.

El Salvador's path to integrating Bitcoin into its economy presents a case study on the challenges and opportunities inherent in navigating the rapidly evolving world of virtual assets. The country has shown some willingness to encourage innovation through the adoption of Bitcoin and the promotion of digital asset issuances, such as stablecoins and tokens representing debts, funds, or agricultural commodities, the findings presented in this report highlight the opportunity to properly implement the regulatory framework in order to mitigate financial crime risks and protect its citizens' privacy.

# KEY CONCEPTS AND DEFINITIONS

**Bitcoin (BTC):** The first cryptocurrency and a decentralized virtual currency. Bitcoins are units of account composed of unique strings of numbers and letters that constitute units of the currency and have value only because individual users are willing to pay for them. Bitcoin runs on blockchain technology, which is composed of two parts: nodes and miners.<sup>1</sup>

**Beneficial Ownership:** According to the Financial Action Task Force, this refers to the natural person who “ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is conducted.”<sup>2</sup>

**Certifier:** Legal person in charge of performing a financial, legal, technical and administrative analysis of the public offerings' material and relevant information contained in the Relevant Information Document (RID). Once the analysis is completed, the certifier issues and submits a report on the issuer's compliance with formal and substantive obligations to the National Commission of Digital Assets.<sup>3</sup>

**Criptojacking:** A cybercrime where a criminal secretly takes advantage of a victim's computing power to generate cryptocurrency. A common modality is when the victim unwittingly installs a program with malicious scripts that allow the victimizer to access

their computer or other Internet-connected device.<sup>4</sup>

**Corruption:** It designates a misuse of public administration for their private benefit. It refers to an abuse of their office for private gain. It encompasses a wide array of behaviors, from bribery to embezzlement.<sup>5</sup>

**Customer due diligence (CDD):** The process used by financial institutions to gather and analyze information regarding a customer or potential customer.<sup>6</sup>

**Decentralized finances (DeFi):** It is the provision of financial services without the need for an intermediary custodian that is not blockchain-based.<sup>7</sup>

**Digital assets (DAs):** Digital representation that can be stored or transferred electronically using technologies such as Blockchain, Distributed Ledger Technology (DLT) or others, where records are linked and protected by encryption methods to ensure the privacy of transactions. Digital assets can be purchased by individuals or companies to exchange, transfer, trade or promote them.<sup>8</sup>

---

<sup>1</sup>Financial Action Task Force. (2014).

<sup>2</sup>Tax Justice System. (2020). What is beneficial ownership? Tax Justice Network. <https://taxjustice.net/faq/what-is-beneficial-ownership/>.

<sup>3</sup>El Salvador Legislative Assembly. (2023). Ley de Emisión de Activos Digitales. <https://www.asamblea.gob.sv/sites/default/files/documentos/decretos/OCDA225C-1B6C-4098-AC3A-D608933C643B.pdf>

---

<sup>4</sup>Interpol. (n.d.). What is Cryptojacking? How does it work?. <https://www.interpol.int/en/Crimes/Cybercrime/Cryptojacking>.

<sup>5</sup>World Bank. (2020). Anti Corruption Fact Sheet <https://www.worldbank.org/en/news/factsheet/2020/02/19/anticorruption-fact-sheet>.

<sup>6</sup>Society of Worldwide Interbank Financial Telecommunication. (n.d.) What is Customer Due Diligence (CDD)? [https://www.swift.com/your-needs/financial-crime-cyber-security/know-your-customer-kyc/customer-due-diligence-cdd#:~:text=Due%20Diligence%20\(CDD\)-,What%20is%20Customer%20Due%20Diligence%20\(CDD\)%3Fa%20customer%20or%20potential%20customer](https://www.swift.com/your-needs/financial-crime-cyber-security/know-your-customer-kyc/customer-due-diligence-cdd#:~:text=Due%20Diligence%20(CDD)-,What%20is%20Customer%20Due%20Diligence%20(CDD)%3Fa%20customer%20or%20potential%20customer).

<sup>7</sup>National Institute of Standards and Technology. Understanding stablecoin technology and related security considerations. (2023). <https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8408.pdf>.

<sup>8</sup>El Salvador Legislative Assembly. (2023). Ley de Emisión de Activos Digitales. <https://www.asamblea.gob.sv/sites/default/files/documentos/decretos/OCDA225C-1B6C-4098-AC3A-D608933C643B.pdf>

**Digital Asset Service Provider (DASP):** “Any natural or legal person whose professional activity involves providing services related to digital assets. This includes, among other things, the exchange of digital assets for fiat money or its equivalent, or for other digital assets, whether using their capital or third-party capital; operating a digital asset exchange or trading platform; and placing digital assets on digital platforms or wallets.”<sup>9</sup>

**Distributed Accounting Technology:** “A technology that aims to generate a distributed record in a digital environment interconnected by a data network.”<sup>10</sup>

**Ether (ETH):** A crypto asset based on a decentralized blockchain that establishes a peer-to-peer network, allowing people to coordinate, make agreements, or transfer digital assets among themselves.<sup>11</sup>

**Human Trafficking:** “Crime that involves forcing or coercing a person to provide labor or services or to engage in sex work. Coercion can be subtle or overt, physical or psychological.”<sup>12</sup>

**Issuer:** A natural or legal person, private or public, that makes a digital asset public, offering to sell or trade it on an exchange platform.<sup>13</sup>

**Know your Customer (KYC):** A set of procedures that enable banks and other financial institutions to confirm the identity of organizations and individuals with which they conduct financial transactions to ensure that they are acting within the legal framework.<sup>14</sup>

**Mass-Destruction Weapon Proliferation (MDWP):** It refers to “the manufacture, acquisition, possession, development, export, transshipment, brokerage, transport, transfer, storage, or use of nuclear, chemical, or biological weapons, as well as their delivery systems and related materials (including both technologies and dual-use goods for non-legitimate purposes).”<sup>15</sup>

**Mixer or Tumbler:** A cryptocurrency mixer is a service that blends the cryptocurrencies of many users to obscure the origins and owners of the funds. Because Bitcoin, Ethereum, and most other public blockchains are transparent, this level of privacy is hard to achieve otherwise.<sup>16</sup>

**Ransomware:** A malware that prevents a person from accessing their device and stored data, usually through encrypting their files. To recover such information, the criminal will demand a ransom or extortion.<sup>17</sup>

---

<sup>9</sup>Global Financial Integrity and Vance Center. (2023). The Virtual Assets Ecosystem In El Salvador: Strengthening Financial Integrity And Transparency. <https://34n8bd.p3cdn1.secureserver.net/wp-content/uploads/2023/10/Crypto-El-Salvador-Report-ENG-FINAL-1.pdf?time=1719550890>

<sup>10</sup>Ministry of Information Technology and Communications of Colombia. DLT/BLOCKCHAIN Borrador - Guía para el uso y la implementación de tecnología de registros distribuidos (DLT/Blockchain) en el sector público. [https://mintic.gov.co/portal/715/articles-149959\\_recurso\\_1.pdf](https://mintic.gov.co/portal/715/articles-149959_recurso_1.pdf)

<sup>11</sup>Ethereum. (n.d.). What is Ethereum?, <https://ethereum.org/en/what-is-ethereum/>.

<sup>12</sup>U.S Department of Justice. (2023). What is human trafficking?. <https://www.justice.gov/humantrafficking/what-is-human-trafficking>.

<sup>13</sup>El Salvador Legislative Assembly. (2023).

---

<sup>14</sup>Society of Worldwide Interbank Financial Telecommunication. (n.d.) The KYC process explained. <https://www.swift.com/your-needs/financial-crime-cyber-security/know-your-customer-kyc/kyc-process>.

<sup>15</sup>Financial Action Task Force.(2021). Guidance on proliferation financing risk assessment and mitigation. <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Proliferation-Financing-Risk-Assessment-Mitigation.pdf.coredownload.inline.pdf>.

<sup>16</sup>Chainalysis Team. (2022). Crypto mixers and AML Compliance. <https://www.chainalysis.com/blog/crypto-mixers/>

<sup>17</sup>National Cyber Security Center .(n.d.). A guide to ransomware, United Kingdom. <https://www.ncsc.gov.uk/ransomware/home>.

**Regulatory sandbox:** A closed testing environment designed to safely experiment with web or software development projects, serving as a testing ground for new business models that are not yet protected by current regulation, under the supervision of regulatory institutions.<sup>18</sup>

**Relevant information document (RID):** “A document that provides the public with essential information about a public offering of a digital asset. It includes the identification of the issuer, the characteristics, and the objectives of the issuance. Additionally, it must specify whether the interests, income, returns, or benefits of the public offering will be paid in fiat money or digital assets.”<sup>19</sup>

**Stablecoin:** A type of digital asset designed to have a stable value, which is backed by one or more fiat currencies or other low-volatility underlying assets.<sup>20</sup>

**Token:** A digital asset used as a unit of account in a network based on DLT or a similar or analogous technology.<sup>21</sup>

**Tokenization:** It is the process of transforming ownership and rights of specific assets into a digital form. Through tokenization, indivisible assets can be converted into tokens.<sup>22</sup>

**Virtual assets (VAs):** “Any digital representation of value capable of being marketed, transferred, or used to do digital payments.” It does not include non-fungible tokens (NFT) like collectibles or digital representations of fiat currency.<sup>23</sup>

**Virtual Asset Service Provider (VASP):** “Any natural or legal person who performs one or more of the following activities or operations on their behalf or on behalf of another: (i) Exchange between virtual assets and legal tender; (ii) Exchange between one or more forms of virtual assets; (iii) Transfer of virtual assets; (iv) Custody and/or administration of virtual assets or instruments that allow control over virtual assets; (v) Providing financial services related to the offering and/or sale of a virtual asset by an issuer.”<sup>24</sup>

---

<sup>18</sup>BBVA. Press Releases. (2017). ¿Qué es un Sandbox Regulatorio?. <https://www.bbva.com/es/que-es-un-sandbox-regulatorio/>

<sup>19</sup>El Salvador Legislative Assembly. (2023). Ley de Emisión de Activos Digitales. <https://www.asamblea.gob.sv/sites/default/files/documentos/decretos/0CDA225C-1B6C-4098-AC3A-D608933C643B.pdf>

<sup>20</sup> El Salvador Ministry of Economy, Reformas a la Ley de Activos Digitales, 2024.

<sup>21</sup>Blockchain Council. (2023). What is Tokenization? A complete guide, <https://www.blockchain-council.org/blockchain/what-is-tokenization/>.

---

<sup>22</sup>Blockchain Council. (2023).

<sup>23</sup>Financial Action Task Force. (2014). Virtual currencies: Key definitions and potential AML/CFT risks. <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>.

<sup>24</sup>Financial Action Task Force. (2021). Virtual assets and virtual asset service providers. <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.inline.pdf>.

# EL SALVADOR INTRODUCTION AND BACKGROUND

El Salvador has a national regulatory framework to ensure transparency and integrity,<sup>25</sup> as well as to combat illicit financial flows related to money laundering (ML). This regulatory framework is aligned with the recommendations and principles of international organizations. The nation has formulated and implemented laws to promote technological innovation and combat crime by taking advantage of Information and Communication Technologies (ICTs). In this context, various regulations on virtual assets (VAs) have also been adopted in the country. For the purposes of this report, the terms "digital asset" and "virtual assets" will be used interchangeably, as under El Salvador's regulatory framework, the term "digital asset" is used, while the International Financial Action Task Force (FATF) standards refer to them as "virtual assets".

In the international arena, El Salvador participated in the evaluation sessions of the Latin American Financial Action Task Force (GAFILAT) between January 8 and 19, 2024, the results of which were published in August of the same year. These included the evaluation of the measures implemented against asset laundering (ML) and

terrorist financing (TF), as well as the level of compliance with the 40 Recommendations of the Financial Action Task Force (FATF), including Recommendation 15 on the use of new technologies, which is strictly related to virtual assets.

## FINANCIAL AND TECHNOLOGICAL ECOSYSTEM IN EL SALVADOR

El Salvador's financial and technological ecosystem is diverse, especially in terms of its regulation and incorporation of new technologies. In addition, it is relevant to consider the pioneering adoption of Bitcoin as legal tender in the country, its use, and other virtual assets available to the population.

The population of El Salvador is approximately 6.3 million inhabitants.<sup>26</sup> Among them, 88% of people did not use Bitcoin during 2023, and 48.8% disagreed with public spending on its adoption.<sup>27</sup> Although the adoption of Bitcoin as a legal tender was intended to boost El Salvador's economic development, between 2019 and 2024, 80.5% of Salvadorans reported not receiving economic benefits from using Bitcoin, and 66.6% believe the cryptocurrency has failed to bring an improvement in their household economic situation.<sup>28</sup> Despite these obstacles, the government continues to push for the adoption of financial technologies, especially digital assets,

---

<sup>25</sup>The regulatory framework for transparency in El Salvador includes laws that regulate the actions of public officials and individuals. Among these are: the Penal Code, the Banking Law, and CLDA regulations. Although behavioral measures and sanctions are established, the lack of control has limited their effectiveness. Private corruption also affects economic development and democracy, so a strategic approach based on anti-corruption risk management is necessary to strengthen transparency in all sectors.

<sup>26</sup>Central Reserve Bank of El Salvador (2023). "Población". <https://estadisticas.bcr.gob.sv/serie/poblacion?lang=es>

<sup>27</sup>La Prensa Gráfica. (2024). Bitcoin no termina de convencer a los salvadoreños. Bitcoin no termina de convencer a los salvadoreños - La Prensa Gráfica ([laprensagrafica.com](http://laprensagrafica.com))

<sup>28</sup>Instituto Universidad de Opinión Pública. (2024). Encuesta de evaluación del quinto año de Gobierno del presidente Nayib Bukele. <https://uca.edu.sv/iudop/wp-content/uploads/2024/06/PPT-Eva-5to-anio-de-NB-1.pdf>

with the goal of improving digital inclusion and economic prosperity.

On the other hand, the El Salvador Government seeks a digital and financial boost through a National Financial Inclusion Policy. It is also important to consider, that 64% of the population has no access to banking services,<sup>29</sup> and only 11% have mobile accounts (eMoney).<sup>30</sup> In that sense, implementing the National Financial Inclusion Policy<sup>31</sup> represents opportunities to incorporate digitalization and financial innovation, and establishes digital transformation as a priority in its Digital Agenda 2020-2030.<sup>32 33</sup>

In addition, to promote the use of Bitcoin and other digital tools in a safe and secure way for users, the government has begun implementing measures such as the approval of a cybersecurity policy and the launch of educational programs.<sup>34</sup> Proper implementation of the regulatory framework could strengthen trust and encourage greater adoption of

new technologies in financial matters.<sup>35</sup>

Globally, El Salvador is viewed favorably in terms of VA regulation<sup>36</sup> even though it ranks 95th in global transaction value.<sup>37</sup> This low performance is partly due to limited financial<sup>38</sup> and technological literacy, which hinders the adoption of technology and the prevention of financial crime. Further, operational challenges in complying with information security standards,<sup>39</sup> and the lack of data protection regulations also contribute to the slow adoption of Bitcoin.<sup>40</sup> For example, the Mutual Evaluation Report (MER) of El Salvador, published in August 2024, noted that in regard to Recommendation 15 (related to the use of new technologies, including virtual assets), the government is only partially compliant (PC).<sup>41</sup>

---

<sup>29</sup>USAID. (2023). El Salvador Digital Ecosystem Country Assessment (DECA). <https://www.usaid.gov/digital-development/el-salvador-deca>.

<sup>30</sup>USAID. (2023). pag. 50.

<sup>31</sup>El Salvador President's Office's Innovation Secretary. (2020). El Salvador. agenda digital 2020-2030. <https://www.innovacion.gob.sv/downloads/Agenda%20Digital.pdf>.

<sup>32</sup>El Salvador President's Office's Innovation Secretary. (2020). El Salvador. agenda digital 2020-2030. <https://www.innovacion.gob.sv/downloads/Agenda%20Digital.pdf>.

<sup>33</sup>The Digital Agenda, which includes the Fintech area (finance and technology), led by the Secretariat of Innovation, is based on several pillars, among which "Innovation, Education and Competitiveness" stand out. The main objective of this initiative is to promote innovation in the financial system through the creation of an appropriate regulatory framework, the promotion of payment gateways and the promotion of financial instruments for social inclusion. El Salvador President's Office's Innovation Secretary. (n.d.). Fintech, <https://www.innovacion.gob.sv/fintech.php>

<sup>34</sup>El Salvador President's Office's Innovation Secretary. (n.d.). Fintech, <https://www.innovacion.gob.sv/fintech.php>

<sup>35</sup>World Bank. (2022). Transformación Digital en El Salvador, reactivando el crecimiento y la inclusión. Transformación Digital en El Salvador, reactivando el crecimiento y la inclusión (bancomundial.org)

<sup>36</sup>Coincub. (2024). Crypto Regulation Report. <https://x.com/coincub/status/1803810784234852725?s=48>

<sup>37</sup>Chainalysis (2023). Geography of Cryptocurrency Report. <https://go.chainalysis.com/geography-of-cryptocurrency-2023.html>.

<sup>38</sup>Global Financial Integrity and Vance Center. (2023). The Virtual Assets Ecosystem In El Salvador: Strengthening Financial Integrity And Transparency. <https://gfintegrity.org/report/the-virtual-assets-ecosystem-in-el-salvador-strengthening-financial-integrity-and-transparency/>

<sup>39</sup>González, Glenda.Criptonoticias.(2024). Hackers filtran código de la Chivo Wallet de El Salvador. <https://www.criptonoticias.com/seguridad-bitcoin/hackers-filtran-codigo-chivo-wallet-elsalvador/>

<sup>40</sup>Barrera, José A. El Mundo. (2021). Aumentan casos por suplantación de identidad de Chivo Wallet. <https://diario.elmundo.sv/econom%C3%ADa/aumentan-denuncias-por-suplantacion-de-identidad-en-la-chivo-wallet>

<sup>41</sup>According to GAFILAT, Recommendation 15, countries and financial entities must identify and assess the risks of asset laundering or terrorist financing that might arise from (a) the development of new products and new business practices, including transfer means; (b) the use of emerging or developing technologies for both new and existing products, adding that countries must ensure that virtual asset providers are regulated for AML/CTF purposes, are licensed or registered, and subject to effective monitoring systems, as well as ensuring their compliance with the relevant measures required in GAFI Recommendations. <https://biblioteca.gafilat.org/wp-content/uploads/2024/07/Recomendaciones-metodologia-actDIC2023.pdf>, Página 16.

It is convenient for El Salvador to include relevant regulations to prevent financial crimes, in line with the country's profile in terms of capabilities, resources and the use of virtual assets at a worldwide level.

## GENERAL REGULATORY FRAMEWORK FOR VA IN EL SALVADOR

In El Salvador, with the enactment of the Bitcoin Law in 2021<sup>42</sup> and the sanctioning of the Digital Asset Issuance Law (DAIL as per its Spanish acronym) in 2023,<sup>43</sup> a regulatory and legal framework was established for the use of Bitcoin as legal tender and for decentralized finances (DeFi). Additionally, substantive criminal legislation<sup>44</sup> was amended to classify crimes related to the illicit use of VA, specifically those committed against Digital Assets or Bitcoin Services Providers (VASPs). These crimes include damage to computer systems, computer fraud, and the hijacking of systems, programs and data. These and other related measures aim to strengthen legal security and build public trust in technology, as well as counter financial crimes related to the use of virtual assets.

From 2021 up to the publication of this report, approximately 20 VA-related regulations of different types have been approved and amended. These include reforms to the DAIL, reinforcing the

---

<sup>42</sup>El Salvador Legislative Assembly. (2021). Ley de Activos Digitales. <https://www.asamblea.gob.sv/sites/default/files/documents/decretos/43DA8049-AA39-4DA8-B892-437B2DD27C1C.pdf>

<sup>43</sup>El Salvador Legislative Assembly. (2023). Ley de Emisión de Activos Digitales. <https://www.asamblea.gob.sv/sites/default/files/documents/dict-amenes/7050D57B-97A1-492F-AA15-CFCAEEF6E138.pdf>

<sup>44</sup>El Salvador Legislative Assembly. (2022). Decreto legislativo No. 236. <https://www.asamblea.gob.sv/sites/default/files/documents/decretos/6141982C-4614-4CF7-B658-D455A9A79616.pdf>

travel rule, providing clearer definitions of stablecoins, removing some regulatory issuance requirements and, unifying VASPs and Bitcoin Services Providers oversight under a single entity — the National Commission of Digital Assets (CNAD as per its Spanish acronym).<sup>45</sup> Additionally, the requirements for electronic invoicing in the Tax Code have been modified.<sup>46</sup> Several specialized regulations and instructions governing Bitcoin, stablecoins, and digital assets issuance, such as underlying or referenced assets, have also been passed. Guidelines for the application of AML/CTF measures for VASP and BSP have been established by the Financial Intelligence Unit (FIU).

Meanwhile, the Legislative Assembly is currently debating various draft bills, including reforms to the Banking Law to incorporate the concept of private investment banks<sup>47</sup> and regulate activities involving stablecoins.<sup>48</sup>

---

<sup>45</sup>Hernández, Claudia. Global Financial Integrity. (2024). Cambios en la ley de activos digitales en El Salvador. <https://criptoabierto.com/cambios-en-la-ley-de-emision-de-activos-digitales-de-el-salvador/>

<sup>46</sup>El Salvador Legislative Assembly. (2024). Decreto legislativo. 960 y 487 Reformas al código tributario. [9BA5E264-CEOD-4CA7-97D7-D8B-AC5CE106A.pdf](https://www.asamblea.gob.sv/sites/default/files/documents/9BA5E264-CEOD-4CA7-97D7-D8B-AC5CE106A.pdf) (asamblea.gob.sv) [A607DD05-7C5C-471B-A7F6-7393107250B7.pdf](https://www.asamblea.gob.sv/sites/default/files/documents/A607DD05-7C5C-471B-A7F6-7393107250B7.pdf) (asamblea.gob.sv)

<sup>47</sup>El Salvador Legislative Assembly. (2024). Diputados estudian reformar ley para establecer banca privada de inversión en El Salvador. <https://www.asamblea.gob.sv/node/13220>

<sup>48</sup>Magaña, Yolanda. Diario El Mundo. (2024). El Salvador crearía bancos privados de inversión para clientes con activos libres desde \$250,000. <https://diario.elmundo.sv/politica/el-salvador-crearia-bancos-privados-de-inversion-para-clientes-con-activos-libres-desde-250000>

Additionally, a law on the Prevention, Control, and Sanction of Asset Laundering, Terrorist Financing, and the Proliferation of Mass-Destruction Weapons is being discussed, which would include VASPs and Bitcoin Services Providers as obligated entities.<sup>49</sup>

These updates reflect the ongoing effort by the Government of El Salvador to adapt to new technologies and ensure their functionality and reliability, posing challenges in their effective application.

## TAX CHANGES

In February 2024, several reforms to the tax code related to electronic and physical invoices for the identification of the buyer or service provider were approved. Those reforms provide for raising the threshold for transactions, from \$200 up to \$25,000 in relation to identification data on final consumer invoices.<sup>50</sup>

In the same vein, in March 2024, Article 3 of the Income Tax Law was to exempt from tax any amount received from any foreign entity, as well as any movement of capital, remuneration, or emolument, in money or in-kind, generated by national or foreign capital investment. This applies to individuals, legal entities, or entities without legal personality, whether

they are inside or outside El Salvador. However, this exemption is limited to income generated outside the country; income earned within El Salvador remains subject to the applicable income tax.<sup>51</sup>

Furthermore, between August and September 2024, the Ministry of Finance published a circular establishing that for sales made by final consumers in transactions under \$25,000, personal data such as identification number, email, mobile number, and economic activity do not need to be provided.<sup>52</sup> Additionally, the FIU indicated that for the commercial sector, Customer Due Diligence (CDD) policies should only be applied to cash transactions over US\$10,000 or transactions over US\$25,000 through any other payment method.<sup>53</sup>

---

<sup>49</sup>Attorney General's Office. (2023). Aprobación de la Ley Especial para la Prevención, Control y Sanción del LA/FT y de la Proliferación de Armas de Destrucción Masiva <https://www.uif.gob.sv/aprobacion-de-la-ley-especial-para-la-prevencion-control-y-sancion-del-la-ft-y-de-la-proliferacion-de-armas-de-destruccion-masiva/>

<sup>50</sup>El Salvador Legislative Assembly. (2024). Decreto legislativo. 960 reformas al código tributario. [9BA5E264-CE0D-4CA7-97D7-D8BAC5CE106A.pdf](https://www.asamblea.gob.sv/9BA5E264-CE0D-4CA7-97D7-D8BAC5CE106A.pdf) ([asamblea.gob.sv](https://www.asamblea.gob.sv/))

---

<sup>51</sup>El Salvador Legislative Assembly. (2024). Decreto legislativo. 960 reformas al código tributario. [9BA5E264-CE0D-4CA7-97D7-D8BAC5CE106A.pdf](https://www.asamblea.gob.sv/9BA5E264-CE0D-4CA7-97D7-D8BAC5CE106A.pdf) ([asamblea.gob.sv](https://www.asamblea.gob.sv/))

<sup>52</sup>The Bitcoin Office. [[@bitcoinofficesv](https://twitter.com/bitcoinofficesv)]. (2024). "Regarding the demands for identification cards some have encountered in shops in El Salvador on purchases of less than \$25,000, please read the notice below from the Ministry of Finance." [Post on X]. <https://x.com/bitcoinofficesv/status/1831534362841465183?s=46>

<sup>53</sup>Attorney General's Office's post on X: "¡ATENCIÓN! La @FGR\_SV a través de la Unidad de Investigación Financiera comunica lo siguiente: Los Sujetos Obligados con Actividades no financieras que realicen transacciones inferiores a los \$10,000 dólares en efectivo o superiores a \$25,000 dólares en otras formas de <https://t.co/srPjVEFUml>" / X

The FIU exempted financial institutions, Designated Non-Financial Businesses and Professions (DNFBPs), BSPs and DASPs<sup>54</sup> from this measure, meaning that these sectors would be required to perform CDD for transactions under US\$25,000.

Finally, on September 17, 2024, the Legislative Assembly approved another amendment to the tax code imposing a fine for the undue requirement of personal data from individuals, nationals, or foreigners, who acquire goods and/or services for an amount less than US\$25,000.

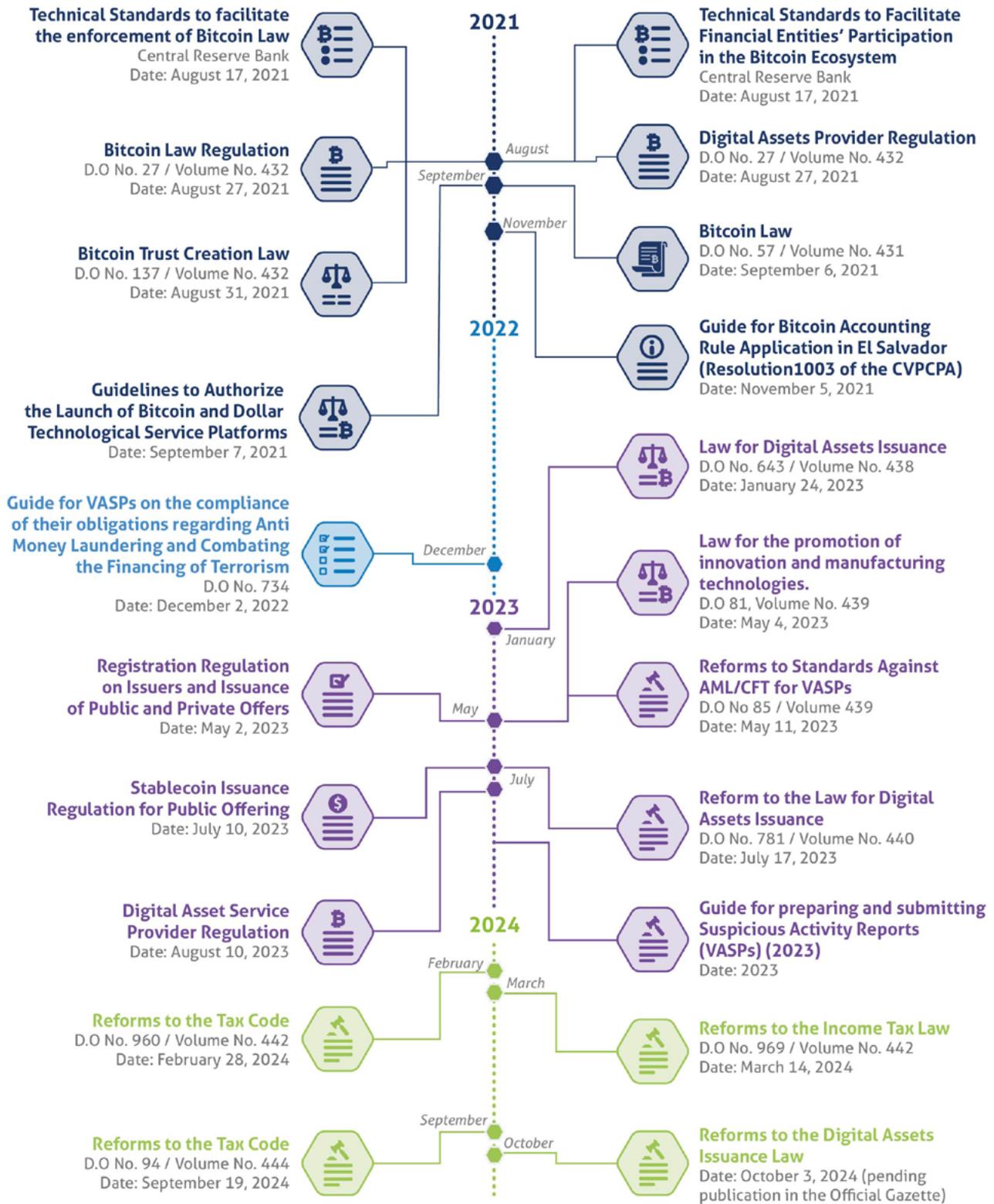
Exceptions include cases where individuals need an invoice to document the transaction or need to deduct the expense, in which case, if they are foreigners, they must present a fiscal document from their country of residence. In the case of legal entities, the corporate name must always be indicated, regardless of the amount. If the operation needs to be documented or the expense deducted, the legal entity must provide its tax identification number or, if it is a foreign entity, the fiscal registration number or another identifying document.

---

<sup>54</sup>Attorney General's Office's post on X: "¡ATENCIÓN! La @FGR\_SV a través de la Unidad de Investigación Financiera comunica lo siguiente: Los Sujetos Obligados con Actividades no financieras que realicen transacciones inferiores a los \$10,000 dólares en efectivo o superiores a \$25,000 dólares en otras formas de <https://t.co/srPjVEFUml>" / X

Graphic 1

**TIMELINE OF VIRTUAL ASSETS REGULATION IN EL SALVADOR**



Source: Global Financial Integrity

## AN OVERVIEW OF EL SALVADOR GOVERNMENT BITCOIN INVESTMENT

GOES' first Bitcoin purchases were made on September 6, 2021, comprising eleven Bitcoin acquisitions.<sup>55</sup> These purchases made a total of 2,381 Bitcoins until November 16, 2022, when it was announced by the social network "X", the decision to buy 1 BTC per day starting the following day.

On November 17, 2022, began with the purchase of 1 BTC per day,<sup>56</sup> accounting until March 14, 2024,<sup>57</sup> the amount of 2,865 bitcoins in total when the address of the cold wallet of the Government of El Salvador was published with the amount of 2,865 bitcoins in total.<sup>58</sup>

---

<sup>55</sup>1. <https://x.com/nayibbukele/status/143496847592824833>  
2. <https://x.com/nayibbukele/status/1435023474494410753>  
3. <https://x.com/nayibbukele/status/1435260422110732300>  
4. <https://x.com/nayibbukele/status/1439815012642611203>  
5. <https://x.com/nayibbukele/status/1453461587948445697>  
6. <https://x.com/nayibbukele/status/1464307422793715716>  
7. <https://x.com/nayibbukele/status/1467000621354135555>  
8. <https://x.com/nayibbukele/status/1473489844521385985>  
9. <https://x.com/nayibbukele/status/1484651539587289091>  
10. <https://x.com/nayibbukele/status/1523742670044413954>  
11. <https://x.com/nayibbukele/status/1542672286490271744>

<sup>56</sup>Bukele, N. [@nayibbukele]. (2022) We are buying one #Bitcoin every day starting tomorrow. Mensaje en X]. <https://x.com/nayibbukele/status/1593113857261965312>

<sup>57</sup>Bukele, N. [@nayibbukele]. (2024). We've decided to transfer a big chunk of our #Bitcoin to a cold wallet, and store that cold wallet in a physical vault within our national territory [Mensaje en X]. <https://x.com/nayibbukele/status/1768425845163503738?s=48>

<sup>58</sup>**A**= 11 compras de Bitcoin realizadas entre el 06 de septiembre de 2021 y el 16 de noviembre de 2022, conforme a las publicaciones realizadas en la plataforma X: 2,381 bitcoins.

**B**= días transcurridos entre el 17 de noviembre y el 14 de marzo de 2024, haciendo un total de 484 días, que bajo la decisión de compra de 1 BTC al día contabilizaría la cantidad de: 484 bitcoins.

**A+B**=2,865 bitcoins.

On March 14, 2024, the date on which the President of El Salvador released the address of the cold wallet through the GOES social network "X" (32ixEdVJWo3kmvJGMTZq5jAQVZZeuwnqzo), the published balance sheet of the cold wallet<sup>59</sup> through the GOES social network "X" (32ixEdVJWo3kmvJGMTZq5jAQVZZeuwnqzo),<sup>60</sup> the published balance sheet of the cold wallet reflected the amount of 5,689.68509200 bitcoins,<sup>61</sup> equivalent on that date to US \$406,607,655.<sup>62</sup>

Likewise, in the same publication, the President announced that this new wallet would be kept in a "physical vault within our national territory".<sup>63</sup>

---

<sup>59</sup>A cold wallet is a hardware device that stores cryptocurrencies, and is not connected to the internet. Coinbase. Cartera de criptoactivos caliente vs fría: ¿cuál es la diferencia? <https://www.coinbase.com/es-es/learn/wallet/hot-vs-cold-crypto-wallet-what-is-the-difference#:~:text=Las%20carteras%20fr%C3%ADas%20son%20basadas,las%20necesidades%20y%20preferencias%20individuales>.

<sup>60</sup>Bukele, N. [@nayibbukele]. (2024). We've decided to transfer a big chunk of our #Bitcoin to a cold wallet, and store that cold wallet in a physical vault within our national territory [Mensaje en X]. <https://x.com/nayibbukele/status/1768425845163503738?s=48>.

<sup>61</sup>Transacción 1: <https://mempool.space/tx/130c87cb615456ca8f-126c502068e53e481611cb42fed248da560f6e01d1fe6a>  
Transacción 2: <https://mempool.space/tx/4d7ee580190b1aadd-4603a5953ef385c5c06b531dc62d1229f5ea87c379b69da>  
Transacción 3: <https://mempool.space/tx/3870a2d9fad1328cdadb2a7ea-2344191d1a507d933de7de115144fdef74427f9>  
Transacción 4: <https://mempool.space/tx/968d0b0f6c697668f-9ca04a4904ed9a3629c20b11e470392510629a32eddeb03>  
Transacción 5: <https://mempool.space/tx/24bd78028879ed7fbd159fc-be16855a506ef46f0b69f9239a201fcc054775f52>  
Transacción 6: <https://mempool.space/tx/6005f0d2a6494501f2bd-c47ae05de749d5fa08042c28dd7db664ae51344f3904>

<sup>62</sup>El precio del Bitcoin al 14 de marzo de 2024 es de US\$69,463.7 <https://es.investing.com/crypto/bitcoin/historical-data>.

<sup>63</sup>Bukele, N. [@nayibbukele]. (2024). We've decided to transfer a big chunk of our #Bitcoin to a cold wallet, and store that cold wallet in a physical vault within our national territory [Mensaje en X]. <https://x.com/nayibbukele/status/1768425845163503738?s=48>.

On May 12, 2024, the National Office of Bitcoin (ONBTC as per its Spanish acronym) published<sup>64</sup> on its website a tool “Bitcoin Explorer” that allows to make transparent the traceability of the GOES address,<sup>65</sup> especially the purchase of 1 BTC per day.<sup>66</sup> This traceability tool is similar to other open-source tools, which contain a search engine to trace BTC addresses, blocks and transaction hashes within the Bitcoin blockchain.<sup>67</sup>

As of the closing date of this report, October 8, 2024, verifying the balance sheet of the GOES management, the amount of 5,896.75942931 bitcoins equivalent to US\$370,458,014 was accounted for.

---

<sup>64</sup>The Bitcoin Office. El Salvador. (s.f.). <https://x.com/bitcoinofficesv/status/1789788632070431046>

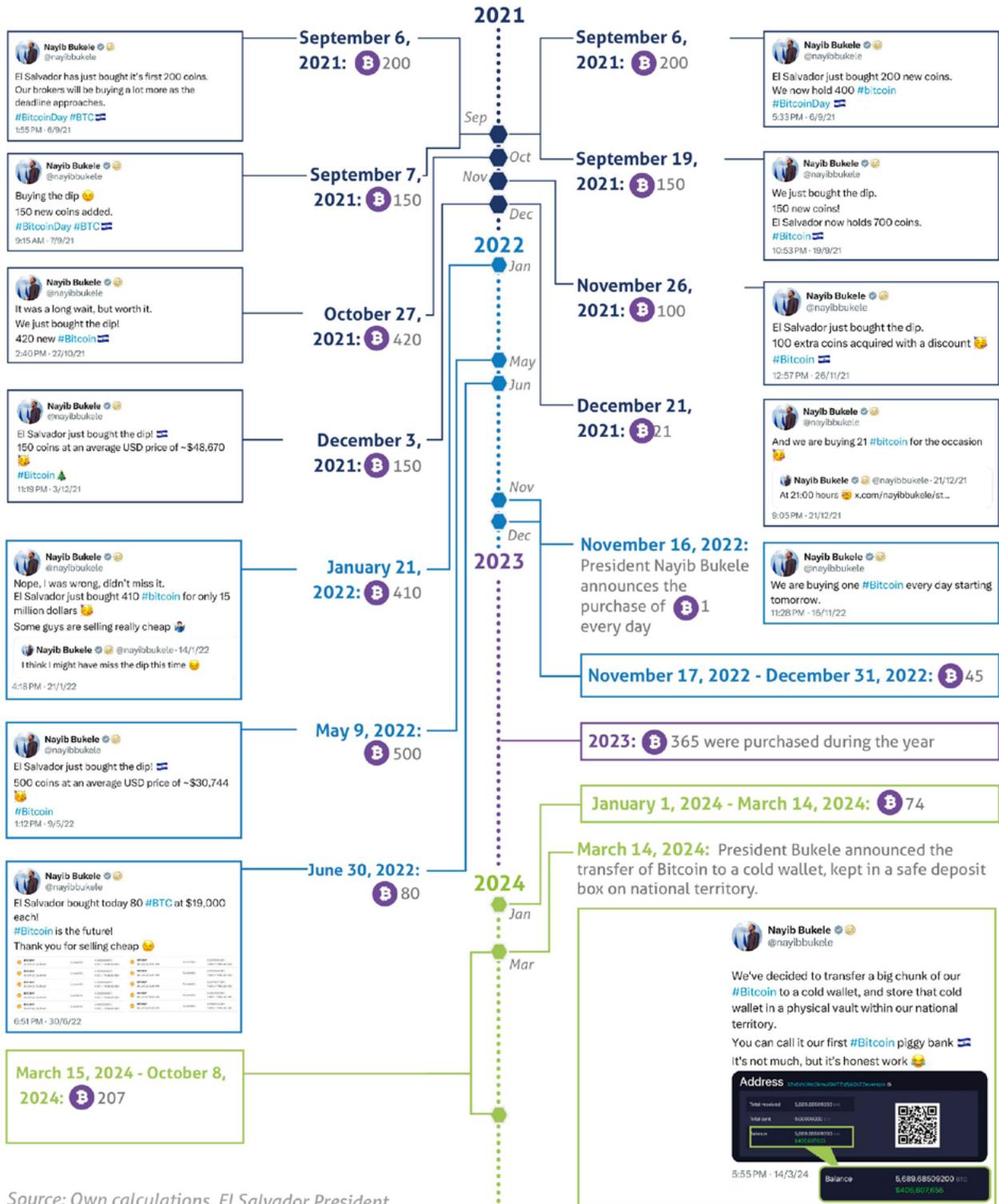
<sup>65</sup>According to open source tools the first GOES address transaction is dated March 13, 2024: <https://glasschain.org/btc/Address/32ixEdVJWo3kmvJGMTZq5jAOVZZeuwnqzo>.

<sup>66</sup>On November 17, 2022, President Bukele posted on the social network X (formerly Twitter) that starting the next day, November 18, 2022, the government would purchase 1 a day. From November 18, 2022 until April 30, 2023, the government bought 164.

<sup>67</sup>Mempool Space, <https://mempool.space/address/32ixEdVJWo3kmvJGMTZq5jAOVZZeuwnqzo>  
Blockchair, <https://blockchair.com/bitcoin/address/32ixEdVJWo3kmvJGMTZq5jAOVZZeuwnqzo>  
[Blockchain.info](https://blockchain.info)

Graphic 2

## EL SALVADOR'S GOVERNMENT BITCOIN PURCHASES: ANALYSIS OF SOCIAL MEDIA POSTS AND BITCOIN BLOCKCHAIN



The safekeeping of the access keys to the cold wallet must be extremely careful,<sup>68</sup> since, like hot wallets, cold wallets, despite not being connected to the Internet, present information security challenges. The GOES cold wallet would be safeguarding 5,896.75942931<sup>69</sup> bitcoins equivalent to US\$370,458,014<sup>70</sup> according to the balance sheet of the same address.

---

<sup>68</sup>Alexander, Doug. The Seattle Times. (2019). Crypto CEO dies holding the only passwords that can unlock millions in customer coins. <https://www.seattletimes.com/business/crypto-ceo-dies-holding-only-passwords-that-can-unlock-millions-in-customer-coins/>

<sup>69</sup>Amount of Bitcoins al 8 de octubre de 2024.

<sup>70</sup>Bitcoin price as of October 8, 2024 was US\$62,673.05. <https://coinmarketcap.com/currencies/bitcoin/>

# 1

## CHAPTER 1

# Legal Framework for the Prevention of Money and Asset Laundering in El Salvador



The institutional and regulatory framework to prevent ML and AL in El Salvador is enshrined in the 1998 Law Against Money and Asset Laundering, aiming to “prevent, detect, penalize, and eradicate money and asset laundering and its cover-up”.<sup>71</sup> It lists twenty entities<sup>72</sup> that are obligated to report suspicious financial transactions or those over the threshold established by the law, as well as training a person appointed as a compliance officer. The primary intervening entity is the Financial Intelligence Unit (FIU), as will be discussed further below.<sup>73</sup>

The AML/CTF legal framework has been addressed recently following the results of the Mutual Evaluation (ME) conducted by GAFILAT during its onsite visit in January 2024.<sup>74</sup> The importance

of this evaluation lies in its ability to identify key areas of improvement for the country to adopt so that its preventive system is strengthened. El Salvador stands out as one of the few countries in the region that has regulated VAs and has pioneered in adopting Bitcoin as a legal tender. In this line of thought, it is important to prevent a potential increase in risks associated with VA use.<sup>75</sup>

Concerning TF, the ME highlighted that El Salvador has focused primarily on classifying gangs and maras as local terrorist groups, whose activities are typically financed through predicate crimes.<sup>76</sup> However, a thorough analysis of TF potential risks and the use of VAs by terrorist organizations must be conducted. Failing to do that would limit the country’s ability to identify and mitigate risks related to this criminal phenomenon.<sup>77</sup>

<sup>71</sup>Legislative Assembly. Anti-money and Asset Laundering (1998), Decree 498. <https://www.asamblea.gob.sv/sites/default/files/documents/decretos/0B869CC3-0E7E-44B0-AFB7-59AC74EA0849.pdf>

<sup>72</sup>Entities obligated under the 1998 Anti-Money and Asset Laundering Law include: (a) all corporations, companies, or entities, domestic or foreign, that form part of a financial institution, group, or conglomerate supervised and regulated by the financial system superintendent; (b) micro-finance institutions, credit unions, and non-bank financial intermediaries; (c) Importers and exporters of agricultural products and inputs, as well as new or used vehicles; (d) Persons or entities systematically or significantly transferring funds, including pawnshops and other lenders; (e) Casinos and gaming houses; (f) Dealers in precious metals and stones; (g) Real estate companies and intermediaries; (h) Travel agencies and transportation companies (air, land, or sea); (i) Individuals or entities handling systematic remittances or shipments; (j) Construction companies; (k) Private security companies and importers or dealers of firearms, ammunition, explosives, and related items; (l) Hotel companies; (m) Political parties; (n) Providers of corporate services and trust management; (o) Non-governmental organizations (NGOs); (p) National and international investors; (q) Pharmacies, pharmaceutical laboratories, and pharmacy chains; (r) Associations, consortia, and business guilds; (s) Any other private or mixed-economy institution, as well as commercial corporations, including lawyers, notaries, accountants, and auditors.

<sup>73</sup>El Salvador’s Legislative Assembly. Anti-Money and Asset Laundering Law (1998), Decree 498. <https://www.asamblea.gob.sv/sites/default/files/documents/decretos/0B869CC3-0E7E-44B0-AFB7-59AC74EA0849.pdf>

<sup>74</sup>GAFILAT. (2024). Informe de evaluación mutua de la República de El Salvador. Informe de Evaluación Mutua de la República de El Salvador – GAFILAT. GAFILAT. (2024) (p. 22, par. 29). GAFILAT. (2024) p. 22, par. 30). GAFILAT. (2024) p. 22, par. 31).

Asamblea Legislativa. Ley contra el lavado de dinero y activos (1998), decreto 498. <https://www.asamblea.gob.sv/sites/default/files/documents/decretos/0B869CC3-0E7E-44B0-AFB7-59AC74EA0849.pdf>

## A. REGULATORY FRAMEWORK

The Law Against Asset and Money Laundering (LAAML), in force since 1998, and its set of rules have been the primary regulatory framework governing related activities and the obligations of involved institutions and obliged entities. Several efforts have aimed to reform and interpret the LAAML between 1998 and 2013.<sup>78</sup> Additionally, in 2018 a draft bill was introduced but subsequently

<sup>75</sup>GAFILAT. (2024) (p. 22, par. 29)

<sup>76</sup>GAFILAT. (2024) p. 22, par. 30).

<sup>77</sup>GAFILAT. (2024) p. 22, par. 31)

<sup>78</sup>Asamblea Legislativa. Ley contra el lavado de dinero y activos (1998), decreto 498. <https://www.asamblea.gob.sv/sites/default/files/documents/decretos/0B869CC3-0E7E-44B0-AFB7-59AC74EA0849.pdf>

archived.<sup>79</sup> It was not until 2023 that a new draft bill was presented (analyzed in this report), which seeks to implement significant changes to the regulatory and institutional framework for Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT). These changes will be elaborated further in this study.

### THE CURRENT LAW AGAINST ASSET AND MONEY LAUNDERING (LAAML) (1998)

The LAAML Law is the main legal framework for combating Asset Laundering and Terrorism Financing (ML/TF), with its primary goal being to prevent, detect, penalize, and eradicate both the cover-up and laundering of funds related to criminal activity.<sup>80</sup> This law regulates the duties of obliged subjects, as well as the roles of supervisors and the Financial Intelligence Unit (FIU).

'Obligated subjects' include a wide range of financial, non-financial and commercial organizations. Also, the law establishes crimes related to money laundering and rules over this and predicate offences.<sup>81</sup> Among the most salient aspects of the regulatory framework is the duty of reporting suspicious transactions and deploying reinforced due diligence measures, particularly for high-risk customers and Politically Exposed Persons (PEP).<sup>82</sup> Additionally, the regulations require the retention

of customer documents and require compliance officers to conduct routine checks to detect unusual transactions.<sup>83</sup>

Moreover, the LAAML and other documents issued by the FIU<sup>84</sup> establish that obligated subjects must register on the FIU platform to report suspicious activities. Additionally, they must register their compliance officer and a substitute<sup>85</sup> and submit documentation regarding: (a) the creation of the Compliance Officer's Office, (b) the designation of the compliance officer, (c) the compliance manual for AML/CTF prevention, (d) a document explaining the alert analysis system and, (e) an audit plan.<sup>86</sup>

<sup>79</sup>El Diario de Hoy, Fiscalía presenta a diputados propuesta de ley para el combate al lavado de dinero y activos. (2018). <https://historico.elsalvador.com/historico/534461/fiscal-general-presenta-reformas-a-ley-de-lavado-de-dinero-que-aumenta-las-penas-menores-de-cinco-a-ocho-anos.html>

<sup>80</sup>Idem.

<sup>81</sup>Idem.

<sup>82</sup>Idem.

<sup>83</sup>Idem.

<sup>84</sup>Attorney General's Office. (2021). Instructivo de la unidad de investigación financiera para la prevención del lavado de dinero y de activos, Attorney General's Office. <https://www.uif.gob.sv/wp-content/uploads/instructivos/InstructivoUifDiarioOficial2021.pdf>.

<sup>85</sup>Attorney General's Office. (2021).

<sup>86</sup>Attorney General's Office. (2021)



## 2023 SPECIAL DRAFT BILL TO PREVENT, CONTROL, AND PENALIZE ASSET LAUNDERING, TERRORIST FINANCING, AND THE PROLIFERATION OF MASS-DESTRUCTION WEAPONS (APL AS PER ITS SPANISH ACRONYM)

By the end of 2023,<sup>87</sup> the Justice and Security Ministry submitted a new draft law to the Legislative Assembly, which aims to reform the current law and comply with FATF and GAFILAT standards. As of the writing of this report, the draft bill was still under discussion in the Public Security and Counter-Narcotics Commission.<sup>88</sup> The debate has involved the Attorney General of the Republic, the Minister of Justice and Public Security, and the deputies that make up the commission, leaving out key sectors such as private banks, PSDAs, BSPs, political parties, academia, and civil society. With their experience, these stakeholders might significantly contribute to strengthening the proposed regulatory framework. Their participation is crucial for the creation of a stronger legal framework with greater legitimacy. The following are some relevant points of the Draft Bill:

- **National System for the Prevention, Control, and Repression of Anti-money Laundering/Counter Terrorist Financing/ Proliferation Financing.**

The Draft Bill of 2023 proposes the creation of the National System for the Prevention, Control, and Repression of ML/TF, which will jointly coordinate

---

<sup>87</sup>El Salvador Legislative Assembly [@AsambleaSV]. (2024). Los diputados emiten dictamen favorable a las siguientes iniciativas: Aprobación de la Ley Especial para la Prevención, Control y Sanción del Lavado de Activos, Financiamiento al Terrorismo y de la Proliferación de Armas de Destrucción Masiva.[ post X]. <https://x.com/AsambleaSV/status/>

<sup>88</sup>El Salvador Legislative Assembly. (n.d.) Comisión de Seguridad y Combate a la Narcoactividad. <https://www.youtube.com/live/u9Bzy-gZbOA>.

the entities that enforce it.<sup>89</sup> This system will be composed of the Attorney General's Office, oversight, regulation, and surveillance entities, as well as the obliged subjects. Its main objective is to centralize and optimize the exchange of information and the coordination of operations between entities, thus improving the capacity to detect and combat illegal activities.

- **Interinstitutional Committee for the Prevention of Asset Laundering and Terrorist Financing.**

The Interinstitutional Committee for the Prevention of Asset Laundering and Terrorist Financing (CIPLAFT as per its Spanish acronym) would act as an advisory and strategic coordination body in charge of designing and proposing to the Executive Branch the policies, strategies, and action plans for the prevention, detection, and combating ML/FT.<sup>90</sup> It would be formed by: (a) the Attorney General, as the head of CIPLAFT; (b) the President of the Supreme Court of Justice; (c) the Minister of Justice and Public Security; (d) the Minister of Justice and Public Security; (d) the Minister of Finance; (e) the Minister of National Defense; (f) the Minister of Economy; (g) the President of the Central Reserve Bank; and (h) the Superintendent of the Financial System.

Among its duties, the CIPLAFT would have the power to include or eliminate obliged subjects from the regulation. To achieve this, it is essential to define and make transparent the criteria under

---

<sup>89</sup>Legislative Assembly. Draft Bill. Special Law to prevent, control, and penalize Asset Laundering, Terrorist Financing, and the Proliferation of Mass-Destruction Weapons, (2023), Title II.

<sup>90</sup>Idem.

which the inclusion or exclusion of obligated subjects would be decided.

### DIGITAL ASSET ISSUANCE LAW AND REFORMS: REGISTRATION, REGULATORS, SUPERVISORS AND PSAV ENFORCEMENT ENTITIES

#### VASP Registration, Regulators, Supervisors, and Sanctioning Entities

For VAs, FATF recommends countries enact regulations to prevent money laundering and terrorist financing-related activities.<sup>91</sup> In El Salvador, the VA ecosystem used to have a dual classification until the reforms passed on October 3, 2024, with the Law of Digital Asset Issuance (LEAD as per its Spanish acronym).<sup>92</sup> Before that reform, PSBs, registration, and licensing were in charge of the Central Reserve Bank (CRB),<sup>93</sup> which was charged with creating a registry and regulating service providers in accordance with the BL’s regulations. Also, the Financial System Superintendence (SSF as per its Spanish acronym)<sup>94</sup> was in charge of overseeing the same regulatory powers used for the traditional financial system.

Following the reform, the National Digital Assets Commission (CNAD) now oversees the registration

related to Digital Assets (DAs),<sup>95</sup> issuers,<sup>96</sup> certifiers,<sup>97</sup> DASPs,<sup>98</sup> and DA issuance.<sup>99</sup> The CNAD is also responsible for supervising and sanctioning registered entities that fail to comply with applicable regulations.<sup>100</sup> With the recent reform to the Digital Assets Law (LEAD), the CNAD has taken over responsibilities for registering, regulating, supervising, and sanctioning Bitcoin Service Providers (BSPs), which are no longer under the jurisdiction of the Central Reserve Bank (BCR as per its Spanish acronym) or the Superintendency.

The reform to LEAD has attempted to simplify the digital assets ecosystem by consolidating regulatory, supervisory, and enforcement functions under a single entity, the CNAD, despite the complexities of the digital financial and compliance systems. The reform also aims to align with the Financial Action Task Force (FATF) Recommendation 15, addressing virtual assets and their service providers.

<sup>91</sup>FATF, Recommendation 15, <https://biblioteca.gafilat.org/wp-content/uploads/2024/07/Recomendaciones-metodologia-actDIC2023.pdf>

<sup>92</sup>Legislative Assembly. (2023).Reform to the Digital Asset Law. <https://www.asamblea.gob.sv/sites/default/files/documents/decretos/DA8F5A99-0267-4830-AA47-D03C37413608.pdf>

<sup>93</sup>El Salvador Central Reserve Bank. (s. f). Registro de Proveedores de Servicios Bitcoin. <https://registrobotcoin.bcr.gob.sv/web/inicio>

<sup>94</sup>Ministry of Economy. (2021). Reglamento de la Ley Bitcoin. (Art. 5), <https://www.iscpcelsalvador.org/wp-content/uploads/Reglamento-Ley-Bitcoin.pdf>

<sup>95</sup>Digital Asset National Commission. (n. d). Registro público <https://cnad.gob.sv/public-registry/>

<sup>96</sup>Digital Asset National Commission. (n. d). Lista de emisores. <https://cnad.gob.sv/issuers/>

<sup>97</sup>Digital Asset National Commission. (n. d). Lista de certificadores. <https://cnad.gob.sv/certifiers/>

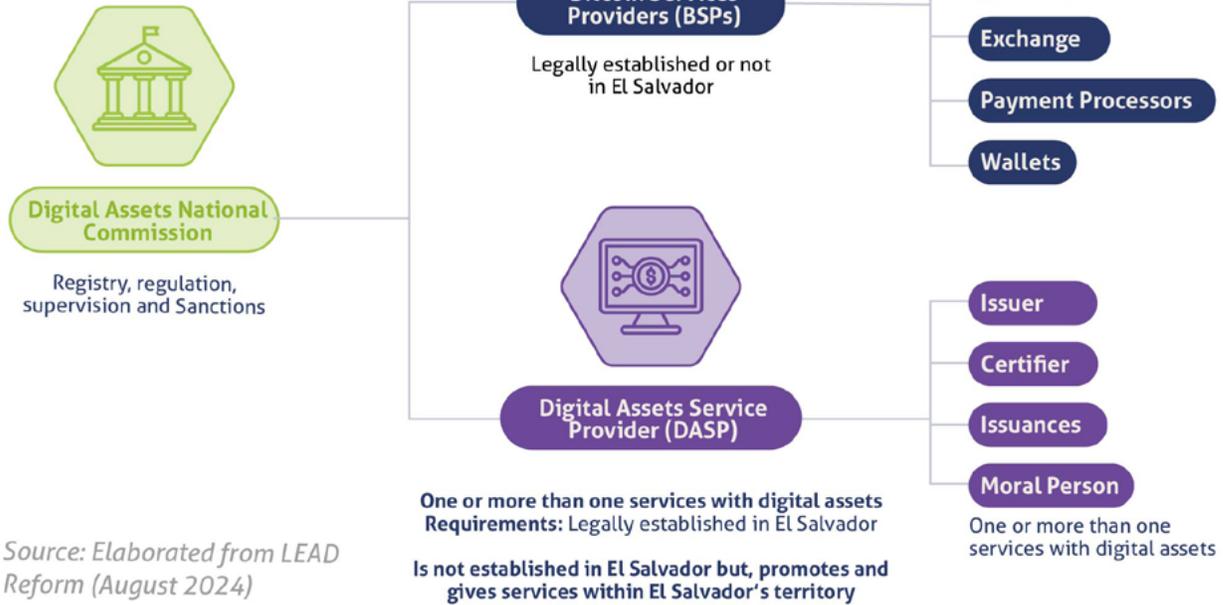
<sup>98</sup>Digital Asset National Commission. (n. d). PSAD. <https://cnad.gob.sv/public-registry/digital-assets-service-provider/>

<sup>99</sup>Digital Asset National Commission. (n. d). Lista de emisores. <https://cnad.gob.sv/issuances/>

<sup>100</sup>Legislative Assembly. (2023). Ley de emisión de activos digitales. <https://www.asamblea.gob.sv/sites/default/files/documents/dictamenes/7050D57B-97A1-492F-AA15-CFCAEEF6E138.pdf>

Graphic 3

**DIGITAL ASSETS ISSUANCE  
LAW LEGAL FRAMEWORK  
REGARDING BSP AND DASP**



**B. INSTITUTIONAL FRAMEWORK**

Below is a brief overview of some of the powers granted to the Financial Intelligence Unit (FIU) within the current regulatory framework, along with its role in ensuring compliance with GAFILAT standards. These include suspicious transaction reporting, customer due diligence, Politically Exposed Persons (PEP), ultimate beneficial owners, and obligated entities. This analysis compares the existing legislation with the Proposed Law (APL), which expands the scope to include additional obligated entities, such as virtual asset service providers (VASPs).

**FINANCIAL INVESTIGATION UNIT (FIU)**

The current LAAML dictates that the FIU is an office reporting to the Attorney General’s Office charged with investigating Money and Asset Laundering crimes.<sup>101</sup> It has functional and technical autonomy, and its organizational structure is determined by the Attorney General’s Office Organic Law.<sup>102</sup> The FIU is the only national center in charge

<sup>101</sup>Legislative Assembly. (2023). Ley de emisión de activos digitales. <https://www.asamblea.gob.sv/sites/default/files/documents/dictamenes/7050D57B-97A1-492F-AA15-CFCAEEF6E138.pdf>

<sup>102</sup>Legislative Assembly. Ley contra el lavado de dinero y activos (1998), Decree 498. <https://www.asamblea.gob.sv/sites/default/files/documents/decretos/0B869CC3-0E7E-44B0-AFB7-59AC74EA0849.pdf>

of receiving and analyzing Suspicious Activity Reports (SARs), as well as any information related to money laundering or terrorist financing.<sup>103</sup> The power of the FIU to proceed as the only center for the analysis and reception of financial information reinforces its role in the national AML/CTF strategy.

integrity of the financial system and prevention of money laundering and terrorist financing. In this regard, the FIU plays a crucial role in providing the tools and legal framework necessary for regulated entities to identify and report suspicious activities in a timely and accurate manner.

### SUSPICIOUS ACTIVITY REPORTING (SAR)

### CUSTOMER DUE DILIGENCE (CDD)

FATF Recommendation Number 20, and its interpretative note, establish the obligation of financial institutions to report suspicious activities, either because there is a suspicion that the funds are derived from criminal activity or that they are related to FT.<sup>104</sup> In the LACD, the reporting obligation extends to designated non-financial activities and professions (APNFD), such as lawyers, notaries, accountants, and auditors.

FATF, in its Recommendation 10, establishes that financial entities must conduct Customer Due Diligence (CDD) to remove anonymous or fictitious accounts and ensure that the information is duly verified for each customer. To carry out the above, an internal due diligence policy should be established, including the identification and verification of the customer (natural or legal person), the Beneficial Owner (BO), the purpose and nature of the business relationship, and ongoing monitoring.<sup>106</sup>

According to the Law in force, a SAR must be made within five working days after the respective analysis has been completed and there are sufficient elements to consider the operation irregular.<sup>105</sup> Conversely, the Draft Bill suggests an expedited 24-hour timeframe to report SAs after finishing the respective analysis, and sufficient elements have arisen to consider the operation suspicious. Strict compliance with suspicious activity reporting obligations is essential for the

When dealing with legal persons, financial entities must identify and verify the client and understand the business activity in order to assess the potential risks of the business, as well as its structure, ownership, and control.<sup>107</sup>

<sup>103</sup>Legislative Assembly. Anti-Money and Asset Laundering Law (1998), Decree <sup>498</sup>. <https://www.asamblea.gob.sv/sites/default/files/documents/decretos/OB869CC3-0E7E-44B0-AFB7-59AC74EA0849.pdf>

<sup>104</sup>Financial Action Task Force. (2023). International Standards on combating ML/TF/PF. <https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf>.

<sup>105</sup>Art. 9 of Anti-Money and Asset Laundering Law (LAMAL) <https://ssf.gob.sv/wp-content/uploads/2022/07/Ley-contra-el-lavado-de-dinero-y-de-Activos-D498.pdf>

<sup>106</sup>CFATF-GAFIC.(n. d.) 40 Recomendaciones del GAFI. RECOMENDACIÓN 10. Due diligence del cliente (cfatf-gafic.org).

<sup>107</sup>Legislative Assembly. Ley contra el lavado de dinero y activos (1998), decreto 498. <https://www.asamblea.gob.sv/sites/default/files/documents/decretos/OB869CC3-0E7E-44B0-AFB7-59AC74EA0849.pdf>

These CDD measures should be implemented using a risk-based approach, which means that where major risks exist, institutions should apply intensified measures to manage and mitigate the risks, and where risks are minor, they can afford to apply simplified measures.<sup>108</sup>

## POLITICALLY EXPOSED PERSONS (PEP)

It is important to have an explicit list of individuals considered Politically Exposed Persons (PEP) in order to facilitate their identification and compliance with applicable regulations. To define who are PEPs, the current law refers to the Constitution of the Republic and the United Nations Convention Against Corruption. Under these, PEPs are considered to be officials who hold the highest public office, whether by popular election, appointment, or designation.<sup>109</sup> In addition, any other public official who meets the criteria set forth in the United Nations Convention against Corruption (UNCAC) shall be considered a PEP. Specifically, those who: a) hold a legislative, executive, administrative, or judicial office in a State party to the UNCAC, whether appointed or elected, permanent or temporary, paid or honorary, regardless of their seniority in office; b) perform a public function, including for a public agency or public company or provide a public service under national law.<sup>110</sup> In these cases, the LAAML sets out the obligation to perform enhanced due diligence.

<sup>108</sup>Idem.

<sup>109</sup>El Salvador Legislative Assembly. (1983) Constitución de la República de El Salvador. <https://www.asamblea.gob.sv/sites/default/files/documents/decretos/69A06B07-4F30-4FOE-8FB1-D664A3E6D8CC.pdf>

<sup>110</sup>United Nations. (2004). Convención de las Naciones Unidas contra la Corrupción. [https://www.unodc.org/pdf/corruption/publications\\_unodc\\_convention-s.pdf](https://www.unodc.org/pdf/corruption/publications_unodc_convention-s.pdf)

## BENEFICIAL OWNERS (BO)

Recommendations 24 and 25 state that countries should ensure transparency in the ownership of legal persons to prevent misuse in illegal activities such as AML/CTF. Countries should implement effective measures to identify and verify the identity of beneficial owners, ensuring that this information is accurate, up-to-date, and accessible to the authorities. These measures include the implementation of mechanisms to ensure that basic information, including information provided to the commercial register, is accurate and updated in a timely manner.<sup>111</sup>

In its recent evaluation, FATF highlighted that the country displays some weaknesses in ensuring that Beneficial Owners' (BOs) information is accurate and up to date. It is necessary to deploy mechanisms to obtain adequate, accurate, and updated information on the BO and the control of trading companies and other legal persons.<sup>112</sup> Similarly, it is necessary to deploy actions to identify and describe the different types, forms, and basic characteristics of legal persons, as well as the processes for their creation and the collection and registration of basic information on BOs. It was also pointed out some lack of analysis of the vulnerabilities that other types of companies, other than corporations, may present and the potential modalities of existing abuses, including TF.<sup>113</sup>

<sup>111</sup>CFATF-GAFIC.(n.d.).Recomendación 24: unidades de inteligencia financiera. (<https://www.cfatf-gafic.org/index.php/es/documentos/ga-fi40-recomendaciones/435-fatf-recomendacion-29-unidades-de-inteligencia-financiera>)

<sup>112</sup>GAFILAT. (2024). Informe de evaluación mutua de la República de El Salvador. (Ct. 286, p. 280). [Informe de Evaluación Mutua de la República de El Salvador – GAFILAT](#)

<sup>113</sup>GAFILAT. (2024). (Ct. 286.p.280)

Currently, the LAAML, as well as the Draft Bill, impose on obliged subjects the responsibility to identify and verify the BOs of the legal persons with whom they operate, ensuring that data on BOs are real, accurate, and accessible. Financial Institutions and obliged subjects must implement due diligence policies to identify the true owners of assets and prevent the use of opaque structures to hide illegal activities. Furthermore, the private sector and population should apply due diligence measures to know who is behind any transaction. Compliance with these regulations is essential to strengthen the transparency and integrity of the Salvadoran financial system.

### **OBLIGED SUBJECTS**

Including risk factors is key in AML/CTF regulation to ensure that there are no loopholes that can be exploited for illegal activities. FATF's evaluation revealed that there are 60,000 obliged subjects in El Salvador. However, only 33% of them are registered in the FIU, which is indicative of non-compliance by some of the most relevant institutions.<sup>114</sup> Consequently, El Salvador will take measures to ensure effective compliance by the obligated subjects under the anti-money laundering regulatory framework.

The Draft Bill 2023 includes emerging sectors, such as DASPs and BSPs, as obliged subjects. However, some are excluded regardless of their high potential risk of ML/TF, such as political parties, the tourism sector, trusts, drug stores, not-for-profit

associations, or foundations NGOs. In January 2024, the President of the Legislative Assembly noted that construction companies, drug stores, pharmaceutical companies, political parties, and non-governmental and trade organizations would be included in the Draft Bill.<sup>115</sup> As of the date of this report, there has been no progress in the discussions or formal inclusion of these obliged subjects.

### **VIRTUAL ASSET SERVICE PROVIDERS**

Virtual Service Providers (VSPs) mainly refer to the infrastructure through which activities related to distributed ledger technology (DRT) are performed, such as through the Bitcoin Blockchain, the Ethereum Blockchain or others such as Tron, Polygon or Avalanche. In PSAVs, transactions can be made from one user to another within the same PSAV or outside, to make transfers, purchases, payments, exchanges or schedule smart contracts.

<sup>114</sup>GAFILAT. (2024). Informe de evaluación mutua de la República de El Salvador. (pág 150, p549). [Informe de Evaluación Mutua de la República de El Salvador – GAFILAT](#)

<sup>115</sup>Guzman, Jessica. El Mundo. (2024). Diputados modificarán dictamen aprobado de la nueva Ley contra el Lavado: incluirán a constructoras, farmacéuticas, partidos y oenegés. <https://diario.elmundo.sv/politica/diputados-modificaran-dictamen-aprobado-de-la-nueva-ley-contra-el-lavado-incluiran-a-constructoras-farmaceticas-partidos-y-oeneges>



In El Salvador, PSAVs refer to legal or natural persons that carry out some of the activities regulated by the LEAD in order to provide their services and offer products within the Salvadoran territory through their platforms or infrastructures; they may be registered in El Salvador or they may be non-domiciled and promote the commercialization of digital assets.<sup>116</sup> To operate, PSAVs must be registered with the CNAD or the BCR. Some of the registered DASPs Bitfinex, Binance, Ditobanx, Blink and Chivo Wallet are in the CNAD<sup>117</sup> and BCR<sup>118</sup> registries.

### (i) Application of AML/CFT Standards.

FATF's Recommendation 15, on the use of new technologies, underlines the importance for countries and financial entities to identify risks related to VAs use through new technologies. In 2018, the FATF<sup>119</sup> issued an interpretative note for this recommendation, specifically regarding information and telecommunication technologies (ICTs). Such a note established that in order to monitor and oversee VAs and VASPs, the existing recommendations should be applied.

---

<sup>116</sup>Decree 643. Law of Issuance of Digital Assets. Date of publication: January 24, 2023. <https://www.asamblea.gob.sv/sites/default/files/documents/decretos/BED5A3F8-8937-4547-A291-CE06802B0B23.pdf>

<sup>117</sup>Registry of Digital Asset Service Providers, CNAD. <https://cnad.gob.sv/es/como-registrarse/psad/>

<sup>118</sup>Bitcoin Service Provider Registry, BCR. <https://registrobotcoin.bcr.gob.sv/web/proveedores-registrados>

---

<sup>119</sup>Financial Action Task Force. (2019). Public Statement, Mitigating risks from virtual assets, <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Regulation-virtual-assets-interpretive-note.html>; [Outcomes FATF Plenary, 20-22 February 2019](https://www.fatf-gafi.org/en/publications/Fatfgeneral/Outcomes-plenary-february-2019.htm) <https://www.fatf-gafi.org/en/publications/Fatfgeneral/Outcomes-plenary-february-2019.htm>.

*Graphic 4*  
**HIGHLIGHTS OF FATF INTERPRETATIVE NOTE TO RECOMMENDATION 15 (2018)**  
**DATE OF ADOPTION (2019)**

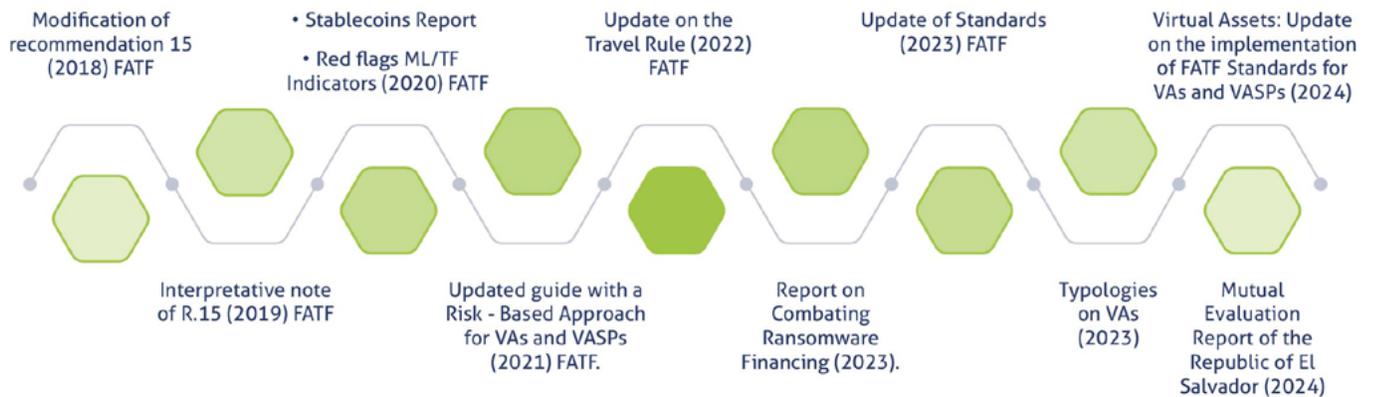


Source: Global Financial Integrity

The implementation of Recommendation 15 reinforces the need for a more rigorous oversight of VASPs, ensuring that they operate within a regulatory framework that mitigates the risks associated with the use of virtual assets. Continuous monitoring and adaptation of preventive measures for new technologies are essential to protect the financial system from emerging threats. That way, El Salvador is aligned with international standards, strengthening its ability to prevent ML/TF in a constantly evolving digital environment.

The interpretative note of 2018 highlighted several key aspects, including classifying virtual assets as value transmitters. It established that the platforms where AV activities are carried out must be licensed and registered, under the oversight and monitoring of competent authorities. These authorities are responsible for regulating adequately to prevent ML/TF, as well as imposing sanctions where appropriate. The note also emphasized five important recommendations:

*Graphic 5*  
**TIMELINE OF FATF EFFORTS REGARDING VIRTUAL ASSETS WITHIN THE SALVADORIAN CONTEXT**



Source: Global Financial Integrity

**R.1:** Risk mitigation AML/TF/PF, **R.10:** Customer due diligence on transactions exceeding 1,000 USD/Euros, **R.16:** Information availability on issuer and beneficiary, **R.35:** Administrative, civil, and criminal liability for VASPs, including directors and managers; **R.37-40:** International cooperation.

Concerning VAs, FATF has issued several important documents related to Recommendation 15 and new technology implementation. The graph below shows a timeline of those document issuances.

In 2023, FATF updated the standards applicable to VAs, and GAFILAT published a guide on AML/CTF typologies across the region, including cases of fraud, human trafficking, and drug trafficking in countries like Guatemala, Colombia, Argentina, and El Salvador. In this guide, a case of fraud

was highlighted in relation to the use of VAs in El Salvador. It may illustrate some of these behaviors in the country.<sup>120</sup> When updating Recommendation 15, FATF focused on three aspects: a lack of robust risk studies in jurisdictions that have already regulated VAs, challenges in implementing the travel rule and, some need for effective prevention via STRs. (Recommendation 20).

The Draft Bill added VASPs and DASPs, as obliged subjects, which is not considered in the current LAAML. This amendment stemmed from the sanctioning of the Bitcoin Law of 2021 and the sanctioning of the DAAIL in 2023 and as a response to FATF/GAFILAT directives to mitigate AML/CTF risks in member countries.

<sup>120</sup>GAFILAT. (2023). Informe de Tipologías Regionales de LA/FT 2021-2022. <https://biblioteca.gafilat.org/wp-content/uploads/2024/07/Informe-de-Tipologias-Regionales-de-LA-2021-2022.pdf>

From a challenges and opportunities perspective, the inclusion of VASPs as an obliged subject in the Draft Bill represents a significant step forward for El Salvador in adapting to international best practices in VA monitoring. However, the implementation of these standards presents the need to establish solid legal frameworks and conduct ongoing risk assessments. The oversight and enforcement role of the authorities for non-compliance with AML/CTF regulations will require inter-agency coordination, international cooperation, and support from the private sector.

### **(ii) Risk Assessment and Focusing on VASP Applicable Policies**

In a FATF report on implementation of Recommendation 15 among FTAF members and additional jurisdictions, it was noted that 2.9% of member jurisdictions have not conducted a risk assessment in relation to VAs. Additionally, 4.64% lack adequate VA-related risk-mitigating regulations on AML/CTF.<sup>121</sup>

FATF dictates<sup>122</sup> that jurisdictions that have not yet identified the AML/CTF<sup>123</sup> risks associated with the use of VAs and VASPs should do so to implement appropriate mitigation measures.

<sup>121</sup>Financial Action Task Force. (2024). "Status of implementation of Recommendation 15 by FATF Members and Jurisdictions with Materially Important VASP Activity", <https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/VACG-Table-Jurisdictions-2024.pdf.coredownload.pdf>

<sup>122</sup>Financial Action Task Force. (2024). Virtual assets: targeted update on implementation of the FATF Standards on VAs and VASPs. p. 4. <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html>

<sup>123</sup>GAFILAT. (2024). Informe de evaluación mutua de la República de El Salvador.(Ct188- pág 259). [Informe de Evaluación Mutua de la República de El Salvador – GAFILAT](#)

It also recommends that jurisdictions supervise and monitor VASPs, regardless of whether they allow or prohibit the use of VA, applying sanctions in case of non-compliance with AML/CTF standards, and stresses the importance of effective regulation and oversight.

El Salvador recently conducted a National Risk Assessment (NRA) on this recommendation stating that "There are no risk assessments on AML/CTF for VASPs, nor an oversight entity has been enabled to perform risk-based monitoring."<sup>124</sup>

Despite the fact that more than 20 VA-related regulations have been passed by El Salvador since 2021,<sup>125</sup> it is necessary that they are included in aim a public policy that is sufficiently broad and comprehensive to foster technology, financial inclusion, and data protection.

To build a solid VA ecosystem, it is essential to implement financial and technological literacy campaigns, foster dialogue between different sectors, including the traditional private sector, and train law enforcement in the use and regulation of these technologies. In addition, it is crucial to strengthen the regulatory, supervisory and sanctioning bodies.

<sup>124</sup>Cripto Abierto. (n.d.). Regulación Cripto. <https://criptoabierto.com/regulacion-cripto/>

<sup>125</sup>Global Financial Integrity and Vance Center. (2023). The Virtual Assets Ecosystem In El Salvador: Strengthening Financial Integrity And Transparency. <https://34n8bd.p3cdn1.secureserver.net/wp-content/uploads/2023/10/Crypto-El-Salvador-Report-ENG-FINAL-1.pdf?time=1724969507>



## SUSPICIOUS ACTIVITY REPORTING OBLIGATIONS FOR BSPS AND DASPS

Today, VASPs are not obliged subjects, therefore the Draft Bill requests obliged subjects to warn about suspicious activities whenever they identify red flags in VA transactions. This empowers the FIU to conduct crime prevention and awareness activities in this area, as well as to create and implement guidelines for BSPs/DASPs to ensure compliance. Regarding Recommendation 20 for obliged subjects, concerning AVs, FATF issued a report on typologies addressing anonymity, the source of funds and assets, transactions, geographic risks, and the characteristics of senders and recipients.<sup>126</sup>

Meanwhile, the Department of Treasury's Office for Foreign Asset Control (OFAC) has published the SDNL (Specially Designated Nationals List), which includes sanctioned VA addresses. These addresses can be consulted and must be considered when implementing the travel rule to prevent BSPs/DASPs from allowing their clients to engage in transactions with these sanctioned addresses. It is crucial for providers to constantly monitor these lists to ensure compliance and avoid involvement in illicit transactions.

Regarding this, GAFILAT's mutual evaluation results note that by applying traceability software for VA and Bitcoin transactions, supervised entities have clarity about the sanctioned addresses and

---

<sup>126</sup>If a financial entity suspects or has reasonable grounds to suspect that funds come from some criminal activity or are related to terrorist financing, it is legally bound to report its suspicions promptly to the Financial Intelligence Unit (FIU). <https://biblioteca.gafilat.org/wp-content/uploads/2024/07/Recomendaciones-metodologia-actDIC2023.pdf>

the corresponding lists.<sup>127</sup> The assessment also highlights the supervisor's obligation to issue guidelines or information to assist DASPs, certifiers, issuers, and acquirers (or investors) in applying the national AML/CTF measures and, in particular, detecting and reporting suspicious activities<sup>128</sup> during the VA issuance process, which will be explained later in the tokenization section.

An effective implementation of STs is crucial for detecting and mitigating risks associated with VA use. Continuous monitoring and the ability of BSPs/DASPs to identify suspicious transactions ensure that the financial system remains resilient against emerging threats. The FIU and supervisory bodies play a key role by providing the necessary tools and guidance to obliged subjects enabling them to identify and report these transactions in a timely and effective manner.

## BENEFICIAL OWNERSHIP (BO) AND BSPS AND DASPS

We have already commented on the importance of knowing BOs and following international guidelines. El Salvador lacks a regulatory framework that includes a robust definition of BOs or a specific register for them. Conversely, the APL requires each obliged subject, in this case, BSPs/DASPs, to identify the BOs of each company in order to recognize the natural person behind the legal entity.

---

<sup>127</sup>GAFILAT. (2024). Informe de evaluación mutua de la República de El Salvador. Página 114. [Informe de Evaluación Mutua de la República de El Salvador – GAFILAT.](#)

<sup>128</sup>GAFILAT. (2024). Informe de evaluación mutua de la República de El Salvador. (CT178, p. 257).

## THE TRAVEL RULE

The application of the travel rule promotes transparency under FATF Recommendation 16 in the context of VAs. FATF has identified several challenges in its implementation, especially related to the collection of information and the interoperability of data-gathering tools. Regarding the travel rule, ME results highlight the following aspects: **i)** DASPs and BSPs do not scan the required information of the originator regarding VA transfers, nor do they specify the origin information of a VA or Bitcoin transaction. That is, not only the originator should be identified through a proper KYC process but also the recipient through the platform where they have a user account. This would apply to both individuals and legal entities engaging in a proper KYC process. Additionally, GAFILAT establishes that transaction information should be properly identified, which is known as Know Your Transaction.

**ii)** El Salvador is not seen as imposing the same obligations on financial institutions regarding the origin or sending of transactions. In this sense, the participation and coordination between the traditional financial sector and the Digital Assets sector, including DASPs and BSPs, is crucial. A relevant example of the travel rule implementation in its relation between a financial institution and DASPs is Europe, which has applied its regulations on crypto assets.<sup>129</sup>

El Salvador, within its regulatory improvement framework, has the legal authority to conduct

Regulatory Impact Assessments (RIA),<sup>130</sup> which would be of great value for implementing technology and financial regulations, eliminating bureaucratic barriers, and ensuring sector oversight.<sup>131</sup> For El Salvador to effectively implement the travel rule, it is essential to involve the financial sector and DASPs and BSPs to consider the country's financial and technological particularities. In the reform of the DAIL, it is specified that the Regulatory Improvement Law will not be applied by the CNAD.<sup>132</sup> However, the application of regulatory improvement principles will be considered for these purposes.

## CUSTOMER DUE DILIGENCE AND VASP

In terms of AML/CTF prevention, CDD is crucial for collecting information that prevents illicit actors from entering the system. However, the information stored by VASPs can be shared to investigate and prosecute crimes, allowing for the identification of the account holder and tracking of their transactions. The implementation of CDD is essential to protect the integrity of the financial system, but it is also important to ensure that the information collected is handled with the utmost confidentiality and security.

<sup>130</sup>A regulatory impact assessment is a "systematic analysis process of the regulation aims, options, and impacts, looking to ensure that benefits are higher than social cost, and that those regulations represent the best alternative to address a specific issue." <https://www.asamblea.gob.sv/sites/default/files/documents/decretos/2A937770-6A46-4FDD-B890-FEBAFO34BODA.pdf>

<sup>131</sup>El Salvador Legislative Assembly. (2019). Ley de Mejora Regulatoria. Regulatorio <https://www.asamblea.gob.sv/sites/default/files/documents/decretos/3EA48492-AC1C-4CDD-BD2E-5AA2B8CEADBDB.pdf>

<sup>132</sup>Legislative Assembly (2024). Reformas a la Ley de Emisión de Activos Digitales. Arts. 42-A y 42-B, <https://x.com/asambleasv/status/1841985362903683367?s=48>

<sup>129</sup>GAFILAT. (2024). Informe de evaluación mutua de la República de El Salvador. (CT 180, p. 257, 258).

The Draft Bill establishes processes like authentication, biometric resources, ID card scanning, Internet Protocols (IP) localization and recognition. It also requires DASPs and BSPs to have the ability to track transactions. In line with FATF Recommendation 10, CDD helps avoid interacting with sanctioned actors, which can be achieved by implementing the travel rule.

It is essential that authorities apply provisions on the chain of custody of digital evidence for its authentication in judicial processes.<sup>136</sup> Cooperation from the private sector is crucial to obtaining information on investigated accounts. This could include requiring at the time of account creation personal data such as wallet address, account status, and IP address.

**INTERNATIONAL COOPERATION: INQUIRIES ON DIGITAL ASSETS SERVICES PROVIDERS ACCOUNTS, FREEZING/SEIZURE, AND ASSET RECOVERY**

The ME results suggest that "There is no appropriate sanction for BSPs and DASPs, including directors and executives."<sup>133</sup>

International cooperation and the preservation of digital evidence are fundamental to the effectiveness of the fight against ML/TF. The ME results for El Salvador highlight that there are doubts about whether VASPs can provide the broadest possible international cooperation in this matter quickly, constructively, and effectively.<sup>137</sup>

Under Salvadoran law, the CNAD and Financial System Superintendency have the legal authority to sanction DASPs and BSPs that do not comply with AML/CTF standards. Mutual evaluation results highlight that BSPs have technological tools that allow for the freezing of VAs,<sup>134</sup> an important finding for the country and a reference for VA freezing. Other jurisdictions, such as the United Kingdom, have opted to directly regulate these procedures,<sup>135</sup> by establishing processes.

---

<sup>133</sup>GAFILAT. (2024). Informe de evaluación mutua de la República de El Salvador. (p. 319). Informe de Evaluación Mutua de la República de El Salvador – GAFILAT

<sup>134</sup>GAFILAT. (2024). Mutual Evaluation Report of the Republic of El Salvador. (p. 6, literal g). "The country has a system that allows it to implement freezing measures based on relevant UNSC lists, which was reformed in January 2024 to ensure that freezes are applied without delay. In this regard, financial institutions and Bitcoin service providers (BSPs) monitor the lists using technological tools and are able to immobilize assets or halt operations when matches are detected."

<sup>135</sup>Stolen Asset Recovery Initiative. (2022) . Guid United Kingdom-update 2022, Stolen Asset Recovery Initiative , <https://star.worldbank.org/publications/asset-recovery-guide-united-kingdom-update-2022>

---

<sup>136</sup>Chainalysis. (2024). The 2024 State of cryptocurrency investigations report. <https://go.chainalysis.com/state-of-crypto-investigations-report-2024.html>

<sup>137</sup>GAFILAT. (2024). Informe de evaluación mutua de la República de El Salvador. (p. 319). Informe de Evaluación Mutua de la República de El Salvador – GAFILAT.

# 2

## CHAPTER 2

# Risks of the VA Ecosystem and Financial Crimes



This section of the report identifies the risks in the Virtual Assets ecosystem in El Salvador and proposes measures to fight them.

## VA AND FINANCIAL CRIME RISKS IN EL SALVADOR

In our previous report, several predicate offenses of AML/CTF were identified in the country, such as human trafficking, extortion, smuggling, drug trafficking, and embezzlement.<sup>138</sup> A specific case involved aggravated fraud targeting U.S. cryptocurrency market investors, with the scammer earning between 25% and 65% monthly returns.<sup>139</sup> Both legal entities and individuals were defrauded of amounts exceeding US\$10,000.<sup>140</sup>

The crimes covered by the Special Law Against Cybercrime and Related Crimes concerning damage to information technology systems, such as the alleged leak of the source code of one of the Chivo ATMs located in the city of San Miguel.<sup>141</sup> This information was published on a website that was seized by the FBI in May 2024.<sup>142</sup> Chivo, S.A. de C.V. assured on its platform

<sup>138</sup>Global Financial Integrity and Vance Center. (2023). The Virtual Assets Ecosystem In El Salvador: Strengthening Financial Integrity and Transparency. <https://34n8bd.p3cdn1.secureserver.net/wp-content/uploads/2023/10/Crypto-El-Salvador-Report-ENG-FINAL-1.pdf?time=1724969507>

<sup>139</sup>Attorney General's Office. [ @FGR\_SV ] (2024). #Captura. La @FGR ordenó la captura de M.. por esta agravada. [post X] [https://x.com/FGR\\_SV/status/1813584006312591409](https://x.com/FGR_SV/status/1813584006312591409)

<sup>140</sup>Attorney General's Office. [ @FGR\_SV ] (2024).

<sup>141</sup>Chivo Wallet. [ @chivowallet ] (2024). Press communiqué. Los datos de nuestros usuarios están protegidos y en ningún momento se ha violado la seguridad de chivo. [post on X]. <https://x.com/chivowallet/status/1782992751354655118?s=46>

<sup>142</sup>Breach Forums. (n.d.) Raidforums Reporting Form. Federal Bureau of Investigation (FBI). <https://breachforums.ic3.gov/>

X account on April 23, 2024, that user data was protected and that the leaked information only pertained to the ATM's operations.<sup>143</sup>

The Attorney General's Office (FGR as per its acronym in Spanish) also posted on its social networks other cases related to the use of VAs, such as the arrest of individuals for illicit association. During the operations, tangible assets, including electronic devices and cryptocurrencies, worth over US\$50,000 were seized,<sup>144</sup> as well as cold cryptocurrency wallets related to digital piracy activities,<sup>145</sup> under Salvadoran jurisdiction.

Despite the existence of a cybersecurity policy<sup>146</sup> that protects the critical infrastructure of public institutions in El Salvador, media outlets have reported the publication of citizen credentials, representing a serious security breach. This could enable cybercriminals to use the obtained information to carry out cyberattacks, forge credentials, or commit computer fraud within the traditional financial system and DASP/BSPs.

<sup>143</sup>Chivo Wallet. [ @chivowallet ] (2024). Comunicado de prensa. Los datos de nuestros usuarios están protegidos y en ningún momento se ha violado la seguridad de chivo. [post X]. <https://x.com/chivowallet/status/1782992751354655118?s=46>

<sup>144</sup>Attorney General's Office. [ @FGR\_SV ] (2024). #Allanamiento. En la vivienda se incautaron de una laptop, una tablet, una lujosa camioneta, 6 teléfonos celulares y más de US\$50,000 en criptomonedas. [post X2]. [https://x.com/fgr\\_sv/status/1545831698797137922?s=48](https://x.com/fgr_sv/status/1545831698797137922?s=48)

<sup>145</sup>Attorney General's Office. [ @FGR\_SV ] (2024). #Condena. La @FGR logró que cada uno de los 8 imputados acusados de piratería digital, fueran condenados a 3 años de prisión. [https://x.com/fgr\\_sv/status/1808293547289813021?s=48](https://x.com/fgr_sv/status/1808293547289813021?s=48)

<sup>146</sup>Diario Oficial de El Salvador. (2022) Política de Ciberseguridad El Salvador (No.90 Tomo. 435)

Moreover, the lack of effective enforcement to prevent AML/CTF may encourage opacity in Bitcoin and digital assets investments. Notably, that some DASPs have collaborated with the FGR of El Salvador, strengthening collaboration in the private sector.<sup>147</sup>

Emerging risks for the VA ecosystem in El Salvador include the possibility of cyberattacks, the misuse of cryptocurrencies for illicit financial flows, lack of transparency in investments, and AML/CFT risks. Some of these emerging risks are outlined below:

### CITIZENSHIP BY INVESTMENT (CBI)

In December 2023, El Salvador passed a law establishing a fast track to Salvadoran citizenship for investors who donate Bitcoin to specific government programs.<sup>148</sup> The law allows investors to bypass the five-year permanent residency requirement before applying for citizenship.<sup>149</sup> This program is limited to 1,000 investors annually, each contributing US\$1 million. The mutual evaluation report suggests there are doubts about

<sup>147</sup>Binance (2024). Binance extiende su colaboración en materia de seguridad junto a la FGR de El Salvador. [https://www.binance.com/es-LA/blog/markets/binance-sigue-ampliando-su-colaboracion-en-materia-de-seguridad-junto-a-la-fiscal-ada-general-de-la-rep-ablca-de-el-salvador-1458883079379785511?utm\\_medium=navigator\\_share\\_link](https://www.binance.com/es-LA/blog/markets/binance-sigue-ampliando-su-colaboracion-en-materia-de-seguridad-junto-a-la-fiscal-ada-general-de-la-rep-ablca-de-el-salvador-1458883079379785511?utm_medium=navigator_share_link)

<sup>148</sup>Legislative Assembly. (2023). Decree 918. Reforma a ley especial de migración y extranjería. [Reform to the Special Law on Migration and Foreign Citizenship]. <https://www.asamblea.gob.sv/sites/default/files/documents/decretos/86F735AF-0AEE-4330-8509-04C9938296D2.pdf>

<sup>149</sup>Arbaiza, Gerardo. (2023). Reuters. El Salvador Offers Citizenship to Foreign Bitcoin Investors, U.S. [https://www.usnews.com/news/world/articles/2023-12-21/el-salvador-offers-citizenship-to-foreign-bitcoin-investors#:~:text=SAN%20SALVADOR%20\(Reuters\)%20%2D%20EL%20social%20and%20economic%20development%20programs](https://www.usnews.com/news/world/articles/2023-12-21/el-salvador-offers-citizenship-to-foreign-bitcoin-investors#:~:text=SAN%20SALVADOR%20(Reuters)%20%2D%20EL%20social%20and%20economic%20development%20programs).

whether proper CDD standards are applied to applicants and whether potential AML/CFT risks are mitigated.<sup>150</sup>

### REAL-WORLD ASSET TOKENIZATION

Classifying asset tokens as securities requires compliance with regulations that ensure transparency and investor protection. This includes AML/CFT and KYC procedures, which are essential for maintaining transaction integrity and security.

Additionally, consumer protection, information security, and risk management measures must be implemented and aligned with FATF standards to prevent criminal activities. The mutual evaluation report identified weaknesses in the identification and assessment of AML/CFT risks in DASPs,<sup>151</sup> including those involved in digital asset issuance.

As part of tokenization, risks to infrastructure have been identified, such as social engineering to gain unauthorized access to exchange platforms, token exploitation by manipulating data input into the blockchain,<sup>152</sup> or attacks on liquidity pools,<sup>153</sup> that is, tokens within smart contracts.

<sup>150</sup>GAFILAT. (2024). Informe de evaluación mutua de la República de El Salvador. (p.24 p. 21). *Informe de Evaluación Mutua de la República de El Salvador – GAFILAT*.

<sup>151</sup>GAFILAT. (2024). Informe de evaluación mutua de la República de El Salvador. (CT 188, P. 259). *Informe de Evaluación Mutua de la República de El Salvador – GAFILAT*.

<sup>152</sup>Benz, Mike, "Risks associated with decentralized finance exploitation, Top 10 vulnerabilities you need to know," 2023. Medium. <https://medium.com/@realMikeBenz/risks-associated-with-decentralized-finance-exploitation-top-10-vulnerabilities-you-need-to-know-848f923964c5>

<sup>153</sup>Antolin, Mike, "What are liquidity pools?", Coindesk, 2022. <https://www.coindesk.com/learn/what-are-liquidity-pools/>



Therefore, information security standards are essential for digital service providers to apply to prevent and mitigate the corresponding risks. This report presents two tokenization case studies as an example of how they were addressed in El Salvador: tokenization of agricultural products, real estate, tokenization of debts and funds. These cases refer to the relevant laws, benefits, and processes to be considered in each case.

## AGRICULTURAL PRODUCTS TOKENIZATION

In April 2024, the CNAD authorized the tokenization of agricultural products,<sup>154</sup> which consisted of the issuance of a token whose underlying digital asset was a bushel of soybeans, equivalent to approximately sixty pounds of soybeans. The tokens were offered on a digital platform managed by a DASP (Digital Assets Service Provider) registered with the CNAD, along with the Relevant Information Document (DIR as per its acronym in Spanish), certified and submitted to the institution for the authorization of the issuance of the digital assets. The tokens circulated on the Polygon,<sup>155</sup> Avalanche,<sup>156</sup> and Linea<sup>157</sup> blockchains, with a total of 7,600,000 tokens residing on the Ethereum blockchain.

---

<sup>154</sup>Egrains. (2024). Notificación de inicio de oferta pública. <https://cnad.gob.sv/wp-content/uploads/2024/06/20240117-egrains-anuncio-de-oferta-publica.pdf>

<sup>155</sup>Polygonscan.(n.d.).The address of the smart contract were the tokens were issued is: 0xb9AE6304706e78d1bb28daCc645499bcF55D6852 <https://polygonscan.com/address/0xb9ae6304706e78d1bb28dacc645499bcf55d6852>

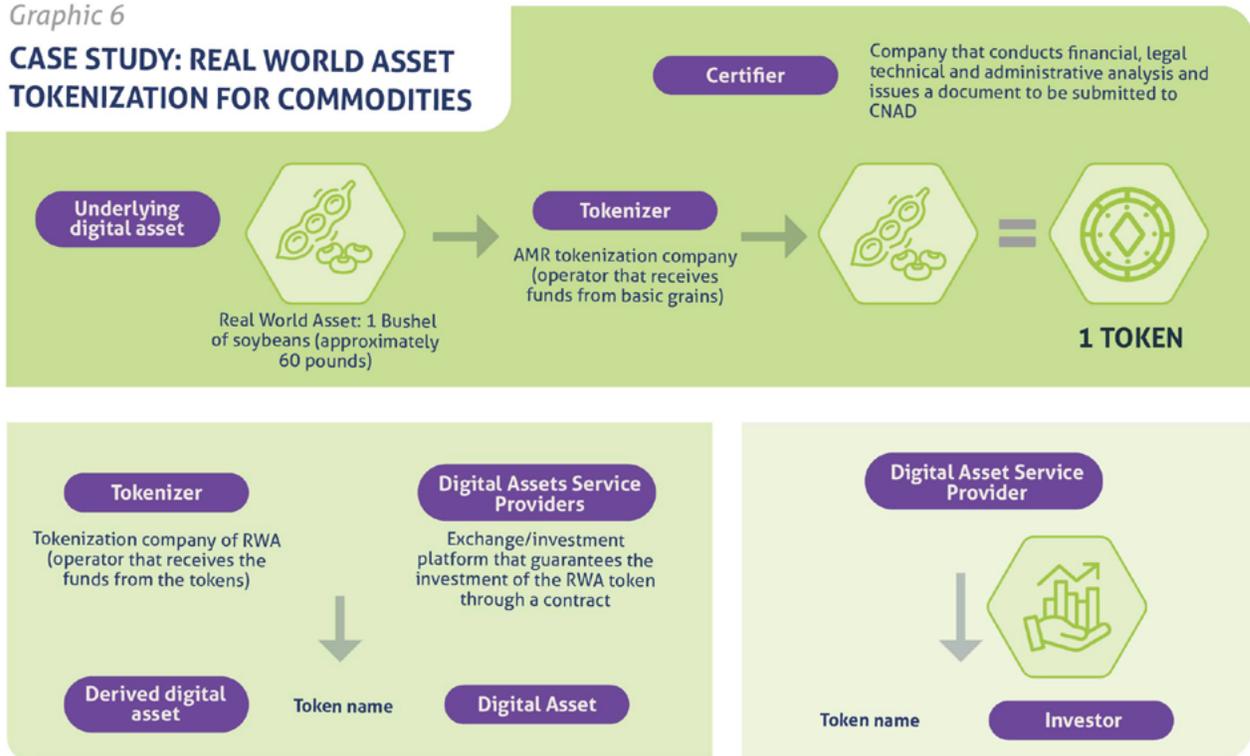
<sup>156</sup>Snowtrace. (n.d.).The address of the smart contract were the tokens were issued is: 0xb9AE6304706e78d1bb28daCc645499bcF55D6852 <https://snowtrace.io/address/0xb9AE6304706e78d1bb28daCc645499bcF55D6852>

<sup>157</sup>Linea. (n.d.) The address of the smart contract were the tokens were issued is: 0xb9AE6304706e78d1bb28daCc645499bcF55D6852 <https://lineascan.build/address/0xb9ae6304706e78d1bb28dac-c645499bcf55d6852>

Regarding taxation, the DIR specifies that taxes will vary according to the national jurisdiction of the acquirer. In the case of El Salvador, the rules of Article 36 of the DAIL will apply, which grants tax exemptions on the nominal value of the underlying asset or its returns. This exemption also applies to the issuer of the record, the certifier, and the Digital Assets Services Providers within the CNAD, including the gains or profits of the stakeholders and partners of the registered legal entities.

Graphic 6

### CASE STUDY: REAL WORLD ASSET TOKENIZATION FOR COMMODITIES



Source: GFI with information from the \$ESoy Token Issuance Relevant Information Document available on the eGrains website.

## DEBT AND FUND TOKENIZATION

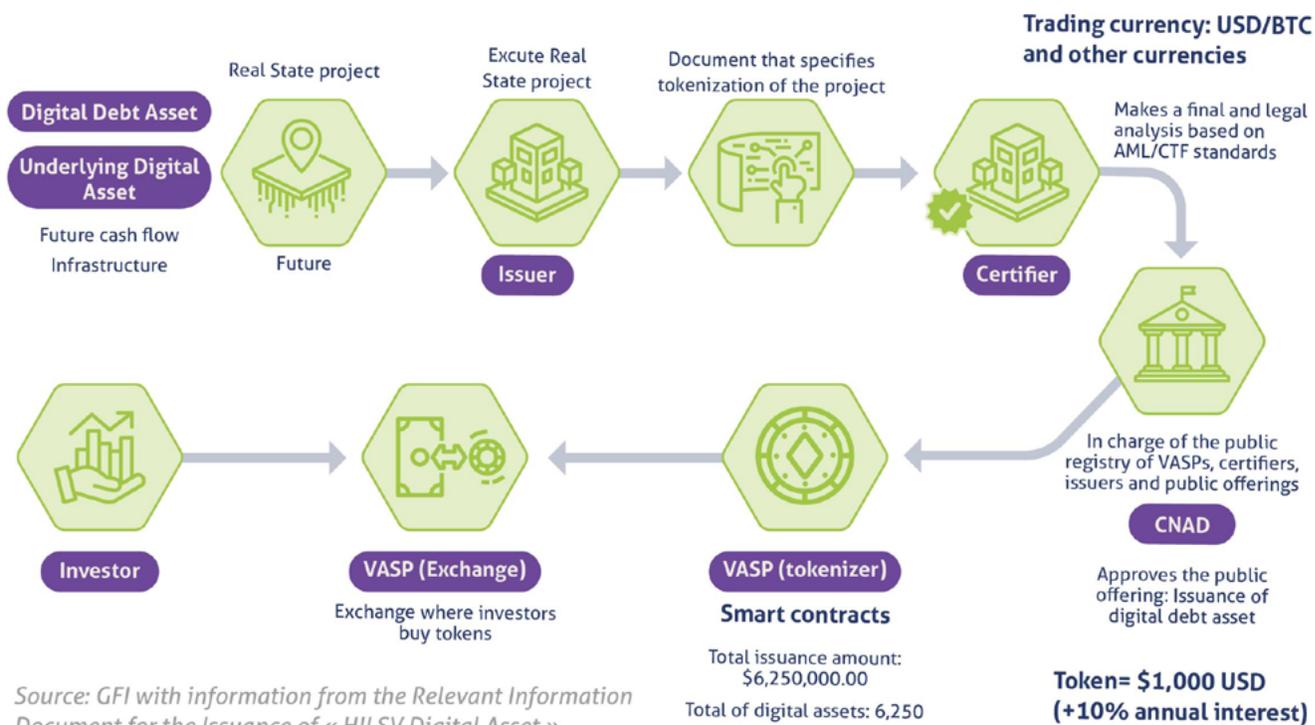
As in the previous issuance process of underlying assets, the following parties are involved: the issuer, the certifier, the tokenizer, and finally, the exchange platform or the DASP. All must be registered with the CNAD. For this type of issuance, it is necessary to include all technical, financial, and legal information in the Relevant Information Document to provide transparency to potential investors.

In the example below, the DA is a debt, the underlying asset is the future cash flow, and the project's infrastructure is construction. The CNAD authorizes the issuance of these debt DAs in a

public offering. Subsequently, the tokenizer or DASP in charge of creating the smart contracts that contain the tokens can technologically proceed to issue them on the blockchain. Once issued, the tokens can be traded within the DASP platform, which facilitates contact with investors. All information related to the issuance must be published on the websites of the DASP platform, the tokenizer, and the issuer.<sup>158</sup>

<sup>158</sup>Legislative Assembly. Ley de Emisión de Activos Digitales [Digital Asset Issuance Law]. (2023). <https://www.asamblea.gob.sv/sites/default/files/documentos/decretos/OCDA225C-1B6C-4098-AC3A-D608933C643B.pdf>

Graphic 7  
CASE STUDY: REAL WORLD DEBT ASSET TOKENIZATION



## STABLECOIN ISSUANCE

Stablecoin issuance is “a type of digital asset designed to have a stable value, referencing, representing, or being backed by one or more fiat currencies or another underlying asset that ensures low volatility.”<sup>159</sup>

In June 2024, the DANC authorized the issuance of the stablecoin aUSD. This issuance allowed two DASPs to promote Tether’s Alloy stablecoin (AbT). This token will enable users to mint aUSD using Tether Gold (XAU) as collateral, resulting

in a digital currency backed by the value of gold. As part of the obligations under the DAAL, the DIR, which complied with the certification process,<sup>160</sup> has been published on the promotional website. The tokens are available on the Ethereum blockchain, and there is no set number of tokens required or authorized for issuance; the DIR states that the number of aUSD will depend on the supply and demand mechanism.

The DIR also specifies that only customers who complete the KYC onboarding process will be able

<sup>159</sup>El Salvador Ministry of Economy, Reformas a la Ley de Activos Digitales [Reforms to the Digital Asset Law], 2024.

<sup>160</sup>TR. Capital. (2024). Stablecoin issuance public offering certification report [https://alloy.tether.to/docs/stablecoin\\_issuance\\_public\\_offering\\_certification\\_report.pdf](https://alloy.tether.to/docs/stablecoin_issuance_public_offering_certification_report.pdf)

to interact with these tokens.<sup>161</sup> Furthermore, it warns of associated risks, such as price fluctuations, market risks, reliability of price information, settlement risks, blacklisting and address blocking, platform disruption and accessibility, cybersecurity threats, insolvency of other users, regulatory risks, conflicts of interest, third-party-related risks, and risks associated with the collateral asset (Tether Gold). Customers are also encouraged to complete the verification process before using the service and to comply with international regulations, such as FATF standards, the U.S. Bank Secrecy Act, and the AML/CTF regulations of the British Virgin Islands and El Salvador.<sup>162</sup>

The applicable tax regime in El Salvador exempts these tokens from any taxes, fees, or contributions, whether ordinary or extraordinary and grants exemptions on capital gains or income derived from the sale or any other form of transfer, including debt forgiveness, of these tokens, as established in the DIR.

## POLITICAL FINANCING

Incorporating VAs into political financing poses some challenges, in terms of transparency and accountability, due to the pseudo-anonymity and decentralization inherent in VAs. Since there is no specific regulation on the matter, a debate has arisen about the convenience and potential risks associated with the use of virtual assets (VAs) in political financing. Additionally, there has been some debate about the appropriateness and

potential risks associated with the use of VAs in political financing.

In El Salvador, political parties are obliged subjects,<sup>163</sup> under the LAAML. Therefore, they have obligations<sup>164</sup> concerning the prevention and detection of AML/CTF. These obligations include registering with the FIU, appointing a compliance officer, maintaining a risk-based AML/CTF program, reporting suspicious activities, establishing an internal due diligence policy to identify donors, and retaining documentation of transactions for five years. However, as of now, there is evidence of specific obligations related to donations made using VAs, particularly Bitcoin, which, according to its law, can be used in any transaction and for any purpose that individuals or entities, whether public or private, require.

During the elections of February and March 2024, most political parties stated they had no intention of accepting donations through virtual assets (VAs), although some mentioned they were studying the issue.<sup>165</sup> This compels the Supreme Electoral Tribunal (TSE as per its Spanish acronym), as the entity responsible for monitoring and controlling political financing, to establish guidelines regarding the functioning, risks, and typologies

<sup>161</sup>Idem.

<sup>162</sup>Idem.

<sup>163</sup>El Salvador Legislative Assembly. (1998). Ley Contra El Lavado de Dinero y Activos. <https://ssf.gob.sv/wp-content/uploads/2022/07/Ley-contra-el-lavado-de-dinero-y-de-Activos-D498.pdf>

<sup>164</sup>Attorney General's Office. (2021). Instructivo de la unidad de investigación financiera para la prevención del lavado de dinero y de activos. <https://www.uif.gob.sv/wp-content/uploads/instructivos/InstructivoUifDiarioOficial2021.pdf>

<sup>165</sup>Acción Ciudadana. (2022). Informe de transparencia 2021: Análisis de los ingresos y gastos de los partidos. (p. 50). [Informe de transparencia 2021: Análisis de los ingresos y gastos de los partidos políticos \(accion-ciudadana.org\)](https://www.transparencia2021.org/)



associated with the use of the digital ecosystem, as well as potential effective oversight of suspicious operations reporting presented to the FIU by political parties.

Regarding transparency of VA contributions received by political parties in El Salvador, it is difficult to assess the volume of VA's from either public or private financing, or the level of due diligence by the parties themselves, especially in the absence of clear regulation.

This scenario shows the need to reinforce political financing regulation and oversight in general.

A robust regulatory framework for auditing, along with an effective supervisory body, is necessary to oversee and monitor donations made in any form of currency or assets. However, it is essential to enforce compliance with the obligated subjects and impose deterrent sanctions when necessary. Both regulation and enforcement are critical to establishing an environment of integrity in politics. Otherwise, an attractive environment for money laundering, corruption, or illicit financing through anonymous, foreign, or over-the-limit donations could be created.

The potential acquisition of VAs with illicit funds and their subsequent donation to political parties is one of the risks political financing may face. The use of "mixing" or "tumbling" platforms for cryptocurrencies could be another strategy to erase transaction traces and conceal the identity of the VA buyer and subsequent political party donor.

Another risk associated with using VA in politics is the possibility of exceeding the thresholds set by the Political Parties Law (LPP). Although El Salvador does not have a maximum limit for private donations, it is prohibited to individually exceed two percent of the previous year's budget approved by the Legislative Assembly to the TSE.<sup>166</sup> This prohibition can be circumvented by using VAs, splitting amounts into smaller portions below the threshold, and sending them from multiple addresses. A proper verification and alert process by DASP/BSP could detect this practice.

---

<sup>166</sup>El Salvador Legislative Assembly.(1993). Ley de partidos políticos. (art. 65). [C212CE14-561E-401D-822F-A38E38483397.pdf \(asamblea.gob.sv\)](https://www.asamblea.gob.sv/C212CE14-561E-401D-822F-A38E38483397.pdf)

# 3

## CHAPTER 3

# VASP and the Data Protection Legal framework in El Salvador





El Salvador has regulations on data protection, such as the Law of Access to Public Information (Ley de Acceso a la Información Pública —LAIP as per its Spanish acronym)<sup>167</sup> and the LECDIC.<sup>168</sup> However, as of the date of this report, there is no specific regulation for personal data protection, as the Data Protection Bill (LPD as per its Spanish acronym) was vetoed by the President of the Republic in May 2021.<sup>169</sup> On the other hand, in March 2022, Agreement 163, containing the Cybersecurity Policy, was approved, with its main goal being to prevent cyber risks<sup>170</sup> and protect data related to the Nation's critical infrastructure.

In this chapter, we will refer to relevant international legislation, digital wallets, and specifically the case of El Salvador's Chivo Wallet.

## A. INTERNATIONAL REFERENCES

### (i) General Data Protection Regulation (GDPR)

The GDPR, a regulation of the European Union, defines personal data as any information related to an identified or identifiable natural person.<sup>171</sup>

<sup>167</sup>El Salvador Legislative Assembly. (2011). Ley de acceso a la información pública. [6FEC6152-A946-4C2E-B232-04C3EA89FCE0.pdf](https://www.asamblea.gob.sv/6FEC6152-A946-4C2E-B232-04C3EA89FCE0.pdf) ([asamblea.gob.sv](https://www.asamblea.gob.sv))

<sup>168</sup>El Salvador Legislative Assembly. (2016). Ley especial contra delitos informáticos y conexos. [DCOADOB7-28EF-461B-991E-563CB879998F.pdf](https://www.asamblea.gob.sv/DCOADOB7-28EF-461B-991E-563CB879998F.pdf) ([asamblea.gob.sv](https://www.asamblea.gob.sv))

<sup>169</sup>Santos, Sandra. Revista Factum. (2022). Nuestros datos personales están desprotegidos [Nuestros datos personales están desprotegidos - Revista Factum](https://www.revistafactum.com/nuestros-datos-personales-estn-desprotegidos)

<sup>170</sup>El Salvador Government. (2022). Política de ciberseguridad. (Diario Oficial No.90 Tomo. 435 del 13, publicado, 13 de mayo de 2022).

<sup>171</sup>European Commission, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)", (2016). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>

This includes not only personal data like names and addresses but also other types of data, such as IP addresses and online identifiers.

The regulation does not provide an exhaustive list of what is excluded from personal data. Instead, it broadly defines what constitutes personal data. However, it acknowledges that anonymous data (data that cannot be linked to an individual) is not considered personal data.<sup>172</sup>

The GDPR includes the following items:<sup>173</sup>

#### **Responsibilities of data processors:**

When using external servers or database providers, the data processor must ensure they provide sufficient guarantees to implement appropriate technical and organizational measures.

**Data transfer standards:** Data transfers to countries outside the European Union must ensure adequate data protection. The GDPR provides specific mechanisms, such as Standard Contractual Clauses or adherence to the EU-U.S. Privacy Shield framework (if applicable).

**Data security requirements:** Companies must implement appropriate security measures to protect data from unauthorized or illegal processing and against loss, destruction, or accidental damage.

**Data breach protocols:** In case of a data breach, companies must notify the relevant regulatory

<sup>172</sup>Idem.

<sup>173</sup>Idem.

authorities and potentially the affected data subjects, especially if the breach represents a high risk to their rights and freedoms.

**Contractual obligations:** Data controllers must have contracts in place with their data processors detailing the subject matter, duration, nature, and purpose of the processing, as well as the controller's obligations and rights.

### (ii) The Gramm-Leach-Bliley (GLBA) Act

The GLBA, a U.S. federal law primarily applicable to financial institutions, defines non-public personal information as "personally identifiable financial information" and includes information that consumers provide to obtain a financial product or service. It excludes publicly available information, such as information in public records, and any data that is encrypted, secured, or anonymized.<sup>174</sup>

The GLBA includes the following directions:<sup>175</sup>

**Safeguard Rule:** Financial institutions must have a written security plan explaining how the company protects customers' non-public personal information, including when external service providers are used.

**Service providers' oversight:** Companies must ensure that their service providers can maintain appropriate safeguards for customer information and are contractually obligated to implement and maintain such safeguards.

**Risk management:** Regular testing and monitoring of the effectiveness of safeguards are required. This should also cover external servers and database providers.

**Information security program:** Financial institutions must develop, implement, and maintain a comprehensive information security program designed to ensure the security and confidentiality of customer information.

**Customer information security:** Companies must protect against any anticipated threats or hazards to the security or integrity of such information, including in external data management scenarios.

## B. CHIVO WALLET: PRIVACY POLICY, TERMS AND CONDITIONS

Chivo Wallet is the e-wallet developed by the El Salvador Government in 2021, available for Android and iOS.<sup>176</sup> Although Chivo Wallet operates as a private entity under Commercial Law,<sup>177</sup> it is closely linked to government operations

<sup>174</sup>Gramm-Leach-Bliley Act of 1999. Public Law 106-102, U.S. Statutes at Large 113 (1999): 1338–1481 <https://www.congress.gov/106/plaws/publ102/PLAW-106publ102.pdf>

<sup>175</sup>Idem.

<sup>176</sup>Gramm-Leach-Bliley Act of 1999. Public Law 106-102, U.S. Statutes at Large 113 (1999): 1338–1481 <https://www.congress.gov/106/plaws/publ102/PLAW-106publ102.pdf>

<sup>177</sup>Gramm-Leach-Bliley Act of 1999. Public Law 106-102, U.S. Statutes at Large 113 (1999): 1338–1481 <https://www.congress.gov/106/plaws/publ102/PLAW-106publ102.pdf>



and funded with public funds.<sup>178</sup> In this sense, it is necessary to clarify whether the Law of Access to Public Information (LAIP) applies to the data used by Chivo Wallet.

Article 7 of LAIP stipulates those entities managing public resources, information, or performing state functions are required to provide access to information related to the administration of such resources.<sup>179</sup> This article states that mixed-economy companies and natural or legal persons using public resources or information or performing acts of state roles must allow access to information related to the administration of public funds or functions assigned to them.<sup>180</sup>

When referring to private information, LAIP states that it is related to an identified or identifiable person and includes details such as nationality, residence, assets, email, and phone number. It also defines sensitive personal data as related to creed, religion, ethnic origin, political affiliation, and physical and mental health, among others.

The terms and conditions only mention that precautions are taken to protect information through effective computer security systems. However, strict security measures are not specified, leaving users without clear knowledge of how their

<sup>178</sup>Chivo Wallet. (n.d.). Chivo Wallet Is an Electronic Wallet Created by the Government of El Salvador for Making Payments in Dollars or Bitcoin. [Inicio | Chivo Wallet](#)

<sup>179</sup>Legislative Assembly. (2011). Ley de acceso a la información pública [Law regarding access to public information]. (art.,7). [6FEC6152-A946-4C2E-B232-04C3EA89FCE0.pdf \(asamblea.gob.sv\)](#)

<sup>180</sup>El Salvador Legislative Assembly. (2011). Ley de acceso a la información pública. (art.,7). [6FEC6152-A946-4C2E-B232-04C3EA89FCE0.pdf \(asamblea.gob.sv\)](#)

data will be protected, especially in comparison to international standards, which will be discussed further.

El Salvador Cybersecurity Policy establishes guidelines and best practices for managing risks, including a process with several steps to analyze and prioritize breaches that may affect organizations' costs and risks. This framework requires institutions to determine the necessary resources to address such breaches.

El Salvador must comply with information security standards to protect users' personal data. Additionally, the nation must consider ISO standards: ISO/IEC 27001:2022,<sup>181</sup> on information security management systems and privacy protection, and ISO/IEC 27035-1:2023 on information security incident management, along with the regulations applicable to banks and VAs.<sup>182</sup>

Other information security and data protection standards come from CNBCR-07/2020 NR-23, which establishes technical standards for information security management applicable to

<sup>181</sup>ISO/IEC 27001:2022 is an international standard that specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). The goal is to help organizations make the information assets they hold more secure. This includes aspects of cybersecurity and privacy protection. The standard requires organizations to assess their information security risks, implement appropriate security controls, and continuously monitor and improve the effectiveness of their ISMS.

<sup>182</sup>Superintendency of Banks, Insurance, and AFP. Weekly Bulletin No. 7. Information Security and Cybersecurity: New Regulation to Promote a Secure and Reliable Environment for the Benefit of Users of Supervised Systems [Seguridad de la información y ciberseguridad: nuevo reglamento para promover un entorno seguro y confiable en beneficio de los usuarios de los sistemas supervisados]. See here. March 2021. Accessed on June 28, 2024.

financial entities<sup>183</sup> and specifically for DASPs through the Regulations for Digital Asset Service Providers. These mention that procedures for governance, identification, protection, detection, response, and recovery should be established, including testing and simulations, to ensure the pillars of information security: confidentiality, availability, and integrity.<sup>184</sup>

### C. VIRTUAL ASSET WALLETS

As explained in prior chapters, it is necessary to be able to pinpoint politically exposed persons when carrying out activities with DASPs.

Digital wallets are increasingly scrutinizing citizens' activities, but also some groups, such as political parties or politically exposed persons, are analyzed in this report to ensure compliance with global AML standards. This approach helps enhance security measures and maintain the integrity of financial transactions. As regulations tighten, it becomes crucial to understand how major digital wallets manage their users. This overview highlights the approaches of platforms like Binance and Kraken in regulating transactions involving PEPs, for example, demonstrating their commitment to international compliance standards. Some specific remarks showing how they address this particular issue follow:

**Binance:** It is a currency exchange requiring all of its users to undergo identity verification to strengthen account security and ensure compliance with applicable regulatory requirements. As part of its internal process, users are asked to disclose if they are PEPs.<sup>185</sup> Those identified as PEPs must complete a specific form detailing their status and may also be asked to provide documentation supporting their Source of Wealth (SOW).

**Kraken:** Similar to Binance, Kraken is a currency exchange incorporating PEP identification in its KYC procedures. The platform aligns with the FATF definition of a PEP, including individuals who have previously held significant public roles. Kraken requires PEPs to provide extensive documentation, including financial and asset statements, to verify their identities and assess potential risks. This approach reinforces Kraken's commitment to preventing financial misuse and enhancing transparency.<sup>186</sup>

These efforts illustrate the proactive steps digital wallets are taking to manage the risks associated with PEPs, ensuring they operate within the boundaries of international financial regulations.

---

<sup>183</sup>Central Reserve Bank, "CNBCR-07/2020 NR-23 que establece las Normas técnicas para la gestión de la seguridad de la información", 2020. <https://www.bcr.gob.sv/regulaciones/upload/NRP-23.pdf>

<sup>184</sup>CNAD, "Reglamento de Proveedores de Activos Digitales", 2023. <https://cnad.gob.sv/es/libreria-de-documentacion/marco-legal/#-flipbook-reglamento-de-proveedores-de-servicios-de-activos-digitales-2023-08-11-esp/1/>

---

<sup>185</sup>Binance, "How to complete de source of health declaration", <https://www.binance.com/en/support/faq/how-to-complete-the-source-of-wealth-declaration-c22109193d1247b3af1027e72fa0d5b7>

<sup>186</sup>Kraken "Political Exposed Person-self declaration", <https://support.kraken.com/hc/en-us/articles/politically-exposed-person-pep-self-declaration-definitions>



## D. A COMPARATIVE ANALYSIS OF VIRTUAL ASSET WALLETS

A review of the privacy policies of various platforms reveals significant discrepancies in compliance with data protection standards. A brief analysis of the development and use of information by VA wallets operating in El Salvador follows.

**Blink:** Its terms allow for the broad use of data, both restricted and unrestricted, for various purposes, including transfers to third parties. The terms specify that third-party servers complying with international security standards like ISO/IEC 27001:2013, PCI-DSS, PII, and HIPAA may be used. They also allow for the non-restrictive revocation of these authorizations and provide an email address to exercise data protection rights.<sup>187</sup>

**Strike:** Its privacy policies are detailed, covering the use of personal information, data transfer to third parties,<sup>188</sup> retention periods, and access to data details. It states that any third-party requests not covered by the privacy policies will be subject to user consent.<sup>189</sup> The terms also mention the use of cookies and acknowledge potential vulnerabilities in data transmission, though they claim to comply with local regulations<sup>190</sup>.

---

<sup>187</sup>Blink, Política de Privacidad (2024). <https://es.blink.sv/en/privacy-policy>

<sup>188</sup>Blink, Política de Privacidad (2024). <https://es.blink.sv/en/privacy-policy>

<sup>189</sup>Blink, Política de Privacidad (2024). <https://es.blink.sv/en/privacy-policy>

<sup>190</sup>Strike, Aviso de Privacidad de Strike (2023). <https://strike.me/legal/privacy/>

**DitoBanx:** It briefly describes the use of collected personal information and users' control over their data, including the option to receive or decline communications.<sup>191</sup> However, it fails to provide detailed information about data management and sharing, posing a potential risk to user data security.<sup>192</sup>

**Bitfinex:** Provides a more detailed account of its data practices, including the types of information collected, the purposes of data collection, storage details, exchange policies, and security measures.<sup>193</sup> It also clarifies the legal basis for data processing and how users can exercise their rights, demonstrating a higher standard of data protection.<sup>194</sup>

VASPs comply with international data protection standards given their inherently transnational nature, which enables users from different jurisdictions to use their products and services.

---

<sup>191</sup>Ditobanx, Política de Privacidad (2024). <https://ditobanx.com/politica-de-privacidad/>

<sup>192</sup>Ditobanx, Política de Privacidad (2024). <https://ditobanx.com/politica-de-privacidad/>

<sup>193</sup>Bitfinex, Bitfinex Privacy Statement (2024), <https://www.bitfinex.com/legal/privacy/>

<sup>194</sup>Bitfinex, Bitfinex Privacy Statement (2024), <https://www.bitfinex.com/legal/privacy/>

# RECOMMENDATIONS

Below are some recommendations addressing the key themes of the report:

## RECOMMENDATIONS TO COUNTER FINANCIAL CRIMES

- Educate the Salvadoran population and users on finance and technology, highlighting the risks of personal data exposition on financial platforms and VAs in order to prevent crimes, such as scams or cyber fraud.
- Promote strict information security standards within El Salvador's financial and technological ecosystem, applying effective sanctions on non-compliance cases.
- Deploy risk-based actions and responses to information security breaches on VASPs and BSPs, detecting threats in real-time and deploying security measures that reinforce investor confidence.

## RECOMMENDATIONS TO PROMOTE AML/CTF/PF

- Deepen a risk-based approach to the use of Bitcoin and other digital assets within El Salvador, including stable currencies, underlying digital assets and derivatives in order to mitigate AML/CTF.

- Strengthen the knowledge of authorities in the prevention, investigation, prosecution, and adjudication of crimes related to VAs, with a focus on the stages of money laundering, criminal typologies, and terrorism financing.

- Develop guidelines or manuals aligned with criminal and procedural legislation for freezing VA by the National Civil Police and the Attorney General's Office and disseminate these practices within the justice sector following an international judicial cooperation approach.

- Strengthen the technical capacities of authorities like the police, Attorney General's Office, and the Supreme Court of Justice in managing digital evidence related to VA-enabled crimes.

- Promote public-private sector cooperation to improve communication in the investigation and prosecution of crimes and infractions, sharing best practices and lessons learned.

- Instruct BSP and VASP supervisors to develop clear guidelines to prevent financial crime in the VA industry and as a part of their platform use, complying with international standards and identifying red flags related to patterns, anonymity, the origin of funds, and other aspects to fight money laundering and terrorist financing.

- Conduct public consultations with various sectors on the adoption of regulations related to finance and technologies to improve a risk-based approach that enables the prevention and identification of money laundering and terrorist financing.

- Foster regulatory collaboration between the traditional financial sector and DASP/BPS in AML/CTF issues.de LA/FT.

- Ensure the electoral overseeing entity is able to oversee PEPs on digital platforms in compliance with international standards so as to ensure user identification and VA origin.

- To have the FIU establish clear guidelines for the implementation of the "travel rule" within the BSP/DASP sector in coordination with the traditional financial sector.

## **RECOMMENDATIONS ON POLITICAL FINANCING**

- Provide the TSE with sufficient human, technological and financial resources to supervise and audit all donations, especially those made through VAs.

- Update the regulatory framework to govern the use of VA in political financing. Establish clear controls and ensure that supervisory entities, such as the Electoral Authority, Ministry of Treasury, Financial Supervisory Superintendency and CNAD, comply with FATF recommendations and international standards.

- Strengthen coordination between electoral process supervisors, including the Electoral Authority, Ministry of Treasury, Court of Accounts of the Republic, Digital Assets National Commission, and DASPs/BSPs, to ensure effective collaboration in identifying red flags in the political arena.

- Establish control guidelines on VA donations for political parties, ensuring compliance with the Political Parties Law (LPP) and regulations related to AML/CTF.

## **RECOMMENDATIONS ON REAL-WORLD ASSET TOKENIZATION**

- Create a secure regulatory ecosystem to prevent fraud and ensure legal protection for investors within the process of tokenization or VA offerings.

- Increase knowledge and training on tokenization and VA issuance to build trust in financial technologies. It is important to establish and define the risks associated with digital asset investments in an accessible and understandable way for investors.

- Promote coordination spaces among the various sectors involved in digital asset issuance to share best practices in preventing financial crime.

- Counter security breaches in line with international information security standards within the token exchange infrastructure to prevent financial crime.

- Identify tokenization opportunities in different sectors, such as construction, agricultural products, funds, and debts, applying risk-based approaches specific to each sector.

- Promote awareness of stablecoins, providing clear information and addressing their relationship with risks associated with AML/CTF.

- Strengthen the technical knowledge of competent authorities on VA and the tokenization process to countering financial or other types of cybercrime.

## **RECOMMENDATIONS ON PERSONAL DATA PROTECTION**

- Require compliance with information security regulations and the implementation of ISO/IEC 27001:2022. Government agencies can use this standard to safeguard citizens' sensitive data, ensuring compliance with national and international regulations while enhancing public trust in government services. Financial entities would also benefit from this standard by securing clients' financial data, preventing fraud, and adhering to strict financial regulations.

- Ensure adherence to information security standards to protect infrastructure and client data, including transactions by VASPs and BSPs. This will require controlled testing conducted by information security experts.



GLOBAL FINANCIAL INTEGRITY



CYRUS R. VANCE CENTER  
FOR INTERNATIONAL JUSTICE