Axelar Network:
Соединение приложений с экосистемами блокчейн

Проект 1.0

Январь 2021

Аннотация

Появляются многочисленные экосистемы блокчейна, которые предоставляют уникальные и отличные от других возможности, привлекательные для пользователей и разработчиков приложений. Однако связь между экосистемами очень редкая и фрагментарная. Чтобы обеспечить приложениям возможность беспрепятственного взаимодействия между экосистемами блокчейн, мы предлагаем Axelar. Стек Axelar предоставляет децентрализованную сеть, протоколы, инструменты и API, которые обеспечивают простую межцепочечную коммуникацию. Набор протоколов Axelar состоит из протоколов трансграничной маршрутизации и передачи данных. Децентрализованная открытая сеть валидаторов обеспечивает работу сети; любой может присоединиться, использовать ее и участвовать. Византийский консенсус, криптография и механизмы стимулирования разработаны для достижения высоких требований к безопасности и оперативности, уникальных для межцепочечных запросов.

1 Введение

Блокчейн-системы быстро набирают популярность и привлекают новые варианты использования для токенизации активов, децен- трализованных финансов и других распределенных приложений. Несколько основных платформ, таких как Ethereum, Monero, EOS, Cardano, Terra, Cosmos, Avalanche, Algorand, Near, Celo и Polkadot, предлагают различные функции и среды разработки, что делает их привлекательными для различных приложений, сценариев использования и конечных пользователей [.5, 11, 4, 21, 20, 23, 24, 19, 6, 14, 25]. Однако полезные функции каждой новой платформы в настоящее время предлагаются менее чем 1% пользователей экосистемы, а именно держателям нативного токена этой платформы. Можем ли мы позволить разработчикам платформ легко подключать свои блокчейны к другим экосистемам? Можем ли мы позволить разработчикам приложений создавать приложения на платформе, наиболее подходящей для их нужд, и при этом взаимодействовать между несколькими экосистемами блокчейн? Можем ли мы позволить пользователям взаимодействовать с любым приложением на любом блокчейне непосредственно из своих кошельков?

Чтобы соединить экосистемы блокчейна и дать приложениям возможность без трения взаимодействовать между ними, мы предлагаем сеть Axelar. Валидаторы коллективно управляют византийским протоколом консенсуса и запускают протоколы, облегчающие межцепочечные запросы. Любой желающий может присоединиться к сети, участвовать и использовать ее. Базовая сеть оптимизирована под высокие требования к безопасности и быстродействию, уникальные для межцепочечных запросов. Сеть Axelar также включает набор протоколов и API. Основными протоколами являются:

- Протокол межцепочечного шлюза (CGP). Этот протокол аналогичен протоколу Border

Gateway Protocol в Интернете. Этот протокол используется для соединения нескольких автономных экосистем блокчейн и отвечает за маршрутизацию между ними. Блокчейнам не нужно "говорить на каком-то своем языке", разработчикам их платформ не нужно вносить какие-либо пользовательские изменения в свои цепи, а их цепи можно легко подключить к глобальной сети.

- Протокол межцепочечной передачи данных (CTP). Этот протокол является аналогом протоколов прикладного уровня File Transfer, Hypertext Transfer Protocols в Интернете. Это стек протоколов прикладного уровня, который располагается поверх протоколов маршрутизации (таких как CGP и другие технологии маршрутизации). Разработчики приложений могут подключать свои dapps к любой цепочке для выполнения межцепочечных запросов. Пользователи могут использовать протокол CTP для взаимодействия с приложениями на любой цепочке с помощью простых вызовов API, аналогичных HTTP GET/POST запросам. Разработчики могут блокировать, разблокировать и передавать активы между любыми двумя адресами на любых платформах блокчейна, выполнять межцепочечные триггеры приложений (например, dapps на цепочке A может обновлять данные на цепочке A).

его состояние, если какое-то другое приложение на цепочке B удовлетворяет некоторым критериям поиска (процентная ставка > X)), и выполнять общие межцепочечные запросы между приложениями на разных цепочках (смарт-контракт на цепочке A может вызвать обновление состояния смарт-контракта на цепочке B). Этот протокол обеспечивает совместимость программ в различных экосистемах блокчейн.

Сеть Axelar предлагает следующие преимущества:

- *Для создателей блокчейн-платформ*: Возможность легко подключать свои блокчейны ко всем другим блокчейн-экосистемам. Для подключения к сети необходимо создать только пороговую учетную запись.
- *Для создателей dapps*: Создатели приложений могут размещать свои dapps в любом месте, блокировать, разблокировать, передавать активы и взаимодействовать с приложениями на любой другой цепочке через CTP API.
- *Для пользователей*: Пользователи могут взаимодействовать со всеми приложениями экосистемы непосредственно из своих кошельков.

Платформа для строителей. Наконец, сеть Axelar - это платформа для разработчиков и глобальное сообщество. Ее модель управления открыта для всех. Разработчики могут предлагать новые точки интеграции, маршрутизацию и протоколы на уровне приложений, а пользователи могут решать, принимать ли их, голосуя за предложения, и, если они будут одобрены, валидаторы примут изменения.

1.1 Существующие решения по операционной совместимости

Предыдущие попытки решить проблему совместимости блокчейн относятся к одной из четырех категорий: централизованные биржи, совместимые экосистемы, обернутые активы и мосты токенов. Ниже мы приводим краткое описание этих подходов.

Централизованные системы. Сегодня централизованные системы являются единственными действительно масштабируемыми решениями для обеспечения совместимости экосистемы. Они могут относительно легко включить в листинг любой актив или подключить любую платформу. Однако известно, что централизованные системы имеют различные проблемы с безопасностью и недостаточно хороши для работы с развивающейся децентрализованной финансовой системой, которая требует надежной безопасности, прозрачности и открытого управления. Сами по себе они не могут обеспечить работу децентрализованных приложений по мере их роста.

Центры операционной совместимости. Такие проекты, как Cosmos, Polkadot, Ava labs, занимаются обеспечением совместимости между *сайдчейнами,* принадлежащими их экосистемам, используя собственные протоколы межцепочечного взаимодействия [23, 25, 24]. Например, можно создать сайдчейн (Cosmos Zone), который может взаимодействовать с хабом Cosmos. Сайдчейн должен быть основан на консенсусе Tendermint и использовать протокол, который понимает Cosmos Hub. Связь с другими блокчейнами и экосистемами, говорящими на разных языках, остается за внешними технологиями.

Парные мосты. Обернутые активы (например, обернутые биткоины) пытаются заполнить недостающий пробел межцепочечного взаимодействия в экосистеме. Одним из примеров является tBTC [9], который представляет собой специальный протокол, где для обеспечения безопасности переводов используется продуманная комбинация смарт-контрактов и залога. Эти решения требуют значительных инженерных усилий для создания - для каждой пары цепочек разработчики должны создать новый смарт-контракт на цепочке назначения, который анализирует доказательства состояния цепочки происхождения (аналогично тому, как каждая боковая цепочка может, в принципе, анализировать состояние других цепочек). Только несколько мостов были развернуты с использованием этого подхода. Эти подходы не масштабируются, когда одна из базовых блокчейн хочет обновить свои правила консенсуса или формат транзакций. Это

связано с тем, что все смарт-контракты, которые зависят от состояния этих цепей, должны быть обновлены. Также необходимо установить валидаторы и потребовать от них заблокировать различные активы, чтобы обеспечить избыточное обеспечение любого перевода активов, что ограничивает экономическую эффективность таких переводов.

Мы также видели несколько других одноцелевых мостов, созданных разработчиками платформ, которые переписали логику перехода состояния в смарт-контрактах для создания мостов к другим экосистемам [1, 7]. Они страдают от многочисленных проблем масштабируемости, не позволяют экосистеме масштабироваться равномерно и вводят дополнительные зависимости для приложений. Например, если одна платформа меняется, то все смарт-контракты на всех мостах должны быть обновлены. Это

в конечном итоге поставит экосистему в тупик, где никто не сможет обновляться. Наконец, если один одноцелевой мост соединяет платформы A и B, а второй одноцелевой мост соединяет B и C, это не означает, что приложения на A смогут общаться с приложениями на C. Возможно, потребуется создать еще один одноцелевой мост или перестроить логику приложений.

Другие попытки решить проблему совместимости включают федеративные оракулы (например, Ren [8]), и взаимодействующие блокчейны для конкретных приложений [10].

Подводя итог, можно сказать, что существующие решения для обеспечения интероперабельности требуют большой инженерной работы как от разработчиков платформ, так и от создателей приложений, которые должны понимать различные протоколы связи для взаимодействия между каждой парой экосистем. Таким образом, функциональная совместимость практически отсутствует в современном блокчейн-пространстве. В конце концов, разработчики платформ хотят сосредоточиться на создании платформ, оптимизировать их под свои нужды и иметь возможность легко подключаться к другим блокчейнам. А разработчики приложений хотят создавать dapps на лучших платформах для своих нужд и при этом использовать пользователей, ликвидность и взаимодействовать с другими dapps на других цепочках.

2 Поиск масштабируемой межцепочечной связи

В своей основе межсетевая коммуникация требует, чтобы разнородные сети обрели способность общаться на одном языке. Чтобы решить эту проблему, мы объясним набор протоколов Axelar, опишем его высокоуровневые свойства и объясним, как эти свойства решают основную задачу масштабируемой межсетевой коммуникации.

1. *Интеграция "Plug-and-play".* Разработчики блокчейн-платформ не должны быть вынуждены выполнять тяжелую инженерную или интеграционную работу, чтобы говорить на каком-то "пользовательском языке" для поддержки кросс-цепочки. Протокол кросс-цепочки должен быть способен без проблем подключаться к любой существующей или новой блокчейн. Новые активы должны добавляться с минимальными усилиями.

2. *Межцепочечная маршрутизация.* Такие функции, как обнаружение сетевых адресов, путей маршрутизации и сетей, лежат в основе Интернета и поддерживаются BGP и другими протоколами маршрутизации. Аналогично, для облегчения коммуникации между экосистемами блокчейн нам необходимо поддерживать обнаружение адресов между ними, приложениями и маршрутизацию.

3. *Поддержка обновляемости.* Если одна из экосистем блокчейна изменяется, это не должно влиять на совместимость других блокчейнов. Система должна распознавать обновления, и для их поддержки должны требоваться минимальные усилия (т.е. не должна переписываться "логика перехода состояния", а приложения не должны ломаться).

4. *Единый язык для приложений.* Приложениям необходим простой протокол для блокировки, разблокировки, передачи и взаимодействия с другими приложениями независимо от того, в какой цепочке они находятся. Этот протокол должен быть независимым от цепочки и поддерживать простые вызовы, аналогично протоколам HTTP/HTTPS, которые позволяют пользователям и браузерам взаимодействовать с любым веб-сервером. По мере того, как все больше сетей и активов присоединяются к протоколам маршрутизации нижнего уровня, приложения должны иметь возможность использовать их для связи без переписывания своих программных стеков.

Далее мы кратко описываем требования безопасности, которым должны удовлетворять эти протоколы.

1. *Децентрализованное доверие.* Сеть и протоколы должны быть децентрализованными, открытыми и позволять каждому принимать справедливое участие.

2. *Высокая безопасность*. Система должна удовлетворять высоким гарантиям безопасности. Система должна сохранять безопасность активов и государства в процессе обработки межцепочечной сетью.

3. *Высокая живучесть*. Система должна удовлетворять высоким гарантиям быстродействия для поддержки приложений, использующих ее межцепочечные возможности.

Удовлетворить подмножество этих свойств легко. Например, можно создать объединенную учетную запись multisig со своими друзьями и блокировать/разблокировать активы на соответствующих цепочках. Такие системы по своей природе уязвимы для атак на сговор и цензуру, и у валидаторов нет надлежащих стимулов для их защиты. Создание децентрализованной сети и набора протоколов, в которых может участвовать любой желающий, будучи правильно стимулированным, может обеспечить беспрепятственную межцепочечную коммуникацию, но решение этой проблемы - трудная задача, требующая тщательного сочетания протоколов консенсуса, криптографии и разработки механизмов.

3 Акселярная сеть

Сеть Axelar предоставляет единое решение для межцепочечной коммуникации, которое удовлетворяет потребности как разработчиков платформ - от них не требуется никакой работы по интеграции, так и создателей приложений - один простой протокол и API для доступа к глобальной ликвидности и взаимодействия со всей экосистемой.

Сеть Axelar состоит из децентрализованной сети, которая соединяет экосистемы блокчейн, говорящие на разных языках, и набора протоколов с API поверх, что облегчает приложениям выполнение межцепочечных запросов. Сеть соединяет существующие автономные блокчейны, такие как Bitcoin, Stellar, Terra, Algorand, и центры интероперабельности, такие как решения Cosmos, Avalanche, Ethereum и Polkadot. Наша задача - дать разработчикам приложений возможность создавать такие приложения проще, используя универсальный протокол и API, не внедряя под них свои собственные межцепочечные протоколы и не переписывая приложения по мере разработки новых мостов. Для этого мы разработали набор протоколов, включающий протокол межцепочечного шлюза (см. раздел 6) и протокол межцепочечной передачи (см. раздел 7).

Основным компонентом сети являются базовые децентрализованные протоколы. Валидаторы коллективно поддерживают сеть Axelar и управляют узлами, которые обеспечивают безопасность блокчейна Axelar. Они избираются в процессе делегирования полномочий пользователями. Валидаторы получают право голоса пропорционально делегированной им доли. Валидаторы достигают консенсуса по состоянию нескольких блокчейнов, к которым подключена платформа. Блокчейн отвечает за поддержание и работу межцепочечных протоколов маршрутизации и передачи данных. Правила управления позволяют участникам сети принимать протокольные решения, например, какие блокчейны соединять и какие активы поддерживать.

Блокчейн Axelar следует модели Delegated Proof-of-Stake (DPoS), аналогичной Cosmos Hub. Пользователи избирают валидаторов, которые должны связать свою долю для участия в консенсусе и поддержания высокого качества обслуживания. Модель DPoS позволяет поддерживать большой децентрализованный набор валидаторов и надежные стимулы, гарантирующие, что валидаторы несут ответственность за поддержание мостов и долей криптографических пороговых схем. В рамках консенсуса валидаторы запускают программное обеспечение light-client других блокчейнов, что позволяет им проверять состояние других блокчейнов. Валидаторы сообщают об этих состояниях в блокчейн Axelar, и как только достаточное их количество сообщает об этом, состояние Bitcoin, Ethereum и других цепочек записывается в Axelar.

Впоследствии базовый уровень Axelar знает о состоянии внешних блокчейнов в любой момент времени, создавая "входящие мосты" из других блокчейнов. Валидаторы коллективно поддерживают *пороговые сиг- налы* на других блокчейнах (например, 80% валидаторов должны одобрить и соподписать любую транзакцию), что позволяет им блокировать и разблокировать активы и состояние между цепочками и размещать состояние на других блокчейнах - "исходящих мостах". В целом, сеть Axelar можно рассматривать как *децентрализованный межцепочечный оракул для чтения/записи*.

В оставшейся части документа описываются предварительные сведения и строительные блоки,

лежащие в основе сети (разд. 4), некоторые технические детали сети (Раздел 5), протокол межцепочечного шлюза (Раздел 6), и протокол межцепочечной передачи (Раздел 7).

4 Предварительная подготовка

4.1 Условные обозначения и допущения

Пусть V обозначает множество валидаторов Axelar в раунде R. Каждый валидатор *имеет вес*, число в (0, 1], обозначающее силу голоса этого конкретного валидатора. Вес всех валидаторов равен 1. Валидатор *корректен*, если он запускает узел, который соответствует правилам протокола Axelar. Для завершения блоков или для подписания межцепочечных запросов Axelar требует корректных валидаторов с общим весом $> F$. Мы называем параметр
$F \in [0.5, 1]$ *порог протокола.*

Axelar может быть основан на блокчейне с *мгновенным завершением Delegated-Proof-of-Stake*. Валидаторы запускают *визан- тинский отказоустойчивый (BFT) консенсус* на каждом раунде i для окончательной обработки i-го$_{th}$ блока. Как только i-й $_{th}$блок завершен, запускается новый консенсус BFT для завершения i+ блока1$_{th}$, и так далее. Валидаторы избираются путем делегирования доли. Пользователь с определенной долей может выбрать узел валидатора или делегировать свое право голоса (долю) существующему валидатору, который затем голосует от его имени. Набор валидаторов может обновляться, валидаторы присоединяются/выходят из него, а пользователи делегируют/не делегируют свое право голоса.

Различные блокчейны работают при разных сетевых предположениях. *Синхронная коммуникация* означает, что существует фиксированная верхняя граница Δ на время доставки сообщений, где Δ известно и может быть встроено в протокол. *Асинхронная связь* означает, что сообщения могут доставляться произвольно долго, и известно, что протоколы BFT не могут быть построены для асинхронных сетей даже при наличии только одного вредоносного валидатора. Реалистичным компромиссом между синхронностью и асинхронностью является предположение о *частично синхронной коммуникации*. Сеть может быть полностью асинхронной до некоторого неизвестного времени глобальной стабилизации (GST), но после GST коммуникация становится синхронной с известной верхней границей Δ [17].

Типичные блокчейны работают при допущении $> F$ корректных валидаторов. Для синхронных сетей обычно задается $F = 1/2$, но для более слабого предположения о частично синхронной сети $F = 2/3$.Bitcoin, его форки и текущая Proof-of-Work версия Ethereum работают только при условии синхронности. Другие, такие как Algorand и Cosmos, требуют только частичной синхронности. При соединении цепочек через Axelar, соединение работает в предположении самой сильной сети из этих цепочек, что в случае соединения Bitcoin и Cosmos, например, является синхронностью. Сам блокчейн Axelar работает в условиях частичной синхронности и поэтому требует $F = 2/3$, но можно повысить пороговое требование, предположив, что другие существующие блокчейны безопасны, и используя их безопасность.

4.2 Криптографические прелиминарии

Цифровые подписи. *Схема цифровой подписи* представляет собой кортеж алгоритмов (*Keygen, Sign, V erify*). *Keygen* выдает пару ключей (*PK, SK*). Только владелец *SK* может подписывать сообщения, но любой может проверить подписи, учитывая открытый ключ *PK*. Большинство блокчейн-систем сегодня используют одну из стандартных схем подписи, таких как ECDSA, Ed25519 или несколько их вариантов [23].

Пороговые подписи. *Пороговая схема подписи* позволяет группе из n сторон разделить секретный ключ для схемы подписи таким образом, что любое подмножество из $t + 1$ или более сторон может сотрудничать для создания подписи, но никакое подмножество из t или менее сторон не может создать подпись или даже узнать какую-либо информацию о секретном ключе. Подписи, созданные пороговыми протоколами для ECDSA и EdDSA, выглядят идентично подписям, созданным отдельными алгоритмами.

Схема пороговой подписи заменяет алгоритмы *Keygen* и *Sign* для обычной схемы подписи

распределенными протоколами *T.Keygen*, *T.Sign для n сторон*. Эти протоколы обычно требуют как публичного широковещательного канала, так и частных парных каналов между сторонами, и обычно включают несколько раундов связи. После успешного завершения *T.Keygen* каждый пользователь имеет долю s_i секретного ключа SK и соответствующего открытого ключа PK. Протокол *T.Sign* позволяет этим сторонам создать подпись для

данного сообщения, которая действительна при открытом ключе PK. Эта подпись может быть проверена любым человеком с помощью функции *Verify*
алгоритм оригинальной схемы подписи.

4.3 Свойства пороговых сигнатур

Есть несколько свойств, которыми может обладать пороговая схема, особенно желательных для децентрализованных сетей:

Безопасность против нечестного большинства. Некоторые пороговые схемы имеют ограничение, что они безопасны только тогда, когда большинство из n сторон являются честными. Таким образом, пороговый параметр t должен быть меньше $n/2$ [15]. Это ограничение обычно сопровождается тем, что для подписания требуется $2t + 1$ честная сторона, хотя только $t + 1$ коррумпированная сторона может сговориться, чтобы восстановить секретный ключ. Схемы, которые не страдают от этого ограничения, считаются *защищенными от нечестного большинства*.

Как обсуждается далее в разделе 5.2платформы межцепочечных сетей должны максимизировать безопасность своих сетей и быть в состоянии терпеть как можно больше коррумпированных сторон. Таким образом, необходимы схемы, которые могут терпимо относиться к нечестному большинству.

Предварительные подписи, неинтерактивное онлайн-подписание. Стремясь уменьшить бремя общения сторон, подписывающих сообщение, несколько последних протоколов определили значительную часть работы по подписанию, которая может быть выполнена "в автономном режиме", до того, как станет известно сообщение, которое нужно подписать [18, 13]. Результат этой автономной фазы называется *предварительной подписью*. Производство предварительных подписей рассматривается как отдельный протокол *T.Presign,* отличный от *T.Keygen* и *T.Sign*. Результаты протокола предварительной подписи должны храниться сторонами в тайне до тех пор, пока они не используют их на этапе подписания. Позже, когда сообщение для подписи становится известным, для завершения подписи в *T.Sign* остается выполнить лишь небольшой объем дополнительной "онлайновой" работы.

Онлайн-фаза *T.Sign* не требует никакого общения между сторонами. Каждая сторона просто выполняет локальные вычисления над сообщением и предварительной подписью, а затем объявляет свою долю s_i подписи. (После обнародования эти доли подписи s_1, ... , s_{t+1} могут быть легко объединены любым человеком для раскрытия действительной подписи s.) Это свойство называется *неинтерактивной онлайн-подписью*.

Надежность. Пороговые схемы гарантируют только то, что подмножество злонамеренных сторон не сможет подписать сообщения или узнать секретный ключ. Однако эта гарантия не исключает возможности того, что злоумышленники могут заблокировать всем остальным возможность получения ключей или подписей. В некоторых схемах злонамеренное поведение даже одной стороны может привести к прерыванию *T.Keygen* или *T.Sign* без полезного результата. Единственным выходом является перезапуск протокола, возможно, с другими сторонами.

Вместо этого для децентрализованных сетей мы хотим, чтобы *T.Keygen* и *T.Sign были* успешными, если по крайней мере $t + 1$ сторон являются честными, даже если некоторые злонамеренные стороны посылают неверно оформленные сообщения или отбрасывают сообщения в протоколах. Это свойство называется *устойчивостью*.

Атрибуция ошибок. Способность выявлять недобросовестных участников *T.Keygen* или *T.Sign* называется *атрибуцией вины*. Без атрибуции вины трудно надежно исключить или наказать плохих участников, и в этом случае издержки, вызванные плохими участниками, должны нести все. Это свойство также важно для децентрализованных сетей, где злонамеренное поведение должно быть идентифицируемым и экономически дестимулируемым с помощью правил слэшинга.

Безопасность в параллельных условиях. Схема подписи должна быть безопасной в параллельной среде, где несколько экземпляров алгоритмов генерирования ключей и подписи могут быть

задействованы параллельно. (Драйверс и др. [16], например, продемонстрировали атаку на мультиподписные схемы Шнорра в таких условиях). Существуют версии схем ECDSA и Schnorr, которые удовлетворяют этим свойствам [1322].

ECDSA и EdDSA, безусловно, являются наиболее широко применяемыми схемами подписи в блокчейне. В связи с этим пороговые версии обеих схем стали предметом недавнего возрождения исследований и разработок. Читатели, интересующиеся новейшей информацией, могут обратиться к [221318] и недавний обзорный документ [12].

5 Акселярная сеть

5.1 Проектирование открытой межцепочечной сети

Мосты, которые поддерживает сеть Axelar, поддерживаются пороговыми учетными записями, так что (почти) все валидаторы должны коллективно санкционировать любой межцепочечный запрос. Проектирование сети, в которой каждый может участвовать, для обеспечения безопасности этих мостов требует выполнения следующих технических требований:

- *Открытое членство*. Любой пользователь должен иметь возможность стать валидатором (следуя правилам сети).
- *Обновление членства*. Когда валидатор честно покидает систему, его ключ должен быть соответствующим образом аннулирован.
- *Поощрения и сокращение*. Вредоносные валидаторы должны быть идентифицируемы, а их действия должны выявляться и устраняться протоколом.
- *Консенсус*. Пороговые схемы сами по себе определяются как отдельные протоколы. Для распространения сообщений между узлами нам нужны как широковещательные, так и частные каналы "точка-точка". Более того, валидаторы должны согласовывать последнее состояние каждого вызова пороговых схем, поскольку они часто имеют несколько раундов взаимодействия.
- *Управление ключами*. Как обычные валидаторы в любой системе PoS должны тщательно охранять свои ключи, так и валидаторы Axelar должны охранять свои пороговые доли. Ключи необходимо чередовать, разделять между онлайн и офлайн частями и т.д.

Axelar начинает работу с модели делегированного доказательства принятия решений, где сообщество выбирает набор валидаторов для проведения консенсуса. Обратите внимание, что стандартные пороговые схемы относятся к каждому игроку одинаково и не имеют понятия "веса" в консенсусе. Следовательно, сеть должна адаптировать их для учета веса валидаторов. Простой подход заключается в назначении нескольких пороговых долей более крупным валидаторам. Ниже описаны три основные функции, которые коллективно выполняют валидаторы.

- *Генерация пороговых ключей*. Существующие алгоритмы генерации пороговых ключей для стандартных схем подписи блокчейна (ECDSA, Ed25519) представляют собой интерактивные протоколы между несколькими участниками (см. раздел 4). Специальная транзакция в сети Axelar инструктирует валидаторов начать выполнение этого протокола с состоянием. Каждый валидатор запускает процесс порогового демона, который отвечает за безопасное хранение секретного состояния. Для каждой фазы протокола:

  1. Валидатор хранит состояние протокола в своей локальной памяти.
  2. Он вызывает секретный демон для генерации сообщений в соответствии с описанием протокола для других валидаторов.
  3. Он распространяет сообщения либо по широковещательным, либо по частным каналам другим валидаторам.
  4. Каждый валидатор выполняет функции перехода состояния для обновления своего состояния, перехода к следующей фазе протокола и повторения описанных выше шагов.

  В конце протокола на цепочке Axelar генерируется пороговый открытый ключ, который может быть отображен обратно пользователю (например, для пополнения счета) или приложению, создавшему первоначальный запрос.

- *Пороговая подпись*. Запросы на подписание в сети Axelar обрабатываются аналогично запросам на генерацию ключей. Они вызываются, например, когда пользователь хочет вывести актив из одной из цепочек. Это интерактивные протоколы, и переход состояния между раундами происходит в зависимости от сообщений, распространяемых через представление блокчейна Axelar и локальную память каждого валидатора.

- *Обработка изменений в составе валидаторов*. Набор валидаторов необходимо периодически менять, чтобы к нему могли присоединиться новые заинтересованные стороны. При обновлении набора валидаторов нам необходимо обновить пороговый ключ, который будет использоваться совместно с новым набором. Таким образом, если бы мы разрешили любому желающему присоединиться в любое время, нам пришлось бы очень часто обновлять пороговый ключ. Чтобы предотвратить это, мы ротируем валидаторы каждые T блоков. В течение интервалов в T раундов набор V и^R пороговый ключ фиксированы. На каждом раунде, который является интегральным кратным параметра T, мы обновляем набор валидаторов следующим образом:

1. В любом раунде R, состояние Axelar отслеживает текущий набор валидаторов V^R . $V = ^{R+1} V$, если только^R
   R + является1 кратным T .
2. Во время раундов $((i - 1)T, iT]$ пользователи публикуют сообщения о связывании и разрыве связей.
3. В конце раунда iT , эти сообщения применяются к V для $^{iT-1}$получения V .^{iT}

- *Генерация порогового ключа и подписание в присутствии ротируемых валидаторов.* Блокчейн Axelar может выдать запрос на новый ключ или пороговую подпись на раунде R. Процесс подписания занимает больше времени, чем один раунд, и мы не хотим замедлять консенсус, поэтому мы просим, чтобы подпись была произведена до начала раунда R + 10. В частности, валидаторы начинают раунд R + 10 только после того, как увидят сертификат для раунда R + и9 подпись для каждого запроса на ключ/подпись, выданного в раунде R. Результат всех запросов раунда R должен быть включен в блок R + 11. Другими словами, предложение блока раунда R, не содержащее исходов раунда R, 11считается недействительным, и валидаторы не голосуют по нему. Чтобы гарантировать, что все пороговые сообщения будут подписаны до обновления набора валидаторов, Axelar не
  выдавать любые пороговые запросы во время раунда, равные $-1, -2, \ldots, -$ по 9модулю T .

5.2 Сетевая безопасность

Безопасность блокчейн-систем зависит от различных криптографических и теоретико-игровых протоколов, а также от децентрализации сети. Например, в блокчейн-системах proof-of-stake без надлежащих стимулов валидаторы могут сговориться и переписать историю, украв при этом средства других пользователей. В сетях proof-of-work без достаточной децентрализации довольно легко создавать длинные форки и двойные траты, что доказали многочисленные атаки на Bitcoin Gold и Ethereum Classic.

Большинство исследований в области безопасности блокчейна было сосредоточено на суверенных цепочках. Но когда цепи взаимодействуют между собой, необходимо учитывать новые векторы атак. Например, предположим, что Ethereum общается с небольшим блокчейном X через прямой мост, управляемый двумя смарт-контрактами, один на Ethereum, другой на X. Помимо инженерных задач, которые мы обобщили в разделе 1.1необходимо решить, что произойдет, если доверие к X будет нарушено. В этом случае, если ETH перешел на X, валидаторы X могут сговориться и подделать историю X, в которой они владеют всеми ETH, разместить поддельные доказательства консенсуса на Ethereum и украсть ETH. Ситуация становится еще хуже, когда X связана с множеством других цепочек через прямые мосты, где в случае форка X последствия распространяются по всем мостам. Установление руководящих принципов управления восстановлением для каждого парного моста - непосильная задача для любого отдельного проекта.

Сеть Axelar решает проблемы безопасности с помощью следующих механизмов:

- *Максимальная безопасность.* Axelar устанавливает порог безопасности на уровне 90%, что означает, что почти всем валидаторам придется сговориться, чтобы вывести средства, заблокированные его сетью, или подделать государственные доказательства[1]. На практике было замечено, что валидаторы PoS имеют очень высокое время работы (близкое к 100%), при условии, что они должным образом стимулированы. Следовательно, сеть Axelar будет производить блоки, даже несмотря на такой высокий порог. Однако в редких случаях, когда что-то пойдет не так и сеть заглохнет, сети необходимы надежные механизмы отката для перезагрузки системы, описанные далее.

- *Максимальная децентрализация.* Поскольку в сети используются схемы пороговых подписей, число валидаторов может быть максимально большим. Сеть не ограничена числом валидаторов, которое мы можем поддерживать, лимитами транзакций или комиссионными, которые возникли бы, например, при использовании нескольких подписей на разных цепочках, где сложность (и комиссионные) линейно возрастают с увеличением числа

валидаторов.[2]

- *Надежные механизмы отката.* Первый вопрос, который необходимо решить в сети с высокими порогами безопасности, как описано выше, - что произойдет, когда сама сеть остановится. Предположим, что сеть Axelar сама остановится. Можем ли мы иметь механизм отката, который позволит пользователям вернуть свои средства? Для решения проблемы возможной остановки самой сети Axelar каждый счет порогового моста на блокчейне X, который коллективно контролируют валидаторы Axelar, имеет "ключ аварийной разблокировки". Этот ключ может быть передан

[1]Окончательный параметр, который будет выбран для развертывания сети, может быть скорректирован.

[2]Для некоторых блокчейнов мультиподписи являются разумной альтернативой, если стоимость газа невелика, а поддерживаемые форматы сообщений подходят. Но они не масштабируются для двух самых крупных платформ, таких как Bitcoin и Ethereum.

и даже может быть пользовательским ключом для блокчейна X, который будет общим для всего сообщества этой цепи. Таким образом, если сеть Axelar остановится, этот ключ будет действовать как запасной вариант и позволит восстановить активы (подробнее см. ниже).

- *Максимальная децентрализация механизмов резервного копирования*. Этот резервный механизм включает в себя вторичный *набор* пользователей для *восстановления,* в котором может участвовать любой желающий без каких-либо затрат. Этим пользователям не нужно быть онлайн, управлять узлами или координировать действия друг с другом. Их "вызывают на службу" только в том случае, если сеть Axelar застопорится и не сможет восстановиться. Безопасность сети повышается за счет очень высокого порога для первичного набора валидаторов и максимально децентрализованного вторичного набора восстановителей.

- *Общее управление*. Общий протокол управляет сетью Axelar. Совместно пользователи могут голосовать за то, какую сеть следует поддерживать через сеть. Сеть также распределяет пул средств, которые могут быть использованы для возмещения расходов пользователей в случае непредвиденных чрезвычайных ситуаций, которые также контролируются протоколами управления.

Ниже рассматриваются различные механизмы безопасности.

Механизмы аварийного разблокирования. Когда Axelar останавливается из-за высокого порога, "аварийный ключ разблокировки" берет на себя контроль над сетью. Существует несколько способов инстанцирования этого ключа разблокировки, и некоторые сети/приложения могут использовать различные варианты "набора восстановления" или полностью отказаться от него:[3]

- *Вариант a*. Передать ключ основателям блокчейн-проектов и авторитетным людям в сообществе.

- *Вариант b*. Разделить между партиями, избранными через механизм делегированных PoS.

- *Вариант c*. Для учетных записей, управляющих активами и информацией для цепочки/приложения X, поделитесь пользовательским ключом с заинтересованными сторонами/валидаторами X. Предполагая, что X имеет механизмы управления на месте, те же механизмы управления могут быть применены для определения курса действий, если Axelar застопорится.

Теперь, учитывая идентификаторы пользователей восстановления и их открытые ключи, простой протокол генерирует доли ключа восстановления, которые никому не известны. Более того, пользователям набора ключей восстановления не нужно находиться в сети до тех пор, пока они не будут вызваны для восстановления через механизмы управления. Следуя стандартным протоколам распределенной генерации ключей, каждый валидатор Axelar передает случайное значение. Секретный ключ восстановления генерируется путем суммирования этих значений. Вместо того чтобы выполнять суммирование в открытом виде, все доли шифруются под открытыми ключами пользователей восстановления, а затем складываются гомоморфно (это предполагает аддитивно гомоморфное шифрование и дополнительный уровень нулевого знания, оба из которых легко достижимы). Результатом этого протокола является открытый ключ восстановления *RPK* и потенциально тысячи шифровок (под открытыми ключами пользователей восстановления) долей соответствующего секретного ключа $Enc_i(s_i)$, которые распространяются среди их владельцев (например, размещаются на цепочке). Мостовые контракты Axelar включают возможность восстановления средств с помощью *RPK* при определенных условиях. Наконец, можно обновить этот ключ восстановления и даже изменить набор пользователей, владеющих его долями, не требуя никакой работы от участвующих акционеров.

Если цепь X, соединенная с Акселаром, оборвется, есть несколько вариантов:

- Установите ограничения на стоимость активов в долларах США, которые могут быть перемещены в/из X в любой отдельный день. Таким образом, вредоносная цепочка X может украсть лишь небольшую часть всех активов, подключенных к ней, прежде чем валидаторы Axelar обнаружат это, и в действие вступят механизмы управления, описанные в следующих

пунктах.

- Модуль управления Axelar можно использовать для голосования о том, что происходит в таких ситуациях. Например, если произошла доброкачественная ошибка и сообщество перезапускает X, управление Axelar может определить, что нужно перезапустить соединение с того места, на котором оно остановилось.
- Если ETH переместился в X, пользовательский ключ восстановления Ethereum может определить, что произойдет с активами ETH.

[3]Окончательное развертывание в сети Axelar будет завершено ближе к запуску сети.

6 Протокол межцепочечного шлюза (CGP)

В этом разделе мы объясним протокол межсетевого шлюза и механизмы маршрутизации на двух основных примерах, общих для потребностей многих приложений:

Синхронизация состояний (раздел 6.2). Поместите информацию о состоянии блокчейна-источника *S* в состояние блокчейна-получателя *D*.

(Например, поместить заголовок блока Bitcoin в блокчейн Ethereum).

Передача активов (Раздел 6.3). Передача цифрового актива из *S* в *D* и обратно.

(Например, перевести биткоины с блокчейна Bitcoin на блокчейн Ethereum, а затем обратно на блокчейн Bitcoin).

Для простоты мы предполагаем, что цепочка *D* имеет хотя бы минимальную поддержку смарт-контрактов, но *S* может быть любой блокчейн.

6.1 Счета в других сетях

Чтобы соединить различные цепочки, в каждой из них создаются пороговые счета, которые контролируют поток ценности и информации между ними. Для цепочки *Chain* обозначим счет *ChainAxelar*.

Биткойн-счет. Для Биткойна и других цепочек не умных контрактов валидаторы Axelar создают пороговый ключ ECDSA в соответствии с разделом 5.1. Этот ключ контролирует счет ECDSA в Bitcoin и является адресом назначения, на который пользователи отправляют депозиты. По запросу пользователя могут быть созданы персонализированные пороговые ключи. Ключ может периодически обновляться, а последний ключ и персонализированные ключи можно найти, запросив узел Axelar.

Пороговый мостовой счет на цепочках с умными контрактами. Обозначим цепочку через SC. валидаторы создают пороговый ключ ECDSA или ED25519 в соответствии с разделом 5.1в зависимости от того, какой тип ключа поддерживает цепочка. Мы обозначаем этот ключ *PKAxelar*, когда нет двусмысленности относительно того, к какой цепочке мы обращаемся. Этот ключ управляет аккаунтом смарт-контракта на SC, обозначаемым *SCAxelar*, и любое приложение на SC может запросить *SCAxelar,* чтобы узнать PK-адрес этого ключа. Таким образом, любое приложение SC может распознать сообщения, подписанные *SKAxelar*. Протокол также должен учитывать вращающиеся значения *PKAxelar*. Это происходит следующим образом:

1. Инициализируйте *SCAxelar* на SC. Он хранит *PKAxelar* как часть своего состояния, которое инициализируется как значение генезиса на Axelar. *SCAxelar* также включает правила для обновления PK.
2. Чтобы обновить *PKAxelar*, должна быть представлена транзакция формата (*update,* PK_{new}) с подписью от текущего *SKAxelar*. Затем контракт устанавливает *PKAxelar* = PK_{new}.
3. Каждый раз, когда валидаторы обновляют пороговый ключ для SC от PK^i до PK^{i+1}, Axelar запрашивает, чтобы валидаторы использовали SK^i для подписи (*update,* PK^{i+1}). Впоследствии эта подпись отправляется в *SCAxelar*, который обновляет *PKAxelar*.

6.2 Синхронизация состояний

Пусть q_S обозначает произвольный вопрос о состоянии цепи *S*. Примерами таких вопросов являются:

- *"В каком раунде блока, если таковой имеется, появился tx транзакции?"*.
- *"Каково значение определенного поля данных?"*.

- *"Каков корневой хэш Меркла всего состояния S в раунде блока 314159?"*.

Пусть a_S обозначает правильный ответ на q_S, и предположим, что конечный пользователь или приложение требует, чтобы a_S было опубликовано в цепочке D. Сеть Axelar удовлетворяет это требование следующим образом:

1. Пользователь размещает запрос q_S на одном из счетов бриджа (который впоследствии подхватывается валидаторами) или непосредственно на блокчейне Axelar.

2. В рамках консенсуса Axelar каждый валидатор должен запустить программное обеспечение узла для цепочек *S*, *D*. Валидаторы Axelar запрашивают API своего программного обеспечения узла цепочки *S* для получения ответа a_S и сообщают ответ цепочке Axelar.

3. Как только > *F* взвешенных валидаторов сообщают один и тот же ответ в раунде *R*, Акселар просит валидаторов подписать *документ*$_S$.

4. Используя пороговую криптографию, проверяющие подписывают a_S. Подпись включается в блок *R* + 11.

5. Любой может взять подписанное значение a_S из блока R+ и 11отправить его в *D*.

6. Запрос был обслужен. Теперь любое приложение на *D* может взять подписанное значение a_S, запросить у $_{DAxelar}$ последний *PKAxelar* и проверить, что подпись a_S соответствует *PKAxelar*. Валидаторы также отправляют a_S в учетную запись моста на цепочке *D*, которую могут получить приложения.

6.3 Межцепочечная передача активов

Сеть позволяет осуществлять межцепочечную передачу цифровых активов, расширяя рабочий процесс синхронизации состояний в разделе 6.2.

Достаточный запас привязанных токенов-S печатается и контролируется $_{DAxelar}$ при его инициализации. Предположим, пользователь требует обменять *x* количество токенов на цепочке-источнике *S* на *x* количество привязанных токенов S на цепочке назначения *D*, которые должны быть помещены на *D-адрес* w_D по выбору пользователя. Мы представляем полностью общий рабочий процесс, который поддерживает произвольные цепочки источников *S - даже такие* цепочки, как Bitcoin, которые не поддерживают смарт-контракты:

1. Пользователь (или приложение, действующее от имени пользователя) отправляет запрос на перевод (x, w_D) на счет порогового моста, который впоследствии направляется в сеть Axelar.

2. Валидаторы Axelar используют пороговую криптографию для коллективного создания свежего адреса депозита d_S для *S*. Они публикуют d_S в блокчейне Axelar.

3. Пользователь (или приложение, действующее от имени пользователя) узнает d_S путем мониторинга блокчейна Axelar. Пользователь отправляет *x* количество *S-токенов* на адрес d_S посредством обычной *S-транзакции tx,* используя$_S$ свое любимое программное обеспечение для цепочки *S*.

   (В силу порогового свойства d_S*, жетоны из d не могут быть потрачены, пока пороговое число валидаторов* $_S$*не даст на это согласия).*

4. *tx* $_S$размещается на Axelar. Валидаторы запрашивают API программного обеспечения своего узла цепочки *S* на предмет существования
   tx и$_S$, если ответ "true", сообщить ответ в цепочку Axelar.

5. Как только > *F* взвешенных валидаторов сообщают "true" для *tx* в $_S$раунде *R*, Axelar просит валидаторов подписать транзакцию a_D, которая отправляет *x* количество токенов pegged-S от $_{DAxelar}$ на w_D.

6. Используя пороговую криптографию, проверяющие подписывают a_D. Подпись включается в блок *R* + 11.

7. Любой может взять подписанное значение a_D из блока R+ и 11отправить его в *D*.

8. Запрос был обслужен, как только на *D* $_D$будет размещено сообщение, перевод будет обработан.

Теперь предположим, что пользователь требует выкупить x^i количество токенов wrapped-S из

цепочки *D* обратно в цепочку *S*, чтобы положить их на *S-адрес* w_S по выбору пользователя. Рабочий процесс выглядит следующим образом:

1. Пользователь инициирует запрос на перевод (x^i, w_S), внося x^i количество токенов wrapped-S в c_D посредством обычной D-транзакции, используя свое любимое программное обеспечение для цепочки *D*.

2. (x^i, w_S) публикуется на Axelar. Валидаторы запрашивают API программного обеспечения узла *D* своей цепочки на предмет существования (x^i, w_S) и, если ответ "true", сообщают ответ цепочке Axelar.

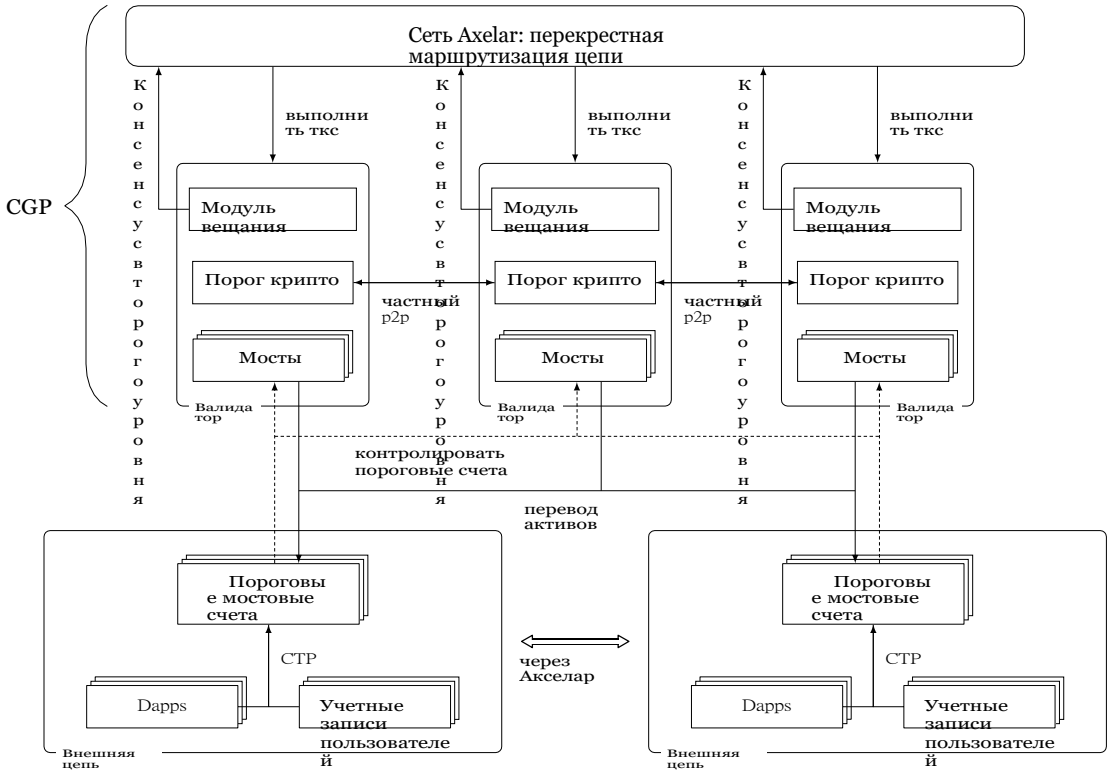

Рисунок 1: Диаграмма компонентов

3. Как только > *F* взвешенных валидаторов сообщают "true" для (x^i, w_S) в раунде *R*, Axelar просит валидаторов подписать транзакцию a_S, которая отправляет x^i количество токенов *S* от $_{SAxelar}$ к $w._S$
4. Используя пороговую криптографию, проверяющие подписывают a_S. Подпись включается в блок *R* + 11.
5. Любой может взять подписанное значение a_S из блока R+ и 11отправить его в *S*.
6. Запрос был обслужен, как только на S_sбудет размещено сообщение, перевод будет обработан.

Дополнительные запросы, поддерживаемые уровнем маршрутизации CGP, включают блокировку, разблокировку или передачу активов по цепочкам.

Достижение атомарного потока межцепочечных транзакций. В зависимости от типа межцепочечного запроса Axelar пытается обеспечить выполнение соответствующих транзакций на нескольких цепях или ни на одной. Для этого каждый запрос может находиться в одном из следующих состояний в блокчейне Axelar: *(инициализирован, ожидает, завершен, тайм-аут)*. Если происходит *тайм-аут* на стадии ожидания, запрос возвращает код ошибки. Некоторые события тайм-аута также запускают событие *возврата*: например, если актив из одной цепи нужно перевести в актив другой цепи, если принимающая цепь не обработала транзакцию, актив возвращается обратно первоначальному пользователю.

7 Протокол межцепочечной передачи (CTP)

CTP - это протокол на уровне приложений, который облегчает приложениям использование возможностей межцепочечного обмена. Мы объясняем интеграцию, сосредоточившись на функциях передачи активов (например, используемых в DeFi). Такие приложения обычно состоят из трех

основных компонентов: графического интерфейса пользователя, смарт-контрактов на одной цепи и узла-посредника, который осуществляет транзакции между внешним интерфейсом и смарт-контрактами. Внешние интерфейсы взаимодействуют с кошельками пользователей для приема депозитов, обработки снятия средств и т.д. Приложения могут использовать возможности межцепочечного взаимодействия

путем вызова запросов CTP, аналогичных методам HTTP/HTTPS GET/POST. Эти запросы впоследствии подхватываются уровнем CGP для выполнения, а результаты возвращаются обратно пользователям.

- *CTP-запросы*. Разработчики приложений могут размещать свои приложения на любой цепочке и интегрировать свои смарт-контракты с пороговыми мостовыми счетами для выполнения CTP-запросов.
- *Счета пороговых мостов*. Предположим, разработчик приложения строит свои контракты на цепочке A. Тогда для получения межцепочечной поддержки он будет ссылаться на пороговые мостовые контракты. Этот контракт позволяет приложениям:
  - Зарегистрировать блокчейн, с которым он хотел бы общаться.
  - Зарегистрировать на блокчейне активы, которые он хотел бы использовать.
  - Выполнять операции над активами, такие как прием депозитов, обработка снятия средств и другие функции (аналогично, скажем, звонкам по контракту ERC-20).

Предположим, что известное приложение DeFi, MapleSwap, которое изначально находится на цепочке A, регистрируется с помощью порогового моста. Валидаторы Axelar коллективно управляют самим контрактом на соответствующей цепочке. Предположим, что пользователь хочет внести депозит в торговую пару между активами X и Y, которые расположены на двух цепочках соответственно. Тогда, когда пользователь подает такой запрос, он направляется через пороговый мостовой счет в сеть Axelar для обработки. Там выполняются следующие шаги:

1. Сеть Axelar понимает, что это приложение зарегистрировано для поддержки кросс-цепочек по всем активам. Она генерирует ключ депозита, используя пороговую криптографию и консенсус для пользователя на соответствующих цепочках A и B.
2. Соответствующие открытые ключи возвращаются в приложение и отображаются пользователю, который может использовать свои любимые кошельки для отправки депозитов. Соответствующий секретный ключ совместно используется всеми валидаторами Axelar.
3. Когда депозиты подтверждены, Axelar обновляет свой кросс-цепной каталог, чтобы записать, что пользователь на соответствующих цепях депонировал эти активы.
4. Валидаторы Axelar выполняют многосторонние протоколы для генерации пороговой подписи, которая позволяет обновить счет порогового моста на цепочке A, где находится приложение.
5. Запрос CTP затем возвращается смарт-контрактам приложения DeFi, которые могут обновить его состояние, обновить формулы доходности, курсы обмена или выполнить другие условия, связанные с состоянием приложения.

На протяжении всего этого процесса сеть Axelar на высоком уровне действует как децентрализованный оракул для чтения/записи между цепочками, CGP - уровень маршрутизации между цепочками, а CTP - прикладной протокол.

Дополнительные кросс-цепные запросы. CTP поддерживает более общие кросс-цепочки между приложениями на разных блокчейнах, такие как:

- Осуществляйте службу имен открытых ключей (PKNS). Это универсальный каталог для сопоставления открытых ключей с номерами телефонов/ручками Twitter (несколько проектов, например Celo, предоставляют эти функции в рамках своих платформ).
- Межцепочечные триггеры приложений. Приложение на цепочке A может обновить свое состояние, если какое-то другое приложение на цепочке B удовлетворяет критерию поиска (процентная ставка < *X*).

- Совместимость смарт-контрактов. Умный контракт на цепочке A может обновить свое состояние на основе состояния контрактов на цепочке B, или вызвать действие для обновления умного контракта на цепочке B.

На высоком уровне эти запросы могут быть обработаны, поскольку в совокупности протоколы CTP, CGP и сеть Axelar могут передавать и записывать произвольную проверяемую информацию о состоянии в блокчейн.

8 Резюме

В ближайшие годы значительные приложения и активы будут построены на базе нескольких экосистем блокчейн. Сеть Axelar может быть использована для объединения этих блокчейнов в единый межцепочечный коммуникационный слой. Этот уровень обеспечивает маршрутизацию и протоколы на уровне приложений, которые отвечают требованиям как создателей платформ, так и разработчиков приложений. Разработчики приложений могут создавать платформы, наиболее подходящие для их нужд, и использовать простой протокол и API для доступа к глобальной межцепочечной ликвидности, пользователям и связи с другими цепочками.

Ссылки

[1] Althea Peggy. https://github.com/cosmos/peggy. [Цитируется по стр. 2.]

[2] Детерминированное использование алгоритма цифровой подписи (dsa) и алгоритма цифровой подписи на эллиптической кривой (ecdsa). https://tools.ietf.org/html/rfc6979. [Цитируется по стр. 5.]

[3] Алгоритм цифровой подписи по кривой Эдвардса (Edwards-curve digital signature algorithm, eddsa). https://tools.ietf.org/html/rfc8032. [Цитируется по стр. 5.]

[4] Eos.io technical white paper v2. https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md. [Цитируется по стр. 1.]

[5] Ethereum: Безопасная децентрализованная обобщенная книга транзакций. https://ethereum.github.io/yellowpaper/paper.pdf. [Цитируется по стр. 1.]

[6] Почти белая бумага. https://near.org/papers/the-official-near-white-paper/. [Цитируется по стр. 1.]

[7] Радужный мост. https://github.com/near/rainbow-bridge. [Цитируется по стр. 2.]

[8] Ren: виртуальная машина с сохранением конфиденциальности, обеспечивающая работу финансовых приложений с нулевым знанием. https://whitepaper.io/document/419/ren-litepaper. [Цитируется по стр. 3.]

[9] tbtc: Децентрализованный выкупаемый токен erc-20, обеспеченный btc. https://docs.keep.network/tbtc/index. pdf. [Цитируется по стр. 2.]

[10] Thorchain: Децентрализованная сеть ликвидности. https://thorchain.org/. [Цитируется по стр. 3.]

[11] Курт М. Алонсо. От нуля до монеро. https://www.getmonero.org/library/Zero-to-Monero-1-0-0.pdf. [Цитируется по стр. 1.]

[12] Жан-Филипп Аумассон, Адриан Хамелинк и Омер Шломовиц. Обзор пороговой подписи ecdsa. Cryptology ePrint Archive, Report 2020/1390, h2020.ttps://eprint.iacr.org/2020/1390. [Цитируется по стр. 6.]

[13] Ран Канетти, Николаос Макрияннис и Уди Пелед. Uc неинтерактивная, проактивная, пороговая ecdsa. Cryptology ePrint Archive, Report 2020/492, 2020. https://eprint.iacr.org/2020/492. [Цитируется по стр. 6.]

[14] cLabs Whitepapers. https://celo.org/papers. [Цитируется по стр. 1.]

[15] Ivan Damg˚ard, Thomas Pelle Jakobsen, Jesper Buus Nielsen, Jakob Illeborg Pagter, and Michael Bæksvang Østerg˚ard. Быстрый пороговый ECDSA с честным большинством. В *SCN*, том 12238 *Лекций по информатике*, страницы 382-400. Springer, [2020. цитируется по стр. 6.]

[16] Ману Драйверс, Касра Эдалатнежад, Брайан Форд, Эйке Кильц, Джулиан Лосс, Грегори Невен и Игорь Степанов. О безопасности двухраундовых мультиподписей. В *симпозиуме IEEE по безопасности и конфиденциальности*, страницы 1084-1101. IEEE, [2019. цитируется по

стр. 6.]

[17] Синтия Дворк, Нэнси Линч и Ларри Стокмайер. Консенсус при наличии частичной синхронности.
https://groups.csail.mit.edu/tds/papers/Lynch/jacm88.pdf. [Цитируется по стр. 5.]

[18] Розарио Дженнаро и Стивен Голдфедер. Одноraундовый пороговый ecdsa с идентифицируемым прерыванием. Cryptology ePrint Archive, Report 2020/540, h2020.ttps://eprint.iacr.org/2020/540. [Цитируется по стр. 6.]

[19] Йосси Гилад, Ротем Гемо, Сильвио Микали, Георгиос Влахос и Николай Зельдович. Algorand: Масштабирование византийских соглашений для криптовалют. Труды 26-го симпозиума по принципам операционных систем, h2017.ttps://dl.acm.org/doi/pdf/10.1145/3132747.3132757. [Цитируется по стр. 1.]

[20] Эван Керейакс, До Квон, Марко Ди Маджио и Николас Платиас. Терра деньги: Стабильность и принятие.
https://terra.money/Terra_White_paper.pdf. [Цитируется по стр. 1.]

[21] Агелос Киайас, Александр Рассел, Бернардо Давид и Роман Олийныков. Уроборос: Доказательно безопасный протокол доказательства доли в блокчейне. https://eprint.iacr.org/2016/889.pdf. [цитируется по стр. 1.]

[22] Челси Комло и Ян Голдберг. Фрост: Гибкие пороговые подписи Шнорра, оптимизированные для раундов. Cryp- tology ePrint Archive, Report 2020/852, 2020. https://eprint.iacr.org/2020/852. [Цитируется по стр. 6.]

[23] Чжэ Квон и Итан Бакман. Космос: Сеть распределенных бухгалтерских книг.
https://cosmos.network/resources/whitepaper. [Цитируется по страницам и1 2.]

[24] Лавинная команда. Лавинная платформа.
https://www.avalabs.org/whitepapers. [Цитируется по страницам и1 2.]

[25] Гэвин Вуд. Polkadot: Видение гетерогенной многоцепочечной структуры.
https://polkadot.network/PolkaDotPaper.pdf. [Цитируется по страницам и1 2.]