ОБЗОР ПРОЕКТА

COSMOS

UBF

Краткое описание и история проекта

Cosmos Network — это децентрализованная сеть независимых, масштабируемых и совместимых блокчейнов, создающая основу для новой экономики токенов.

До создания Cosmos Network блокчейны были изолированы и не могли общаться друг с другом. Их было сложно построить, и они могли обрабатывать очень небольшое количество транзакций в секунду. Cosmos решает некоторые из самых сложных проблем блокчейна, связанных с масштабируемостью, удобством использования и функциональной совместимостью.

История Cosmos начинается в 2014 году, когда был основан Tendermint — основной участник сети. В 2016 году была опубликована белая бумага (white paper) Cosmos, а в 2017 году состоялась продажа токенов сети. Токены сети Cosmos называются Атом (ATOM) и зарабатываются они с помощью гибридного алгоритма proof-of-stake, тем самым помогая поддерживать безопасность Cosmos Hub (флагманского блокчейна проекта). Эта криптовалюта также играет роль в управлении сетью.

Cosmos SDK — это удобная для разработчиков модульная структура, каждая из которых основана на византийском отказоустойчивом алгоритме консенсуса (Byzantine Fault- Tolerant consensus algorithm — BFT), что позволяет разработчикам полностью настраивать свои децентрализованные приложения и сосредоточиться на бизнес-логике.

Показатели проекта

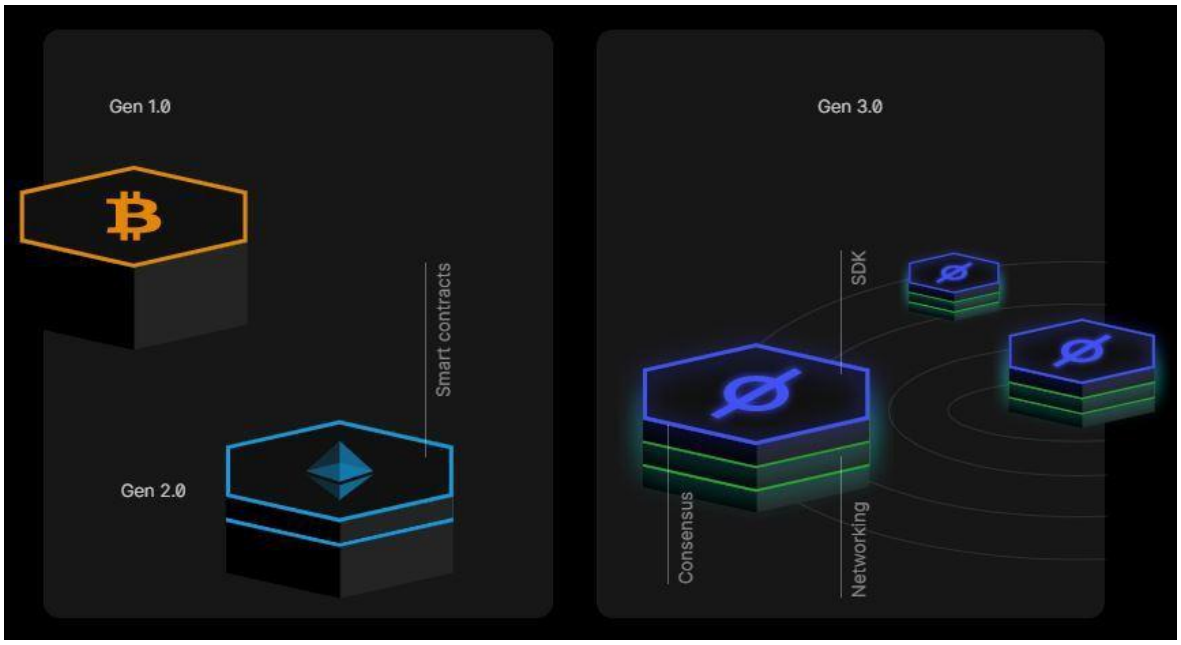
На 99% ниже углеродный след (по сравнению с традиционными сетями)

263 + приложений и сервисов

$148B+ средств сообщества

7 секунд — время подтверждения транзакции

$0,01 — размер комиссий



Кто мы такие

Interchain Foundation (ICF) — это швейцарский некоммерческий фонд, созданный для поддержки развития Cosmos и экосистемы, которая будет способствовать развитию сети Cosmos. ICF принимает заявки на гранты.

All in Bits Inc (dba Tendermint Inc) — компания по разработке программного обеспечения, нанятая ICF для разработки сети Cosmos.

IRIS Foundation Ltd. — поддерживается ICF для создания IRISnet, Cosmos Hub, который облегчает создание распределенных бизнес-приложений.

Cosmos Hub — это первый из множества хабов, запущенных в рамках Cosmos Network суверенных блокчейнов.

Tendermint BFT — это название протокола консенсуса Proof-of-Stake, на котором основаны Cosmos Hub и Cosmos SDK.

Команда

Соучредителями Tendermint были Джэ Квон, Зарко Милошевич и Итан Бухман. Хотя Квон по-прежнему указан в качестве главного архитектора, он ушел с поста генерального директора в 2020 году. Однако он утверждает, что по-прежнему участвует в проекте, но теперь сосредоточен на других задачах. Его пост генерального директора Tendermint занял Пэн Чжун, а весь совет директоров получил существенное обновление. Их цели включают в себя расширение опыта разработчиков, создание сообщества энтузиастов для Cosmos и
создание образовательных ресурсов, чтобы большее количество людей знало, что способна дать эта сеть.

Jae Kwon *jae@tendermint.com*

Ethan Buchman *ethan@tendermint.com*

Основные команды разработчиков Cosmos:

Agoric Akash Althea Chainapsis ChainSafe Confio Informal Systems Interchain GmbH Iqlusion IRIS Network PeggyJV Regen Network Sikka SnowFork Tendermint VitWit Zondax

Технологическая часть проекта

Cosmos — это сеть из множества независимых блокчейнов, называемых зонами. Зоны управляются Tendermint BFT, который обеспечивает высокопроизводительный, согласованный и безопасный механизм консенсуса, подобный PBFT (Practical Byzantine Fault Tolerance), где строгая ответственность за разветвление гарантирует контроль над поведением злоумышленников. Алгоритм консенсуса Tendermint BFT хорошо подходит для масштабирования общедоступных блокчейнов с доказательством доли (proof-of-stake).

Хаб и зоны

В то время как существующие предложения направлены на создание «единого блокчейна» с полным глобальным порядком транзакций, Cosmos позволяет множеству блокчейнов работать одновременно друг с другом, сохраняя при этом совместимость.

Первая зона в Cosmos называется Cosmos Hub.

В своей основе Cosmos Hub управляет множеством независимых блокчейнов, называемых «зонами» (иногда называемых «осколками» в связи с методом масштабирования базы данных, известным как «шардинг»). Постоянный поток последних коммитов блоков из зон, размещенных в хабе, позволяет хабу быть в курсе состояния каждой зоны. Точно так же каждая зона поддерживает состояние концентратора (но зоны не синхронизируются друг с другом, кроме как косвенно через концентратор). Затем пакеты информации передаются из одной зоны в другую путем публикации доказательств Меркла в качестве доказательства того, что информация была отправлена и получена. Этот механизм называется межблочной коммуникацией или сокращенно IBC.

Любая из зон сама по себе может быть хабом для формирования ациклического графа, но для ясности мы опишем только простую конфигурацию, где есть только один хаб и много зон, не являющихся хабами.

Cosmos Hub

Cosmos Hub — это блокчейн, в котором размещен распределенный реестр с несколькими активами, где токены могут храниться отдельными пользователями или самими зонами. Эти токены можно перемещать из одной зоны в другую в специальном пакете IBC, называемом «пакетом монет». Хаб отвечает за сохранение глобальной неизменности общей суммы каждого токена в зонах. Транзакции пакетов монет IBC должны быть зафиксированы цепочками блоков отправителя, концентратора и получателя.

Поскольку Cosmos Hub действует как центральная книга для всей системы, безопасность Hub имеет первостепенное значение. В то время как каждая зона может быть блокчейном Tendermint, который защищен всего четырьмя (или даже меньше, если не требуется консенсус BFT), Хаб должен быть защищен глобально децентрализованным набором валидаторов, которые могут противостоять самым серьезным сценариям атак, таким как как раздел континентальной сети или атака, спонсируемая национальным государством.

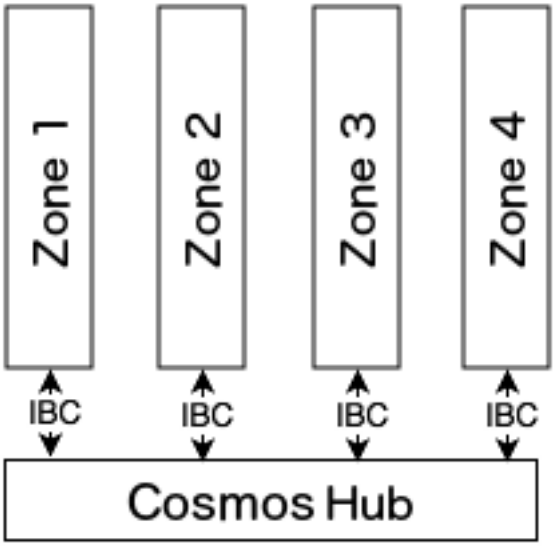
Эта архитектура решает многие проблемы, с которыми сегодня сталкивается пространство блокчейна, такими как: совместимость приложений, масштабируемость и возможность беспрепятственного обновления. Например, к Cosmos Hub можно подключить зоны, созданные на базе Bitcoind, Go-Ethereum, CryptoNote, ZCash или любой другой блокчейн- системы. Эти зоны позволяют Cosmos бесконечно масштабироваться для удовлетворения глобального спроса на транзакции. Зоны также отлично подходят для распределенного обмена, который также будет поддерживаться.

Зоны

Зона Cosmos — это независимая цепочка блоков, которая обменивается сообщениями IBC с хабом. С точки зрения концентратора зона — это учетная запись с несколькими активами, динамическим членством и несколькими подписями, которая может отправлять и получать токены с использованием пакетов IBC. Как и учетная запись криптовалюты, зона не может передавать больше токенов, чем у нее есть, но может получать токены от других, у которых они есть. Зона может быть обозначена как «источник» одного или нескольких типов токенов, что дает ей возможность увеличивать предложение токенов.

Атомы Cosmos Hub могут быть поставлены валидаторами зоны, подключенной к Hub. В то время как атаки с двойным расходом на эти зоны приведут к сокращению атомов с помощью форк-подотчетности Tendermint, зона, в которой более ⅔ голосов принадлежит византийцам, может зафиксировать недействительное состояние. Cosmos Hub не проверяет и не выполняет транзакции, совершенные в других зонах, поэтому пользователи обязаны отправлять токены в зоны, которым они доверяют. В будущем система управления Cosmos Hub может передать предложения по улучшению Hub, которые учитывают сбои зон. Например, исходящие передачи токенов из некоторых (или всех) зон могут быть

ограничены, чтобы обеспечить аварийное прерывание цепи зон (временную остановку передачи токенов) при обнаружении атаки.



Tendermint

Cosmos Hub — это первый общедоступный блокчейн в Cosmos Network, работающий на алгоритме консенсуса Tendermint BFT. Проект с открытым исходным кодом Tendermint появился в 2014 году для решения проблем скорости, масштабируемости и экологических проблем алгоритма консенсуса Proof-of-Work Bitcoin. Используя и улучшая проверенные алгоритмы BFT, разработанные в Массачусетском технологическом институте (MIT) в 1988 году, команда Tendermint стала первой, кто концептуально продемонстрировал криптовалюту с доказательством доли, которая решает проблему «ничего на кону», от которой страдает доказательство первого поколения — стейкинг криптовалют, таких как NXT и BitShares1.0.

Сегодня практически все мобильные биткойн-кошельки используют доверенные серверы для подтверждения транзакций. Это связано с тем, что доказательство работы требует ожидания множества подтверждений, прежде чем транзакция может считаться необратимо зафиксированной. Атаки с двойной тратой уже были продемонстрированы на таких сервисах, как CoinBase.

В отличие от других систем консенсуса на блокчейне, Tendermint предлагает мгновенную и доказуемо безопасную проверку платежей мобильных клиентов. Поскольку Tendermint никогда не разветвляется, мобильные кошельки могут получать мгновенное подтверждение транзакции, что делает ненадежные и практичные платежи реальностью на смартфонах.
Это также имеет значительные последствия для приложений Интернета вещей.

Валидаторы в Cosmos играют ту же роль, что и майнеры биткойнов, но вместо этого используют криптографические подписи для голосования. Валидаторы — это безопасные специализированные машины, которые отвечают за фиксацию блоков. Не-валидаторы могут

делегировать свои токены стейкинга (называемые «атомами») любому валидатору, чтобы заработать часть комиссий за блок и вознаграждения за атомы, но они несут риск наказания (сокращения), если валидатор-делегатор будет взломан или нарушит протокол. Проверенные гарантии безопасности консенсуса Tendermint BFT и залоговый депозит заинтересованных сторон — валидаторов и делегаторов — обеспечивают доказуемую, измеримую безопасность для узлов и легких клиентов.

Валидаторы

В классических алгоритмах византийской отказоустойчивости (BFT) каждый узел имеет одинаковый вес. В Tendermint узлы имеют неотрицательное число голосов, а узлы с положительным числом голосов называются валидаторами. Валидаторы участвуют в протоколе консенсуса, транслируя криптографические подписи или голоса для согласования следующего блока.

Право голоса валидаторов определяется при генезисе или детерминировано изменяется блокчейном, в зависимости от приложения. Например, в приложении для подтверждения доли, таком как Cosmos Hub, право голоса может определяться количеством токенов стейкинга, переданных в качестве залога.

Консенсус

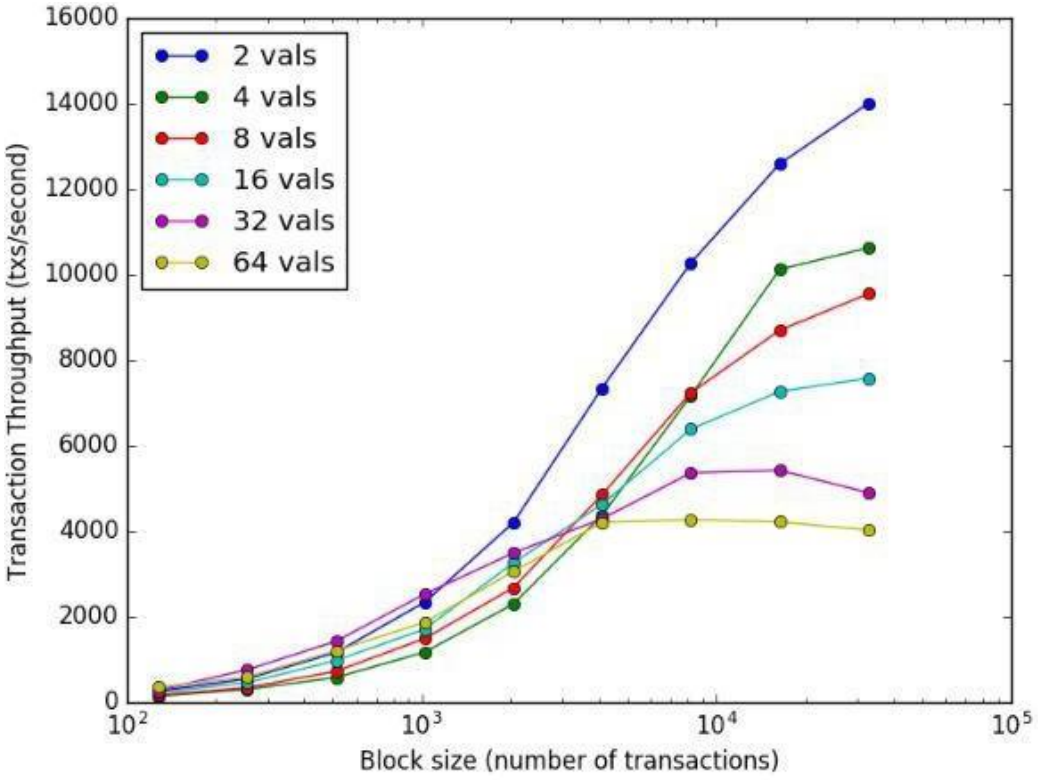
Tendermint — частично синхронный протокол консенсуса BFT, созданный на основе алгоритма консенсуса DLS. Tendermint отличается простотой, производительностью и форк- отчетностью. Для протокола требуется фиксированный известный набор валидаторов, где каждый валидатор идентифицируется своим открытым ключом. Валидаторы пытаются прийти к консенсусу по одному блоку за раз, где блок представляет собой список транзакций. Голосование за консенсус по блоку проходит по раундам. В каждом раунде есть лидер раунда, или предлагающий, который предлагает блок. Затем валидаторы поэтапно голосуют за то, принять ли предложенный блок или перейти к следующему раунду. Предлагающий раунд выбирается детерминистически из упорядоченного списка валидаторов пропорционально их количеству голосов.

Безопасность Tendermint проистекает из использования оптимальной византийской отказоустойчивости за счет квалифицированного большинства (> ⅔) голосования и механизма блокировки. Вместе они гарантируют, что:

- ≥⅓ права голоса должно быть византийским, чтобы вызвать нарушение безопасности, если совершено более двух значений;
- Если какому-либо набору валидаторов когда-либо удастся нарушить безопасность или даже попытаться это сделать, они могут быть идентифицированы протоколом. Это включает в себя как голосование за конфликтующие блоки, так и трансляцию необоснованных голосов.

Несмотря на сильные гарантии, Tendermint обеспечивает исключительную производительность. В бенчмарках 64 узлов (нод), распределенных по 7 центрам обработки данных на 5 континентах, в обычных облачных экземплярах консенсус

Tendermint может обрабатывать тысячи транзакций в секунду с задержкой фиксации порядка одной-двух секунд. Примечательно, что производительность, превышающая тысячу транзакций в секунду, сохраняется даже в условиях состязательности, когда валидаторы дают сбои или транслируют злонамеренно созданные голоса. Подробности см. на рисунке ниже.



Алгоритм консенсуса Tendermint реализован в программе Tendermint Core. Tendermint BFT — это независимый от приложений «механизм консенсуса», который может превратить любое детерминированное приложение «черный ящик» в распределено реплицированный блокчейн. Tendermint BFT подключается к блокчейн-приложениям через Application Blockchain Interface (ABCI). ABCI — это интерфейс, определяющий границу между механизмом репликации (блокчейн) и конечным автоматом (приложением). Используя протокол сокетов, мы позволяем механизму консенсуса, работающему в одном процессе, управлять состоянием приложения, работающим в другом.

Таким образом, ABCI позволяет программировать блокчейн-приложения на любом языке, а не только на том языке программирования, на котором написан механизм консенсуса. Кроме того, ABCI позволяет легко заменить уровень консенсуса любого существующего стека блокчейна.

Проводим аналогию с известной криптовалютой Bitcoin. Bitcoin — это криптовалютная цепочка блоков, в которой каждый узел поддерживает полностью проверенную базу данных неизрасходованных транзакций (UTXO). Если бы кто-то захотел создать биткоин- подобную систему поверх ABCI, Tendermint BFT отвечал бы за:

- Совместное использование блоков и транзакций между узлами;
- Установление канонического/неизменного порядка транзакций (блокчейн).

В то время как приложение ABCI будет отвечать за:

- Ведение базы данных UTXO;
- Проверка криптографических подписей транзакций;
- Предотвращение расходования транзакциями несуществующих средств;
- Разрешение клиентам запрашивать базу данных UTXO.

Tendermint может декомпозировать дизайн блокчейна, предлагая очень простой API между процессом подачи заявки и процессом консенсуса.

Управление

Распределенные публичные реестры должны иметь конституцию и систему управления. Bitcoin полагается на Фонд Биткоин и майнинг для координации обновлений, но это медленный процесс. Ethereum разделился на ETH и ETC после хард-форка для решения проблемы взлома TheDAO, в основном потому, что не было ни предварительного общественного договора, ни механизма для принятия таких решений.

Валидаторы и делегаторы в Cosmos Hub могут голосовать за предложения, которые могут автоматически изменять предустановленные параметры системы (такие как лимит блокированного газа), координировать обновления, а также голосовать за поправки к удобочитаемой конституции, которые регулируют политику Cosmos Hub. Конституция обеспечивает сплоченность заинтересованных сторон по таким вопросам, как кража и ошибки (например, инцидент с TheDAO), что позволяет решать их быстрее и тщательнее.

Каждая зона также может иметь свою собственную конституцию и механизм управления. Например, Cosmos Hub может иметь конституцию, обеспечивающую неизменяемость в Hub (без откатов, за исключением ошибок реализации узла Cosmos Hub), в то время как каждая зона может устанавливать свои собственные политики в отношении откатов.

Обеспечивая взаимодействие между различными зонами политик, сеть Cosmos предоставляет своим пользователям полную свободу и возможность экспериментировать без разрешения.

Atom

Хотя Cosmos Hub представляет собой распределенный реестр с несколькими активами, существует специальный собственный токен, называемый Atom. Atom — единственный токен для ставок Cosmos Hub, а также лицензия для держателя на голосование, валидацию или делегирование другим валидаторам. Как и Ethereum, Atom также могут использоваться для оплаты транзакционных комиссий и уменьшения спама. Дополнительные инфляционные Atom и комиссии за транзакцию блоков вознаграждаются валидаторам и делегаторам, которые делегируют полномочия валидаторам.

Транзакция BurnAtomTx может использоваться для восстановления любого пропорционального

количества токенов из резервного пула.

Сбор средств

Первоначальное распределение токенов атома и валидаторов на Genesis будет осуществляться среди доноров Cosmos Fundraiser (75%), ведущих доноров (5%), Cosmos Network Foundation (10%) и ALL IN BITS, Inc (10%). Начиная с генезиса, 1/3 от общего количества атомов будет вознаграждаться связанными валидаторами и делегатами каждый год.

Ограничение количества валидаторов

В отличие от Bitcoin или других блокчейнов с доказательством работы, блокчейн Tendermint работает медленнее с большим количеством валидаторов из-за повышенной сложности связи. К счастью, мы можем поддерживать достаточное количество валидаторов, чтобы создать надежную глобально распределенную цепочку блоков с очень быстрым временем подтверждения транзакций, а по мере увеличения пропускной способности, хранилища и мощности параллельных вычислений мы сможем поддерживать больше валидаторов в будущем.

В день генезиса максимальное количество валидаторов будет установлено на 100, и это число будет увеличиваться со скоростью 13% в течение 10 лет и установится на уровне 300 валидаторов.

Пример:

Year 0: 100

Year 1: 113

Year 2: 127

Year 3: 144

Year 4: 163

Year 5: 184

Year 6: 208

Year 7: 235

Year 8: 265

Year 9: 300

Year 10: 300.

Становление валидатором после генезиса

Владельцы Atom, которые еще не являются валидаторами, могут подписаться и отправить транзакцию BondTx. Количество атомов, предоставляемых в качестве залога, должно быть ненулевым. Каждый может стать валидатором в любое время, за исключением случаев, когда размер текущего набора

валидаторов превышает максимально допустимое

количество валидаторов. В этом случае транзакция действительна только в том случае, если количество атомов больше, чем количество эффективных атомов, удерживаемых наименьшим валидатором, где эффективные атомы включают делегированные атомы.
Когда новый валидатор таким образом заменяет существующий валидатор, существующий валидатор становится неактивным, а все атомы и делегированные атомы переходят в несвязанное состояние.

Штрафы для валидаторов

На валидаторов будет наложено наказание за любое преднамеренное или непреднамеренное отклонение от санкционированного протокола. Некоторые доказательства сразу принимаются, например, двойной знак одинаковой высоты и круглой формы или нарушение «prevote-the-lock» (правило протокола консенсуса Tendermint).
Такие доказательства приведут к тому, что валидатор потеряет свою репутацию и связанные с ним атомы, а его пропорциональная доля токенов в резервном пуле (именуемая «долей») будет сокращена.

Иногда валидаторы будут недоступны из-за сбоев в региональной сети, сбоя питания или по другим причинам. Если в какой-либо момент прошлых блоков ValidatorTimeoutWindow голос валидатора за коммит не будет включен в блокчейн больше, чем ValidatorTimeoutMaxAbsent раз, этот валидатор станет неактивным и потеряет ValidatorTimeoutPenalty (по умолчанию 1%) своей доли.

Некоторое «злонамеренное» поведение не дает явных различимых доказательств в блокчейне. В этих случаях валидаторы могут внепланово координировать свои действия, чтобы принудительно инициировать тайм-аут этих злонамеренных валидаторов, если есть консенсус квалифицированного большинства.

В ситуациях, когда Cosmos Hub останавливается из-за того, что ≥⅓ коалиции с правом голоса отключается, или в ситуациях, когда ≥⅓ коалиции с правом голоса подвергает цензуре доказательства злонамеренного поведения от входа в блокчейн, Hub должен восстановиться с помощью реорганизации хард-форка.

Операционные издержки

Валидаторы Cosmos Hub могут принимать любой тип токена или комбинацию типов в качестве платы за обработку транзакции. Каждый валидатор может субъективно установить любой обменный курс, который он хочет, и выбирать любые транзакции, которые он хочет, до тех пор, пока не будет превышен BlockGasLimit. Собранные сборы за вычетом любых налогов, указанных ниже, перераспределяются между связанными заинтересованными сторонами пропорционально их связанным атомам каждый ValidatorPayoutPeriod (по умолчанию 1 час).

Из собранных комиссий за транзакцию ReserveTax (по умолчанию 2%) пойдет в резервный пул, чтобы увеличить резервный пул и повысить безопасность и ценность сети Cosmos. Эти средства также могут распределяться в соответствии с решениями, принимаемыми
системой управления.

Владельцы Atom, которые делегируют свое право голоса другим валидаторам, платят делегированному валидатору комиссию. Комиссию может устанавливать каждый валидатор.

Стимулирование хакеров

Безопасность Cosmos Hub зависит от безопасности базовых валидаторов и выбора делегирования делегатами. Чтобы поощрять обнаружение и раннее сообщение о найденных уязвимостях, Cosmos Hub поощряет хакеров публиковать успешные эксплойты через транзакцию ReportHackTx, в которой говорится: «Этот валидатор был взломан.
Пожалуйста, отправьте награду на этот адрес». После такого эксплойта валидатор и делегаторы станут неактивными, HackPunishmentRatio (по умолчанию 5%) всех атомов будет слэширован, а HackRewardRatio (по умолчанию 5%) всех атомов будет вознагражден на адрес вознаграждения хакера. Валидатор должен восстановить оставшиеся атомы,
используя их резервный ключ.

Чтобы предотвратить злоупотребление этой функцией для передачи нераспределенных атомов, доля наделенных и не наделенных полномочиями атомов валидаторов и делегаторов до и после ReportHackTx останется неизменной, а хакерское вознаграждение будет включать некоторые нераспределенные атомы, если таковые имеются.

Спецификация по управлению

Cosmos Hub управляется распределенной организацией, которой требуется четко
определенный механизм управления для координации различных изменений в блокчейне, таких как переменные параметры системы, а также обновления программного обеспечения и конституционные поправки.

Все валидаторы несут ответственность за голосование по всем предложениям. Несвоевременное голосование по предложению приведет к автоматической деактивации валидатора на период времени, который называется AbsenteeismPenaltyPeriod (по
умолчанию 1 неделя).

Делегаторы автоматически наследуют голос делегированного валидатора. Это голосование может быть отменено вручную. Несвязанные атомы не имеют права голоса.

Каждое предложение требует внесения токенов MinimumProposalDeposit, которые могут представлять собой комбинацию одного или нескольких токенов, включая атомы. По каждому предложению избиратели могут проголосовать за внесение залога. Если более половины избирателей решили принять депозит (например, потому что предложение было спамом), депозит переходит в резервный пул, за исключением любых атомов, которые сожжены.

За каждое предложение избиратели могут проголосовать следующими вариантами:

- Да (Yea)
- Да с силой (YeaWithForce)
- Нет (Nay)
- Нет с силой (NayWithForce)
- Воздержаться (Abstain)

Для принятия решения по предложению (или решения как отклоненного) требуется строгое большинство голосов Да или Да с силой (или голосов против), но 1/3+ могут наложить вето на решение большинства, проголосовав «с силой». Когда строгое большинство накладывает вето, каждый наказывается потерей VetoPenaltyFeeBlocks (блоки по
умолчанию за 1 день) в размере сборов (за исключением налогов, которые не будут затронуты), а сторона, наложившая вето на решение большинства, будет дополнительно наказана потерей VetoPenaltyAtoms (по умолчанию 0,1%) его атомов.