ЄВРОІНТЕГРАЦІЙНІ МЕХАНІЗМИ ПРОТИДІЇ ЗЛОВЖИВАННЮ ЦИФРОВИМИ АКТИВАМИ

ТЕТЯНА ДМИТРЕНКО,
ДОКТОР ЕКОНОМІЧНИХ НАУК,
СТАРШИЙ ДОСЛІДНИК, ГОЛОВА UMDS

ПРОФЕСОР ІПО ДННУ АКАДЕМІЯ
ФІНАНСОВОГО УПРАВЛІННЯ

ХРОНОЛОГІЯ

ТРАВЕНЬ 2015 РЕГЛАМЕНТ (ЄС) 2015/847
– **TFR** (16 REC. FATF) – **WIRE TRANSFERS**
– **TRAVEL RULES**

ТРАВЕНЬ 2018 5 AMLD

ЖОВТЕНЬ 2018 ОНОВЛЕНА 15 REC. FATF
– **NEW TECHNOLOGIES**

ЧЕРВЕНЬ 2019
КЕРІВНИЦТВО FATF ЩОДО РИЗИК-ОРІЄНТОВАНОГО ПІДХОДУ ДО ВА ТА ППВА:
ЛІЦЕНЗУВАННЯ/РЕЄСТРАЦІЯ
KYC + KYT
TRAVEL RULES

ЛИПЕНЬ 2022
ОНОВЛЕНА СТРАТЕГІЯ ЄС В ОБЛАСТІ ЦИФРОВИХ ФІНАНСІВ

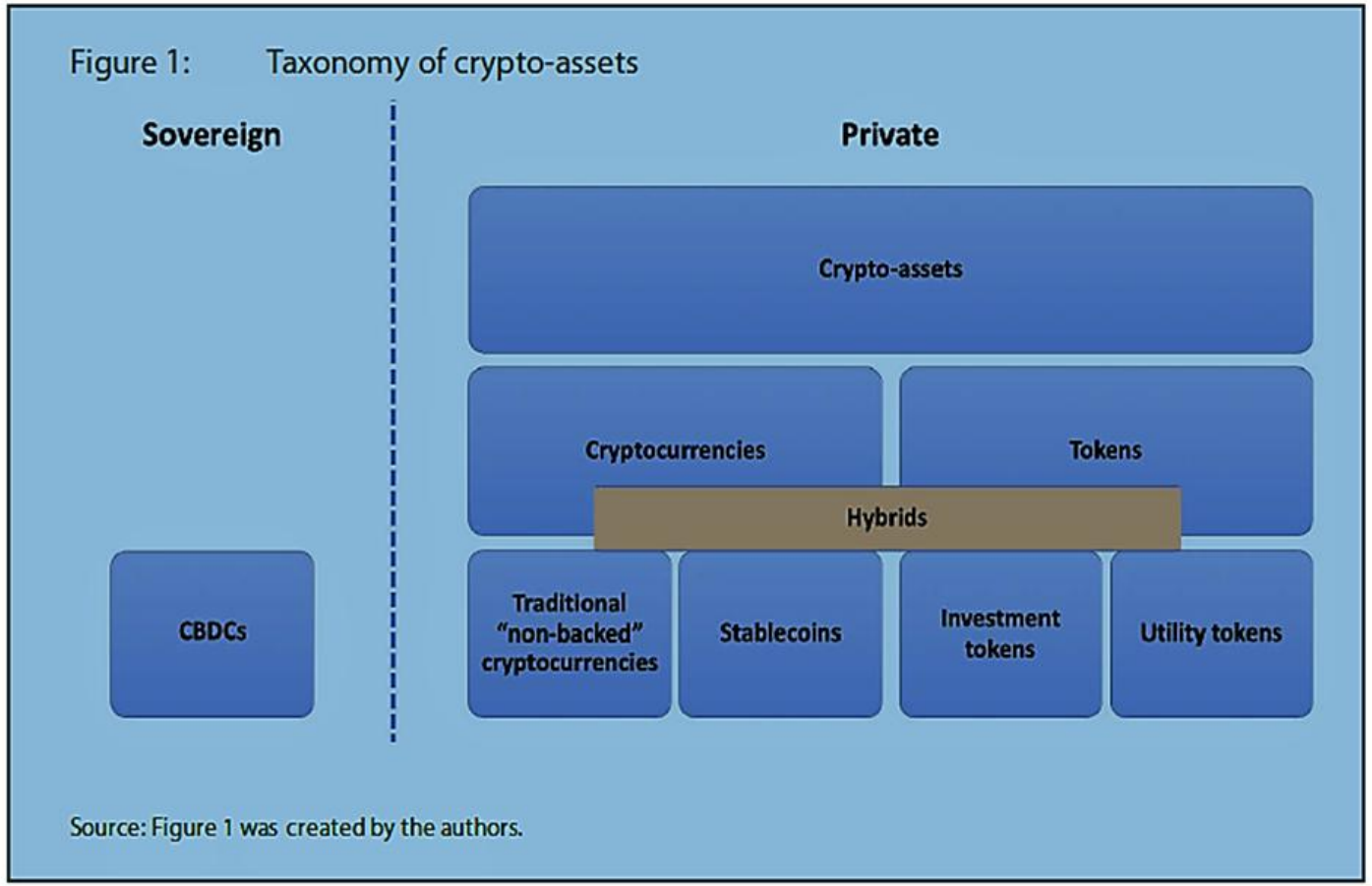
ТАКСОНОМІЯ ЦИФРОВИХ АКТИВІВ

CBDC + VA

CRYPTOCURRENCY + TOKEN

ЗАБЕЗПЕЧЕНІ + НЕЗАБЕЗПЕЧЕНІ

ГІБРИДИ



ТАКСОНОМІЯ ВІРТУАЛЬНИХ АКТИВІВ

Financial instruments

Electronic money

None of the foregoing

Типи криптоактивів		
	Токен, забезпечений електронними грошима, Ст. 3 (1) №4	EMD2 (Директива ЄС 2009/110/ЕС)
	Токен, забезпечений активами Ст. 3 (1) №3	Інвестиційні токени MiFiD II
	Службові токени Ст. 3 (1) №5	Незабезпечені токени

DeFi, NFT, MEMEcoin,
монеты блокчейнов с закрытым кодом (Monero, Zcash, Dash)
Metaverse

MIFID2 , EMD2, MICA + DORA, DAC8, TFR

Формування законодавства ЄС

MiCA

Markets in Crypto assets

Регламенти ЄС

MiCA прагне регулювати 3 підкатегорії криптоактивів:

1. «Службові токени», що випускаються з нефінансовою метою для надання доступу до електронних програм, послуг або ресурсів, доступних у мережах DLT.

2. «Токени, пов'язані з активами», спрямовані на підтримку цінової стабільності з метою збереження купівельної спроможності. Використовуються як засіб платежу для купівлі товарів, послуг та збереження вартості.

3. «Токени електронних грошей» - криптоактиви зі стабільною вартістю - еквівалент фіатних валют, які повинні функціонувати подібно до електронних грошей (замінюючи фіатну валюту в платежах), як визначено в Директиві ЄС 2009/110/ЄК про створення та здійснення діяльності установами-емітентами.

DORA

Digital Operational Resilience Act

Регламенти ЄС

DORA - Регламент ЄС щодо операційної стійкості цифрових технологій у секторі фінансових послуг спрямовано на створення всеосяжної та уніфікованої основи для гармонізації процесів та стандартів, пов'язаних із операційною стійкістю цифрових технологій у фінансовому секторі.

Регламент запроваджує єдину систему правил регулювання та нагляду за забезпеченням операційної стійкості щодо цифрових технологій у фінансовому секторі. Це передбачає необхідність значних інвестицій з боку фінансових установ для підвищення їхньої стійкості до кіберризиків.

Щоб відповідати вимогам DORA, організації повинні мати встановлені та надійні процеси управління ризиками.

DORA вимагає, щоб фінансові установи тестували свої системи з урахуванням пов'язаних із ними ризиків – сканування вразливостей, тестування на проникнення, а також надійну перевірку безперервності бізнесу та плану аварійного відновлення.

DORA

Digital Operational Resilience Act

Регламенти ЄС

Інцидент	Тип/вектор	Ключовий наслідок	Атрибут, який відрізняє кіберризик від «звичайної» операційної події
NotPetya (червень 2017)	Деструктивне шкідливе ПЗ з масовим поширенням	Офіційні урядові оцінки Велика Британія прямо покладають відповідальність на російські військові структури і підкреслю-ють транснаціональні економічні наслідки; Міністерство юстиції США в обвинувальних матеріалах описує NotPetya як один із найбільш деструк-тивних інструментів і наводить оцінку втрат для окремих жертв на рівні майже $1 млрд	Каскад і масштаб через ланцюги постачання/оновлення; «ворожий противник»; системний ефект, який не випливає з історичної OR-статистики однієї установи
SolarWinds Orion (2020)	Supply chain компрометація оновлень ПЗ	CISA описує APT-компрометацію державного і приватного секторів, що почалася щонайменше у березні 2020 року та вимагає складного «eviction» процесу, демонструючи довгу латентну фазу і роль постачальника ПЗ як вектора	Third-party як первинний вектор, латентність, трудність повного «вичищення», необхідність спеціалізованої технічної реакції
Capital One (2019)	Компрометація даних у хмарно-му середовищі, пов'язана з недоліками контролів	OCC у документах щодо штрафу вказує на провали в управлінні ризиками хмарного середовища, включно з дизайном мережевих контролів і DLP, а CERT-EU у мемо фіксує масштаб інциденту та хмарний контекст	Кіберризик прив'язаний до architecture/security-by-design у хмарі та до контролів постачальника, що не «видно» з RCSA без технічної декомпозиції експозиції
ICBC Financial Services (листопад 2023)	Ransomware	SEC описує, що ransomware призвів до порушення доступу та оновлення books & records і до необхідності відключити конективність із кліринговими фірмами/агентами, що миттєво надає інциденту ринковий вимір	Порушення критичних ринкових функцій, вимоги до безперервності даних і регуляторного доказу, швидкість «зупинки» конективності
DDoS-атаки на банки і держоргани (15 лютого 2022)	Масована DDoS	CERT-UA[у зведенні за 15.02.2022 прямо згадує DDoS у відношенні вебресурсів українських банків та держустанов; Держспецзв'язку повідомляє про перебої у вебсервісах ПриватБанк та Ощадбанк	Одночасність атак на кілька системно значимих гравців, високий репутаційний ефект і вимога до стійкості каналів доступу «тут і зараз»
Кібератака на державні реєстри (грудень 2024)	Цілеспрямована атака на цифрову інфраструктуру реєстрів	У звіті Держспецзв'язку інцидент описано як резонансний із суттєвими збоями клю-чових сервісів; окремі офіційні повідом-лення пов'язують зупинку реєстрів із мас-штабною зовнішньою кібератакою на реєстри у компетенції Міністерство юстиції України	Демонстрація системної залежності процедур (митниця/кордон/виконавчі провадження), що переноситься на фінсектор через KYC/виконавчі процеси/ідентифікації, тобто «кіберризик ланцюга довіри»

DAC8

Directive on Administrative Cooperation

Регламенти ЄС

DAC8 розширює обсяг автоматичного обміну інформацією в рамках DAC до інформації, яку постачальники послуг крипто активів повинні повідомляти про транзакції (передачу або обмін) крипто активів та електронних грошей.
ЄС приймає Директиву, яка запроваджує правила податкової прозорості для крипто активів (DAC8). Держави-члени Європейського Союзу (ЄС) офіційно ухвалили поправки до Директиви 2011/16/ЄС щодо адміністративного співробітництва в галузі оподаткування DAC8.

TRANSFER OF FUNDS REGULATION

Travel rules

Регламенти ЄС

Відповідно до статті 2, новий TFR застосовується до всіх переказів криптоактивів, якщо CASP ініціатора або бенефіціара має зареєстрований офіс у Союзі. Зі сфери застосування TFR виключені передачі криптоактивів від людини до особи, які здійснюються без участі CASP, і передачі криптоактивів, де і ініціатором, і бенефіціаром є CASP, які діють від свого імені.

Зобов'язання постачальника послуг криптоактивів (ініціатора)

- ім’я відправника
- адреса розподіленої книги ініціатора та номер рахунку крипто-активів ініціатора, де обліковий запис існує та використовується для обробки транзакції
- номер рахунку криптоактиву автора
- адресу відправника, включаючи назву країни, номер офіційного особистого документа та ідентифікаційний номер клієнта, або, альтернативно, дату та місце народження відправника
- поточний LEI або, за відсутності, будь-який інший доступний еквівалентний офіційний ідентифікатор ініціатора. Крім того, CASP ініціатора повинен надати таку

інформацію про бенефіціара:

- назва
- адреса розподіленої книги
- номер рахунку криптоактивів
- поточний код LEI бенефіціара. Цю інформацію має надати CASP заздалегідь або одночасно чи паралельно з передачею криптоактивів і в безпечний спосіб відповідно до Загального регламенту захисту даних. У разі передачі чи передачі криптоактивів на самостійну адресу, CASP ініціатора зобов’язаний отримати вищезазначену інформацію, зберігати її та забезпечити індивідуальну ідентифікацію передачі криптоактивів. У разі переказу суми, що перевищує 1000 євро на власну адресу, CASP зобов’язаний визначити, чи належить власна адреса ініціатору чи контролюється ним.

EUROPEAN SYSTEM OF FINANCIAL SUPERVISION (ESFS)

EUROPEAN SUPERVISORY AUTHORITIES (ESA):

EBA (ЄВРОПЕЙСЬКИЙ ОРГАН З БАНКІВСЬКОЇ ДІЯЛЬНОСТІ)

EIOPA (ЄВРОПЕЙСЬКЕ УПРАВЛІННЯ ЗІ СТРАХУВАННЯ ТА ПРОФЕСІЙНИХ ПЕНСІЙ)

ESMA (ЄВРОПЕЙСЬКИЙ ОРГАН З ЦІННИХ ПАПЕРІВ І РИНКІВ)

(ESFS – EUROPEAN SYSTEM OF FINANCIAL SUPERVISION)

ЄДИНИЙ ЄВРОПЕЙСЬКИЙ ОРГАН ФІНАНСОВОЇ РОЗВІДКИ

ПРОВЕДЕННЯ НАЛЕЖНОЇ ПЕРЕВІРКИ КЛІЄНТА (CDD)

ПОДАННЯ ЗВІТІВ ПРО ПІДОЗРІЛУ ДІЯЛЬНІСТЬ (STR)

РЕЄСТРАЦІЯ В МІСЦЕВИХ КОМПЕТЕНТНИХ ОРГАНАХ

1. ПРОДАЖ НЕДОЗВОЛЕНИХ ТОВАРІВ
2. ВИМАГАННЯ
3. ШАХРАЙСТВО
4. КІБЕРЗЛОЧИННІСТЬ
5. УНИКНЕННЯ САНКЦІЙ

The **Office of Foreign Assets Control** (**OFAC**)

Злочинна діяльність із криптоактивами

РОЗВИТОК ТЕХНОЛОГІЙ ТА ПОТЕНЦІЙНІ ЗАГРОЗИ

За 2024 рік 3,1 трильйона доларів незаконних коштів переміщено по всьому світу

AMLBot

Crystal

Ukrainian Modern Digital Science Community organization

purefi

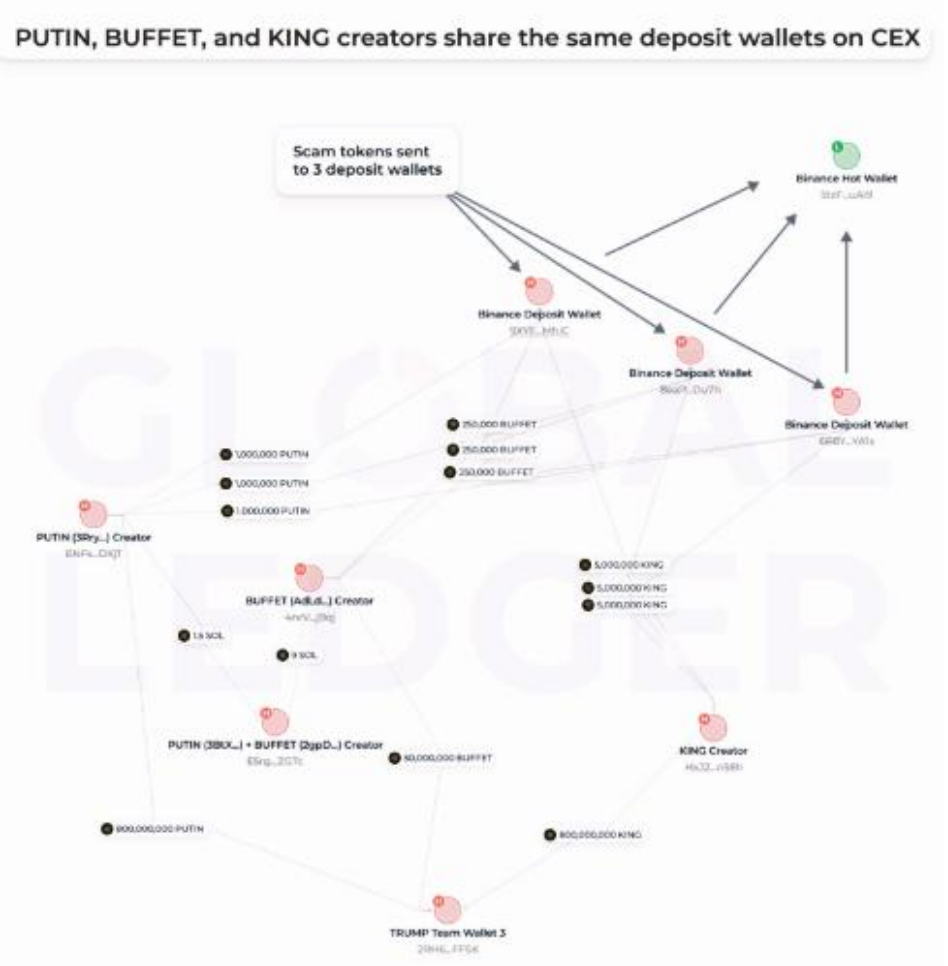
GLOBAL LEDGER

РОЗВИТОК ТЕХНОЛОГІЙ ТА ПОТЕНЦІЙНІ ЗАГРОЗИ

Заробіток на хайпі $TRUMP: щонайменше $857,5 млн дісталися шахраям

Не дивно, що мем-коїни, пов'язані з відомими особами, часто приваблюють шахраїв. Але одна особливо зухвала схема привернула увагу команди Global Ledger.

Шахраї скористалися монетою $TRUMP для реалізації схеми «pump-and-dump». Проте вони не купували й не продавали сам мем-коїн. Досліджена нами схема виявилася водночас складнішою та простішою, принісши шахраям щонайменше $857,5 мільйона.



ДЯКУЮ ЗА УВАГУ!

ТЕТЯНА ДМИТРЕНКО, Д.Е.Н, СТ. ДОСЛІДНИК, ГОЛОВА UMDS