ОБЗОР ПРАВИЛ КРИПТО ПЕРЕВОДОВ Travel Rule

Распространение
в Российской Федерации

PALMINA
INVEST

incore
gwp

Русский перевод оригинальной версии с английского языка «Travel Rule Report»

Введение

Появление блокчейн технологий и их использования для финансовых/платежных услуг стало в последнее десятилетие одним из главных изменений в мировой финансовой системе. Эта новая тенденция принесла инновации, повысила эффективность и привела к появлению альтернативных финансовых инструментов.

Крипто-валюты или виртуальные активы (VA), как часть финансовых рынков, привлекли внимание регулирующих органов, в том числе Группы Разработки Финансовых Мер по Борьбе с Отмыванием Денег (FATF). Как международный орган, устанавливающий стандарты, FATF вырабатывает рекомендации по борьбе с отмыванием денег и правила по осуществлению финансовых переводов, которые впервые были введены в 2012 году. Эти стандарты требуют обмена данными о клиентах между финансовыми посредниками. Стандарты пересматриваются и обновляются на регулярной основе.

Данный обзор познакомит Вас с новыми правилами для крипто переводов (транзакций), даст ответ на вопрос, как финансовые посредники могут соблюдать эти стандарты, и продемонстрирует различия между регулированием стран, которые уже внедрили эти рекомендации.

Кроме этого, в отчете дается технический обзор существующих протоколов, которые могут быть внедрены в соответствии с правилами крипто переводов.

Цюрих, декабрь 2020

Содержание

1 Обзор правовой ситуации

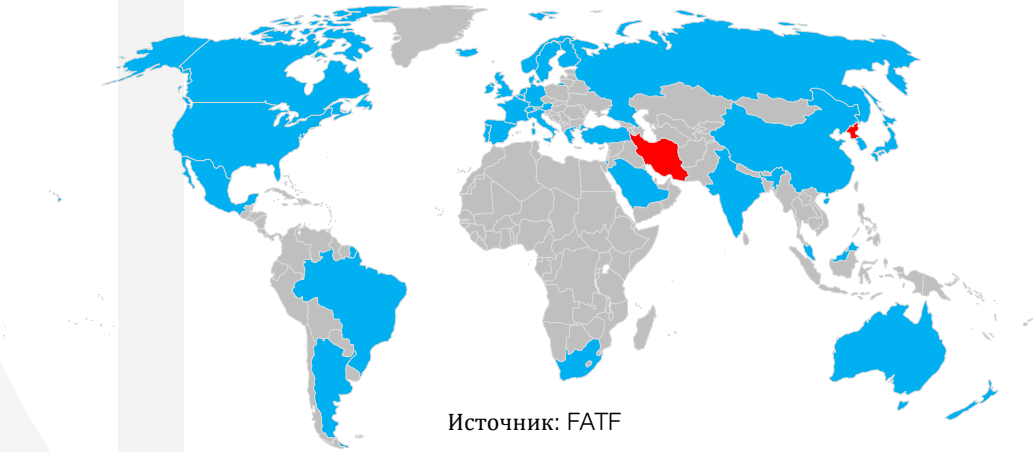
Эволюция правил переводов

Правило переводов было впервые введено в 1996 году Агентством по борьбе с финансовыми преступлениями (FinCEN), федеральным бюро Министерства финансов США, в соответствии с которым банки и компании, оказывающие денежные услуги, должны обмениваться информацией как об отправителях, так и о получателях платежей, связанных с платежами на сумму 3'000 долларов США и выше. В 2012 году в перечень отчитываемых транзакций были внесены изменения, включающие электронные денежные переводы.

FATF приняла правило переводов только в 2012 году в соответствии со своими рекомендациями. К 2018 году регуляторы по всему миру ужесточили крипто регулирование, и возникла необходимость в применении правила переводов к виртуальным активам (VA) и поставщикам услуг в области виртуальных активов (VASP).

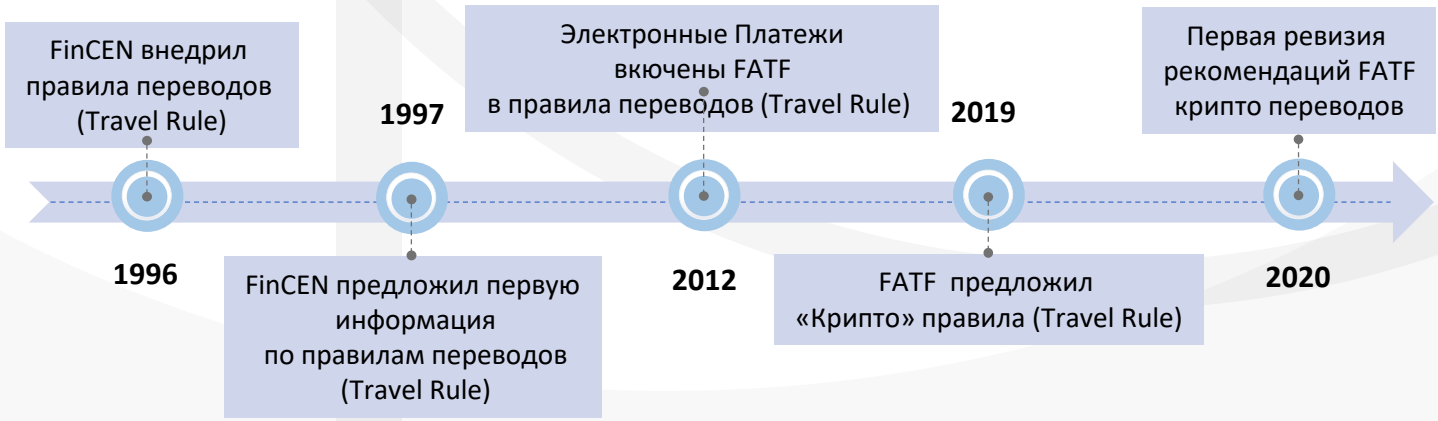
В июне 2019 года FATF предложила глобальные стандарты в отношении обмена информацией о бенефициарах и отправителях между поставщиками услуг виртуальных активов (VASP) на основе правила, разработанного FinCEN в Соединенных Штатах. Субъектами, на которые распространяются эти правила, являются крипто-валютные биржи, кошельки для хранения, децентрализованные биржевые операторы или другие субъекты, определение которых основано на толковании правил в каждой конкретной юрисдикции.

Страны - члены FATF (синий) и черный список (красный)



Источник: FATF

Эти "правила" переводов средств предназначены для оказания поддержки правоохранительным органам в выявлении, расследовании и преследовании за преступления связанные с отмыванием денег и другие финансовые преступления путем сохранения информационного следа о лицах, отправляющих и получающих средства через системы перевода средств.



Требования к правилам переводов

Все требования, изложенные в Рекомендации 16 FATF, применяются к Поставщикам Услуг в Области Виртуальных Активов (VASPs) и другим задействованным организациям, которые связаны с переводами виртуальных активов, включая обязательства по получению, хранению и передаче требуемой информации об отправителе и получателе для того, чтобы идентифицировать и сообщать о подозрительных операциях, контролировать доступность информации, принимать меры по замораживанию и запрещать операции с подозреваемыми лицами и организациями.

Поэтому страны должны обеспечить выполнение учреждениями-посредниками или другими обязанными организациями, такими как финансовые посредники, участвующими в передаче виртуальных активов (VA), получения и хранения требуемой достоверной информации об отправителе и требуемой информации о получателе, а также представления этой информации учреждениям-бенефициарам. Точная информация изложена в следующей выдержке из руководства FATF по применению риск-ориентированного подхода к Виртуальным Активам (VA) и Поставщикам Услуг в Области Виртуальных Активов (VASPs):

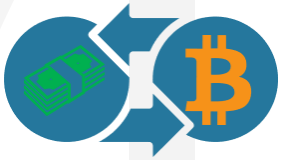
Выдержка из рекомендаций FATF (июнь 2019 года).
Рекомендации, основанные на оценке рисковых параметров при работе с виртуальными активами и поставщиками услуг, связанных с виртуальными активами.
FATF, Париж

“Требуемая информация включает в себя

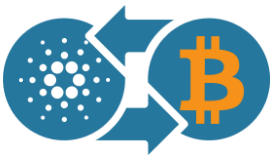
- имя инициатора перевода (т.е. отправителя);
- номер счета отправителя (например, кошелек с виртуальными активами);
- физический (географический) адрес отправителя или национальный идентификационный номер, или идентификационный номер клиента (отличный от номера транзакции), который идентифицирует отправителя в учреждении заказчика, или дата и место рождения;
- имя получателя;
- номер счета получателя, если такой счет используется для обработки операции (например, кошелек с виртуальными активами). Нет необходимости прикреплять информацию непосредственно к самому переводу виртуальных активов. Информация может быть представлена как прямо, так и косвенно, как указано в Пояснительной записке к Рекомендации (INR) 15".

Кто подпадает под категорию VASP

Провайдеры услуг, которые характеризуются как поставщики услуг виртуальных активов (VASPs)



Фиат-Крипто Обменники



Крипто Биржи

Платежные Системы

Выпускающие токены

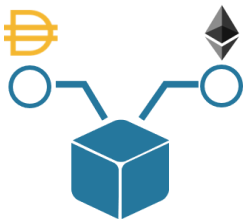
Крипто Банкоматы

Услуги Хранения Кошельков (Кастоди)

Крипто Фонды

Провайдеры услуг, которые могут характеризоваться как поставщики услуг виртуальных активов (VASPs)

P2P



DeFi

DApps

Согласно определению FATF, поставщиком услуг виртуальных активов (VASP) может быть любое физическое или юридическое лицо, которое предоставляет эти услуги в рамках своей деятельности:

- Обмен фиата на виртуальные активы;
- Обмен виртуальных активов;
- Передача виртуальных активов;
- Хранение виртуальных активов; или
- Деятельность, связанная с выпуском или андеррайтингом цифровых активов.

Ревизия FATF в июне 2020

В июне 2019 года FATF завершила работу над поправками к своим глобальным стандартам, чтобы четко разъяснить требования по борьбе с отмыванием денег и финансированием терроризма при работе с виртуальными активами. FATF также согласилась провести 12-месячную ревизию для оценки темпов внедрения пересмотренных стандартов юрисдикциями и частным сектором, а также мониторинга любых изменений в типологии, рисках и рыночной структуре сектора виртуальных активов.

В обновленном докладе FATF за 12-месячный период, начиная с июня 2020 года, было выявлено несколько проблем, связанных с пересмотренными стандартами и рекомендациями FATF. Проблемы были определены с помощью обратной связи FATF с участниками контактных групп, задействованных в работе с виртуальными активами. В докладе отмечается, что новые требования по борьбе с отмыванием денег и финансированием терроризма принимаются большинством стран - членов FATF. Аналогичным образом, достигнут прогресс в разработке технологических решений для правил переводов. Однако не все члены глобальной сети FATF сообщили о том, что к июню 2020 года были приняты меры в соответствии с измененными стандартами. Исследование, проведенное FATF, также показало, что во многих странах до сих пор широко распространено несоблюдение правил перевода, а также выявлены случаи полного игнорирования новых требований.

Поскольку юрисдикции должны адаптировать пересмотренные стандарты FATF в своих национальных законодательствах, были определены области, в которые можно было бы внести большую ясность. Например, в контексте так называемых стейблкоин (stablecoins), следует ли юрисдикциям относиться к ним как к традиционным или виртуальным активам. Кроме того, необходимо разработать более четкие указания в отношении хранения, управления или передачи виртуальных активов.

В ближайшее время ожидается позитивная динамика

Следующая 12-месячная ревизия внедрения в крипто индустрии стандарта FATF назначена на июнь 2021 года. Недавние регулятивные меры FATF также включают тематические публикации выявляющие риски «red flags indicators» для поддержки дальнейшего понимания рисков отмывания денег и финансирования террористической деятельности, связанных с крипто индустрией.

К числу других вопросов, требующих рассмотрения, относятся частные переводы виртуальных активов, когда поставщик услуг виртуальных активов (VASP) не участвует в качестве посредника и такие виды операций прямо не подпадают под действие обязательств по контролю за операциями по отмыванию денег и противодействию террористической деятельности, в соответствии с пересмотренными стандартами FATF. Отсутствие четкого охвата частных (peer-to-peer) операций через частные кошельки вызывает озабоченность в ряде юрисдикций, включая Швейцарию. Согласно докладу, анонимные или частные сделки не претерпели существенных изменений с июня 2019 года. В связи с недостаточностью доказательств авторы делают вывод о том, что такие частные сделки не создают повышенного риска отмывания денег и террористической деятельности.

Однако запуск новых виртуальных активов может изменить риски отмывания денег и террористической деятельности, особенно если существует массовое принятие активов, которое позволяет проводить анонимные частные сделки. Например, если власти сочтут риск слишком высоким, они, возможно, запретят или откажут в лицензировании платформ, которые позволяют осуществлять передачу частных «unhosted» кошельков, введут лимиты на транзакции/объемы или установят обязательный порядок проведения операций с использованием проверки на риск отмывания денег и террористической деятельности.

Поиск стандартизированного решения

Для того, чтобы соответствовать правилу переводов, в процессе взаимодействия с контрагентом поставщик услуг виртуальных активов (VASP) должен быть в состоянии определить легальный статус контрагента в юрисдикции проведения сделки и убедиться, что транзакции выполняются надлежащим образом с учетом правил проверки на риск отмывания денег и риск террористической деятельности. Вопрос заключается в том, как своевременно и безопасно провести надлежащую проверку контрагента. Одним из предлагаемых способов может быть создание глобального списка контрагентов, в котором будет обобщаться информация из всех юрисдикций и доступ к ней будет осуществляться через согласованную центральную базу данных. Но управление такой базой данных будет децентрализовано и координироваться участниками рынка. В связи с этим предложением частного сектора возникает вопрос кто будет отвечать за сбор и хранение информации, кем этот процесс будет контролироваться и кому разрешать доступ к данным.

Решение могло бы заключаться в том, чтобы делегировать ответственность стран - членов FATF за ведение локального списка поставщиков услуг виртуальных активов. Этот вариант все еще вызывает те же самые вопросы, о том, как и кем он должен управляться. Все эти требования должны быть удовлетворены до того, как будет разработано решение.

Как адаптируются правила платежей в Швейцарии?

Швейцария

Разъяснения Швейцарского регулятора FINMA по блокчейн транзакциям от 02/2019 гласит, что поставщики услуг виртуальных активов обязаны, например, проверять личность своих клиентов, устанавливать личность выгодоприобретающего собственника, применять риск-ориентированный подход к мониторингу деловых отношений и при наличии достаточных оснований подозревать отмывание денег и подавать отчет в Управление по отчетности в области борьбы с отмыванием денег Швейцарии (MROS). В отличие от стандартов FATF, Статья 10 AMLO-FINMA не предусматривает никаких исключений для платежей с участием нерегулируемых поставщиков кошельков.

Такое исключение благоприятствовало бы неподнадзорным поставщикам услуг и привело бы к тому, что поднадзорные поставщики не смогли бы предотвратить осуществление «подозрительных платежей».

Высокие стандарты Швейцарии в отношении соблюдения законодательства по борьбе с отмыванием денег и предотвращением терроризма (AML/CTF) в отношении виртуальных активов подразумевают определенные трудности для швейцарских посредников в сотрудничестве с другими юрисдикциями. Не так много юрисдикций вводят аналогичные высокие стандарты. Исключением может быть Сингапур (MAS, Закон о платежных услугах, 2019 г.) или США (FinCEN, руководство для поставщиков услуг виртуальных активов (VASPs), май 2019 г.), которое включает применение правила переводов. Высокие требования к стандартам, различия в подходах и непоследовательность требований в других странах затрудняют надлежащую функциональность и соблюдение требований к транзакциям между Швейцарией и другими странами, где требования к нерегулируемым кошелькам менее строгие или неопределенные. Это также приведет к удорожанию сделок. Эта тема требует более тщательной проработки со стороны FATF.

Швейцарский регулятор характеризует поставщиков услуг виртуальных активов профессиональными финансовыми посредниками (ФП), если они отвечают следующим критериям:

а) доход в размере более 50 000 швейцарских франков за календарный год;

б) установлены деловые отношения с более чем 20 договаривающимися сторонами, которые взаимодействуют с ФП более одного раза в календарный год;

в) неограниченный контроль над средствами третьих лиц, превышающими 5 млн. швейцарских франков, или

г) осуществляет операции в объеме более 2 млн. швейцарских франков в год.

Сравнение соответствия рекомендациям в Швейцарии, США и Сингапуре

В отличие от стандартов FATF, статья 10 AMLO-FINMA в Швейцарии не предусматривает никаких исключений для платежей с участием нерегулируемых поставщиков кошельков. Такое ограничение препятствует сделкам с неконтролируемыми поставщиками и предотвращает подозрительные платежи.

До тех пор, пока учреждение, находящееся под надзором FINMA, не сможет отправлять и получать информацию, необходимую для проведения платежных операций, такие операции разрешены только с подтвержденными кошельками, принадлежащими клиенту данного учреждения. Право собственности на кошелек должно быть доказано с помощью соответствующих технических средств. Сделки между клиентами одного и того же учреждения разрешены. Перевод с внешнего кошелька или на внешний кошелек, принадлежащий третьему лицу, возможен только в том случае, если контролирующее сделку учреждение провело предварительную проверку и установило личность третьего лица, личность бенефициарного владельца и с помощью подходящих технических средств доказал право собственности третьего лица на внешний кошелек.

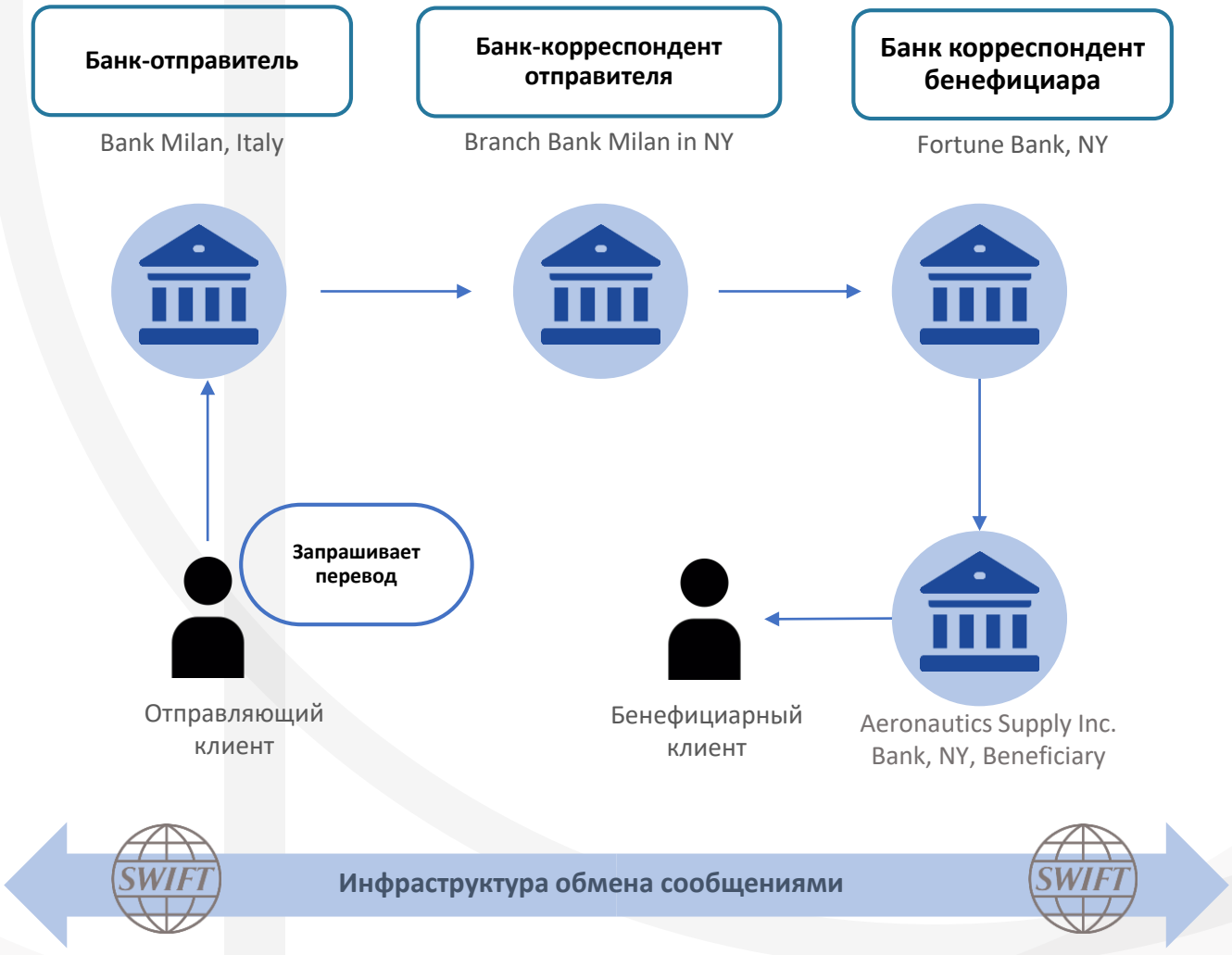
	Швейцария AMLO 02/2019	**FATF** R.16 Travel Rule	**США FinCEN** Travel Rule	**Сингапур** PSA
Минимальная сумма транзакции, требующая проверки	Более 1000 CHF (применимо с 01/2021)	Финансовый посредник должен делиться информацией по транзакциям более 1000 USD или EURO	Более USD 1,000	Более $1,500
Данные отправителя	• Имя • Номер счета • Адрес проживания, номер паспорта или дата и место рождения	• Имя • Номер счета • Адрес проживания, номер паспорта или дата и место рождения	• Имя • Номер счета • Адрес проживания	• Паспорта или свидетельство о рождении • Паспорт или Бизнес сертификат
Данные бенефициара	• Имя • Номер счета	• Имя • Номер счета	• Имя • Номер счета • Уникальный идентификатор	• Имя • Номер счета • Уникальный идентификатор

2 Внедрение нового стандарта

От SWIFT к “Крипто SWIFT»

Обеспечение исторического контекста - SWIFT может быть решением для VASP и VA. Протокол правил переводов можно сравнить с функциональностью SWIFT. Чтобы решить проблему трансграничных платежей в сфере коммуникаций, в 1973 году банки сформировали кооперативное предприятие - Общество Всемирных Межбанковских Финансовых Телекоммуникаций (SWIFT) со штаб-квартирой в Бельгии.

SWIFT запустил свои службы обмена сообщениями в 1977 году, заменив технологию Telex, которая преимущественно использовалась для обмена сообщениями. Основные компоненты исходных служб включали платформу обмена сообщениями, компьютерную систему для проверки и маршрутизации сообщений, а также набор стандартов сообщений. Стандарты были разработаны, чтобы обеспечить общее понимание данных через лингвистические и системные границы, а также обеспечить беспрепятственную автоматическую передачу, получение и обработку сообщений, которыми обмениваются пользователи. Прервав ручные процессы, которые были нормой в прошлом, SWIFT теперь представляет собой глобальную финансовую инфраструктуру, которая охватывает все континенты, более 200 стран и территорий и обслуживает более 11 000 учреждений по всему миру.



Источник: FinCEN

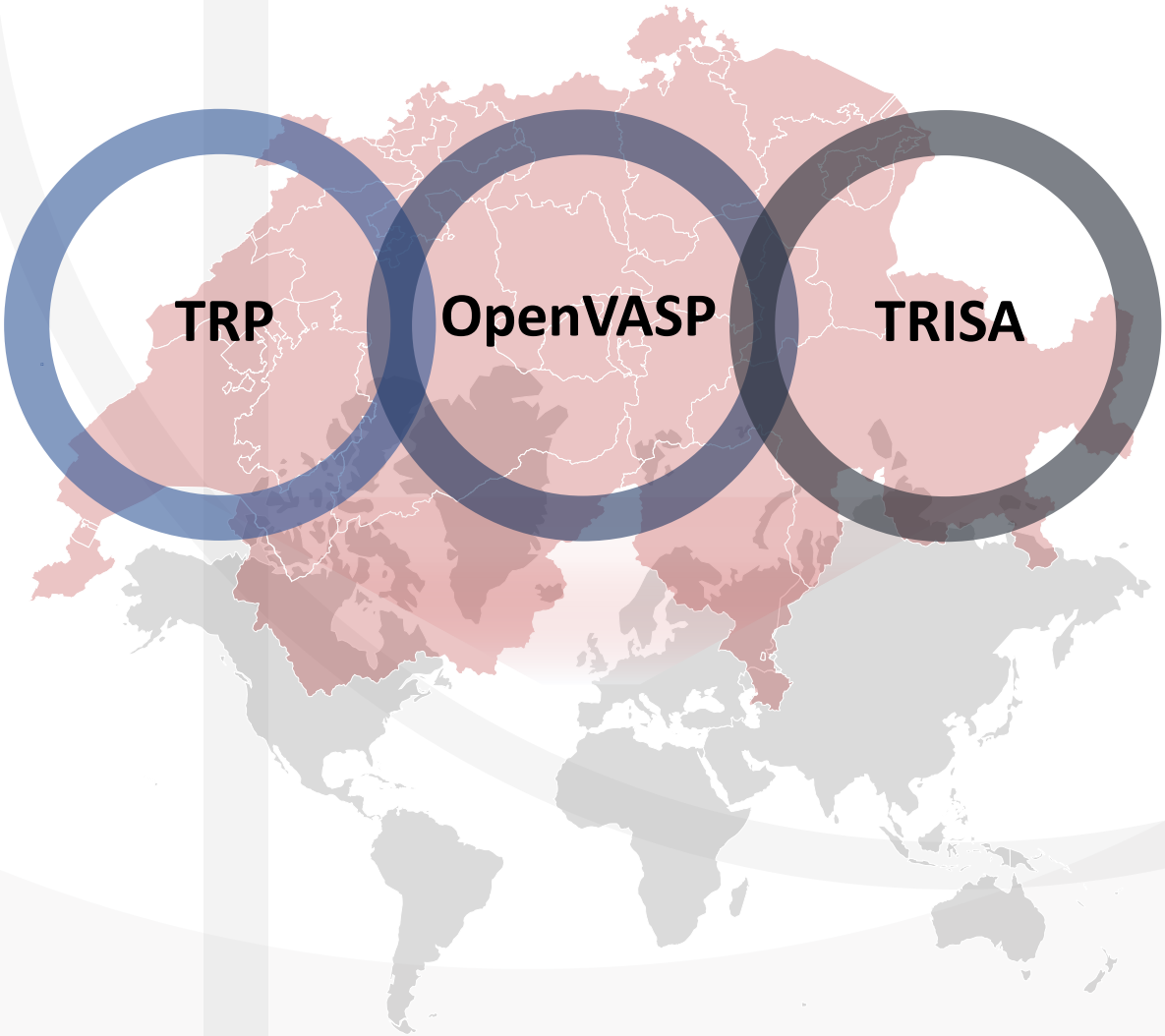
Глобальный обзор «Протоколов»

С лета 2019 года многие разработчики и компании сосредоточились на внедрении решения или протокола, максимально приближенного к рекомендациям FATF. В большинстве случаев за протоколом не стоят центральные органы или организации, а есть ряд ведущих отраслевых участников со всего мира, которые объединились в группы и открыто участвуют в реализации и дальнейшей разработке решения. Несмотря на то, что все они преследуют единую цель - создать простое решение, которое не будет налагать ненужных дополнительных требований, интегрироваться в существующий бизнес-решения и обеспечивать возможность взаимодействия, выбранные подходы различаются по своей основной архитектурной философии.

Есть несколько ведущих разработчиков и компаний, которые уже представили свой подход к рынку. Некоторые из них все еще находятся на стадии тестирования, другие уже запущены. К августу 2020 года произошла первая передача данных между двумя швейцарскими VASPs с использованием протокола TRP, реализованного в качестве программного решения швейцарским разработчиком программного обеспечения 21 Analytics.

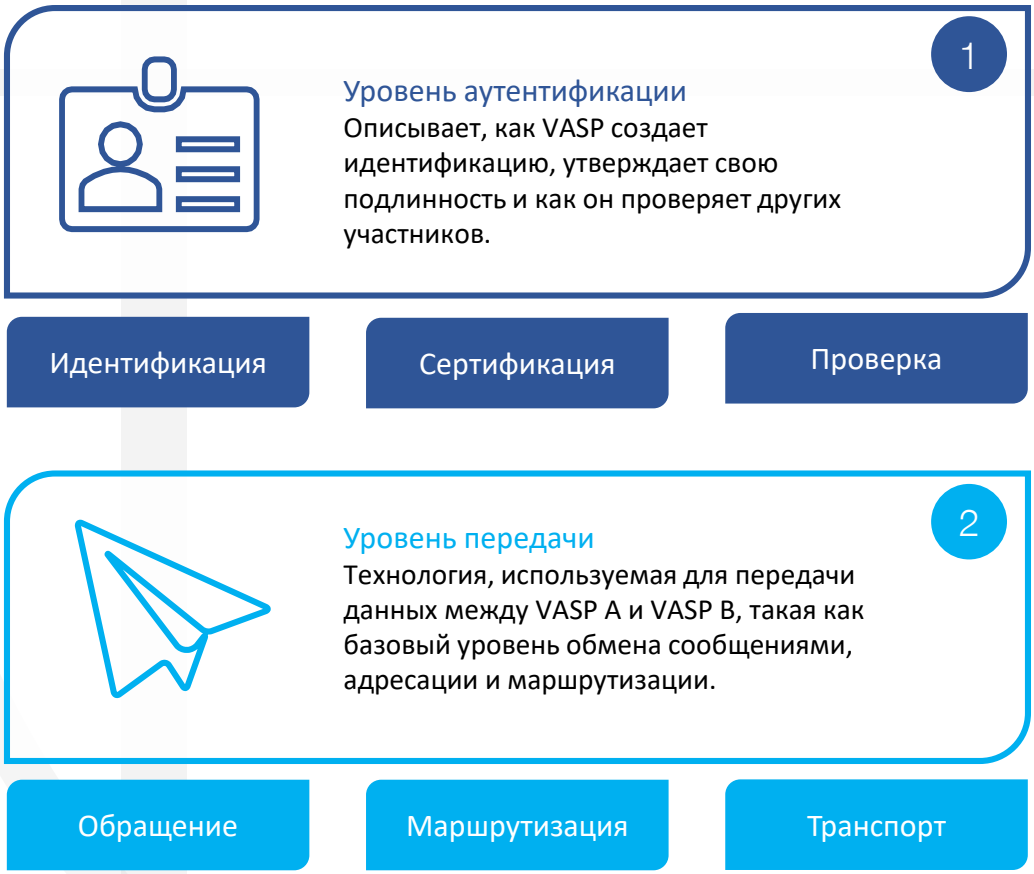
Протоколы лидеры

Команда gwp проанализировала наиболее известные некоммерческие решения Travel Rule с открытым исходным кодом: TRP, OpenVASP и TRISA.

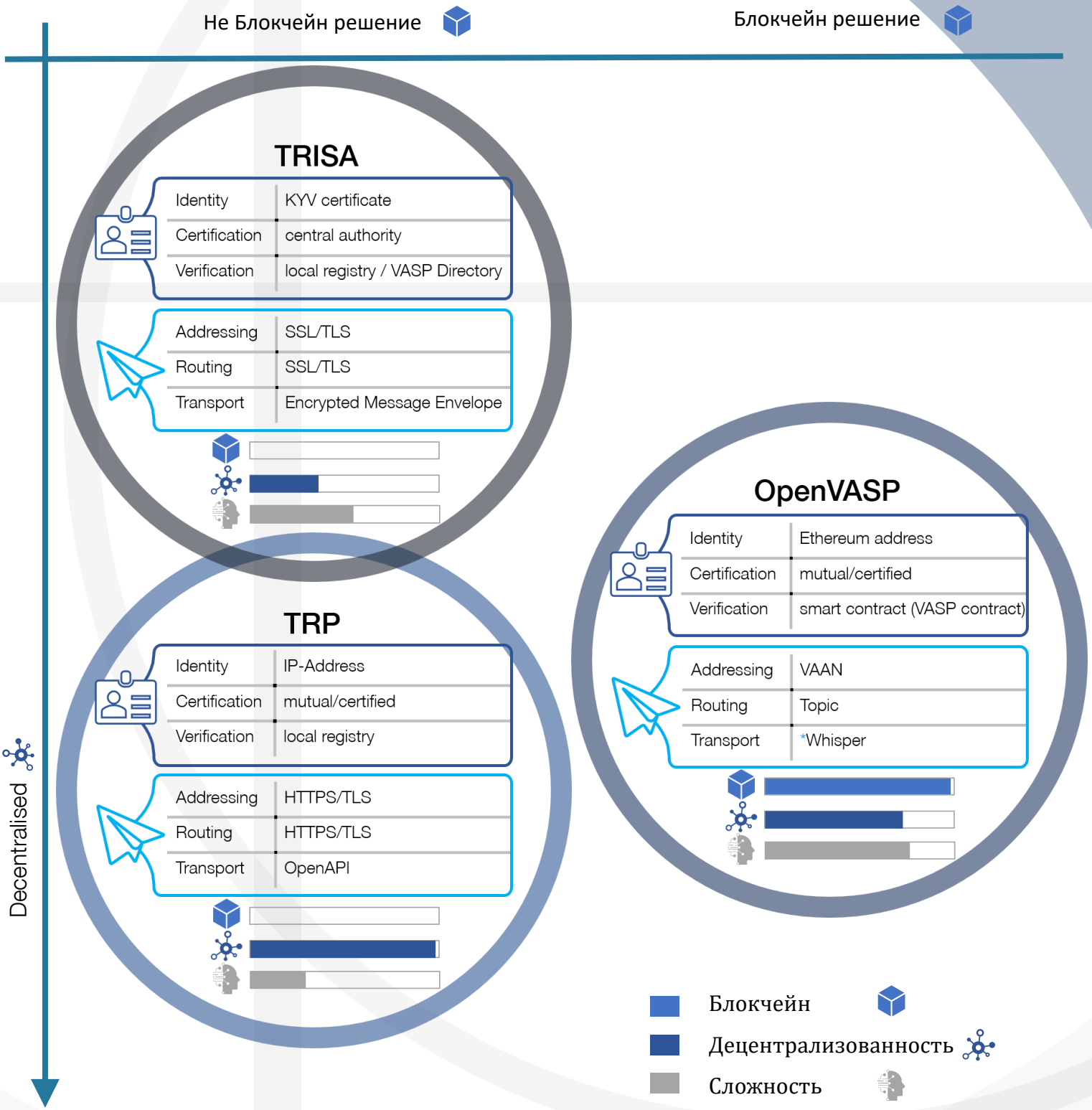


Методология

Идентифицируются две критические характеристики, которые являются адекватным фактором для сравнения архитектуры протоколов: уровень аутентификации и уровень передачи. Соответственно, мы сосредоточились на трех аспектах каждого уровня с целью дать читателю возможность понять основные различия и оценить возможные последствия при внедрении/ интеграции протокола в свою собственную инфраструктуру. В этой главе представлен подробный технический обзор каждого протокола.



Характеристики



* Учитывая минимальные требования протокола OpenVASP, существует широкий спектр возможных уровней обмена сообщениями, которые могут быть использованы. Whisper - это только один пример возможной реализации.

Travel Rule Protocol (TRP)

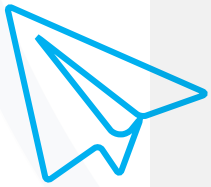
Минимальный и прагматичный API для соответствия рекомендациям FATF по Travel Rule для виртуальных активов

Команда проекта предлагает открытую совместно управляемую инфраструктуру, которая предлагает участникам VASP способ соблюдать рекомендации FATF Travel Rule для виртуальных активов. Основной подход проекта - разработать простое в использовании решение, сосредоточившись на рекомендациях FATF, ограничивая объем и стараясь не предъявлять ненужных дополнительных требований к участникам. Таким образом обеспечивается возможность интеграции любых предприятий или решений с минимальными трудностями и усилиями.

1

Уровень аутентификации TRP основан на взаимной аутентификации. В основном каждый участник ведет собственный список проверенных и, следовательно, доверенных контрагентов, который обычно создается при установлении деловых отношений. При такой настройке нет необходимости в центральном приложении или базе данных, вместо этого протокол работает в самой инфраструктуре каждого VASP.

2

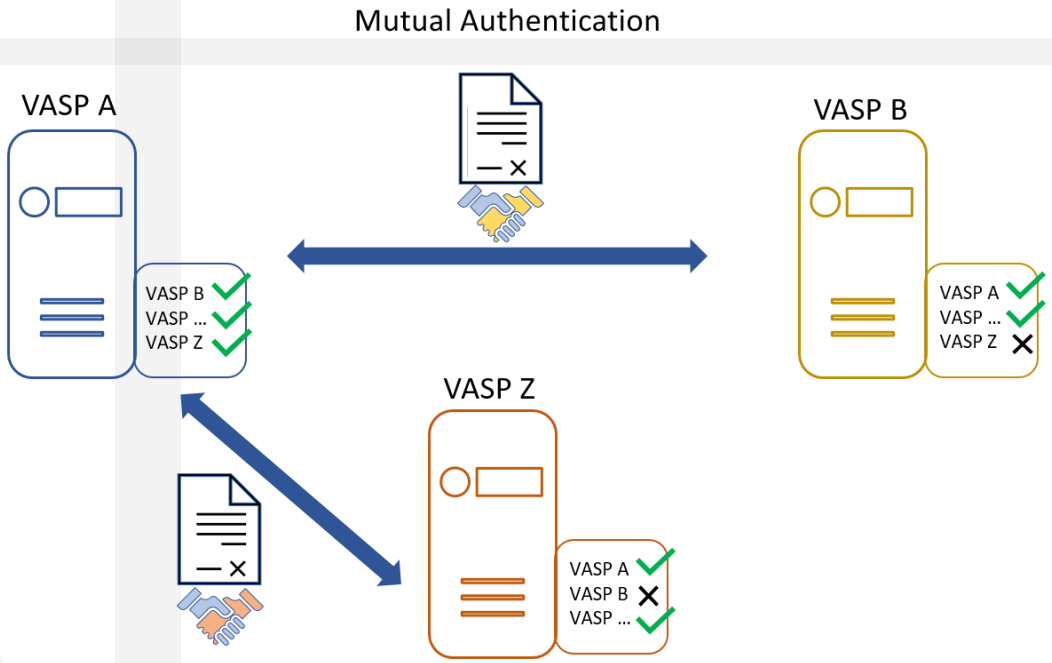


Уровень связи основан на простом наборе конечных точек RESTful и минимальном, работоспособном и прагматичном решении API. Таким образом, базовый уровень обмена сообщениями полагается на общие HTTP-запросы для передачи данных между двумя участниками.

1 Аутентификация

Идентификация

Идентификация VASP, использующего TRP, определяется его базовой технологией, которой в данном случае является интернет-протокол. Таким образом, как обычный участник Интернета, VASP будет идентифицироваться по его IP-адресу, и к нему можно будет получить доступ с помощью правильной маршрутной информации (“handshake”) и методов аутентификации (криптографические ключи).



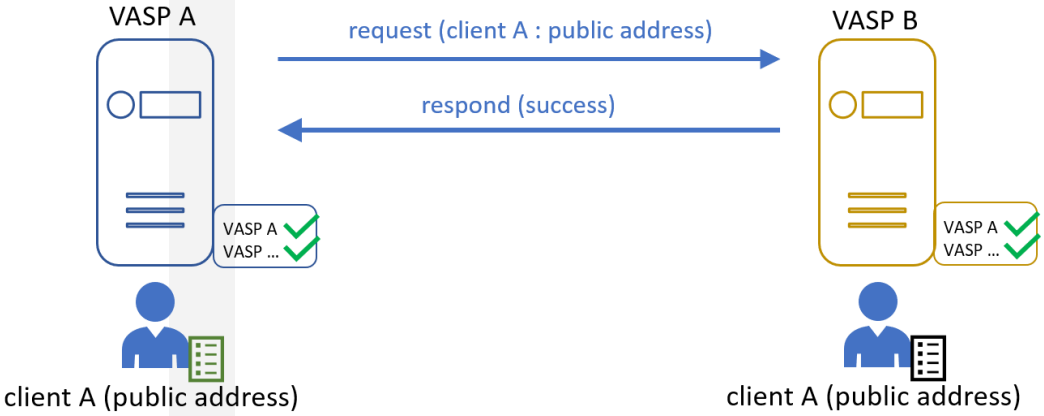
Сертификация / проверка

Подобно взаимодействию пользлвателя с Интернетом, при открытии адреса веб-сайта (например, URL-адреса) пользователь должен знать адрес или искать его, чтобы подключиться к веб-сайту. То же самое относится к VASP, которые пытаются передать данные получателю VASP. Чтобы подключиться к другому VASP, необходимо заранее обменяться идентификаторами (например, VASP A и VASP B), что обычно делается на основе взаимного соглашения между VASP во время процесса адаптации, но также может быть предоставлено сертифицированным органом . После этого каждый VASP будет вести список / регистр известных и проверенных VASP, который необходим для установления соединения и выполнения любых связанных вызовов API к соответствующему VASP.

2 Трансмиссия

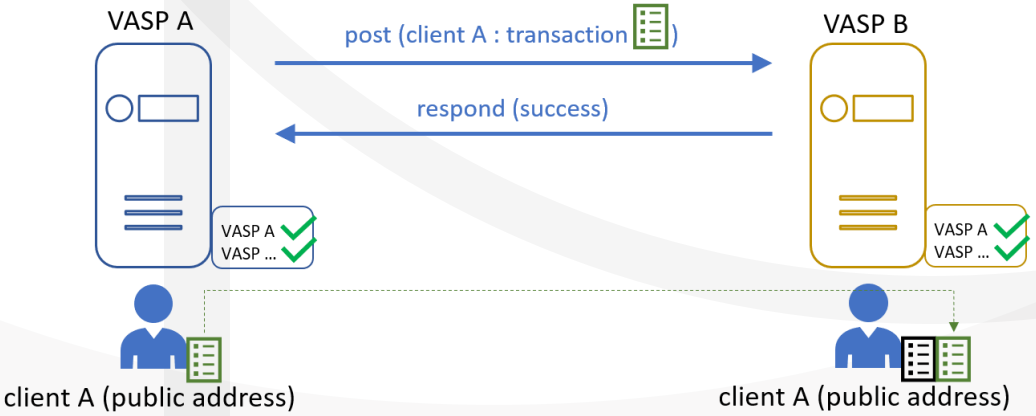
Адресация / Маршрутизация

В целях адресации TRP использует информацию, совместно используемую во время аутентификации VASP-контрагента, для установления соединения между VASP A (отправитель) и VASP B (получатель). Приложение представляет собой API, который может быть интегрирован с другой серверной системой для автоматического запуска различных сервисов для создания, чтения, обновления или удаления данных (например, информации о получателе в отношении рекомендаций FATF). Как только соединение между двумя VASP установлено, исходный VASP A может запросить адрес получателя VASP B. Когда вызывается API, получатель VASP ответит, в зависимости от того, известен ли данный адрес и находится ли он под управлением.



Передача: уведомление о транзакции OpenAPI

Спецификация OpenAPI (OAS) определяет стандартный, не зависящий от языка интерфейс для RESTful API, который позволяет пользователям и компьютерам обнаруживать и понимать возможности службы без доступа к исходному коду, документации или через проверку сетевого трафика. Каждый раз, когда происходит транзакция между двумя VASP, VASP-отправитель передает информацию о получателе (например, клиент A), используя службу POST, определенную спецификацией OpenAPI.



OpenVASP

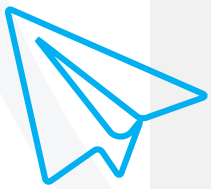
Открытый протокол для реализации правила переводов FATF для виртуальных активов.

Протокол OpenVASP основан на «децентрализованной» философии разработчиков и участников. Это отражено в конструкции и архитектуре протокола. Используя некоторые возможности блокчейна Ethereum, протокол утверждает, что обеспечивает криптографически защищенную связь и аутентификацию с целью обеспечения конфиденциальности данных без необходимости в центральном органе.

1

В качестве уровня аутентификации OpenVASP использует так называемый контракт VASP, который представляет собой идентификатор VASP в децентрализованной инфраструктуре открытых ключей Ethereum. Поэтому развертывается смарт-контракт, содержащий учетные данные VASP. Чтобы установить деловые отношения между VASP, идентификация VASP обменивается прямым взаимным или сертифицированным способом.

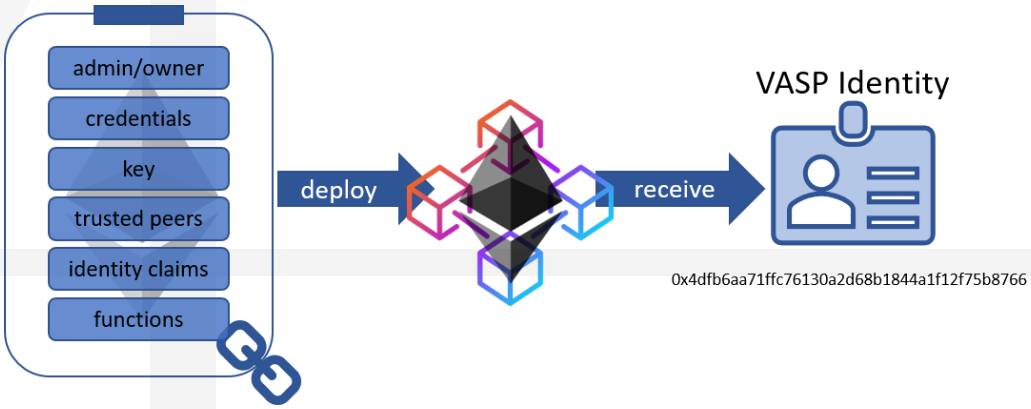
2



Возможный уровень обмена сообщениями построен поверх инфраструктуры Ethereum с использованием Whisper. Whisper можно отнести к категории основанных на идентичности псевдонимных низкоуровневых систем обмена сообщениями, которые объединяют аспекты распределенных хэш-таблиц DHT и систем обмена дейтаграммами (например, UDP). Одним из основных принципов его дизайна являются модульные функции конфиденциальности и анонимности.

* Учитывая минимальные требования протокола OpenVASP, существует широкий спектр возможных уровней обмена сообщениями, которые могут быть использованы. Whisper - это только один пример возможной реализации.

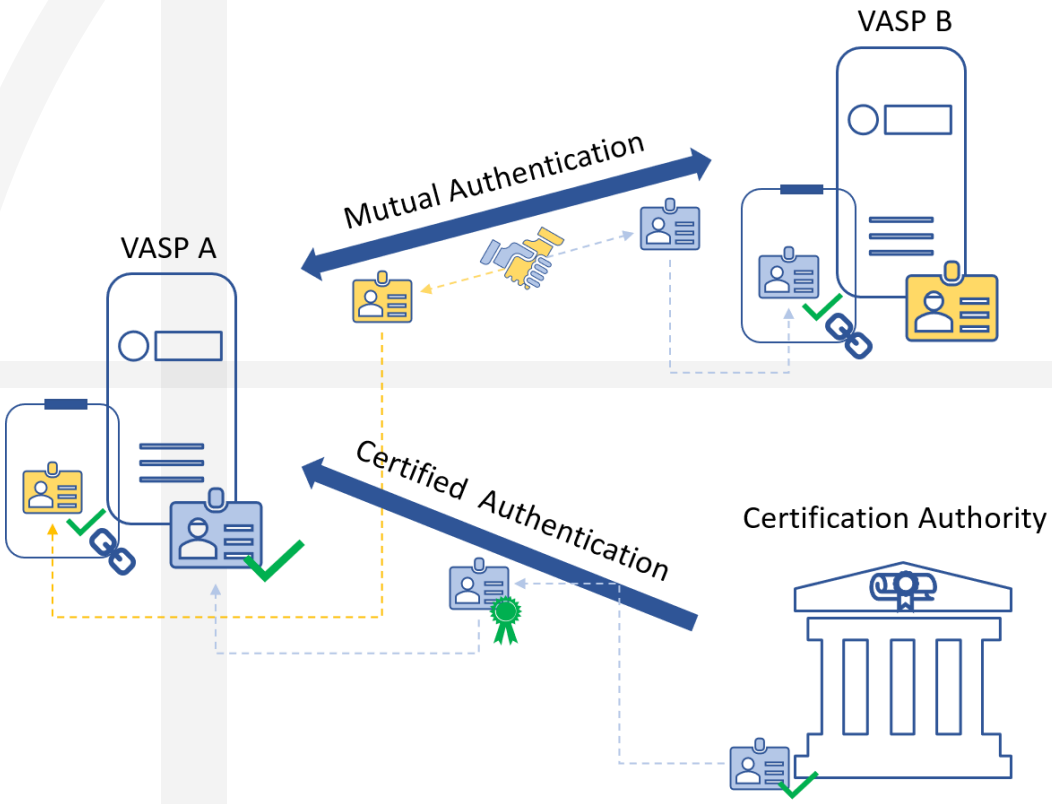
1 Аутентификация



Идентификация: договор VASP / идентификатор VASP

Для того, чтобы VASP использовал протокол OpenVASP, одним из первых шагов является создание VASP личности в блокчейне Ethereum. Для этого каждый VASP развернет стандартизированный смарт-контракт, содержащий учетные данные VASP (упрощенные на рисунке выше), криптографические ключи (рукопожатие и подпись), спецификации администратора / владельца (для управления смарт-контрактом) и набор используемых функций для управления доверенными узлами или для получения удостоверения от третьей стороны. Развернув смарт-контракт, вы автоматически получите адрес контракта Ethereum, который определен как идентификатор VASP.

1 Аутентификация



Сертификация / верификация

Поскольку развертывание смарт-контракта открыто для всех, наличие идентификатора VASP само по себе не является гарантией подлинности VASP. Протокол OpenVASP рассматривает два разных подхода к аутентификации между VASP.

Взаимная аутентификация

Всякий раз, когда два VASP устанавливают деловые отношения, их соответствующие личности могут быть непосредственно идентифицированы, то есть есть свидетельства из первых рук, что идентичность другого VASP подлинная. Следовательно, VASP A добавит идентификатор VASP B в качестве доверенного VASP в свой смарт-контракт.

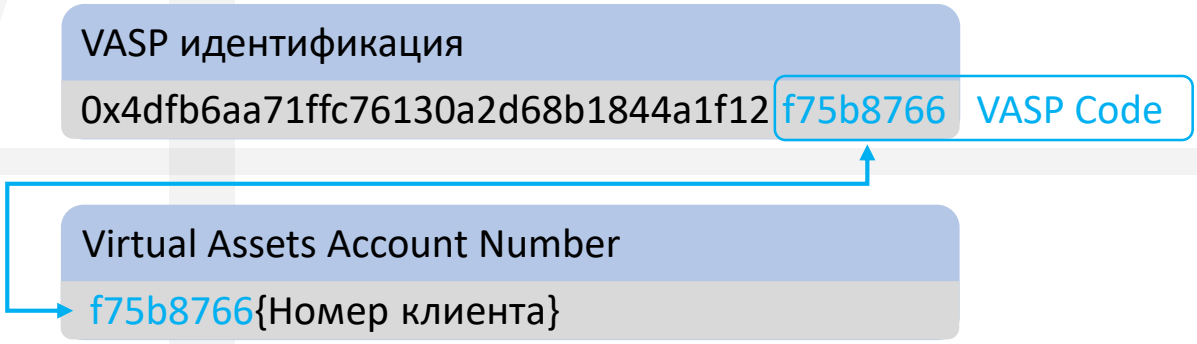
Сертифицированная аутентификация

Подход с сертифицированной аутентификацией основан на использовании доверенной третьей стороны, которую можно сравнить с действующим центром сертификации для выдачи цифровых подписей или сертификатов Secure Socket Layer (SSL). Таким образом, VASP A должен запросить идентификацию в центре сертификации. Такие центры сертификации могут включать в себя сертификат о лицензии или статусе регистрации VASP, выданный соответствующими органами. Каталог OpenVASP предназначен для работы в качестве такого центра сертификации.

2 Трансмиссия

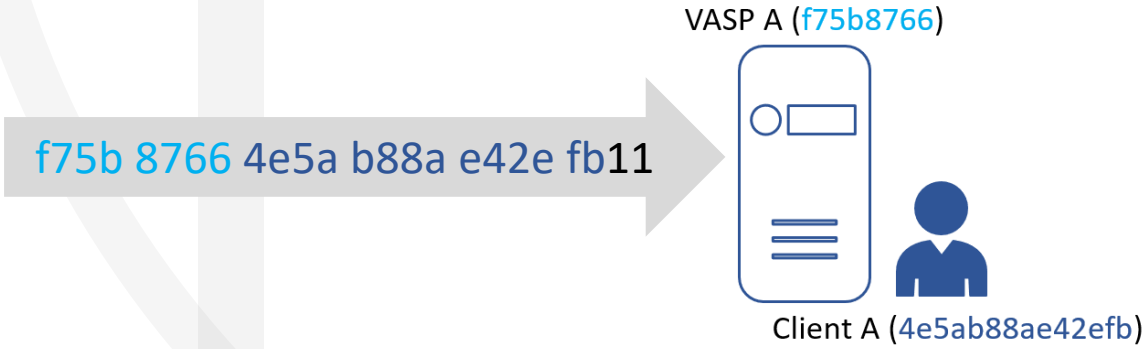
Адресация: код VASP и номер счета виртуальных активов (VAAN)

Протокол OpenVASP использует адрес VASP Identity для создания уникального кода VASP и номера счета виртуальных активов (VAAN). В то время как код VASP определяется последними 32 битами идентификационного адреса VASP, VAAN представляет собой комбинацию кода VASP и определенного для клиента числа в 56 бит.



Информация о маршрутизации

Информация о маршрутизации используется для объявления адреса получателя. Традиционная банковская система использует общие стандарты, такие как BIC / SWIFT или IBAN, которые представляют собой комбинацию идентификатора банка и соответствующего номера счета. Подобно этим подходам, номер VAAN включает идентификатор VASP (код VASP) и адрес получателя (номер для конкретного клиента, например, 4e5ab88ae42efb).



Передача: Whisper

Как только принимающий VASP и клиент идентифицированы и соответствующие меры аутентификации были выполнены, последним шагом протокола является передача данных, как определено FATF Travel Trule, между VASP. На высоком уровне уровень обмена сообщениями Whisper использует асимметричное или симметричное шифрование для шифрования сообщения, которое, следовательно, может быть дешифровано только определенным получателем. Хотя сообщение отправляется в децентрализованную сеть, что означает, что оно будет получено несколькими участниками (узлами), только определенный получатель сможет расшифровать сообщение и раскрыть содержимое, что приведет к обеспечению анонимности для получателя. Чтобы избежать ненужных вычислительных ресурсов для расшифровки всех входящих сообщений, Whisper включает 4-байтовую «тему», которая является указанием получателю следить за сообщением и пытаться расшифровать. Протокол OpenVASP извлекает выгоду из ранее объясненного формата адреса VAAN за счет использования кода VASP в качестве темы, что приводит к меньшим вычислительным ресурсам и более быстрой передаче в сети.

Travel Rule Information Sharing Architecture (TRISA)

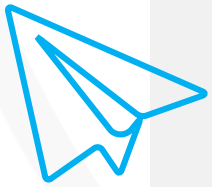
Инфраструктура для решения проблем взаимодействия, представленных требованиями Travel Rule FATF

Цель TRISA - обеспечить соблюдение Travel Rule без изменения основных протоколов цепочки блоков и наличия открытого органа управления. Таким образом, они сосредоточены на децентрализованном подходе с открытым исходным кодом, учитывая и поддерживая совместимость с другими подходами. Протокол предлагает одноранговый механизм с минимальными затратами для участников, сохраняя высокопроизводительные транзакции и защищая конфиденциальность пользователей.

1

Основной уровень аутентификации в протоколе TRISA следует модели центра сертификации (CA). Под ним понимается орган, который выдает так называемые сертификаты открытых ключей, хранящиеся в центральном каталоге. Этот сертификат представляет собой идентификацию VASP и используется для установления безопасной связи между VASPs. Чтобы VASP мог получить такой сертификат, он должен пройти процесс регистрации, включая проверку личности.

2

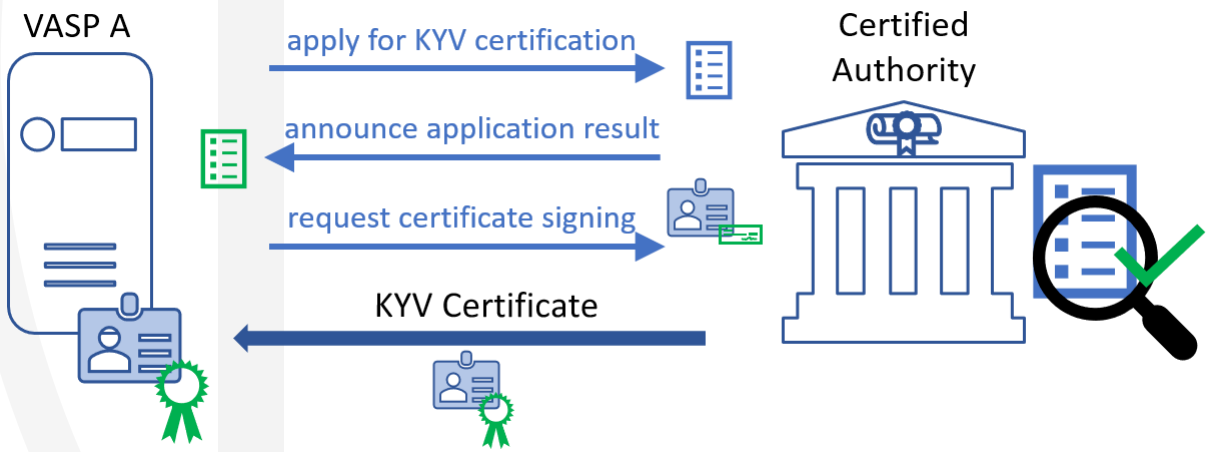


Чтобы установить безопасный канал передачи между двумя VASP, протокол TRISA использует соединение SSL / TLS с взаимной аутентификацией. Это обеспечивает конфиденциальность данных на этапе перехода и позволяет сохранять соединение открытым для множества транзакций через одно одноранговое соединение. Кроме того, TRISA предлагает формат зашифрованного сообщения, чтобы данные оставались доступными в любое время в случае необходимости дальнейшей проверки (например, финансового расследования, регистрации SAR).

1 Аутентификация

Идентификация и сертификация: “Know your VASP”

Процесс регистрации под названием «Знай свой VASP» предназначен для выполнения и проверки всех юридических требований любого применяющего VASP. Для этой цели VASP A должен отправить запрос на сертификацию со всеми соответствующими бизнес-учетными данными в зарегистрированный центр сертификации, чтобы получить «Знай свой сертификат VASP», идентификатор VASP A. Затем данные проверяются по ряду критериев. , например, их регистрация бизнеса, проверка KYC, юрисдикция, мошенничество и санкции, а также, при необходимости, соответствие другим критериям расширенной проверки. Если все требования были выполнены, центр сертификации подпишет запрос на подпись сертификата от применяющего VASP A и выдает сертификат Know Your VASP.



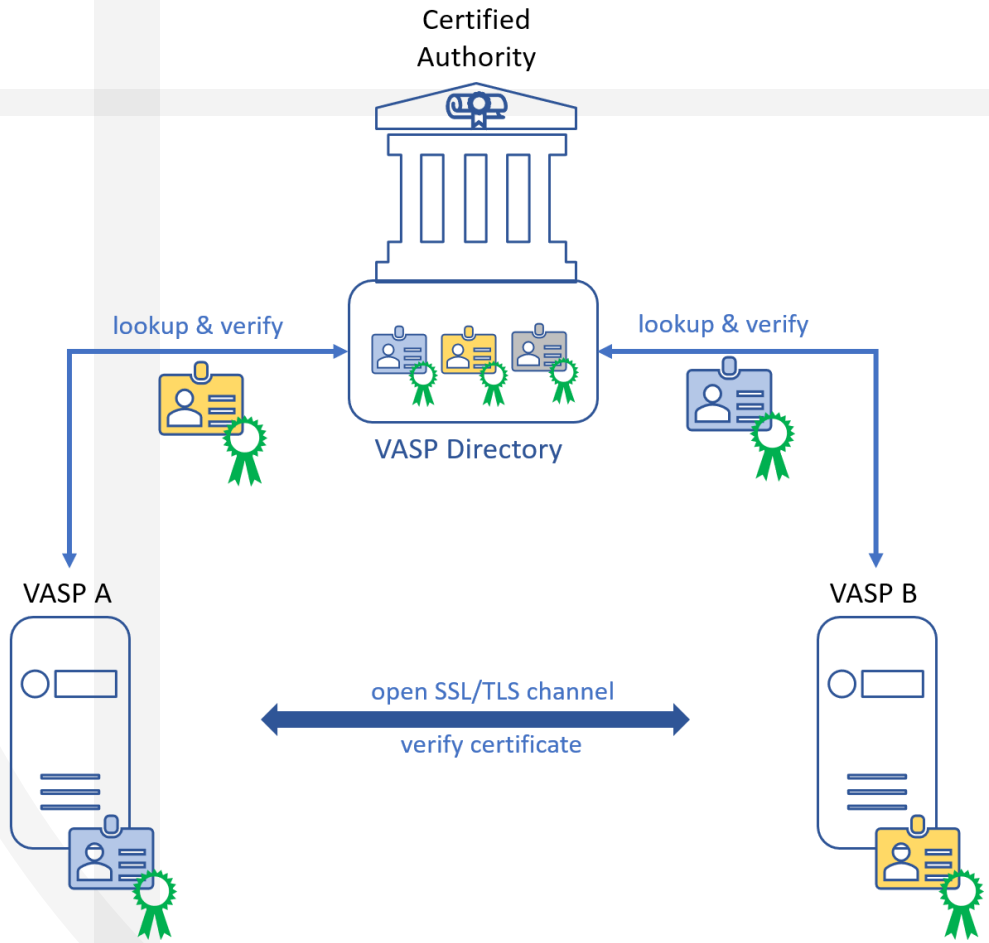
Верификация: TRISA VASP Directory

TRISA управляет центром сертификации, который поддерживает каталог VASP для всех зарегистрированных VASP. В качестве средства проверки, как только VASP A захочет подключиться к VASP B, он может просто проверить сертификат Know Your VASP B или найти бизнес-учетные данные в каталоге VASP, учитывая, что получатель VASP B является законным участником и соответствует требованиям Know Your VASP. Это дает возможность VASP принимать обоснованное решение о соответствии перед отправкой или получением транзакции виртуального актива.

2 Трансмиссия

Addressing & Routing

На основе сертификата Know your VASP, выданного сертифицированным центром, адресация работает путем взаимной аутентификации между VASP A и VASP B. По сути, это включает только обмен идентификаторами VASP (общедоступный адрес). Фактически, идентификация контрагента гарантирует его аутентификацию, и поэтому достаточно для открытия безопасного канала SLL / TLS, используемого для обмена информацией, при этом сохраняя конфиденциальность пользователя. Таким образом, будучи прямым одноранговым соединением, дополнительная информация о маршрутизации не требуется.



Передача

Представленный канал SSL / TLS для отправки криптографически защищенной частной информации будет удовлетворять требованиям FATF в отношении конфиденциальности и безопасности данных. Для улучшения обработки данных TRISA предложила использовать дополнительное шифрование на транспортном уровне, зашифрованный конверт транзакции. Добавляя этот дополнительный уровень, состоящий из ключа шифрования и ключа HMAC, VASP могут безопасно хранить полные данные транзакции независимо от используемой серверной части, сохраняя при этом полную воспроизводимость.

3 Глоссарий и Источники

Глоссарий

- **Обязательство по противодействию отмывания денег и борьбе с терроризмом:** Закон налагает несколько обязательств, если вы ведете бизнес, который подпадает под определение подотчетной организации.
- **AMLO-FINMA:** Федеральный закон Швейцарии о борьбе с отмыванием денег и финансированием терроризма.
- **dApps:** Децентрализованные приложения (dApps) - это цифровые приложения или программы, которые существуют и работают на блочной цепи или сети P2P компьютеров вместо одного компьютера и находятся вне контроля одного органа.
- **DeFi**: **Децентрализованные финансовые сервисы**, или **децентрализованные финансы** — общее название для аналогов традиционных финансовых инструментов, реализованных в децентрализованной архитектуре. Эти сервисы общедоступны, являются проектами с открытым исходным кодом и чаще всего основаны на смарт-контрактах.
- **FATF 12-месяцев ревизия**: Обзор для оценки внедрения пересмотренных стандартов юрисдикциями и частным сектором, а также мониторинг любых изменений в типологии, рисках и рыночной структуре сектора виртуальных активов.
- **FATF Страны входящие в черный список (юрисдикции высокого риска):** Корейская Народно-Демократическая Республика, Иран.
- **FATF Государства-члены:** Австралия, Австрия, Аргентина, Бельгия, Бразилия, Германия, Греция, Дания, Европейская комиссия, Гонконг, Китай, Совет сотрудничества стран Залива, Израиль, Индия, Ирландия, Исландия, Испания, Италия, Канада, Китай, Республика Корея, Люксембург, Малайзия, Мексика, Нидерланды, Королевство, Новая Зеландия, Норвегия, Португалия, Российская Федерация, Саудовская Аравия, Сингапур, Соединенное Королевство, Соединенные Штаты, Турция, Финляндия, Франция, Швейцария, Швеция, Южная Африка, Япония.
- **FATF:** Группа разработки финансовых мер борьбы с отмыванием денег, межправительственная организация, разрабатывающая политику в области борьбы с отмыванием денег и финансированием терроризма.
- **FCA**: Управление по финансовому поведению, орган финансового регулирования Великобритании.
- **Финансовый посредник (Financial Intermediary):** Относится к финансовому учреждению в последовательной или охватывающей платежной цепочке, которое получает и передает электронный перевод от имени отправляющего финансового учреждения и получающего финансового учреждения или другого транзитного финансового учреждения.
- **FinCEN**: Сеть по борьбе с финансовыми преступлениями - федеральное бюро Соединенных Штатов, которое анализирует информацию о финансовых операциях в целях борьбы с отмыванием денег, финансированием терроризма и другими финансовыми преступлениями.
- **FINMA:** Управление по надзору за финансовыми рынками Швейцарии (FINMA) является государственным органом Швейцарии, отвечающим за финансовое регулирование. Сюда входит надзор за банками, страховыми компаниями, биржами и торговцами ценными бумагами, а также за другими финансовыми посредниками в Швейцарии.
- **HMAC ключ**: HMAC (иногда расширяемый либо как код аутентификации хэш-сообщения, либо как код аутентификации сообщения на основе хэша) - это особый тип кода аутентификации сообщения (MAC), включающий криптографическую хэш-функцию и секретный криптографический ключ.
- **MAS Закон о платежных услугах 2019**: Закон о платежных услугах является перспективной и гибкой основой для регулирования деятельности платежных систем и поставщиков платежных услуг в Сингапуре. Он предусматривает регулятивную определенность и потребительские гарантии, поощряя при этом инновации и рост платежных услуг и FinTech отрасль. Парламент принял Закон о платежных услугах 14 января 2019 года.

Глоссарий

- **ML/TF риск**: Клиентский риск - это риск или уязвимость, с которой клиенты могут быть вовлечены в деятельность по отмыванию денег или финансированию терроризма. Риск клиентов ML/TF в значительной степени зависит от характера и/или свойств клиента.
- **OpenVASP**: открытый протокол для реализации правила поездок, включающий все имена: Bitcoin Suisse AG|Lykke | SEBA Bank AG | Sygnum Bank AG | MME Legal Tx Compliance | Avaloq Evolution AG | EPAM Systems, Inc.| 21 Analytics AG | Notabene, Inc. | Web3 Foundation | Coinfirm | Tezos Foundation | TRM Labs | Netki, Inc. | Merkle Science.
- **P2P:** В сети P2P "peer to peer" (равный-равному) - это компьютерные системы, которые соединены между собой через Интернет. Файлы могут совместно использоваться непосредственно между системами в сети без необходимости использования центрального сервера. Другими словами, каждый компьютер в сети P2P становится как файловым сервером, так и клиентом.
- **Подход, основанный на риске:** Риск-ориентированный подход означает, что страны, компетентные органы и банки выявляют, оценивают и понимают риск отмывания денег и финансирования терроризма, которому они подвергаются, и принимают соответствующие меры по его снижению в соответствии с уровнем риска.
- **SSL/TLS канал**: Безопасность транспортного уровня (TLS), а также его современный предшественник, Secure Sockets Layer (SSL), представляют собой криптографические протоколы, разработанные для обеспечения безопасности коммуникаций в компьютерной сети.
- **SWIFT**: Общество всемирных межбанковских финансовых телекоммуникаций (SWIFT), юридически S.W.I.F.T. SCRL, обеспечивает сеть, которая позволяет финансовым учреждениям во всем мире отправлять и получать информацию о финансовых операциях в безопасной, стандартизированной и надежной среде.
- **Travel Rule**: Правило Закона о банковской тайне (BSA) [31 CFR 103.33(g)] - часто называемое правилами "поездок" (переводов) - требует, чтобы все финансовые учреждения передавали определенную информацию следующему финансовому учреждению, в определенных переводах средств с участием более чем одного финансового учреждения.
- **TRISA** открытый протокол для реализации правила транзакций, который включает в себя : CipherTrace | Ripple | Paxful | MIT Connection Science ¬ Engineering | Bradley Arant Boult Cummings LLP | Luminous Group Limited.
- **TRP** открытый протокол для реализации правила транзакций, включающий : 21 Analytics | AGA&D ForensicsBC Group | OSL | BitGo | CipherTrace |Complifact AML Inc. | Crypto Finance AG | Diginex/EQUOS.io | Electric Coin Company | Elliptic | Digivault | Fidelity Digital Assets | Geissbühler Weber & Partner (gwp) | HashKey | Hex Trust | Hodlnaut Pte. Ltd. | ING | Komainu (Jersey) Limited | KPMG Advisory | KYC-Chain | Metaco | MIT Connection Science & Engineering | Netki | Notabene | OKCoin | Onchain Custodian | Ospree | Paxful | Peter Davey and Associates Limited | Standard Chartered Bank | TP ICAP | Trisa | Xreg.
- **Нерегулируемые кошельки**: это программное обеспечение, размещенное на компьютере, телефоне или другом устройстве человека, которое позволяет ему хранить и проводить операции с криптографическими активами.
- **UDP:** User Datagram Protocol (Пользовательский протокол датаграмм) - это минимальный, безсоединенный сетевой протокол, который используется в качестве транспортного уровня в Интернет-протоколе, для отправки сообщений (датаграмм) на другие узлы.
- **VA:** Виртуальные активы.
- **VAAN**: Номер счета виртуальных активов.
- **VASP**: Поставщики услуг по обслуживанию виртуальных активов, которые являются организациями-хранителями, осуществляющими обмены "фиат-к-крипто" или "крипто-к-крипто", или ведущими бизнес, связанный с передачей и хранением виртуальных - активов и финансовых услуг.

Источники

Admin.ch. 1997. Federal Act On Combating Money Laundering And Terrorist Financing. [online] Available at: <https://www.admin.ch/opc/en/classified-compilation/19970427/202002180000/955.0.pdf> [Accessed 21 September 2020].

Bryant, A., 2019. Using Instant Messenger To Explain The FATF Travel Rule For Vasps — Andy Bryant. [online] andybryant.me. Available at: <https://www.andybryant.me/blog/2019/9/25/using-instant-messenger-to-explain-the-fatf-travel-rule-fornbspvasps> [Accessed 23 September 2020].

Docs.google.com. 2020. *Travel Rule Protocol 20200617*. [online] Available at: <https://docs.google.com/document/u/0/d/1UubLDy9rlvUfS4WxkLjWiQxM-2KP_GrRdCh5PzwilTM/mobilebasic> [Accessed 17 September 2020].

Eidgenössische Finanzmarktaufsicht FINMA. 2020. *FINMA Guidance 02/2019*. [online] Available at: <https://www.finma.ch/en/documentation/finma-guidance/> [Accessed 17 September 2020].

Ethereum Wiki. n.d. *Whisper Poc 2 Protocol Spec*. [online] Available at: <https://eth.wiki/en/concepts/whisper/poc-2-protocol-spec> [Accessed 17 September 2020].

Fatf-gafi.org. 2020. 12-MONTH REVIEW OF THE REVISED FATF STANDARDS ON VIRTUAL ASSETS AND VIRTUAL ASEET SERVICE PROVIDERS. [online] Available at: <http://www.fatf-gafi.org/media/fatf/documents/recommendations/12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf> [Accessed 23 September 2020].

Fatf-gafi.org. 2019. VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS. [online] Available at: <https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> [Accessed 21 September 2020].

Fatf-gafi.org. 2020. *Outcomes FATF Virtual Plenary, 24 June 2020*. [online] Available at: <https://www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-fatf-plenary-june-2020.html> [Accessed 17 September 2020].

Fatf-gafi.org. 2020. *What We Do - Financial Action Task Force (FATF)*. [online] Available at: <https://www.fatf-gafi.org/about/whatwedo/> [Accessed 17 September 2020].

Fincen.gov. 2020. *Fincen Advisory*. [online] Available at: <https://www.fincen.gov/sites/default/files/advisory/advissu7.pdf> [Accessed 17 September 2020].

Jevans, D., 2019. *Travel Rule Information Sharing Architecturefor Virtual Asset Service Providers (TRISA)*. [online] Linkedin.com. Available at: <https://www.linkedin.com/pulse/travel-rule-information-sharing-architecture-virtual-asset-jevans> [Accessed 17 September 2020].

Kirkpatrick, K., Telep, J., Das, S. and Gerber, J., 2020. *Fincen 'Travel Rule' Update Sets Challenges For Crypto Cos.*. [online] Kslaw.com. Available at: <https://www.kslaw.com/attachments/000/007/286/original/FinCEN_'Travel_Rule'_Update_Sets_Challenges_For_Crypto_Cos..pdf?1571236052 > [Accessed 17 September 2020].

KYC-Chain. 2020. *How The FATF's Travel Rule Is Being Implemented Around The World - KYC-Chain*. [online] Available at: <https://kyc-chain.com/fatf-travel-rule-around-the-world/> [Accessed 17 September 2020].

Riegelnig, D., 2019. *Openvasp: An Open Protocol To Implement FATF'S Travel Rule For Virtual Assets*. [online] Openvasp.org. Available at: <https://openvasp.org/wp-content/uploads/2019/11/OpenVasp_Whitepaper.pdf> [Accessed 17 September 2020].

Swagger.io. 2020. *Openapi Specification - Version 3.0.3 | Swagger*. [online] Available at: <https://swagger.io/specification/> [Accessed 17 September 2020].

Switzerland, F., 2020. *Swiss 21 Analytics Completes First Automated And Compliant Bitcoin Transaction | Fintech Schweiz Digital Finance News - Fintechnewsch*. [online] Fintech Schweiz Digital Finance News - FintechNewsCH. Available at: <https://fintechnews.ch/blockchain_bitcoin/swiss-financial-intermediaries-successfully-complete-first-automated-and-compliant-bitcoin-transaction/38328/> [Accessed 17 September 2020].

Sygna. 2020. FATF Announces New 12-Month "Travel Rule" Review For June 2021 - Sygna. [online] Available at: <https://www.sygna.io/blog/fatf-plenary-new-travel-rule-12-month-review-for-june-2021/> [Accessed 23 September 2020].

Sygna. n.d. Singapore Crypto Regulation: A Licensing Guide For DPT Exchanges - Sygna. [online] Available at: <https://www.sygna.io/blog/singapore-cryptocurrency-regulations-and-digital-payment-token-service-licensing/> [Accessed 21 September 2020].

Sygna. 2020. *What FATF R.16 Crypto Travel Rule Solutions Are Currently In The Market? - Sygna*. [online] Available at: <https://www.sygna.io/blog/types-of-fatf-r16-crypto-travel-rule-solutions/> [Accessed 17 September 2020].

Trisa.io. 2020. *Travel Rule Information Sharing Architecture For Virtual Asset Service Providers*. [online] Available at: <https://trisa.io/trisa-whitepaper/#_Toc48780351> [Accessed 17 September 2020].

Unchained Podcast. 2020. *Why The Travel Rule Is One Of The Most Significant Regulations In Crypto - Unchained Podcast*. [online] Available at: <https://unchainedpodcast.com/why-the-travel-rule-is-one-of-the-most-significant-regulations-in-crypto/> [Accessed 17 September 2020].

Фото

Shutterstock, Unsplash, Pixabay

Михаэл Баумгартнэр
Глава Продаж по Банковским Операциям и Цифровым Активам
michael.baumgartner@incorebank.ch
+41 44 403 93 20

Лараг Велти
Глава по Маркетингу
laragh.welti@incorebank.ch
+41 44 403 93 19

Екатерина Энтони
Старший Менеджер по Крипто Комплайнс
Руководитель группы DLT
ekaterina.anthony@gwp.ch
+41 76 582 09 74

Евгений Борисов
DLT/Консультант по Цифровым Технологиям
jeff.borisov@gwp.ch
+41 44 221 91 61

Сандро Муччионе
DLT/Консультант по Цифровым Технологиям
sandro.muccione@gwp.ch
+41 44 221 91 28

Анна Пальмина
Управляющий Директор, PALMINA INVEST
anna.palmina@palmina-invest.com
+7 985 168 66 88

Распространение
в Российской Федерации

PALMINA INVEST

geissbühler weber & partner
Bleicherweg 72
8002 Zürich

+41 44 221 91 00
info@gwp.ch |
www.gwp.ch