Серійний номер: ДСФМУ-ДК-2024-025
Вересень 2024

ЗВІТИ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ та ОКРЕМИХ ЮРИСДИКЦІЙ

Технології США, що підживлюють війну росії в Україні

Документ підготовлений Постійним підкомітетом Сенату США з розслідувань і зосереджений на ролі американських виробників напівпровідників у постачанні компонентів для російської військової техніки, яка використовується під час війни в Україні. Основна увага приділяється таким компаніям, як Analog Devices, Intel, Texas Instruments та AMD, продукція яких була знайдена в російській зброї, що вражала цивільні та військові об'єкти в Україні, включно з ракетами типу X-101.

Основна проблема, яку розглядає звіт, полягає в недостатній ефективності заходів експортного контролю, які вводились урядом США з 2022 року. **Хоча нові правила були розроблені для обмеження доступу Росії до високотехнологічних американських компонентів, американські мікрочипи та інші електронні елементи продовжують потрапляти в російське військове обладнання через треті країни, такі як Китай, Гонконг, Туреччина, Казахстан та інші**. Компанії-виробники були піддані критиці через недостатньо оперативну відповідь на експортні обмеження та їхні недосконалі внутрішні системи аудиту.

Звіт також виявляє, що продажі напівпровідників до країн, які підтримують Росію, значно зросли після початку війни, і це вказує на серйозні прогалини в експортному контролі. Наприклад, поставки напівпровідників до Казахстану зросли в понад 550 разів у порівнянні з довоєнним періодом. Розслідування також показує, що компанії-виробники напівпровідників в основному виявляють проблеми тільки після того, як їх уже зафіксувало Бюро промисловості та безпеки (BIS), а не завдяки своїм внутрішнім механізмам.

Ключові висновки:

1. **Недостатня ефективність експортного контролю США та недоліки корпоративного контролю:** Документ демонструє, що, незважаючи на введення нових експортних обмежень з боку США з початку російської агресії проти України у 2022 році, російська військова машина продовжує отримувати критичні електронні компоненти від американських виробників через треті країни. Ключовим елементом проблеми є неналежний рівень внутрішнього контролю та недостатньо активна участь самих компаній у відстеженні

кінцевих споживачів їхньої продукції. Після введення санкцій поставки напівпровідників до країн, таких як Китай, Казахстан, Вірменія, Туреччина та інші, значно зросли, що свідчить про недоліки в управлінні експортним контролем і слабкі корпоративні механізми контролю.

2. **Проблеми з виявленням транзакцій із високим ризиком:** Компанії, включно з такими гігантами, як Texas Instruments, Intel, Analog Devices та AMD, не змогли своєчасно виявити підозрілі транзакції та покупців, які можуть бути пов'язані з Росією або її партнерами. Це зумовлено відсутністю належного використання доступних інструментів ризик-менеджменту і недостатньо активними перевірками дистриб'юторів. Багато компаній не використовували наявне програмне забезпечення для моніторингу ланцюга поставок, що могло б допомогти ідентифікувати такі ризики ще до того, як до них звернулося Бюро промисловості та безпеки (BIS). Наприклад, виявлення ризиків могло б бути більш оперативним, якби компанії використовували доступні комерційні аналітичні системи для відстеження транзакцій.
3. **Неналежні програми аудиту експортного контролю:** Звіт показує, що жодна з чотирьох розглянутих компаній не має належної системи щорічних перевірок власних програм експортного контролю, хоча це є важливим елементом у мінімізації ризику незаконних поставок. Крім того, більшість компаній не проводять регулярного аудиту своїх дистриб'юторів, що залишає суттєві прогалини в захисті від можливих порушень. Це означає, що компанії залишаються вразливими до схем транзиту та перепродажу, які можуть призвести до постачання їхніх компонентів у Росію.
4. **Пасивність у взаємодії з зовнішніми слідчими організаціями:** Компанії, такі як Texas Instruments, Analog Devices та Intel, продемонстрували слабку реакцію на запити від зовнішніх організацій, які займаються відстеженням походження компонентів у російській зброї. Відповіді на запити були або запізнілими, або неповними. Наприклад, Texas Instruments отримав понад 100 запитів від таких організацій, як Conflict Armament Research (CAR), але компанія не надала жодної детальної відповіді до лютого 2024 року, що викликало занепокоєння з боку державних органів. Тільки AMD більш-менш оперативно реагував на ці запити, надаючи інформацію про виробництво, дистрибуцію та кінцевих користувачів компонентів.
5. **Зростання експорту напівпровідників до третіх країн:** Після початку війни в Україні обсяг поставок напівпровідників до таких країн, як Казахстан, Вірменія та Туреччина, різко зріс. Наприклад, у 2023 році експорт напівпровідників до Казахстану збільшився в 550 разів у порівнянні з 2021 роком. Це свідчить про те, що ці країни стали важливими транзитними пунктами для передачі технологій Росії, що потребує посиленого контролю та перевірок. Підприємства, ймовірно, продовжують продавати напівпровідники до цих країн через слабкий внутрішній моніторинг та недоліки у виконанні вимог експортного контролю.
6. **Недостатня інтеграція сучасних технологій моніторингу ризиків:** Особливо у випадку Texas Instruments, компанії не використовують сучасні аналітичні системи для виявлення ризикових транзакцій, що дозволяє недобросовісним покупцям обходити заборони. Компанія використовує застарілі методи перевірки клієнтів, які включають ручні списки санкцій, що значно відстає від можливостей сучасних систем аналізу ризиків.

Основні висновки з цього звіту вказують на значні прогалини в системах експортного контролю американських компаній, які виробляють напівпровідники. **Недостатні внутрішні аудити, слабкий моніторинг дистриб'юторів і пасивність у взаємодії з зовнішніми слідчими організаціями створюють умови для того, щоб американські технології продовжували використовуватися Росією** у війні проти України. **Звіт рекомендує впровадження більш жорстких і систематичних заходів для запобігання витоку критичних технологій до ворожих країн, включно з щорічними аудитами, посиленою співпрацею з урядовими органами та застосуванням сучасних технологій для моніторингу транзакцій.**

http://surl.li/smxtcm

Звіт ФБР про шахрайство з криптовалютами

Документ "2023 Cryptocurrency Fraud Report" від Федерального бюро розслідувань (ФБР) надає детальний огляд шахрайств, пов'язаних з криптовалютами, та їх зростання за 2023 рік. Зокрема, **він описує види шахрайств, пов'язаних з використанням криптовалют, з акцентом на інвестиційні схеми, які призвели до значних втрат. Згідно з даними, за рік було подано понад 69 тисяч скарг на криптовалютні шахрайства, а загальні втрати склали понад 5,6 мільярдів доларів США, що на 45% більше порівняно з попереднім роком.**

Основними схемами шахрайства були інвестиційні афери, що становили 71% від загальних втрат, за ними йшли технічна підтримка та шахрайства з підробленими державними представниками. Особливу увагу приділено новим варіаціям інвестиційних шахрайств, зокрема схемам, що використовують довіру жертви через соціальні мережі або застосунки для знайомств.

Документ також аналізує тенденції використання криптовалютних кіосків, що набувають популярності серед шахраїв, які використовують їх для анонімних транзакцій, та описує шахрайські схеми відновлення втрачених криптовалют, де жертви після шахрайства знову стають мішенню.

Кілька ключових висновків зі звіту:

1. **Інвестиційне шахрайство залишається домінуючим:** інвестиційне шахрайство спричинило 71% усіх збитків, пов'язаних із криптовалютою, на загальну суму $3,96 мільярда. Це підкреслює необхідність чіткості регуляторного периметру, надійної ідентифікації та перевірки контрагентів, щоб уникнути втягнення в шахрайські схеми.
2. **Вік є фактором:** хоча шахраї націлені на інвесторів будь-якого віку, демографічна група старше 60 років зазнала найбільших загальних збитків на суму $1,6 мільярда. Належна перевірка CASP і VASP є критично важливою незалежно від демографічної категорії.
3. **Криптовалютні банкомати під загрозою:** у звіті спостерігається зростання шахрайства з використанням криптовалютних кіосків, збитки яких перевищують 189 мільйонів доларів. Анонімністю, яку пропонують ці машини, можна скористатися, якщо немає належного моніторингу.
4. **Шахрайство із обміном SIM-карти (SIM swapping[1]):** злочинці також використовують SIM swapping, щоб отримати доступ до гаманців жертв, що призвело до збитків у розмірі 30 мільйонів доларів. Це підкреслює, що злами відбуваються не тільки он-чейн;

Доповідь закликає користувачів подавати скарги через платформу IC3 і пропонує поради щодо захисту від шахрайств. Окрім того, описується роль новоствореного підрозділу FBI — Віртуального активного підрозділу (VAU), що відповідає за боротьбу з криптовалютними злочинами на глобальному рівні.

Цей звіт служить посібником як для правоохоронних органів, так і для широкої громадськості, щоб бути поінформованими про поширені види криптовалютних шахрайств і захиститися від них.

https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3CryptocurrencyReport.pdf

[1] тип шахрайства, при якому зловмисники отримують контроль над мобільним номером жертви, переміщуючи його на іншу SIM-карту, яка належить їм. Маючи доступ до номера, шахраї можуть обходити двофакторну аутентифікацію та отримувати доступ до особистих акаунтів і фінансової інформації.

Шахрайство з авторизованим push-платежами: ризик-орієнтований підхід до обробки платежів

Документ є консультаційним посібником від Управління фінансової поведінки (FCA) Великобританії. Він **акцентує увагу на загрозі зростання шахрайства з авторизованими пуш-платежами [2] (APP fraud), де шахраї обманюють жертв, змушуючи їх виконувати платежі на рахунки, що належать злочинцям.** У відповідь на це уряд запроваджує нові регулювання для платіжних систем, щоб допомогти банкам та постачальникам платіжних послуг (PSP) виявляти й запобігати таким шахрайствам.

Посібник детально описує, як законодавство щодо затримок платежів (payment delays legislation) надає PSP можливість затримати транзакції, якщо вони мають підозри на шахрайство, і дозволяє банкам більше часу для розслідування підозрілих переказів. Важливо, що PSP не зобов'язані затримувати всі платежі, але можуть це робити в разі підозр, за умови обґрунтованої підозри шахрайства. **Законодавство передбачає, що PSP повинні відшкодовувати клієнтам збитки, якщо вони стали жертвами APP fraud**.

Ключові висновки:

1. **Значне зростання APP fraud і необхідність посилення заходів з протидії.**

Протягом останніх років у Великобританії було зафіксовано стрімке зростання кількості випадків шахрайства з авторизованими платіжними переказами. Цей вид шахрайства характеризується тим, що жертва добровільно виконує платіж на рахунок, який належить злочинцю, але заздалегідь введена в оману щодо його законності. Згідно з даними UK Finance, збитки від APP fraud досягли £459,7 мільйонів у минулому році, з яких £376,4 мільйони стосувалися особистих втрат, а £83,3 мільйони — втрат бізнесу. Такий масштаб шахрайства потребує нових регуляторних заходів та підходів для протидії.

2. **Запровадження обов'язкового відшкодування втрат постраждалим користувачам.**

Однією з головних змін є вимога, щоб постачальники платіжних послуг (PSP) відшкодовували, у більшості випадків, втрачену суму жертвам APP fraud. Ця нова вимога, яка набуде чинності з 7 жовтня 2024 року, покликана замінити добровільний "Модельний кодекс умовного відшкодування" (Contingent Reimbursement Model Code), запроваджений у 2019 році. Тепер PSP нестимуть відповідальність за відшкодування втрат своїм клієнтам, що стимулюватиме банки інвестувати більше ресурсів у системи захисту від шахрайства.

3. **Гнучкість у підході до затримки платежів для перевірки шахрайства.**

Нове законодавство надає PSP можливість затримувати платіж на термін до чотирьох робочих днів, якщо є обґрунтовані підозри щодо шахрайства або нечесності. Ця затримка дозволить банкам і фінансовим установам отримати додатковий час для розслідування платежу, зв'язку з клієнтом або правоохоронними органами, щоб виявити можливі шахрайські дії. Проте важливо відзначити, що PSP не зобов'язані автоматично затримувати всі підозрілі платежі, і цей механізм має застосовуватися виключно в контексті ризик-орієнтованого підходу.

4. **Захист законних користувачів і забезпечення швидкої обробки транзакцій.**

---

[2] тип транзакції, коли ініціатором є платник, який самостійно відправляє кошти на рахунок одержувача. Платіж характерний тим, що платник контролює ініціювання та суму переказу, на відміну від pull payments, де одержувач ініціює зняття коштів з рахунку платника. Push payments широко використовуються в системах миттєвих або цифрових платежів.

Незважаючи на впровадження нових механізмів для запобігання шахрайству, FCA акцентує на важливості мінімізації впливу цих змін на законні транзакції. Банки повинні забезпечувати, щоб затримки у виплатах не створювали необґрунтованих незручностей для законних користувачів, і що платежі продовжували оброблятися швидко та ефективно. FCA прагне зберегти баланс між боротьбою з шахрайством і забезпеченням належного обслуговування клієнтів.

5. **Посилена співпраця з правоохоронними органами та іншими фінансовими установами.**

Документ пропонує PSP активніше співпрацювати з правоохоронними органами та іншими платіжними установами для підвищення ефективності боротьби з шахрайством. Наприклад, PSP можуть затримати платіж на підставі інформації від правоохоронних органів або інших фінансових установ, які мають підтвердження про підозрілі дії платника або отримувача. Така міжвідомча взаємодія допоможе швидше виявляти шахраїв і захищати споживачів.

6. **Стандарти для ідентифікації підозрілих платежів.**

FCA у своєму посібнику надає рекомендації, які фактори можуть збільшити ризик шахрайства під час обробки платежів. Серед основних критеріїв — нові одержувачі платежів, невідповідність імен отримувача з даними в платіжному дорученні, раптові зміни у поведінці користувача або невідповідність суми й частоти переказу звичкам платника. Крім того, PSP повинні звертати увагу на такі типові схеми шахрайства, як "безпечні рахунки"[3], романтичні шахрайства[4], інвестиційні афери, а також шахрайства з рахунками-фактурами.

7. **Моніторинг впровадження нових правил та оцінка їх ефективності.**

FCA планує регулярно оцінювати, наскільки ефективно PSP використовують додатковий час для затримки платежів для виявлення шахрайства. Цей моніторинг включатиме аналіз кількості та вартості затриманих платежів, тривалості затримок та кількості платежів, що виявилися шахрайськими. Це допоможе визначити, наскільки нові заходи допомагають запобігати шахрайству і чи не спричиняють вони зайві незручності для споживачів.

8. **Управління зобов'язаннями щодо компенсацій та зменшення витрат для PSP.**

Затримка платежів дозволить банкам уникнути зайвих витрат на відшкодування збитків, оскільки вони отримують більше часу для розслідування підозрілих транзакцій. Однак у випадку помилки чи неправомірної затримки PSP зобов'язані компенсувати своїм клієнтам нараховані відсотки або додаткові витрати, що виникли внаслідок затримки. Це стимулює банки приймати рішення про затримку платежу лише у випадках реальних підозр на шахрайство.

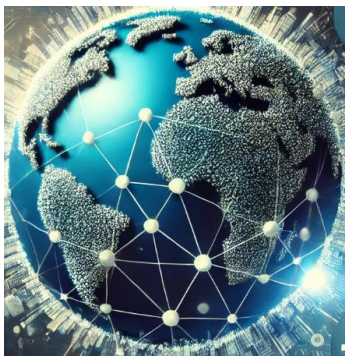
https://www.fca.org.uk/publication/guidance-consultation/gc24-5.pdf

Відповідь на консультації Ради з фінансової стабільності (FSB) щодо регулювання та нагляду за транскордонними платіжними послугами та узгодженням інфраструктури даних

[3] Safe Account Scam - вид шахрайства, коли злочинці переконують жертву перевести гроші на так званий "безпечний рахунок" для захисту від нібито шахрайської активності. Насправді, цей рахунок контролюється шахраями.

[4] Romance Scam - шахраї створюють фальшиві профілі в соціальних мережах або на сайтах знайомств, щоб створити довірчі стосунки з жертвою. Після встановлення емоційного зв'язку шахрай починає вимагати гроші, використовуючи різні приводи, наприклад, для допомоги в складній ситуації або на "переїзд для зустрічі".

Документ Вольфсберзької Групи надає відповідь на два ключових запити FSB щодо рекомендацій з регулювання та нагляду за банківськими і небанківськими транскордонними платіжними послугами, а також щодо вирівнювання та узгодження даних в межах міжнародних платіжних систем.



Вольфсберзька Група у своєму коментарі висловлює підтримку запропонованим ініціативам FSB, проте акцентує увагу на необхідності забезпечення всебічного підходу до запобігання фінансовим злочинам. Це включає інтеграцію заходів ПВК/ФТ/ФР, а також відповідність податковому законодавству і санкціям. Група пропонує залучити приватний сектор до консультацій, підкреслюючи, що участь приватних компаній має бути не просто формальною, а суттєвою, щоб запропоновані рішення були практичними та ефективними.

Крім того, Вольфсберзька Група наполягає на узгодженні регулювання для всіх учасників платіжної екосистеми, незалежно від того, чи є вони банками або небанківськими платіжними провайдерами (PSP). Вони підтримують принцип "однакова діяльність – однакові ризики – однакові правила", зазначаючи, що регулювання має бути однаковим для всіх, аби уникнути регуляторного арбітражу.

Документ також порушує питання про те, що інновації у платіжних системах створюють нові виклики для регулювання. **Використання віртуальних валют і VASPs повинно бути включене в сферу регулювання для забезпечення послідовного підходу до управління фінансовими злочинами**. Вольфсберзька Група підкреслює, що без такого підходу ризики, пов'язані з віртуальними активами, можуть залишатися непоміченими.

Також у відповідь наведено рекомендації стосовно підвищення прозорості транзакцій, важливості узгоджених стандартів для передавання платіжної інформації та необхідності вдосконалення нагляду та ліцензування платіжних провайдерів.

https://dev.wolfsberg-group.org/news/74

РЕГУЛЮВАННЯ

Пояснення нових правил FinCEN з ПВК для консультантів

Документ «Deciphering FinCEN's New Anti-Money Laundering Rules for Advisers» присвячений аналізу нових правил протидії відмиванню коштів та фінансуванню тероризму (ПВК/ФТ) для інвестиційних консультантів, запроваджених мережею FinCEN у США. Основна увага приділяється тому, як ці правила впливають на зареєстрованих інвестиційних консультантів (RIAs) і консультантів зі звільненням від звітування (ERAs). Нові вимоги включають впровадження програм ПВК/ФТ, подання звітів про підозрілі операції (SARs), збереження документів, а також нагляд з боку Комісії з цінних паперів і бірж США (SEC). Правила вступають у дію 1 січня 2026 року.

Ключові висновки

1. **Запровадження нових вимог до інвестиційних консультантів (RIAs) та консультантів зі звільненням від звітування (ERAs):**

   Нові правила FinCEN зобов'язують інвестиційних консультантів впроваджувати програми ПВК/ФТ. Ці програми мають бути ризик-орієнтованими і спрямованими на захист фінансової системи від нелегальної діяльності. Консультанти повинні впроваджувати незалежне тестування своїх програм, забезпечувати відповідне навчання персоналу і постійний моніторинг клієнтів та транзакцій.

2. **Розширення повноважень SEC щодо нагляду за дотриманням вимог ПВК/ФТ:**

   FinCEN делегувала Комісії з цінних паперів і бірж США (SEC) повноваження щодо нагляду за виконанням нових правил з боку інвестиційних консультантів. Це означає, що SEC буде контролювати, як інвестиційні консультанти виконують вимоги ПВК/ФТ, проводити аудити та оцінювати ефективність цих програм.

3. **Посилений контроль за приватними фондами:**

   Приватні фонди, особливо венчурні та хедж-фонди, можуть бути використані для нелегальної фінансової діяльності, наприклад, для обходу санкцій або фінансування тероризму. FinCEN зазначає, що приватні фонди часто діють у юрисдикціях зі слабкими ПВК/ФТ механізмами, що підвищує ризик незаконних фінансових операцій. Консультанти, які працюють з такими фондами, повинні ретельно оцінювати ризики і впроваджувати додаткові заходи для зменшення цих ризиків.

4. **Вимога щодо подання звітів про підозрілі операції (SARs):**

   Всі зареєстровані інвестиційні консультанти зобов'язані подавати звіти про підозрілу активність (SARs) у випадку, якщо транзакція, сума якої перевищує $5000, підозріло пов'язана з нелегальною діяльністю або має інші ознаки, що можуть свідчити про відмивання коштів або фінансування тероризму. Консультанти повинні подавати звіт не пізніше ніж через 30 днів після виявлення підозрілої активності.

5. **Збереження конфіденційності даних та документів:**

   Документ особливо підкреслює необхідність суворого дотримання конфіденційності інформації щодо звітів про підозрілі операції (SARs). Будь-яка спроба розкрити інформацію, пов'язану із SARs, суворо заборонена, і якщо інвестиційний консультант або його співробітники отримають запит на розкриття таких даних, вони зобов'язані відмовити і повідомити про це FinCEN.

6. **Мінімальні вимоги до програм ПВК/ФТ:**

   Програми ПВК/ФТ мають включати незалежне тестування для оцінки їх ефективності, призначення відповідальних осіб за реалізацію програми, постійне навчання персоналу та впровадження процедури постійного моніторингу клієнтів. Особливу увагу слід приділяти ризикованим клієнтам, серед яких можуть бути іноземні інвестори або клієнти з приватних фондів.

7. **Застосування правил для іноземних інвестиційних консультантів:**

   Іноземні консультанти, що ведуть діяльність у США або обслуговують американських інвесторів, також повинні виконувати вимоги цих нових правил. Це поширюється навіть на іноземні фонди з американськими інвесторами, що ускладнює структуру ведення бізнесу для іноземних консультантів.

8. **Консультанти повинні оцінювати ризики своїх клієнтів:**

   Інвестиційні консультанти зобов'язані впроваджувати процедури ретельного вивчення своїх клієнтів, щоб ідентифікувати потенційні ризики, пов'язані з відмиванням коштів або фінансуванням тероризму. Вони мають збирати необхідну інформацію про клієнтів, включаючи структуру власності фондів, які вони обслуговують, а також оцінювати потенційні ризики, якщо інформація про клієнтів недоступна.

9. **Дата набрання чинності правил:**

   Остаточна версія правил набуде чинності 1 січня 2026 року. Це дає інвестиційним консультантам час на впровадження необхідних програм і процедур у сфері ПВК/ФТ, щоб відповідати новим вимогам.

https://is.gd/r49bqo

САНКЦІЇ

Китай зіткнувся з санкціями США за підтримку Пакистану у будівництві балістичних ракет

США ввели нові санкції проти кількох китайських організацій через їхню участь у підтримці програми балістичних ракет Пакистану. Серед цих організацій є Beijing Research Institute of Automation for Machine Building Industry, який постачав Пакистану технології та матеріали для ракетних систем Shaheen-3 і Ababeel, здатних нести ядерні боєголовки. Ці санкції спрямовані на стримування розповсюдження ракетних технологій. Китай виступив із різкою критикою цих дій США, звинувачуючи їх у порушенні міжнародного права та пообіцяв захистити свої національні інтереси та компанії.

Нові санкції є частиною ширшої американської стратегії стримування розповсюдження ракетних і ядерних технологій у нестабільних регіонах. Вони включають заморожування активів, заборону на фінансові операції та обмеження на експорт товарів і технологій. Особливу увагу приділено тим китайським компаніям, які постачають ключові компоненти для розвитку ракетних систем Пакистану, що викликає занепокоєння з боку США щодо розширення пакистанських можливостей в ядерній сфері.

Загалом, напруженість між США та Китаєм зростає на фоні цих санкцій, оскільки Китай вбачає в них спробу перешкодити своїй міжнародній діяльності та торгівельним відносинам з іншими країнами, зокрема з Пакистаном.

https://regtechtimes.com/china-faces-u-s-sanctions-for-ballistic-missiles/

Зростання операцій із золотом: стратегія росії для обходу санкцій

Стаття детально аналізує стратегію Росії з використання золота для обходу міжнародних санкцій, накладених після її військового вторгнення в Україну. **Після того як західні країни, включаючи США та Європейський Союз, ввели жорсткі економічні санкції проти Росії, зокрема виключили російські банки з глобальної платіжної системи SWIFT, Росія була змушена шукати альтернативні методи підтримки своєї економіки та фінансової системи.**

Основні аспекти статті:

1. Збільшення операцій із золотом:

- Росія значно збільшила купівлю та видобуток фізичного золота, використовуючи його як стратегічний резерв та засіб міжнародних розрахунків.
- Золото експортується до країн, які не підтримують санкції проти Росії, таких як Китай та Індія. Особливо виділяється роль Гонконгу як транзитного пункту для продажу російського золота.

2. Обхід доларової залежності:

- Використання золота дозволяє Росії уникати транзакцій у доларах США, що важливо в умовах санкцій, які обмежують доступ до доларових ринків.

- Золото слугує альтернативним засобом збереження вартості та розрахунків, сприяючи процесу дедоларизації російської економіки.

3. Підтримка економічної стабільності:

- Збільшення золотих резервів допомагає Росії зміцнювати національну валюту та забезпечувати фінансову стабільність в умовах зовнішнього тиску.
- Золото використовується для підтримки ключових секторів економіки, зокрема енергетичного, шляхом здійснення розрахунків з іноземними партнерами.

4. Створення альтернативних фінансових механізмів:

- Росія розвиває власні фінансові інструменти та системи, такі як СПФС (Система передачі фінансових повідомлень), яка є аналогом SWIFT, для забезпечення безперебійних фінансових транзакцій зі своїми партнерами.

5. Міжнародні наслідки та реакція:

- Такі дії Росії можуть мати вплив на глобальний ринок золота, підвищуючи попит і впливаючи на світові ціни.
- Західні країни розглядають можливість розширення санкцій, включаючи обмеження на операції з російським золотом, щоб закрити цю лазівку.

6. Ризики та обмеження стратегії:

- Залежність від золота як основного засобу обходу санкцій має свої ризики, зокрема через волатильність ринку золота та обмежену ліквідність у глобальному масштабі.
- Використання золота не може повністю компенсувати втрати від обмеження доступу до міжнародних фінансових ринків і технологій.

7. Потенційний вплив на глобальну фінансову систему:

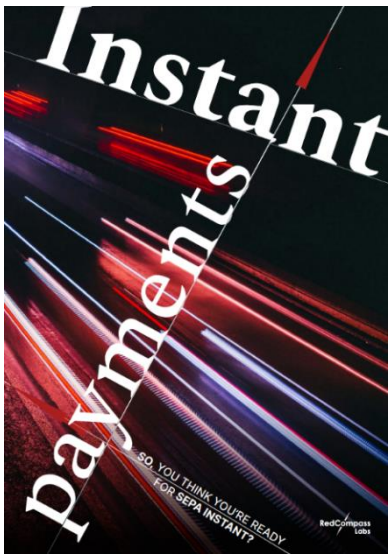
- Дії Росії можуть стимулювати інші країни до пошуку альтернатив долару США та західним фінансовим інститутам, що може призвести до змін у світовій фінансовій архітектурі.
- Підвищується інтерес до створення багатополярної фінансової системи, де золото та інші активи відіграватимуть більшу роль.

Стратегія Росії з використання золота для обходу санкцій є відповіддю на безпрецедентний економічний тиск з боку Заходу. Хоча це допомагає країні підтримувати певний рівень економічної стабільності та фінансувати державні програми, така тактика має свої обмеження і не є довгостроковим рішенням. Міжнародна спільнота уважно стежить за цими діями, і можливе подальше посилення санкцій може вплинути на ефективність цієї стратегії. Стаття підкреслює важливість глобальної співпраці у вирішенні питань фінансової безпеки та необхідність адаптації міжнародних фінансових інститутів до нових викликів.

https://regtechtimes.com/rise-of-gold-transactions-russias-strategy-to-byp/

ЗВІТИ ОКРЕМИХ КОМПАНІЙ та ЕКСПЕРТІВ

Миттєві платежі SEPA



Документ під назвою "So, you think you're ready for SEPA instant?" досліджує процес впровадження та виклики, з якими стикаються європейські банки в контексті переходу на миттєві платежі у рамках SEPA (Єдина зона платежів в євро). Виходячи з прийняття нового законодавства Європейським Парламентом та Радою, документ аналізує амбіційні терміни впровадження миттєвих платежів, що вимагають від банків та постачальників платіжних послуг можливості обробляти миттєві перекази без додаткової плати та із захистом від шахрайства. Документ містить результати опитування 200 представників вищого керівництва з платіжних систем, яке було проведене для вивчення їхніх поглядів на поточний стан готовності до цих змін, виклики та переваги переходу на миттєві платежі.

Основні проблеми, з якими стикаються банки, включають необхідність адаптації до нових вимог щодо верифікації одержувача, інтеграції процесів KYC (знай свого клієнта) та санкційного контролю, а також збільшення обсягів обробки платежів. Одним із ключових викликів є обробка масових платежів, наприклад, заробітної плати та пенсій, які можуть містити сотні тисяч транзакцій. **Документ також розглядає важливість надійних систем захисту від шахрайства та забезпечення цілодобової доступності платіжних систем**.

Опитування показує, що більшість банків усвідомлює важливість інвестування у нові технології для відповідності вимогам, хоча багато хто недооцінює масштаб необхідних змін. **Основні переваги впровадження миттєвих платежів для корпоративних клієнтів банків включають підвищення зручності користувачів, зменшення витрат на транзакції та покращення управління робочим капіталом.**

Ключові висновки:

1. **Необхідність значних технічних інвестицій та модернізації платіжних систем:** Нове законодавство ЄС щодо SEPA миттєвих платежів ставить перед банками амбітні вимоги: всі банки та платіжні сервіс-провайдери повинні мати можливість обробляти миттєві платежі (отримання до 9 січня 2025 року та відправлення до 9 жовтня 2025 року). Це вимагає значних інвестицій у технічну модернізацію, оскільки миттєві платежі повинні оброблятися в режимі реального часу 24/7, що накладає величезне навантаження на існуючу інфраструктуру банків. Багато банків використовують застарілі системи, які працюють у пакетному режимі, тому їм необхідно переходити на архітектуру реального часу для забезпечення обробки платежів без затримок, що значно підвищує вимоги до їхніх можливостей.
2. **Недооцінка банками обсягів транзакцій та необхідності масштабованості:** Дослідження показує, що більшість банків недостатньо підготовлені до збільшення обсягу транзакцій, які необхідно буде обробляти в режимі миттєвих платежів. Лише невеликий відсоток банків здатен обробляти більше 1000 транзакцій на секунду, що необхідно для обробки масових платежів від корпоративних клієнтів, таких як виплати заробітної плати або пенсій. Наприклад, обробка таких файлів може містити сотні тисяч транзакцій, що створює значний виклик для інфраструктури навіть найбільших банків. Недооцінка масштабів та вимог до пропускної здатності може призвести до затримок і перебоїв у роботі платіжних систем.
3. **Запровадження систем верифікації одержувача (VoP) та боротьба з шахрайством:** Для захисту клієнтів від шахрайства нові правила вимагають впровадження системи верифікації одержувача (Verification of Payee). Ця функція дозволить відправникам перевірити, чи відповідає ім'я одержувача номеру його рахунку до завершення транзакції, що зменшить кількість шахрайських операцій. Враховуючи, що миттєві платежі є безвідкличними, запобігання шахрайству стає критично важливим завданням. Хоча такі системи існують у

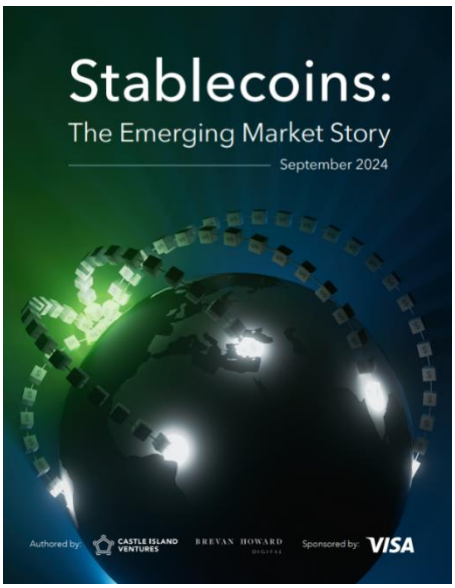
ряді європейських країн (Франція, Італія, Іспанія та інші), вони ще не є стандартом для транскордонних платежів, і розробка такої схеми потребує швидкої координації між усіма країнами-членами ЄС.

4. **Впровадження миттєвих платежів як інструмент боротьби з монополією карткових систем:** Миттєві платежі можуть суттєво змінити карткову індустрію, зокрема зменшити домінування Mastercard і Visa. Багато торговців прагнуть використовувати миттєві платежі як альтернативу картковим, щоб уникнути високих комісій за транзакції, які стягуються картковими системами. Це сприяє розвитку нових методів збору платежів, особливо в сфері електронної комерції та на POS (точках продажу), де карткові платежі традиційно домінували. Цей тренд також підкріплюється ініціативами на рівні ЄС, такими як Європейська платіжна ініціатива (EPI), яка спрямована на створення альтернативних платіжних рішень.
5. **Переваги для корпоративних клієнтів:** Основними перевагами SEPA миттєвих платежів для корпоративних клієнтів є:
   - *Оптимізація управління робочим капіталом*: Миттєві платежі надають компаніям можливість швидше отримувати кошти, що дозволяє їм краще управляти своїми фінансами, швидше реагувати на ринкові зміни та інвестувати в нові можливості. Це особливо корисно для компаній у конкурентних середовищах, де швидкість доступу до фінансових ресурсів є критично важливою.
   - *Покращення клієнтського досвіду*: Миттєві платежі дозволяють компаніям запропонувати своїм клієнтам кращий досвід, наприклад, через можливість отримання миттєвих відшкодувань або швидке виконання транзакцій. Це підвищує лояльність клієнтів та покращує взаємодію.
   - *Підвищення впевненості у платежах*: Корпорації цінують високу впевненість у термінах надходження платежів. Нові правила SEPA гарантують, що транзакції будуть завершені протягом 10 секунд у будь-який час доби, що суттєво підвищує довіру між партнерами та може призвести до покращення умов співпраці.
6. **Виклики з підтримкою цілодобової доступності (24/7):** Для успішної роботи миттєвих платежів банки повинні забезпечити постійну доступність своїх систем 24/7. Це означає, що банки повинні розробляти архітектури, здатні функціонувати без простоїв, навіть під час технічного обслуговування або оновлення. Така постійна доступність потребує значних інвестицій у резервні системи (stand-in modules), які можуть тимчасово виконувати роль основної системи у випадку технічних збоїв. Крім того, це створює виклики для управління ліквідністю, оскільки банки повинні бути впевнені, що можуть обробляти всі запити в реальному часі.
7. **Зниження операційних витрат:** Одна з ключових переваг миттєвих платежів для компаній — це зниження операційних витрат. Миттєві платежі дешевші за традиційні карткові операції, оскільки не включають посередників, таких як карткові системи, і дозволяють уникати високих комісій за обробку транзакцій.
8. **Недооцінка деякими банками вимог до інвестицій та готовності:** Хоча більшість банків планують інвестувати в технології для забезпечення відповідності вимогам нових правил, дослідження показує, що багато хто може недооцінювати як масштаби необхідних інвестицій, так і обсяги транзакцій, які будуть проходити через їхні системи. Це особливо стосується банків у Німеччині, де лише 55% опитаних готові інвестувати у необхідні технології, тоді як в інших країнах цей показник значно вищий. Більшість банків очікують витрати від 1 до 3 мільйонів євро на модернізацію, але для багатьох цих інвестицій може виявитися недостатньо.

У підсумку, миттєві платежі в рамках SEPA є не лише технологічним викликом, але й стратегічною можливістю для банків покращити свою інфраструктуру, знизити витрати та запропонувати своїм клієнтам нові конкурентні переваги. Однак це потребує серйозного підходу до інвестицій, модернізації систем та забезпечення безперебійної роботи 24/7.

http://surl.li/ofgjwi

Стейблкоїни: історія ринку, що розвивається



Документ під назвою "Stablecoins: The Emerging Market Story" досліджує використання стейблкоїнів (stablecoins) в економіках, що розвиваються, таких як Бразилія, Індія, Індонезія, Нігерія та Туреччина. Основна увага приділяється тому, як ці країни використовують стейблкоїни для транзакцій, заощаджень та міжнародних переказів, пропонуючи економічні та фінансові вигоди порівняно з традиційними банківськими системами. Документ підкреслює значне зростання обігу стейблкоїнів у глобальній економіці і зазначає, що їх загальна кількість в циркуляції перевищила $160 млрд.

Ключовим питанням є переваги стейблкоїнів над традиційними фінансовими системами, включаючи програмованість, швидкі та дешеві транзакції, можливість самостійного зберігання активів, і що найважливіше — стабільність, яку надають прив'язані до долара або інших фіатних валют активи. Документ містить результати опитування користувачів криптовалют у п’яти основних країнах, що розвиваються, і пояснює, як стейблкоїни використовуються не тільки для криптоторгівлі, але й для заміщення національних валют, оплати товарів та послуг, міжнародних платежів і як засіб заощаджень.

Також документ підкреслює потенційні регуляторні виклики та наслідки використання стейблкоїнів у таких країнах. Наприклад, у країнах з високим рівнем інфляції, як Аргентина та Венесуела, стейблкоїни стають засобом збереження вартості і захистом від знецінення місцевої валюти.

Ключові висновки:

1. **Зростання популярності стейблкоїнів:** Стейблкоїни вже не використовуються виключно для криптоторгівлі, а набули широкого застосування в реальних економічних сценаріях, особливо в країнах, що розвиваються. Вони стали основним засобом збереження вартості та здійснення платежів у цих регіонах. Наприклад, у Нігерії 77% користувачів регулярно конвертують свої місцеві валюти в стейблкоїни.
2. **Використання для транскордонних платежів та бізнес-транзакцій:** Багато користувачів, особливо в країнах, що розвиваються, використовують стейблкоїни для швидких та дешевих транскордонних платежів. Традиційні банківські послуги можуть бути занадто дорогими або недоступними, тому стейблкоїни стають привабливою альтернативою, особливо для малого та середнього бізнесу.
3. **Стейблкоїни як заміна банківським послугам:** У деяких країнах стейблкоїни фактично замінили банківські рахунки в доларах США. У країнах із високою інфляцією та нестабільними банківськими системами люди все частіше зберігають свої заощадження в стейблкоїнах замість національних валют. Наприклад, у Туреччині стейблкоїни використовуються для отримання прибутку через DeFi-протоколи, а також для збереження заощаджень.
4. **Технологічні та фінансові переваги:** Стейблкоїни мають вбудовану інтероперабельність, що дозволяє їм легко взаємодіяти з різними блокчейнами та децентралізованими фінансовими системами (DeFi). Це надає користувачам більше можливостей для управління своїми фінансами, зокрема шляхом доступу до програмованих фінансових продуктів або отримання прибутку від заощаджень. Наприклад, у країнах на зразок Бразилії стейблкоїни вже використовуються для проведення платежів і нарахування зарплат.
5. **Виклики регулювання:** Незважаючи на значні переваги, стейблкоїни викликають занепокоєння у регуляторів, особливо через ризики "доларизації" економік, де національні валюти можуть бути витіснені використанням стейблкоїнів, прив'язаних до долара США. Деякі країни вже почали приймати заходи для регулювання цього процесу, щоб запобігти негативним наслідкам для їх фінансових систем.

Документ підсумовує, що стейблкоїни швидко переходять із суто криптовалютної сфери в реальну економіку, особливо в країнах, що розвиваються. Їх зростання створює нові можливості для фінансової інклюзії, одночасно викликаючи регуляторні виклики, які потребують уважної уваги з боку влади.

https://castleisland.vc/wp-content/uploads/2024/09/stablecoins_the_emerging_market_story_091224.pdf

Перегляд моделі відмивання коштів «Розміщення–Розшарування–Інтеграція»

Документ досліджує традиційну модель "Placement-Layering-Integration" (P-L-I) у відмиванні коштів та аналізує її актуальність у сучасних умовах з урахуванням нових технологій, таких як криптовалюти та цифрові гаманці. У звіті ставиться питання про те, наскільки ефективною є ця модель в епоху цифрової економіки, та пропонуються альтернативні підходи для боротьби з відмиванням коштів. Через аналіз різних методів і сучасних кейсів, таких як TBML та використання криптовалют, дослідження підкреслює обмеження P-L-I моделі та закликає до розширення концептуальних рамок боротьби з відмиванням коштів.

Ключові висновки:

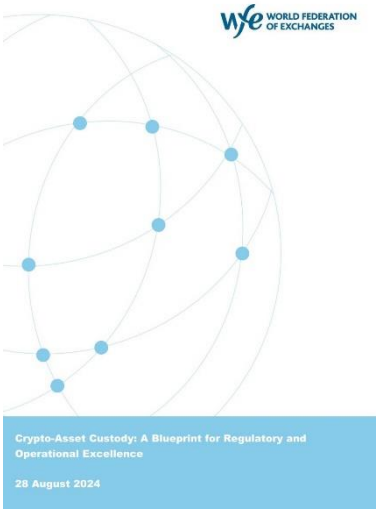
1. **Застарілість моделі P-L-I:** Традиційна модель "Placement-Layering-Integration" (розміщення, розшарування, інтеграція) була створена для виявлення відмивання коштів у класичних фінансових системах, але сучасні злочинці використовують нові методи, що дозволяють обійти цю модель. Наприклад, використання криптовалют, цифрових платформ і транзакцій з використанням анонімних рахунків значно ускладнює відстеження джерел фінансування. P-L-I модель фокусується на внесенні готівки в офіційні фінансові системи, але не враховує нові методи, такі як шахрайські інвестиційні схеми або цифрові валюти.
2. **Альтернативні моделі:** В документі пропонуються декілька альтернатив традиційній P-L-I моделі. Одна з них, модель "Generation–Consolidation–Placement–Layering–Integration–Realisation", додає нові етапи, такі як генерація та консолідація нелегальних доходів до їхнього розміщення в фінансових системах. Це дозволяє краще зрозуміти, як злочинці планують і організовують відмивання коштів, а також які механізми використовуються для консолідації цих коштів перед розшаруванням та інтеграцією.
3. **Новітні методи відмивання коштів:** В документі зазначається зростання ролі криптовалют у процесах відмивання коштів. Кримінальні групи використовують цифрові валюти для здійснення анонімних транзакцій, зокрема через міксери криптовалют та децентралізовані біржі (DEXs). Це ускладнює відстеження походження коштів і маскує їхні джерела. Крім того, все більше уваги приділяється TBML, де маніпуляції з рахунками-фактурами використовуються для маскування нелегальних доходів.
4. **Роль професійних "помічників" у схемах відмивання коштів:** Документ підкреслює важливість ролі адвокатів, бухгалтерів та фінансових консультантів, які надають послуги для маскування нелегальних доходів. Ці фахівці можуть створювати офшорні компанії, відкривати рахунки в іноземних банках та створювати трасти, які допомагають дистанціювати справжнього власника коштів від їхнього походження. Це створює вигляд законності для нелегальних фінансових операцій.
5. **Недоліки в традиційних регуляторних системах:** Незважаючи на посилення міжнародних зусиль щодо боротьби з відмиванням коштів, злочинці адаптуються до нових законодавчих вимог швидше, ніж уряди можуть впроваджувати нові заходи. Такі сектори, як міжнародна торгівля та неформальні системи грошових переказів (наприклад, Хавала), залишаються вразливими до використання в схемах відмивання коштів через відсутність належного нагляду та регуляторного контролю.

6. **Необхідність глобальної координації:** У документі наголошується на важливості міжнародного співробітництва у боротьбі з відмиванням коштів. Транскордонні транзакції, особливо з використанням криптовалют та цифрових платформ, ускладнюють виявлення злочинної діяльності, що вимагає більш тісної співпраці між юрисдикціями, обміну інформацією та нових підходів до регулювання.

Документ вказує на необхідність модернізації підходів до боротьби з відмиванням коштів, з урахуванням технологічних інновацій, міжнародного співробітництва та розвитку нових механізмів виявлення фінансових злочинів.

http://surl.li/wkjris

Кастодіальні послуги для криптоактивів: Регуляторна дорожня карта та операційні стандарти від WFE



Документ «Crypto-Asset Custody: A Blueprint for Regulatory and Operational Excellence», опублікований Всесвітньою федерацією бірж (World Federation of Exchanges, WFE) 28 серпня 2024 року, аналізує важливі аспекти регулювання та операційного управління кастодіальними послугами для криптоактивів. В основі документа лежить проблема зростання криптовалютного ринку, де кількість активів перевищує 23 000, а обсяги торгів перевищують $275 млрд щоденно. В умовах відсутності чіткого регуляторного підходу багато країн стикаються з труднощами у визначенні правил для захисту інвесторів та збереження ринкової цілісності.

Документ порівнює послуги постачальників послугзі зберігання криптоактивів у традиційних фінансових ринках з аналогічними послугами у криптоіндустрії. Основна увага зосереджена на питаннях захисту активів клієнтів у разі банкрутства компаній, ризиках, пов'язаних з кібербезпекою, і важливості прозорості у розкритті ризиків для користувачів. Важливим аспектом є те, що криптоактиви часто не захищені на законодавчому рівні в разі банкрутства платформ, що може призвести до втрати коштів інвесторів.

Ключові висновки:

1. **Сегрегація активів клієнтів**. Одним з основних аспектів, що потребує регулювання у сфері зберігання криптоактивів, є чітке розмежування активів клієнтів і активів компаній-провайдерів. Якщо активи клієнтів не будуть відокремлені, у випадку банкрутства криптотрейдингової платформи (CTP) або постачальника послуг зі зберігання криптоактивів, клієнти можуть втратити свої кошти, оскільки їхні активи можуть бути включені в майно компанії. У деяких юрисдикціях, таких як Швейцарія та Німеччина, вже розроблені нормативні акти, які захищають клієнтські активи в таких ситуаціях, що є прикладом для інших країн.
2. **Кібербезпека та управління технологічними ризиками**. З огляду на численні кібернапади на криптоплатформи, кібербезпека стала критичним аспектом для постачальників послуг зі зберігання криптоактивів. Документ підкреслює необхідність побудови сучасних кібербезпекових програм і використання передових технологій для мінімізації ризиків. У цьому контексті важливо, щоб кастодіальні сервіси впроваджували багаторівневі заходи безпеки, що включають багатофакторну аутентифікацію та колективне схвалення транзакцій, з метою запобігання шахрайським діям як ззовні, так і зсередини компаній.
3. **Прозорість і розкриття ризиків**. Постачальники послуг зі зберігання криптоактивів повинні надавати чітке і зрозуміле роз'яснення щодо всіх ризиків, пов'язаних з утриманням криптоактивів. Це особливо важливо для роздрібних

клієнтів, які можуть не усвідомлювати всіх небезпек, таких як правовий статус активів у разі банкрутства або ризики, пов'язані з кіберзлочинами. Документ акцентує на тому, що користувачі повинні бути поінформовані про умови захисту їхніх активів та можливі обмеження відповідальності постачальників послуг і зберігння крипоактивів.

4. **Необхідність незалежного аудиту**. Документ рекомендує постачальникам послуг зі зберігання криптоактивів звертатися до авторитетних аудиторів для проведення незалежного аудиту своїх фінансових звітів та операційних процесів. Це допоможе створити додатковий рівень довіри до провайдера і забезпечити прозорість роботи з активами клієнтів. При цьому наголошується, що аудити не повинні обмежуватися лише перевіркою активів під управлінням (Proof of Reserves), але також включати оцінку зобов'язань (Proof of Liabilities), щоб виявляти можливі приховані ризики.
5. **Управління конфліктами інтересів**. Вертикальна інтеграція криптотрейдингових платформ, які одночасно займаються торгівлею, зберіганням активів і послугами зі зберігання кастодіальних гаманців, створює серйозні ризики конфлікту інтересів. Документ рекомендує чітко розділяти ролі та функції послуг зі зберігання криптоактиів від інших бізнес-процесів компанії для зниження цих ризиків. Необхідно впроваджувати сильні механізми корпоративного управління, бар'єри етичної поведінки та процедури контролю, які дозволять уникнути використання активів клієнтів для власних цілей компанії.
6. **Операційна стійкість**. Важливим аспектом є забезпечення стійкості постачальників послуг зі зберігання криптоактивів, що включає надійність підтримки послуг, кібероперацій та залежності від третіх сторін. Документ рекомендує постачальникам послуг зі зберігання криптоактивів впроваджувати комплексні програми управління операційними ризиками, визначати критичні бізнес-функції та розробляти плани безперебійної роботи для мінімізації впливу можливих інцидентів на доступ клієнтів до їхніх активів.
7. **Страхування активів**. У документі підкреслюється важливість адекватного страхування активів, які зберігаються під управлінням постачальників послуг зі зберігання криптоактивів. Незважаючи на те, що повне страхування всіх активів може бути економічно недоцільним, провайдери повинні забезпечити достатній рівень страхування і прозоро інформувати клієнтів про умови та обмеження своїх страхових полісів.

http://surl.li/dnvyal

Еволюція транскордонних платежів: від векселів до розподілених реєстрів

Документ представляє всебічний огляд еволюції, сучасного стану та майбутнього розвитку транскордонних платежів. Він висвітлює історичний розвиток, починаючи з використання векселів і до сучасних цифрових систем, з особливою увагою до трансформаційної ролі технології розподіленого реєстру (DLT). У документі підкреслюється потенціал DLT для вирішення існуючих проблем транскордонних транзакцій, таких як високі витрати, тривалі терміни обробки та відсутність прозорості. Значна частина документа присвячена дослідженню інноваційної Платформи цифрових активів (DAP) від Blade Labs, яка спрямована на покращення взаємодії, ефективності та управління ризиками у міжнародних платежах. Також детально розглядається дорожня карта G20 щодо покращення транскордонних платежів, яка має на меті підвищення швидкості, зниження витрат, покращення доступу та прозорості, показуючи узгодженість технологічних досягнень із глобальними фінансовими цілями.

Ключові висновки:

1. **Еволюція транскордонних платежів**: Транскордонні платежі пройшли довгий шлях розвитку від використання векселів у давнину до сучасних електронних платіжних систем, таких як CHIPS (1970) і SWIFT (1973). Ці системи стали основою для стандартизації та оптимізації міжнародних фінансових повідомлень, що значно покращило швидкість та надійність платежів.

2. **Сучасний стан транскордонних платежів**: Обсяг транскордонних фінансових транзакцій продовжує стрімко зростати через глобалізацію, розвиток міжнародних ланцюгів постачання, зростання електронної комерції та збільшення обсягів грошових переказів. Прогнозується, що до 2027 року загальний обсяг транскордонних платежів перевищить 250 трлн доларів, що підкреслює необхідність подальших інновацій для управління цим зростанням.

3. **Ініціатива G20 щодо покращення транскордонних платежів**: У 2020 році G20 розробила дорожню карту, яка ставить за мету зробити транскордонні платежі швидшими, дешевшими, прозорішими та доступнішими. Вона спрямована на вирішення чотирьох ключових проблем: високих витрат, повільної швидкості, обмеженого доступу та недостатньої прозорості.

4. **Роль технології розподіленого реєстру (DLT)**: DLT пропонує низку значних переваг для транскордонних платежів, таких як створення спільної інфраструктури з розподіленим реєстром, що забезпечує покращену взаємодію між платіжними системами. Це також дозволяє значно скоротити час обробки транзакцій до рівня, близького до реального часу, що вирішує одну з основних проблем традиційних систем – тривалу обробку платежів.

5. **Переваги DLT для прозорості та ефективності**: Завдяки використанню розподіленого реєстру, DLT підвищує прозорість транзакцій, дозволяючи сторонам відстежувати платежі в режимі реального часу, що вирішує проблему прихованих витрат та невизначеності часу доставки коштів. Крім того, технологія сприяє усуненню посередників у процесі платежів, що знижує витрати та зменшує ризики.

6. **Інноваційний підхід Blade Labs**: Blade Labs розробила Платформу цифрових активів (DAP), яка дозволяє підприємствам та фінансовим установам здійснювати транскордонні платежі з підвищеною ефективністю та надійністю. Основні переваги DAP включають токенізацію активів, програмованість транзакцій, управління ризиками, зниження витрат та стандартизацію відповідно до міжнародних норм.

7. **Потенціал для інклюзії та фінансових інновацій**: DLT має великий потенціал для розширення доступу до фінансових послуг, особливо для населення з обмеженим доступом до традиційних банківських систем. Завдяки зниженню бар'єрів для входу та зменшенню витрат на перекази, технологія може стати вирішальною для розвитку інклюзивних платіжних систем, особливо в контексті грошових переказів до країн, що розвиваються.

8. **Комплаєнс та безпека**: Технології DLT пропонують нові можливості для автоматизації комплаєнсу, зокрема перевірки клієнтів (KYC) та протидією відмиванню коштів (ПВК). Смарт-контракти на основі DLT можуть автоматично виконувати регуляторні вимоги, що значно знижує ризики порушень і підвищує безпеку транзакцій у міжнародних рамках.

Документ показує, що технологічні рішення, такі як DLT, мають великий потенціал для подальшої трансформації транскордонних платежів, роблячи їх швидшими, дешевшими, прозорішими та доступнішими.

http://surl.li/ekugio

Лідерство в майбутньому відкритих та миттєвих платежів

Документ "World Payments Report 2025" охоплює глобальні зміни у сфері платежів та підкреслює важливі тенденції у фінансових технологіях, зокрема впровадження миттєвих платежів та відкритих фінансів. Він **аналізує те, як цифрові платежі поступово замінюють готівкові операції, підкреслюючи зростання кількості безготівкових транзакцій**, особливо у регіоні Азії та Тихоокеанського регіону. **Основна увага приділяється впровадженню технологій миттєвих платежів, що мають глобальний вплив і створюють нові можливості для банків та фінансових установ, а також відкритим фінансам, які розширюють межі відкритого банкінгу, забезпечуючи споживачів та бізнес доступом до персоналізованих фінансових продуктів**. Відкриті фінанси та миттєві платежі обіцяють революціонізувати фінансовий ландшафт, але прийняття цих технологій є нерівномірним у різних регіонах.

Документ також розглядає вплив інновацій на корпоративні платежі. Використання таких технологій сприяє підвищенню видимості коштів і покращенню операційної ефективності, що може бути ключовим фактором для бізнесу у різних галузях. У звіті наголошується, що банки повинні переходити від тимчасових тактичних рішень до довгострокової гнучкості транзакцій.

Серед ключових викликів для банків – потреба адаптуватися до миттєвих платежів та впроваджувати стратегії запобігання шахрайству та відмиванню коштів.

Ключові висновки:

1. **Миттєві платежі та відкриті фінанси як рушії інновацій.**

Звіт підкреслює, що поєднання миттєвих платежів та відкритих фінансів створює потужний вплив на глобальну фінансову систему. Миттєві платежі забезпечують швидкість і прозорість транзакцій, підвищують ефективність операцій та покращують обслуговування клієнтів. Відкриті фінанси, які базуються на концепції відкритого банкінгу, дозволяють користувачам і бізнесам отримувати доступ до персоналізованих фінансових продуктів завдяки обміну даними через безпечні API. Це сприяє більшій фінансовій прозорості та полегшенню взаємодії з фінансовими установами. Крім того, банки мають можливість отримувати нові джерела доходів, розширюючи спектр послуг і адаптуючи їх під потреби клієнтів. Хоча впровадження відкритих фінансів не однакове по всьому світу, їхній потенціал для трансформації фінансової індустрії величезний.

2. **Нерівномірність адаптації нових технологій у різних регіонах.**

Азіатсько-Тихоокеанський регіон (APAC) виявився лідером у впровадженні миттєвих платежів і безготівкових транзакцій, демонструючи найвищі темпи зростання на рівні 17.7% на рік. У той час як такі ринки, як Європа та Північна Америка, також демонструють значні темпи зростання, їхні ринки вже більш зрілі. Європа, наприклад, у 2023 році показала ріст на 15.5% у сфері безготівкових транзакцій, що є результатом запровадження SEPA Instant Credit Transfer та активної роботи щодо гармонізації платіжної інфраструктури. У Латинській Америці та регіоні Близького Сходу і Африки також спостерігається значне зростання, оскільки ці ринки активно переходять від використання готівки до цифрових рішень. Зокрема, Бразилія завдяки системі PIX значно підвищила популярність миттєвих платежів серед широких верств населення. Водночас, країни, що повільніше впроваджують ці технології, ризикують відстати у цифровій трансформації своїх фінансових ринків.

3. **Важливість інфраструктури для успіху миттєвих платежів.**

Однією з основних проблем для банків є потреба у модернізації своїх операційних систем, оскільки старі банківські інфраструктури часто не здатні підтримувати постійні 24/7 операції, які потребують

миттєві платежі. Банки стикаються з необхідністю переходу до безперервної обробки платежів, що вимагає значних інвестицій у технології та посилення заходів безпеки для боротьби з новими ризиками шахрайства. Ці зміни потребують значних ресурсів та часу для імплементації. Крім того, для захисту від зростання кіберзагроз та шахрайських операцій банки повинні інтегрувати передові системи запобігання відмиванню коштів та забезпечення кібербезпеки.

4. **Корпоративні платежі та реальна видимість коштів у режимі реального часу.**

У світі корпоративних фінансів миттєві платежі та відкриті фінанси пропонують безпрецедентні можливості для покращення операційної ефективності. Завдяки можливостям реальної видимості коштів компанії можуть точніше керувати грошовими потоками та покращувати прогнозування фінансів. Наприклад, миттєві платежі можуть значно спростити процеси рахунків до сплати та рахунків до отримання, що дозволить бізнесу зменшити затримки та підвищити ліквідність. Проте, багато корпоративних банківських процесів все ще не відповідають очікуванням компаній через проблеми з прогнозуванням та видимістю коштів. Це створює значні фінансові втрати, оцінювані у мільярди доларів щорічно.

5. **Необхідність стратегічного бачення для банків.**

Перехід від тимчасових тактичних рішень до довгострокової стратегії є важливим викликом для банків. В умовах, коли конкурентний тиск з боку фінтех-компаній та небанківських платіжних провайдерів зростає, банки повинні шукати нові способи адаптації. Використання моделей Payment-as-a-Service (PaaS) стає популярним шляхом для прискорення переходу до більш гнучких і масштабованих систем платежів. Банки, які впроваджують інноваційні рішення на основі хмарних технологій, можуть не лише швидше адаптуватися до мінливих умов ринку, а й покращити взаємодію з клієнтами, пропонуючи нові продукти та послуги. Успішна адаптація до цих умов вимагає інтеграції миттєвих платежів і відкритих фінансів як ключових елементів банківської стратегії.

6. **Можливості для подальшого зростання цифрових платежів.**

Важливими факторами зростання цифрових платежів залишаються як регуляторні ініціативи, так і нові індустріальні ініціативи. Наприклад, впровадження цифрових валют центральних банків (CBDC) та подальший розвиток стандартів, таких як ISO 20022, сприятимуть гармонізації міжнародних платежів і створять умови для розвитку нових фінансових продуктів. Крім того, активна робота над інтеграцією систем миттєвих платежів між країнами, як це робить APAC через QR-код платежі, може значно спростити міжнародні транзакції та сприяти фінансовій інклюзії.

Ці висновки вказують на те, що для того, щоб залишатися конкурентоспроможними та отримувати нові можливості для розвитку, банки та фінансові установи повинні гнучко адаптуватися до змін та впроваджувати інноваційні технології, зокрема миттєві платежі та відкриті фінанси.

https://www.capgemini.com/wp-content/uploads/2024/09/WPR_2025_web.pdf

ІНШІ НОВИНИ

Екс-глава Swedbank Біргітте Боннесен отримала 15 місяців ув'язнення за скандал з відмиванням коштів в Естонії

Голову правління «Swedbank» Біргітте Боннесен було засуджено до 15 місяців ув'язнення за шахрайство та відмивання коштів в естонській філії «Swedbank».

Звільнену з посади у 2019 році Брігітте було виправдано за іншими звинуваченнями, висунутими проти неї, і, як повідомляється, вона подасть апеляцію на це рішення.

За повідомленнями ЗМІ, шведський апеляційний суд визнав колишню генеральну директорку «Swedbank» Біргітте Боннесен винною у грубому шахрайстві під час виконання нею процедур з протидії відмиванню коштів в Естонії, засудивши її до 15 місяців ув'язнення.

Засудження Боннесен стало наслідком двох інтерв'ю, які вона дала шведським ЗМІ в жовтні 2018 року, під час яких суд визнав, що вона надала «оманливе повідомлення» щодо проблем «Swedbank» з відмиванням коштів в його естонській філії.

Хоча Боннесен була визнана винною за одним пунктом, з неї було знято шість додаткових звинувачень, включаючи грубе шахрайство і маніпулювання ринком, згідно з рішенням суду.

Апеляційний суд встановив, що Боннесен надала недостовірну інформацію під час інтерв'ю шведській газеті «Svenska Dagbladet» та інформаційному агентству «TT», що стосувалися звіту «Swedbank» за третій квартал 2018 року.

Обвинувальний вирок колишньому генеральному директору «Swedbank» є знаковою подією для спільноти, що займається питаннями комплаєнсу у сфері протидії відмиванню коштів, оскільки ця справа є одним з найбільших скандалів у Європі з відмивання коштів, в якому обвинувачення було висунуто керівнику банку.

Ця справа, ймовірно, матиме величезний вплив на формування ставлення топ-менеджменту до комплаєнсу в сфері протидії відмиванню коштів.

Справа Swedbank також підкреслює вразливість країн Балтії до відмивання коштів, особливо після російсько-української війни, оскільки ці країни розташовані в безпосередній близькості до Росії. Європейським банкам, розташованим у цьому регіоні, можливо, доведеться посилити свої правила протидії відмиванню коштів через їхню вразливість до використання суб'єктами, що підпадають під санкції та експортний контроль.

https://is.gd/wDrID6

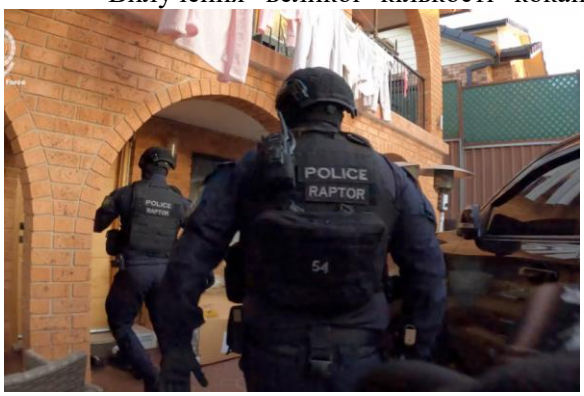
Поліція Нового Південного Уельсу ліквідувала велику злочинну мережу «The Commission», яка ймовірно пов'язана з продажем наркотиків на 1,8 мільярда доларів

Новина стосується масштабної операції поліції Нового Південного Уельсу (NSW) з ліквідації великої кримінальної мережі, яка займалася торгівлею кокаїном. У результаті цієї операції було розкрито організовану злочинну групу, що брала участь у продажі наркотиків на мільярди доларів.

Основні моменти операції включають:

- Розкриття масштабної мережі торгівлі наркотиками, яка працювала на території Сіднея та інших частин Нового Південного Уельсу.

- Вилучення великої кількості кокаїну, а також арешт ключових осіб, пов'язаних із злочинними угрупуваннями.



- Операція стала результатом тривалого розслідування, що базувалося на розвідувальних даних і залученні спеціалізованих підрозділів поліції.

Ця кримінальна мережа є однією з найбільших у регіоні, і її ліквідація вважається значним кроком у боротьбі з торгівлею наркотиками в Австралії. Поліція зазначає, що ця мережа не лише поширювала кокаїн, але й брала участь в інших злочинах, зокрема відмиванні коштів і корупції.

Співробітники поліції виявили великі суми готівки та активи, що свідчить про масштаб операцій злочинців. Важливим аспектом операції стало також захоплення осіб, які керували мережею. Операція тривала протягом кількох місяців і стала результатом співпраці різних правоохоронних структур.

Ця операція є значним кроком у боротьбі з наркоторгівлею в регіоні, підкреслюючи важливість комплексних заходів, спрямованих на ліквідацію великих кримінальних мереж.

https://www.abc.net.au/news/2024-09-19/nsw-sydney-underworld-cocaine-drug-bust/104370116

Компрометація корпоративної електронної пошти: афера на 55 мільярдів доларів

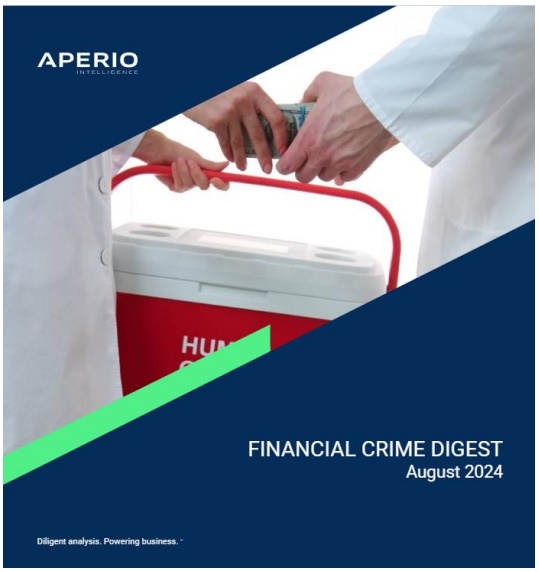
Федеральне бюро розслідувань (ФБР) опублікувало попередження для фінансових установ, у якому вказується масштаб шахрайства, пов’язаного з компрометацією корпоративної електронної пошти (BEC), яке, за їхніми підрахунками, призвело до збитків у розмірі 55 мільярдів доларів США між 2013 і 2023 роками. Шахрайство здійснюється, коли законні корпоративний або особистий обліковий запис електронної пошти зламано через соціальну інженерію або комп’ютерне вторгнення з метою здійснення несанкціонованих переказів коштів. У період з грудня 2022 року по грудень 2023 року кількість виявлених глобальних втрат зросла на 9%. У 2023 році зросла кількість звітів BEC, у яких кошти надсилалися безпосередньо до фінансових установ, де розміщені кастодіальні рахунки, які тримають сторонні платіжні процесори, однорангові платіжні процесори та криптобіржі.

Жертви шахрайства BEC повинні негайно звернутися до свого банку та правоохоронних органів, оскільки кошти можуть бути повернуті. У повідомленні ФБР також надано поради щодо запобігання, які можуть застосувати компанії.

https://www.ic3.gov/Media/Y2024/PSA240911

Financial Crime Digest

Документ "Financial Crime Digest" охоплює основні події та новини у сфері протидії відмиванню коштів та фінансуванню тероризму за серпень. У дайджесті розглянуто актуальні випадки фінансових злочинів, нові законодавчі ініціативи, а також ключові рішення регуляторів, спрямовані на боротьбу з фінансовими злочинами на глобальному рівні.



Огляд ключових новин з ПВК/ФТ:

1. Регулювання криптоактивів

Посилення регулювання криптовалют стало глобальною тенденцією у відповідь на їхнє дедалі частіше використання для відмивання коштів (ПВК) та фінансування тероризму (ФТ). Зокрема, кілька країн розробили нові правила щодо AML/CFT для криптопровайдерів, включаючи суворіші вимоги до реєстрації, звітності та перевірки клієнтів.

2. Банківський нагляд та транзакції

Великі фінансові установи перебувають під постійним тиском для дотримання нових стандартів щодо перевірки підозрілих транзакцій та поліпшення прозорості у фінансових операціях. Зокрема, в декількох юрисдикціях впроваджуються додаткові вимоги щодо розкриття інформації та контролю над транзакціями, особливо при роботі з клієнтами з високим рівнем ризику.

3. Порушення санкційних режимів

Важливим моментом серпня стало кілька гучних справ, пов'язаних із порушенням санкцій. Виявлено, що деякі компанії та особи намагалися обходити санкції через треті країни. Це призвело до посилення міжнародного контролю та співпраці між регуляторами для виявлення таких схем та запобігання майбутнім порушенням.

4. Міжнародне співробітництво

Серпень ознаменувався підписанням нових угод між різними юрисдикціями про обмін фінансовою інформацією та співпрацю у розслідуванні випадків ПВК та ФТ. Особливо важливим стало посилення співробітництва у протидії фінансуванню тероризму та поширенню зброї масового знищення (ЗМЗ), що стало ключовим викликом для багатьох міжнародних організацій.

Ці новини демонструють, як світові регулятори адаптуються до нових викликів у сфері боротьби з фінансовими злочинами, зокрема у сфері криптовалют, міжнародної торгівлі та співпраці в рамках глобальної системи ПВК/ФТ.

https://www.aperio-fcd.com/fcd-monthly?report_id=93

Ключові крипто новини минулого тижня

1. 1inch Network представляє новий кросс-чейн протокол обміну

1inch запустив протокол 1inch Fusion Atomic Swap, який обіцяє безпечні кросс-чейн свопи між мережами L1 і L2. Цей гібридний протокол усуває вразливості крос-чейн мостів і зміцнює інфраструктуру DeFi.

2. Sony вдосконалює блокчейн Soneium за допомогою інтеграції Chainlink

Sony співпрацює з Chainlink, щоб покращити масштабованість і розвиток блокчейну Soneium. Інтеграція викликала 10% зростання ціни токена Chainlink, що зміцнило його позиції.

3. Ether.fi Запускає Visa Crypto Card у Scroll Network

Ether.fi представили картку Visa, яка використовує мережу Scroll, що дозволяє користувачам використовувати криптовалюту для щоденних покупок. Картка пропонує кешбек 3% і інтегрується з Apple Pay для легких транзакцій.

4. Circle розширює підтримку USDC на Arbitrum

Circle інтегрував Arbitrum у свою платформу Web3, розширивши утиліту USDC для глобальних платежів, електронної комерції та ігор. Цей крок позиціонує USDC як найсильнішого конкурента Tether.

5. Власники токенів Starknet схвалюють механізм стейкінгу

Власники токенів Starknet переважною більшістю голосів (98% - за) проголосували за впровадження стейкінгу. Нова система стейкінгу буде запущена в 4 кварталі 2024 року, пропонуючи винагороди для користувачів, які володіють понад 20 000 STRK.

ДЛЯ ЗАГАЛЬНОГО РОЗВИТКУ

Що таке номінальні угоди

Номінальна угода — це коли фізична чи юридична особа (номінальний представник) призначається діяти від імені іншої фізичної чи юридичної особи з метою приховування особи справжнього вигодоодержувача.

По суті, номінальний представник діє як «прикриття», тоді як справжній власник або контролер залишається анонімним. Ці угоди можуть бути формальними (з письмовою угодою) або неформальними (без письмової угоди). Хоча номінальні угоди можуть служити законним цілям, вони також схильні до зловживань.

Як номінальні угоди використовувати легально?

↳ **Приватність**: Номінальні представники захищають особистість осіб, які не бажають публічно асоціюватися з активами чи бізнесом.

↳ **Корпоративні операції**: у корпоративних структурах номінальні особи часто використовуються для тимчасового утримання активів або акцій для справжнього власника, зберігаючи конфіденційність або для спрощення правових вимог, особливо під час злиття та поглинання.

↳ **Планування майна**[5]: номінальні особи можуть керувати активами від імені бенефіціарів, особливо якщо бенефіціари неповнолітні або не можуть самостійно керувати активами.

Але номінальні угоди також можуть бути використані для незаконних цілей, зокрема:

↳ Приховування справжньої власності з метою відмивання коштів

↳ Ухилення від сплати податків

↳ Ухилення від юридичної відповідальності

↳ Ухилення від санкцій

↳ Шахрайство та корупція

Фахівцям з ПВК складно відрізнити законну номінальну угоду від незаконної. Завжди глибше вивчайте бенефіціарну власність і переконайтеся, що ваші процеси протидії відмиванню коштів стосуються можливого зловживання номінальними власниками.

Що вважається стейблкоїном відповідно до MiCA?

Стейблкоїни стали перспективною альтернативою волатильним криптовалютам, пропонуючи користувачам відносну стабільність. Однак крах Terra Luna в 2022 році підкреслив ризики, пов'язані з цими токенами. Ці стейблкоїни втратили свою прив'язку до долара США, що спричинило значні збитки для інвесторів.

Які зміни відбудуться з MiCA?

[5] це процес планування та управління розподілом активів і майна людини після її смерті або в разі непрацездатності. Метою такого планування є забезпечення того, щоб майно було передане відповідно до бажань власника з мінімальними податковими наслідками, правовими витратами та конфліктами між спадкоємцями. До елементів estate planning можуть входити складання заповіту, створення трастів, призначення опікунів для неповнолітніх, а також планування податків і управління активами на випадок неспроможності.

Регулювання ринку криптоактивів (MiCA), європейське регулювання криптовалют, визнає три категорії стейблкоїнів:

1. **Токени, прив’язані до активів (ARTs)**

↳ ARTs призначені для забезпечення стабільності та передбачуваності в порівнянні з традиційними криптовалютами, ціна яких може бути волатильною. Вони зберігають стабільну вартість, прив’язуючись до іншого активу або їх комбінації, включаючи одну або кілька офіційних валют.

2. **Токени електронних грошей (EMTs)**

↳ EMTs — це тип криптовалюти, спеціально розроблений для використання як засіб платежу.

Вони зазвичай підкріплені однією фіатною валютою, такою як євро або долар США. EMTs підлягають жорсткішому регулюванню, ніж інші типи криптовалют, що покликано захистити споживачів та сприяти фінансовій стабільності.

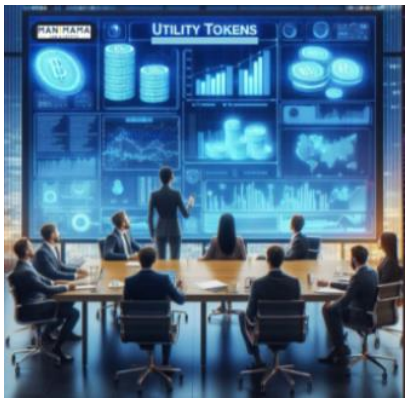
3. **Інші криптоактиви, окрім ARTs та EMTs**

↳ Ця категорія охоплює всі криптоактиви, що не підпадають під визначення ART або EMT, — широкий спектр токенів, таких як токени корисності, інвестиційні токени та токени децентралізованих фінансів (DeFi).

А як щодо алгоритмічних стейблкоїнів?

Алгоритмічні стейблкоїни, які використовують складні алгоритми для підтримки своєї вартості, не будуть вважатися стейблкоїнами відповідно до MiCA. Той факт, що алгоритмічні стейблкоїни не підпадають під визначення стейблкоїнів, матиме наслідки для існуючих проєктів алгоритмічних стейблкоїнів, що працюють в ЄС.

Регулювання токенів корисності згідно з MiCA



Регуляція токенів корисності (utility tokens) у межах MiCA (Regulation (EU) 2023/1114) визначає чіткі правила для цих активів, які призначені для фінансування криптопроєктів і надання доступу до товарів або послуг, пропонованих емітентом токенів. На відміну від інших токенів, таких як токени, які прив’язані до активів чи токени електронних грошей, токени корисності не зобов'язані підтримувати стабільну вартість і можуть коливатися залежно від попиту і пропозиції. MiCA також визначає вимоги щодо прозорості, реєстрації та звітності для емітентів токенів, які планують торгувати на відкритих ринках.

Зокрема, емітенти токенів повинні діяти професійно, відкрито інформувати користувачів та забезпечувати дотримання безпеки в обміні токенами. Якщо токени надають доступ до послуги або продукту, що вже існують, вони можуть бути звільнені від обов'язкової публічної пропозиції. Однак це виключення не діє, якщо емітент заявляє про намір торгувати токенами на публічних біржах.

Ключові моменти щодо регулювання токенів корисності відповідно до MiCA:

1. Визначення токенів корисності

Токени корисності — це криптоактиви, що створені для фінансування проєктів і надають доступ до товарів або послуг, пропонованих емітентом. Вони не функціонують як засіб обміну (як електронні гроші) чи засіб збереження вартості (як токени, прив'язані до активів). Їх вартість може коливатися

в залежності від попиту, пропозиції та корисності самого токена. Ключовим аспектом є те, що такі токени зазвичай використовуються у межах певної платформи або екосистеми, створеної емітентом, створюючи замкнену систему.

2. Принципи регулювання для емітентів токенів корисності

Відповідно до MiCA, емітенти токенів корисності повинні виконувати певні зобов'язання, зокрема:

- Діяти чесно, справедливо та професійно.
- Інформувати власників і потенційних власників токенів прозоро та без обману.
- Виявляти, запобігати, керувати та розкривати конфлікти інтересів.
- Забезпечувати безпеку своїх систем і протоколів відповідно до стандартів ЄС.

3. Вимоги до білої книги

Емітенти, що планують публічні пропозиції своїх токенів, повинні підготувати білу книгу (white paper), яка має містити детальну інформацію про проєкт, емітента, права власників токенів, ризики, технологію, що використовується, та можливі впливи на довкілля. Важливо, щоб інформація була чіткою, чесною та не вводила в оману користувачів. Біла книга також повинна бути надана відповідним органам у країнах-членах ЄС і бути опублікована для загального доступу.

4. Виключення з вимог MiCA

Токени корисності можуть бути звільнені від деяких вимог MiCA, якщо вони використовуються виключно для доступу до товарів або послуг, що вже існують на ринку і не призначені для публічної торгівлі. Однак, якщо емітент або третя сторона планує торгівлю цими токенами на публічних біржах, вони повинні дотримуватись усіх правил, включно з підготовкою білої книги.

5. Маркетингові повідомлення

Усі маркетингові матеріали щодо токенів корисності повинні бути чітко визначеними як такі. Вони мають відповідати інформації в білій книзі та не вводити в оману. Крім того, якщо в токена є біла книга, маркетингові повідомлення повинні вказувати на її наявність і містити контактні дані емітента або платформи для отримання додаткової інформації.