2020

Decimal Yellow Paper

version 1.0

Содержание

Дисклеймер

Настоящий документ не является публичной офертой, не содержит никаких юридических рекомендаций и не может служить достаточным основанием для принятия каких-либо решений.

Настоящий документ не является официальным документом и не подпадает под действие правовой системы.

Настоящий документ составлен исключительно в информационных целях. Единственная цель настоящего документа – представить потенциальным пользователям сервисы экосистемы и программного обеспечения Decimal и токены DEL в связи с их продажей. Разработчикам, покупателям, инвесторам и иным лицам заинтересованным в работе экосистемы и программного обеспечения Decimal и токенах DEL, следует проконсультироваться со своим юристом, прежде чем руководствоваться и предпринимать определенные действия в связи с материалом, опубликованным в настоящем документе.

Отчеты, таблицы, оценки и финансовые данные, приведенные в настоящем документе, носят прогнозный характер и связаны с рисками неопределенности в экономическом и правовом контексте. В этой связи, такого рода информация приведена в настоящем документе исключительно в демонстрационных целях и не является гарантией достижения указанных значений (показателей) в будущем.

Компания DECIMAL PTE. LTD. оставляет за собой право вносить изменения в настоящий документ в одностороннем

порядке без какого-либо специального уведомления. Измененные условия будут считаться вступившими в силу сразу после публикации.

Документ не является предложением покупки ценных бумаг в любой юрисдикции, привлечением инвестиций или инвестиционным советом.

Документ составлен на русском языке и английском языке. В случае возникновения противоречий редакций документа приоритет имеет редакция документа на английском языке.

Компания DECIMAL PTE. LTD. не несет ответственности перед пользователями за любой тип понесенных ими убытков, независимо от причины, повлекшей за собой убытки.

Правовой статус криптографических токенов, цифровых активов и блокчейн-технологий носит неопределенный характер. Изменения в правовом регулировании цифровых активов технологии могут отрицательно влиять на токены DEL, сервисы экосистемы, программного обеспечения Decimal и могут привести к запрету на распределение токенов и работу наших сервисов, а также иным негативным последствиям.

1. Введение

В настоящем документе представлено техническое описание блокчейна Decimal, разработкой которого занимается наша команда разработчиков. При оформлении документа мы ставили себе целью дать общее представление о проекте, а также предоставить более детальное описание ключевых элементов Decimal.

Документ написан техническим языком, но без чрезмерного погружения в нюансы технологий и технических решений. Если же Вы ищете более общую информацию о проекте, то просим ознакомиться с Decimal White Paper (https://decimalchain.com).

2. Общая структура сервисов Decimal

На рисунке ниже представлена общая архитектура Decimal. Системообразующим элементом является непосредственно блокчейн, база данных, структурированная в виде цепочки блоков. В рамках системы блокчейн физически существует в виде реплик базы данных, которые хранятся на каждой из полных нод (мастернода, валидатор).

Чтобы маршрутизировать высокое количество запросов на считывание информации из блокчейна, а фактически к репликам блокчейна, мы организовали следующую структуру.

В сети работает ряд служб - воркеры (Workers), которые собирают данные, поступающие непосредственно в блокчейн. Данные - это блоки и транзакции разных типов: отправка, покупка, продажа, создание монет и т.д. Несколько одинаковых служб необходимы на случай выхода части из них из строя, ни один бит информации не должен быть потерян на этом участке процесса, впрочем, как и на любых других участках.

Выборка данных на выходе воркеров поступает в индексер, который структурирует, сортирует и индексирует поступающую информацию, после чего все данные сохраняются в главной (ведущей) базе данных (Master). Далее данные многократно копируются и располагаются в ведомых хранилищах (Slave).

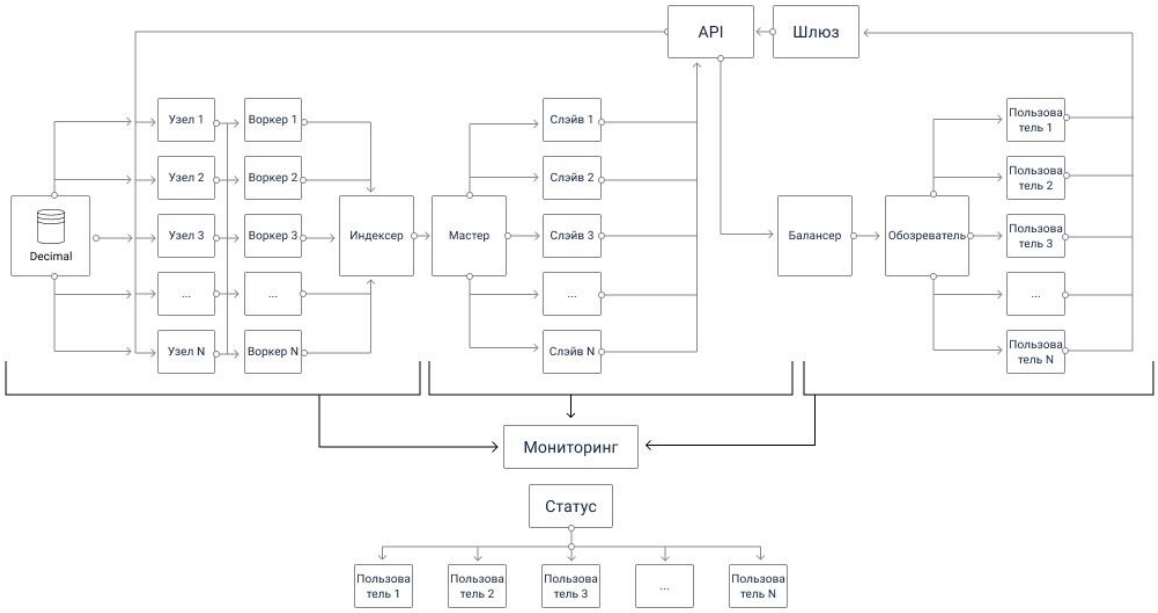


Рис. 1 - общая архитектура Decimal.

Пользователи Обозревателя (Explorer) осуществляют запросы на поиск всевозможной информации о блокчейне. Все эти запросы проходят через специальный балансировщик (Balancer), который равномерно распределяет нагрузку и направляет соответствующие запросы на считывание из Slave хранилищ.

Таким образом осуществляется буферизация данных и настроен канал доступа на считывание из блокчейна с высокой пропускной способностью.

Также в системе организован канал для записи информации в блокчейн. Посредством специального API интерфейса Gateway, который связан непосредственно с нодами системы, обеспечивается работа Консоли, десктопных кошельков и приложений кошельков для мобильных устройств. Структура всех этих сервисов полностью децентрализованная, пользователи владеют seed-фразами и приватными ключами. После формирования соответствующих транзакций (запросов на запись в блокчейн), пользователь подписывает их своей подписью и отправляет в сеть. Далее транзакции обрабатываются, верифицируются, включаются в блоки и после достижения консенсуса валидаторами обеспечивается запись в цепочку блоков с репликацией на каждой полной ноде.

В архитектуре Decimal присутствует специальный сервис Статус. Служба мониторинга отслеживает, собирает и предоставляет общие параметры сети.

3. Стек технологий

3.1. Языки программирования

Для корректной совместимости с Cosmos SDK и Tendermint в качестве языка программирования для реализации функционала Decimal, а именно программного обеспечения мастернод (валидаторов), мы выбрали **Golang**.

Для написания бэкенд-модулей мы выбрали **TypeScript**, который строго типизирован и удобен в процессе разработки, а также компилируется в **JavaScript**, исполняется в современных браузерах и совместим с **NodeJS**. В частности на TypeScript написаны воркеры (**Workers**) и индексер (**Indexer**).

Для реализации десктоп-приложений кошельков команда Decimal использовала **ElectronJS**, который позволяет на основе **JavaScript**, **HTML**, и **CSS** создавать кроссплатформенные десктоп приложения.

3.2. Фреймворки

3.3. Прочие технологии/решения

4. Cosmos SDK

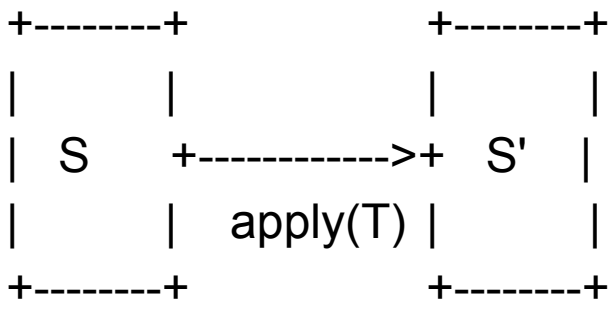
Блокчейн Decimal разработан на базе Cosmos SDK - это фреймворк (набор инструментов) для разработки блокчейн-приложений, ориентированных на решение конкретных задач (проблем). Cosmos SDK предоставляет безопасное и надежное решение большинства общих для блокчейнов задач, таких как организация сетевого взаимодействия между узлами сети и обеспечение надежного консенсуса между узлами, участвующими в формировании блоков сети. В Cosmos SDK это достигается благодаря активному использованию библиотеки Tendermint Core (подробнее ниже).

Благодаря построению на базе Cosmos SDK, блокчейн Decimal совместим[1] со всеми блокчейнами в составе

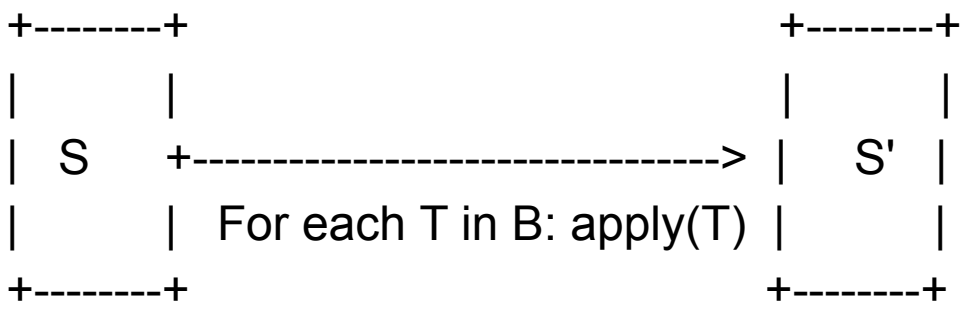
[1] После реализации и запуска Inter-Blockchain Communication (https://cosmos.network/ibc)

Cosmos Network, которая уже сейчас[2] насчитывает 112 проектов: https://cosmonauts.world/.

По своей сути, блокчейн является реплицированной машиной взаимосвязанных состояний.



Машина состояний - это концепция компьютерной науки, согласно которой машина может иметь несколько состояний, но только одно в любой момент времени. Существует состояние, которое описывает текущее состояние системы, и транзакции, которые запускают переходы в состояние.



[2] На май 2020 года

Учитывая состояние S и транзакцию T машина состояния возвращает новое состояние S'.

В контексте блокчейна машина состояний является детерминированной. Это означает, что если узел запускается в заданное состояние и повторяет одну и ту же последовательность транзакций, то на выходе будет всегда одно и то же конечное состоянием.

Cosmos SDK предоставляет разработчикам максимальную гибкость в определении состояния их приложения, типов транзакций и функций перехода в состояние.

5. Tendermint

Tendermint - это передовое решение проблемы консенсуса, основанного на BFT (Byzantine Fault Tolerance). BFT консенсус гарантирует корректную работу компьютерной сети, пока хотя бы 2/3 узлов блокчейн сети, участвующих в формировании блоков (валидаторы), работает корректно.

Tendermint состоит из двух основных технических компонентов: движок механизма консенсуса и интерфейс-приложения. Движок механизма консенсуса, называемый Tendermint Core, обеспечивает запись одних и тех же транзакций на каждой машине в одном и том же порядке. Интерфейс приложения, называемый Application BlockChain Interface (ABCI), позволяет обрабатывать транзакции на любом языке программирования.

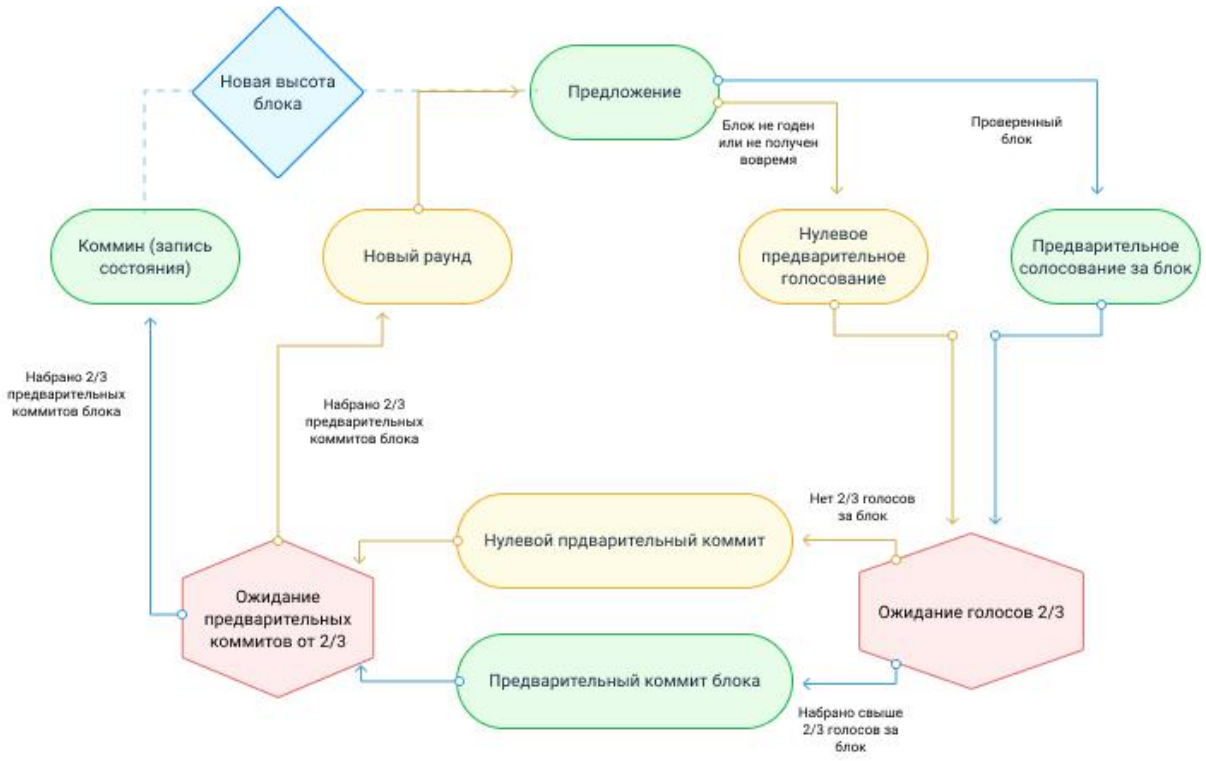


Рисунок 2 - процесс установления консенсуса в Tendermint.

Другими словами Tendermint обеспечивает эффективную ретрансляцию изменений в блокчейне по всей сети, гарантируя, что каждый узел сети имеет один и тот же журнал транзакций и состояние блокчейна.

Механизм консенсуса pBFT (practical Byzantine Fault Tolerance) является ключевым звеном блокчейна Decimal и используется нами без каких-либо изменений.

6. Эмиссия DEL

Нативная монета Decimal, называется **DEL**. В тестовой сети **tDEL**. Эмиссия DEL происходит во время генерации каждого блока блокчейна. Вознаграждение за блок = Базовое вознаграждение за блок + Суммарная комиссия всех транзакций в блоке. Исходное базовое вознаграждение за блок составит 50 DEL. И далее каждые 432 000 блоков (примерно 30 календарных дней) оно будет увеличиваться согласно следующему алгоритму:

- первые 12 месяцев (1й год) - увеличение на 5 DEL;
- следующие 12 месяцев (2й год) - увеличение на 17 DEL;
- следующие 12 месяцев (3й год) - увеличение на 29 DEL;
- следующие 12 месяцев (4й год) - увеличение на 41 DEL;
- следующие 12 месяцев (5й год) - увеличение на 53 DEL;
- следующие 12 месяцев (6й год) - увеличение на 65 DEL;
- следующие 12 месяцев (7й год) - увеличение на 77 DEL;
- следующие 12 месяцев (8й год) - увеличение на 89 DEL;
- следующие 12 месяцев (9й год) - увеличение на 101 DEL;
- после этого (на 10й год) выплата базовых вознаграждений за блок прекратится полностью и останется только суммарная комиссия всех транзакций в блоке.

На рисунке ниже представлен график базовых вознаграждений за блок примерно на протяжении 9 лет с момента запуска.

Например, в январе 2020 - 50 DEL, в январе 2028 - 4658 DEL.

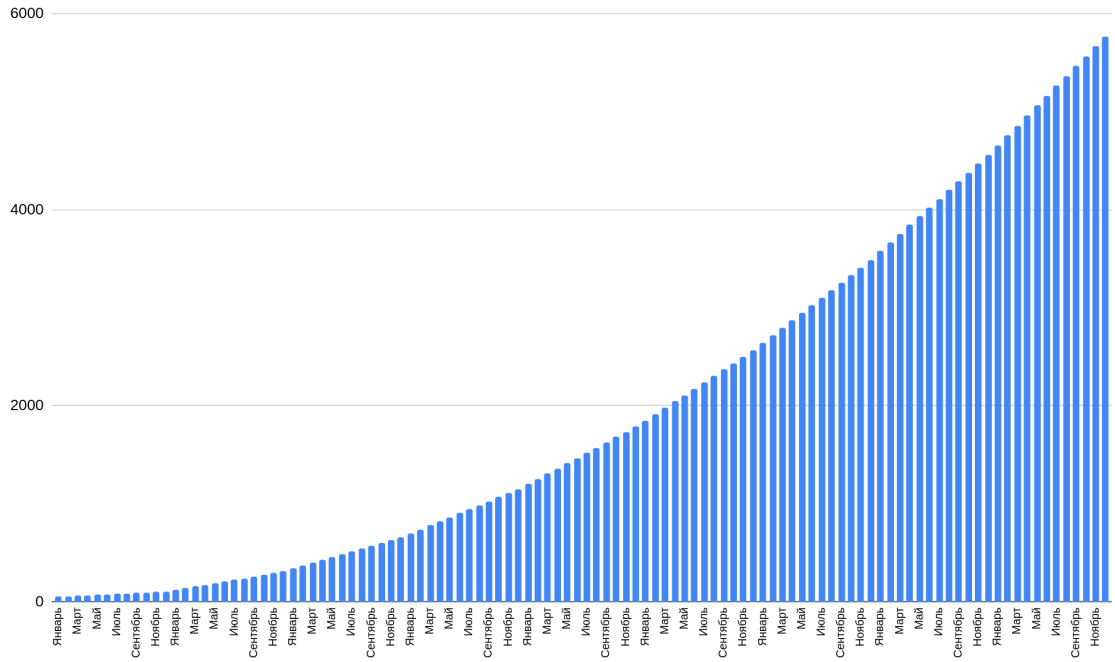


Рисунок 3 - эмиссия DEL на протяжении 9 лет.

В таблице ниже представлен размер базового вознаграждения за блок в течение первых двух лет функционирования блокчейна Decimal.

Месяц, 2020	**Вознаграждение, DEL**	**Месяц, 2021**	**Вознаграждение, DEL**
Январь	50	Январь	122
Февраль	55	Февраль	139
Март	60	Март	156
Апрель	65	Апрель	173
Май	70	Май	190
Июнь	75	Июнь	207
Июль	80	Июль	224
Август	85	Август	241
Сентябрь	90	Сентябрь	258
Октябрь	95	Октябрь	275
Ноябрь	100	Ноябрь	292
Декабрь	105	Декабрь	309

Таблица 1 - размер базового вознаграждения за блок.

При запуске сети в генезис-блоке будет произведён пре-майн DEL, который составит 200 000 000 DEL. При этом каждый из 4 стартовых валидаторов получит по 40 000 000 DEL (в сумме 160 000 000 DEL).

Остальные 40 000 000 DEL будут выставлены на продажу и реализованы инвесторам проекта.

7. Типы транзакций

В Decimal реализованы следующие типы транзакций:

1) **Send** (отправка монет);
2) **Buy** (покупка монеты);
3) **Sell** (продажа монеты);
4) **Sell All** (полная продажа монет);
5) **Multisend** (отправка нескольким адресатам);
6) **Delegate** (делегирование монеты валидатору);
7) **Unbond** (отзыв монеты у валидатора);
8) **Redeem Check** (погашение чека);
9) **CreateMultisig** (создает адрес с мультиподписью);
10) **CreateTransaction** (создает транзакцию на вывод с адреса с мультиподписью);
11) **SignTransaction** (уникальный идентификатор мультисиг транзакции);

12) **CreateCoin** (создание монеты);
13) **DeclareCandidate** (создание кандидата в валидаторы);
14) **EditCandidate** (редактирование данных кандидата в валидаторы);
15) **SetOnline** (активация валидатора);
16) **SetOffline** (деактивация валидатора).

8. Комиссии за транзакции

В блокчейне Decimal размер комиссии за транзакцию состоит из суммы фиксированной ставки за тип транзакции и стоимости единицы за объём транзакции в байтах.

Фиксированная ставка: 1 юнит = 0,001 DEL

- send (отправить) - 10 юнитов - 0.01 DEL
- multisend (мультиотправка) - 10+(n-1)x5 юнитов (n - количество получателей) - 15 юнитов (2 получателя)
- sell (продать) - 100 юнитов - 0,1 DEL
- sell (продать) - 100 юнитов - 0,1 DEL

- buy (купить) - 100 юнитов - 0,1 DEL
- declare candidacy (декларирование кандидата) - 10 000 юнитов - 10 DEL
- edit candidate (редактирование кандидата) - 10 000 юнитов - 10 DEL
- delegate (делегирование) - 200 юнитов - 0,2 DEL
- unbond (отвязка) - 200 юнитов - 0,2 DEL
- set online (активирование) - 100 юнитов - 0,1 DEL
- set offline (деактивирование) - 100 юнитов - 0,1 DEL
- create multisig (создание мультисига) - 100 юнитов - 0,1 DEL
- create multisig transaction (создание предложения) - 100 юнитов - 0,1 DEL
- sign transaction (подписание предложения) - 100 юнитов - 0,1 DEL
- redeem check (погасить чек) - 30 юнитов - 0,03 DEL

создать монету

- 3 буквы - DEL 1 000 000
- 4 буквы - DEL 100 000
- 5 букв - DEL 10 000
- 6 букв - DEL 1 000
- 7-10 букв - DEL 100

Стоимость 1 байта итогового объёма транзакции:

2 юнита (0,002 DEL)

По сути, транзакция - это просто информационное сообщение. В нём указано, что, сколько, кому и от кого отправляется, а также служебные данные. Объём транзакции - это объём всей информации, из которой состоит транзакция:

- служебная (подписи, параметры и т.д.);
- пользовательская (длина тикера отправляемой монеты, длина тикера монеты комиссии, отправляемая сумма, текстовое сообщение).

Исходя из опыта тестирования при разработке Decimal, мы располагаем следующими ориентировочными данными по стоимости каждой транзакции:

- send (отправить) ~ 0.41 DEL
- multisend (мультиотправка) ~ 0,479 DEL (2 получателя)
- sell (продать) ~ 0.484 DEL
- sell (продать) ~ 0.444 DEL
- buy (купить) ~ 0.54 DEL

- declare candidacy (декларирование кандидата) ~ 10.674 DEL
- edit candidate (редактирование кандидата) ~ 10.494 DEL
- delegate (делегирование) ~ 0,564 DEL
- unbond (отвязка) ~ 0,604 DEL
- set online (активирование) ~ 0.396 DEL
- set offline (деактивирование) ~ 0.394 DEL
- create multisig (создание мультисига) ~ 0.494 DEL
- create multisig transaction (создание предложения) ~ 0.542 DEL
- sign transaction (подписание предложения) ~ 0.544 DEL
- redeem check (погасить чек) ~ 0.03 DEL

9. Мультиподпись

В Decimal будут доступны адреса с мультиподписью. Это очень удобно при распределении средств или при принятии совместного решения, когда существует несколько независимых участников и условия консенсуса между ними. Например, средства из общего кошелька

выводятся только если на это согласятся 80% участников. (4 участника из 5).

Мультиподпись будет работать почти как смарт-контракт мультиподписи в блокчейне Ethereum. Для реализации функционала будут имплементированы три типа транзакции - CreateMultisig, CreateTransaction, SignTransaction:

1. **CreateMultisig** создает кошелек с мультиподписью, с указанием владельцев, веса их голоса и порогового значения (например, 3 из 5 или 2 из 3). При этом адрес с мультиподписью генерируется с добавлением “соли”[3], чтобы позволить создавать много адресов с одинаковыми параметрами, и сохраняется в хранилище.
2. **CreateTransaction** создает транзакцию на вывод указанного количества указанных монет на указанный адрес, создатель транзакции сразу же подписывает эту транзакцию. Каждой такой транзакции присваивается уникальный идентификатор.
3. Другие владельцы кошелька с мультиподписью могут запросить неподтвержденные транзакции по данному адресу, их параметры и идентификаторы. После этого они просто отправляют транзакцию типа **SignTransaction** в блокчейн, в которой в параметрах

[3] https://ru.wikipedia.org/wiki/%D0%A1%D0%BE%D0%BB%D1%8C_(%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F)

будет уникальный идентификатор транзакции из п. 2. После проверки подписи количество собранных "голосов" у транзакции увеличивается в соответствии с весом подписчика в п. 1. Если пороговое значение достигнуто, операция исполняется, происходит перевод средств, меняются балансы адреса с мультиподписью и адреса получателя.

Как результат, данной схемой взаимодействия участников мультиподписи мы исключаем оффлайн общение между ними. По крайней мере оно становится необязательным.

10. CRR

Отличительной особенностью блокчейна Decimal является специфика экономической модели монет. Из неё вытекают все преимущества: простой выпуск монет, возможность обменивать их на любые другие в рамках сети, оплата комиссии любыми монетами экосистемы Decimal.

Нативная монета DEL помимо традиционных функций криптовалюты выполняет функцию обеспечения вновь созданных монет. Каждая кастомная монета подкрепляется гарантийным обеспечением в виде того или иного количества DEL. Размер этого гарантийного обеспечения по отношению к общему выпуску кастомной монеты напрямую влияет на кривую стоимости этой монеты.

Параметр CRR устанавливается при создании монет и далее кривая стоимости остаётся неизменной навсегда. При изменении рыночных условий и баланса спрос/предложение стоимость монеты двигается по рассчитанной кривой, вверх или вниз.

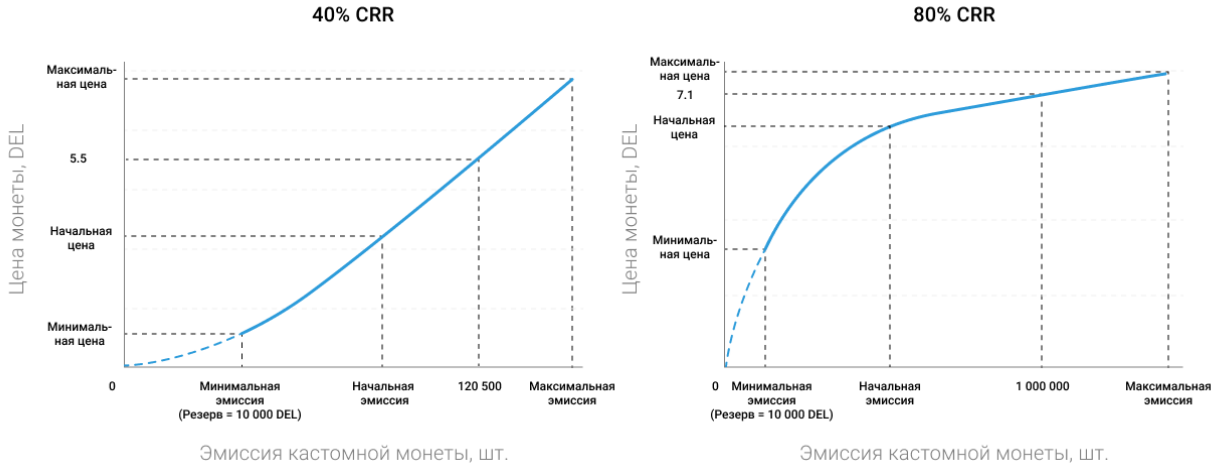


Рисунок - монеты с разным CRR.

11. Формулы определения стоимости монет

Ключевыми параметрами в сети Decimal являются Резерв, CRR и общее количество выпуска монет. Все они задействованы и при расчёте стоимости покупки либо продажи.

Само наличие двух формул является следствием нелинейного характера изменения стоимости монет.

Расчет стоимости покупки монеты:

Сумма покупки = Резерв * (-1+(((хочуКупить + Эмиссия) / Эмиссия) ^ (100 / CRR))

, где

Резерв - текущий резерв в DEL;
хочуКупить - количество монет к покупке;
Эмиссия - общее количество монет;
CRR - коэффициент Постоянного Соотношения к Резерву (например, 20 для 20%).

Расчет стоимости продажи монеты:

Сумма продажи = Резерв * (1 — (1 — хочуПродать / Эмиссия) ^ (100/ CRR))

, где

Резерв - текущий резерв в DEL;
хочуПродать - количество монет к продаже;
Эмиссия - общее количество монет;
CRR - коэффициент Постоянного Соотношения к Резерву (например, 20 для 20%).

Расчёт текущей цены 1 монеты:

Цена = Резерв * (1-(1-1/Эмиссия)^ (100 / CRR))

, где

Резерв - текущий резерв в DEL;
Эмиссия - общее количество монет;
CRR - коэффициент Постоянного Соотношения к Резерву (например, 20 для 20%).

12. Что такое мастернода

В Decimal имеется 2 вида узлов сети. Полный узел и неполный узел (обычный).

Мастернода (она же Полный узел) - это узел сети Decimal хранящий реплику блокчейна и участвующий в установлении консенсуса.

Мастернода является программно-аппаратным комплексом, который выполняет функцию валидатора в сети. Оборудование подключено к интернету и непосредственно к другим валидаторам для обеспечения главной задачи - консенсус.

Требования к обрудованию:

4GB RAM - объём оперативной памяти;

1 TB SSD - объём и тип жёсткого диска;

x64 2.0 GHz 4 vCPUs - характеристики CPU.

Каждая мастернода сети Decimal хранит полную копию блокчейна (список всех транзакций, всех блоков, все сообщения, начиная с генезис-блока). Данная копия называется репликой. Она идентична репликам на каждой из остальных мастернод.

Кроме того, на мастерноде развёрнуты дополнительные сервисы и службы, которые необходимы для установления соединения с другими мастернодами по протоколу Gossip, верификации транзакций пользователей, формирования из транзакций блоков, записи всего и вся непосредственно в локальную реплику блокчейна.

Каждая мастернода работает в строгих условиях наказание/поощрение.

Вознаграждение полагается за корректную и надёжную работу. Сумма вознаграждения пропорциональна совокупному стейку каждой мастерноды в общей сумме стейков. Чем больше стейк валидатора, тем большую часть вознаграждений за блок получит данный валидатор (мастернода).

Штрафами наказывается некорректная работа мастерноды. Например, недоступность валидатора в течение периода формирования 12 блоков из 24 последних наказывается 1% от общей суммы стейка валидатора. Причём в общую сумму стейка входят все делегированные данному валидатору средства.

Также штрафом наказываются валидаторы, совершающие попытку мошеннических действий в процессе установления консенсуса. В том числе в процессе формирования подписи 2 разных блоков во время проведения раунда верификации и голосования за блок кандидатов. Это серьезное нарушение, которое

может привести к форкам цепочки блоков. В случае появления форка часть пользователей сети будет ориентироваться на один вариант состояния блокчейна (транзакции, балансы счетов), в то время как другая часть пользователей будет ориентироваться на второй вариант цепочки блоков уже с другим состоянием и балансами. В этом случае валидатор будет наказан 5% штрафом. Плюс все делегированные данному валидатору монеты вернутся своим владельцам (уменьшится его стейк).

Ещё раз:

1) Недоступность в течение 12 блоков из последних 24 блоков - штраф на 1% стейка + отключение валидатора;
2) Двойная подпись - штраф на 5% стейка и принудительное разделегирование монет.

Стоит отметить, что штрафные средства не перечисляются куда бы то ни было, а просто сжигаются. Уменьшая при этом общую эмиссию DEL.

13. Обычный узел

Второй тип узлов - это обычный узел. Это все участники сети, за исключением мастернод (валидаторов).

Это обычные пользователи сети: владельцы кошельков, эмитенты кастомных монет, бизнесы и частные лица, делегаторы монет и другие.

У каждого из них находятся во владении приватные ключи от своих кошельков и они пользуются всеми сервисами и приложениями доступными в экосистеме Decimal. На своих некастодиальных кошельках они хранят DEL и другие кастомные монеты. Отправляют их другим пользователям, делегируют понравившимся валидаторам, получают вознаграждение от валидаторов.

В общем, обычным узлам доступен весь функционал, кроме обязанности участвовать в установлении консенсуса и хранить реплику блокчейна.

14. Эксплорер

Широкому кругу пользователей Decimal требуется всегда понимать, что происходит в сети блокчейна в данный момент времени, какие его основные параметры. Пользователи хотят перепроверять и искать информацию о своих транзакциях, о блоках, о комиссиях, о вознаграждениях и т.д.

Поэтому мы разработали блок эксплорер.

Полагая, что пользователям будет интересен очень большой объём информации о состоянии и процессах в сети Decimal, а именно детали транзакций, блоки, валидаторы и их параметры, выпущенные монеты и т.д. и т.п., мы должны позаботиться о доступности всех этих данных и обеспечить их корректное и быстрое отображение. С течением времени и увеличением блокчейна, обрабатывать запросы будет всё сложнее. Возможны значительные временные задержки при выборке данных непосредственно из реплик блокчейна. Но мы организуем хранение в базе данных, способной удовлетворить огромное количество запросов и

гарантированно предоставить нужную пользователям информацию.

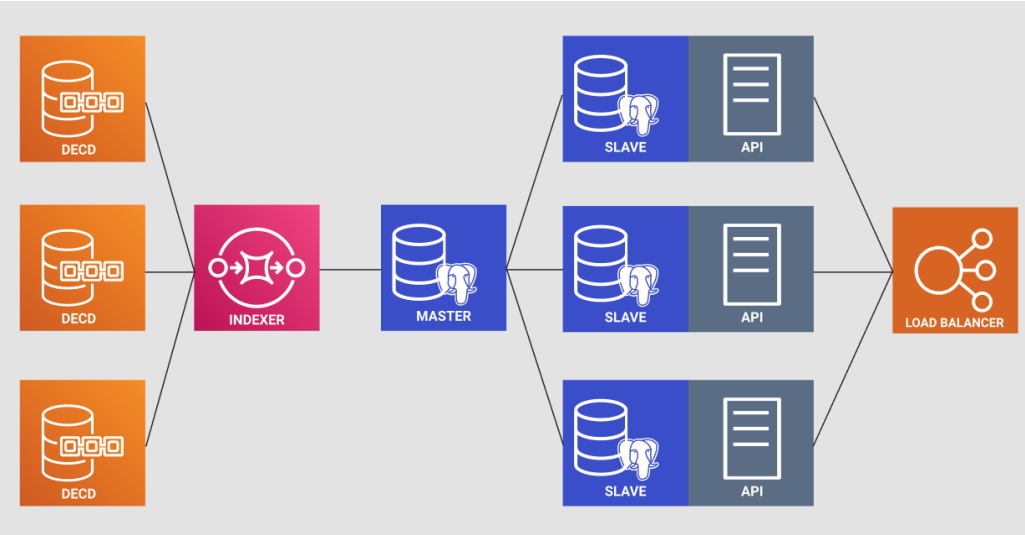


Рис - архитектура блок эксплорера Decimal.

На рисунке выше представлена архитектура нашего решения. Процесс организован следующим образом.

Изменения состояния в блокчейне генерируют события (ивенты, events), которые мониторятся специальными службами (Воркеры, workers). Данные службы распарсивают всю поступающую информацию из блоков и транзакций и передают в Индексер, в котором данные сортируются и индексируются. После этого упорядоченные данные записываются в PostgreSQL базу данных. Записываются в ведущую базу (Master) и дублируются на ведомых (Slave) для гарантии сохранности.

Все запросы от Эксплорера поступают на ведомые базы данных через балансировщик (Load Balancer), организующий через программный интерфейс (API) равномерное распределением нагрузки. Такая схема горизонтально масштабируемая, т.е., если возрастает нагрузка, то можно добавлять ведомые базы. При этом мастерноды, где непосредственно хранятся реплики блокчейна, не нагружаются т.к. архитектурно отделены от запросов пользователей и внешних служб. Благодаря индексированию и партиционированию базы данных, способны с минимальными задержками выдать информацию о любых событиях и состояниях в блокчейне, вне зависимости от размера самой базы данных.

15. Консоль

Decimal уже на старте проекта предоставляет пользователю ряд сервисов, раскрывающих главные возможности. Мы считаем очень важным обеспечение удобного доступа ко всем сервисам. Поэтому все они были сведены вместе на одной площадке. Она называется Консоль Decimal (https://console.decimalchain.com).

Кошелёк (https://console.decimalchain.com/wallet) - адрес кошелька, баланс ваших средств в DEL, список монет во владении, список совершённых транзакций и их параметры, функционал отправки монет.

Конвертация (https://console.decimalchain.com/convert) - сервис для обмена, купли и продажи любых монет в сети Decimal.

Делегирование (https://console.decimalchain.com/delegation) - взаимодействие с валидаторами, передача своих монет для увеличения их стейка и получения вознаграждения от них. Также здесь можно отозвать делегированные монеты.

Делегирование средств пользователя валидаторам является ключевой особенностью блокчейна Decimal. В условиях наличия большого количества монет мы хотим предоставить пользователю удобный инструмент для организации делегирования. Поэтому мы реализовали автоматическое делегирование. На предварительном этапе мы предлагаем сформировать в автономном режиме либо онлайн пакет транзакций и отдельной транзакцией настроить запустить автоматический запуск делегирования.

Мастернода (https://console.decimalchain.com/masternode) - сервис организует процесс подключения и запуска функционала валидатора. Количество валидаторов в Decimal

регламентируется и увеличивается пропорционально росту сети. На страте блокчейна будет 4 валидатора и 12 слотов дополнительных слотов, т.е. максимум на старте возможно наличие 16 валидаторов. Далее каждый календарный месяц будут добавляться 4 валидатора.

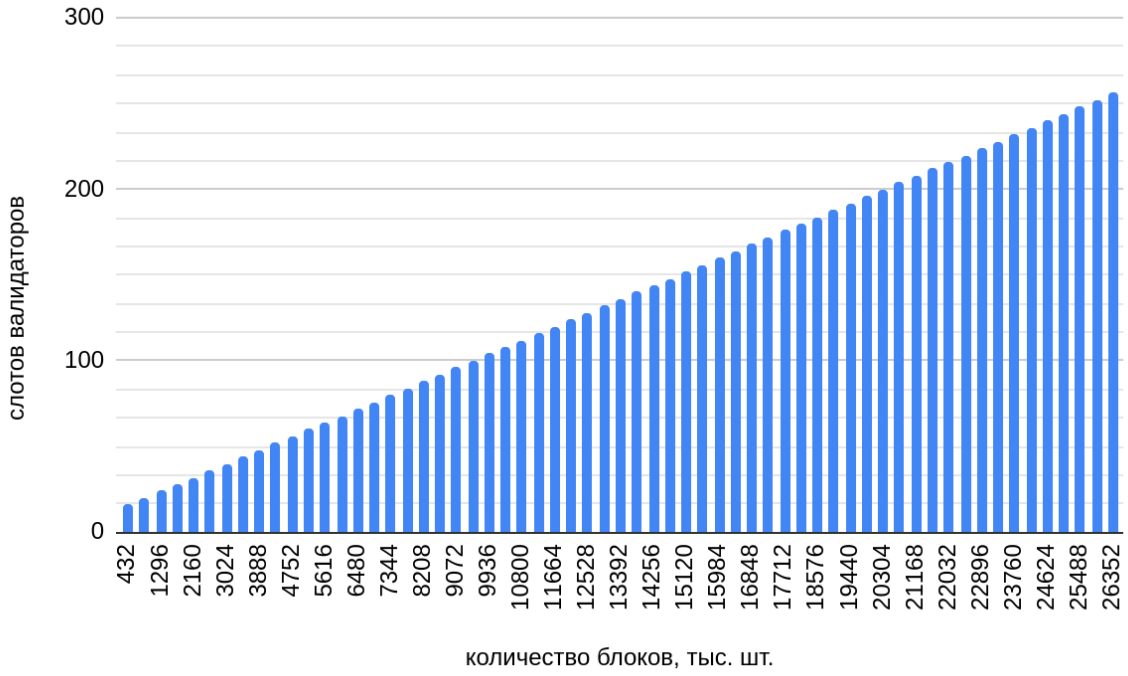


Рисунок - увеличение количества слотов для валидаторов.

Прежде чем стать валидатором, требуется заявить его кандидатуру. В механизме консенсуса принимают участие валидаторы с наибольшим размером стейка. Стейк пересчитывается каждый блок. Соответственно, кандидат выбирается исходя из этого параметра, а также на основе

показателей качества (доступность в сети, отсутствие штрафов) своей работы.

Мы развернули тестовую сеть Decimal, которая архитектурно полностью идентична главной сети. Это даёт нам возможность отладить процессы запуска и управления мастерноды. Для ознакомления перейдите по ссылке https://testnet.console.decimalchain.com

Выпуск монеты (https://console.decimalchain.com/issue-a-coin) - здесь реализован функционал создания монеты. Алгоритм простой, требуется заполнить пять полей и монета создана. Чтобы понять каким образом будет себя вести стоимость Вашей кастомной монеты при покупках, продажах и обменах, мы сделали дополнительный сервис - Калькулятор (https://calculator.decimalchain.com). В нём Вы создаёте виртуальную монету, осуществляете соответствующие транзакции и наблюдаете изменение стоимости монеты.

Бродкаст (https://testnet.console.decimalchain.com/broadcast) - это сервис для отправки в сеть Decimal транзакций, сгенерированных пользователями в оффлайн режиме. Так как безопасность является одним из ключевых приоритетов, мы предлагаем инструмент, который исключит любые возможности компрометации приватных данных пользователей. Здесь мы генерируем для

пользователя параметр **nonce**, который включается в транзакцию. После создания транзакции оффлайн, пользователь сможет её отправить в сеть, не беспокоясь о своих приватных ключах.

Статус (https://status.decimalchain.com) - на этом ресурсе отображаются главные глобальные метрики Decimal на текущий момент времени, такие как статус сети, сервисов и служб блокчейна, количество выпущенных монет и т.п.

API & SDK (https://help.decimalchain.com/api-sdk) - это описание программного интерфейса для взаимодействия с сервисами Decimal и инструментов для построения приложений на основе блокчейна Decimal.

Help / FAQ (https://help.decimalchain.com/ru/) - традиционный раздел, необходимый для пояснений технических и нетехнических деталей, разного рода руководства, справочники, ответы на часто задаваемые вопросы и т.п. Несмотря на то, что с точки зрения использования в Decimal всё просто, на техническом уровне много различных технологий и нюансов. Мы стремимся облегчить освоение Decimal и помочь максимально широкому кругу пользователей.

16. Статус

Как сказано выше, сервис Статус организован на базе службы мониторинга. Она состоит из нескольких частей развёрнутых на мощностях Decimal и узлах сети:

1) сервер мониторинга;
2) база данных;
3) веб-интерфейс;
4) демон агент, на объектах мониторинга.

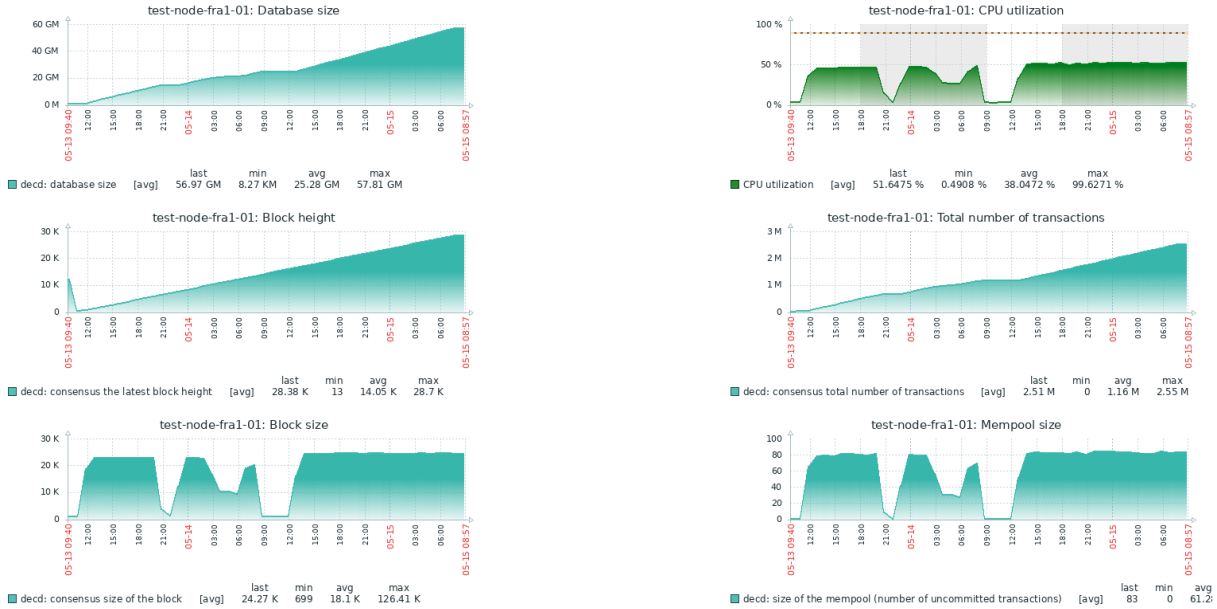


Рис - пример мониторинга на этапе разработки Decimal.

Для ознакомления с сервисом перейдите по ссылке https://status.decimalchain.com

Информация о транзакциях, блоках, комиссиях, валидаторах, временных параметрах, монетах, собирается непосредственно из блокчейна.

Например, для параметра **Сеть (Network)** мы каждые 30 секунд проверяем, формируются ли новые блоки на узлах валидаторов. Если новые блоки формируются, то сеть находится в статусе **“Активна”**.

Для сервисов **Обозреватель (Explorer)** и **Шлюз (Gate)** мы проверяем, запущены ли они на серверах, а также доступны ли они (отвечают на запросы или нет).

17. Кошелёк

Все официальные кошельки Decimal являются децентрализованными, т.е. некастодиальными (non-custodial). Seed-фразы и приватные ключи хранятся строго на стороне пользователя и decimal никоим образом не имеет к ним доступ. Вся ответственность за

сохранность этих приватных данных и средств на кошельках полностью лежит на владельцах кошельков.

На старте проекта доступны следующие приложения кошельков:

1) для десктоп браузеров https://wallet.decimalchain.com;
2) для десктоп браузеров через консоль https://testnet.console.decimalchain.com/wallet;
3) для Android устройств https://play.google.com/store/apps/details?id=com.chain.decimal&hl=en;
4) для iOS устройств

5) десктоп версии для Windows, macOS и Windows

Приватные ключи генерируются на основе стандарта BIP39.

Эллиптическая кривая **secp256k1**.

Seed-фраза состоит из **24** слов.

18. Формат адресов (Bech32)

Одной из специфических особенностей блокчейнов (сначала Bitcoin, а потом и многих других) являются форматы адресов. Они представляют собой последовательность букв латинского алфавита и цифр. Проблема в том, что это значительно затрудняет их корректное считывание пользователями.

Энтузиаст и разработчик блокчейна Питер Уилле (Pieter Wuille) предложил модернизировать формат адресов в сети Bitcoin. Это предложение известно как BIP 173[4] или bc1 адреса и на май 2020 года оно было успешно внедрено[5] в значительное количество крипто-проектов, в том числе за рамками блокчейна Bitcoin.

На данный момент внедрённые изменения известны как Bech32 формат адресов.

Команда Decimal, целиком поддерживая Bech32, обеспечит его уже на старте проекта.

Адрес Bech32 имеет длину, которая не превышает 90 символов, и содержит:

[4] https://github.com/bitcoin/bips/blob/master/bip-0173.mediawiki
[5] https://en.bitcoin.it/wiki/Bech32_adoption

1) Часть, удобную для чтения человеком. Сюда входят данные, которые могут понадобиться для передачи или которые имеют какое-либо отношение к владельцу адреса, длина минимум 1 символ. Например, по умолчанию для адресов mainnet используются символы «bc», а для testnet символы «tb».
2) Разделитель, который всегда равен «1». Если «1» разрешен внутри человекочитаемой части, то разделителем является последний из символов «1».
3) Часть с данными имеет длину как минимум 6 символов и состоит только из буквенно-цифровых символов, исключая «1», «b», «i», и «o».
4) Чексумма. Последние шесть символов части данных образуют контрольную сумму и не содержат никакой информации.
5) Все буквы являются строчными, хотя для генерации QR кода возможно их преобразование в заглавные.

Рисунок - структура адреса пользователя Decimal.

19. Консольный клиент

Для облегчения процесса создания и отладки тех или иных процессов или сценариев взаимодействия с Decimal, будь то ончейн или оффчейн сервисы, исполнение скриптов, исполнение запросов к блокчейну, отправка любых типов транзакций или получение служебной информации и параметров, наша команда подготовила консольный клиент.

Файл для запуска клиента - deccli.

Клиент работает как REST-сервер, который предоставляет возможности для создания широкого набора запросов к блокчейну.

По сути, консольный клиент является «лёгкой нодой» (light node) или «лайт демоном» (light daemon) и перенаправляет запросы в полную ноду, а потому не требует синхронизации с блокчейном (не хранит реплику блокчейна), занимает очень мало дискового пространства, но при этом обладает богатым исчерпывающим функционалом.

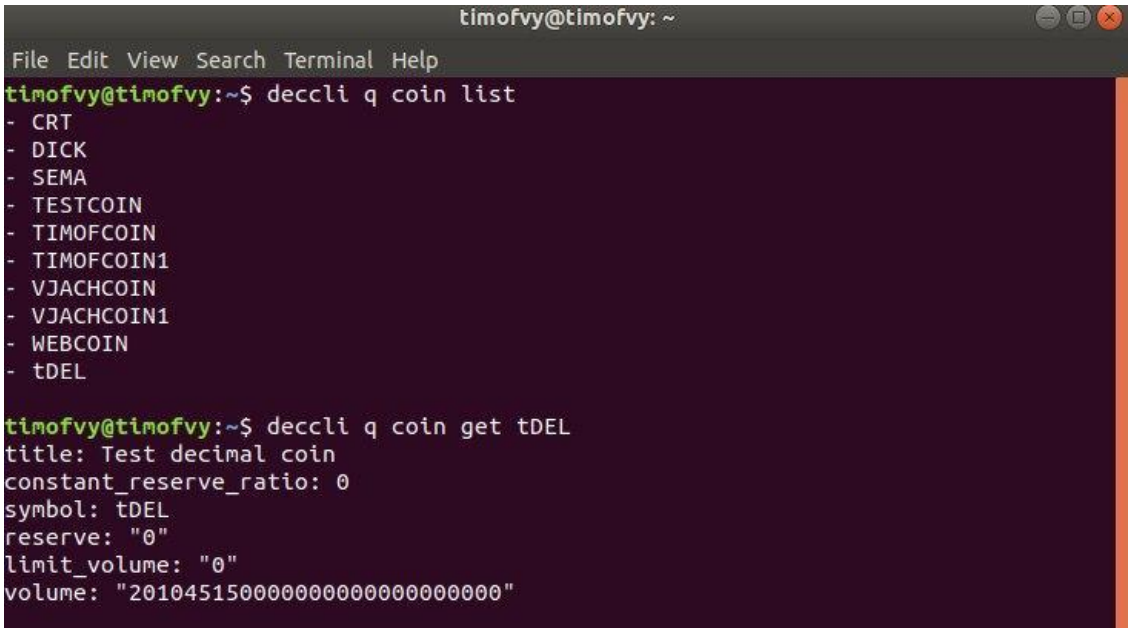


Рис - интерфейс консольного клиента, команды coin list и coin get.

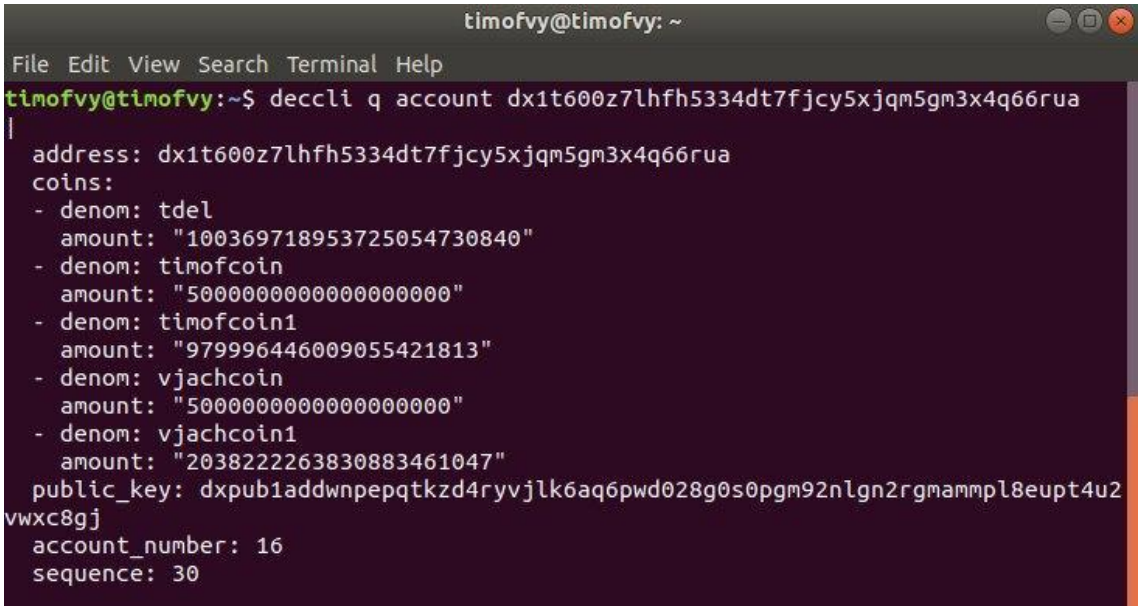


Рис - интерфейс консольного клиента, информация об аккаунте

20. Роли

20.1. Валидатор

Участник сети Decimal, который хранит на своём оборудовании реплику блокчейна, обеспечивает верификацию транзакций, формирование блоков цепи, участвует в процессе установления консенсуса. Одной из главных характеристик валидатора является сила голоса (Voting power), которая прямо пропорциональна размеру стэйка данного валидатора. Чем больше размер стэйка валидатора в абсолютных цифрах и чем больше его доля в совокупном стэйке всех валидаторов, тем большей силой голоса он обладает, тем чаще он производит блоки, тем больше вознаграждения получает за свою работу.

Валидатор должен обеспечивать надёжность своей работы, быть доступным в сети, корректно исполнять свои обязанности в процедуре установления консенсуса, гарантировать доступ внутренних служб сети Decimal к своей реплики блокчейна, обеспечивать целостность хранимых данных.

Функционирование валидатора - это не только получение вознаграждений за работу, но и риск быть

оштрафованным за некорректное исполнение обязанностей. Валидатор рискует потерять часть своего стэйка в результате штрафов, а также понести репутационные потери, если пользователи перестанут доверять ему свои средства для делегирования. Репутационные потери могут очень сильно влиять на деятельность валидаторов.

Стэйк валидатора состоит из собственных средств и средств делегированных (переданных “в аренду”) ему другими участниками сети.

20.2. Делегатор

Участник сети Decimal, который передаёт “в аренду” свои средства валидатору. Передача осуществляется не в буквальном смысле. Сумма переданных средств просто блокируется на счёте делегатора и он не может ей распоряжаться, пока не осуществит отвязку своих средств.

Процесс передачи средств называется делегированием. Суть его заключается в передаче прав и ответственности пользователя. Делегатор увеличивает стэйк валидатора и получается, что валидатор исполняет свои обязанности от имени делегатора, в рамках размера делегированных средств. Соответственно права и ответственность распространяются как на получение вознаграждения так и на штрафы. Вознаграждения и штрафы распределяются пропорционально доли средств делегатора в совокупном

стэйке валидатора. Если валидатор получит 5% штраф, то значит и делегатор получит такой же 5% штраф автоматически.

20.3. Койнер

Участник сети Decimal, который выпускает собственную кастомную монету. Как вы уже знаете из Decimal White Paper, сферы применения криптомонет безграничны. Мы сделали процесс создания монеты исключительно простым и быстрым.

После установки исходных параметров, таких как размер резерва в DEL, количество выпуска монеты и коэффициента постоянного резервирования (CRR) в сеть отправляется специальная транзакция. На этом процесс закончен. Вы получаете готовую монету с полным функционалом.

Более того, далее вам не надо заботиться о технических механизмах ценообразования кастомной монеты. Любые операции обмена с участием вашей монеты будут производиться на основе математических формул, заложенных в программное обеспечение Decimal и автоматических алгоритмов блокчейна. Больше спрос - выше цена монеты и наоборот.

Любая кастомная монета может быть делегирована валидатору. Её можно обменять на любую другую кастомную монету Decimal либо на DEL.

Комиссия за транзакции также уплачиваются любой кастомной монетой в вашем распоряжении.

20.4. Пользователь

Все остальные участники сети Decimal являются простыми пользователями. Мы рассматриваем каждого пользователя, как потенциального койнера, делегатора и валидатора. После успешного опыта хранения монет Decimal, их отправки, оплаты товаров и услуг, а также остальных применений в реальной жизни, шаг в сторону создания своей монеты будет простым. Наша миссия и задача устранить все барьеры на пути обычного пользователя к своим целям.

21. Делегирование

Делегирование - это процесс привязки (bonding) монет пользователя (DEL либо любых кастомных) валидатору (-ам). Процесс осуществляется с помощью специальной транзакции **Delegate** (см. Типы транзакций). Пользователь, делегирующий монеты, называется **Делегатор**. После

привязки монет делегированные средства блокируются на счёте пользователя, т.е. они никуда не отправляются, но на балансе пользователя **НЕ** отображаются. Зато эти средства отображаются в общем стейке валидатора, при этом увеличивается его вес по отношению к другим валидаторам и сила голоса в механизме консенсуса. Валидатор не имеет возможности распоряжаться делегированными средствами никоим образом, не имеет к ним доступа, не может их потратить или вывести.

Напомним, что среди валидаторов организована конкуренция: валидаторы с большим стейком наиболее часто участвуют в установлении консенсуса и получают больше вознаграждения.

В Decimal существует операция отвязки (unbond) делегированных монет. Данная транзакция может быть инициирована и отправлена в сеть либо самим пользователем, либо валидатором, либо программным обеспечением автоматически. В первом случае средства незамедлительно будут доступны на балансе пользователя. Во втором и третьем случаях средства поступят в распоряжение пользователя через 432 000 блоков (~ 30 дней).

Т.к. при некачественной или некорректной работе на валидаторов налагаются штрафы (см. Что такое мастернода), поэтому количество делегированных монет на балансе делегатора может уменьшиться на размер

штрафов. Делегатор несёт личную ответственность за свой выбор валидатора, поэтому этот выбор надо делать очень тщательно.

Делегирование монет происходит в так называемые слоты. У каждого валидатора есть 1000 слотов. Каждая отдельная монета делегируется в свой слот. Т.е. Все монеты DEL будут зачислены в один слот, а для каждой следующей монеты будет предусмотрен следующий слот. Количество монет в слоте не ограничивается. Но если у делегатора заполнены все 1000 слотов, то следующий делегатор должен отправить монет **НЕ** менее, чем количество монет, находящихся в последнем слоте. Если он отправляет больше, то средства в слоте номер 1000 принудительно разделегируются и немедленно появляются на балансе владельца.

За делегирование (процесс привязки (bonding) монет пользователя (DEL либо любых кастомных) валидатору или нескольким валидаторам) пользователь получает вознаграждение.

Вознаграждение начисляется каждые 120 блоков.

Сумма вознаграждения зависит от ряда факторов: количества делегированных монет, количества валидаторов, общего объема стейков, размера базового вознаграждения за блок, наложенных штрафов и тд.

22. Помощь / ЧаВо

Наши технические специалисты оформили техническое описание структуры, технологий и сервисов Decimal. Это облегчает понимание внутренних процессов, деталей процедур и механизмов, заложенных в блокчейн. В списке присутствует как техническое описание, адресованное девелоперам либо владельцам бизнесов, так и широкому кругу обычных пользователей, которые ищут ответы на свои вопросы и способы устранения каких-либо затруднений при взаимодействии с Decimal.

Для ознакомления с информацией перейдите по ссылке https://help.decimalchain.com

Статьи и ответы на вопросы будут регулярно обновляться и пополняться новой информацией по мере развития комьюнити и самого блокчейна Decimal.

23. Структура блока

Блок - это основополагающая сущность блокчейна. Элемент цепочки блоков, который содержит в себе транзакции пользователей, транзакции эмиссии DEL, подписи валидаторов, комиссии, хэш текущего и предыдущего блока и прочую служебную информацию.

В блокчейне Decimal блоки генерируются примерно каждые 5,5 - 6 секунд.

Блок содержит от 0 до 10 000 транзакций, весом примерно 180 байтов каждая. Вознаграждение за блок происходит согласно модели эмиссии, на старте 50 DEL с последующим увеличением каждые 432 000 блоков (~ 30 календарных дней).

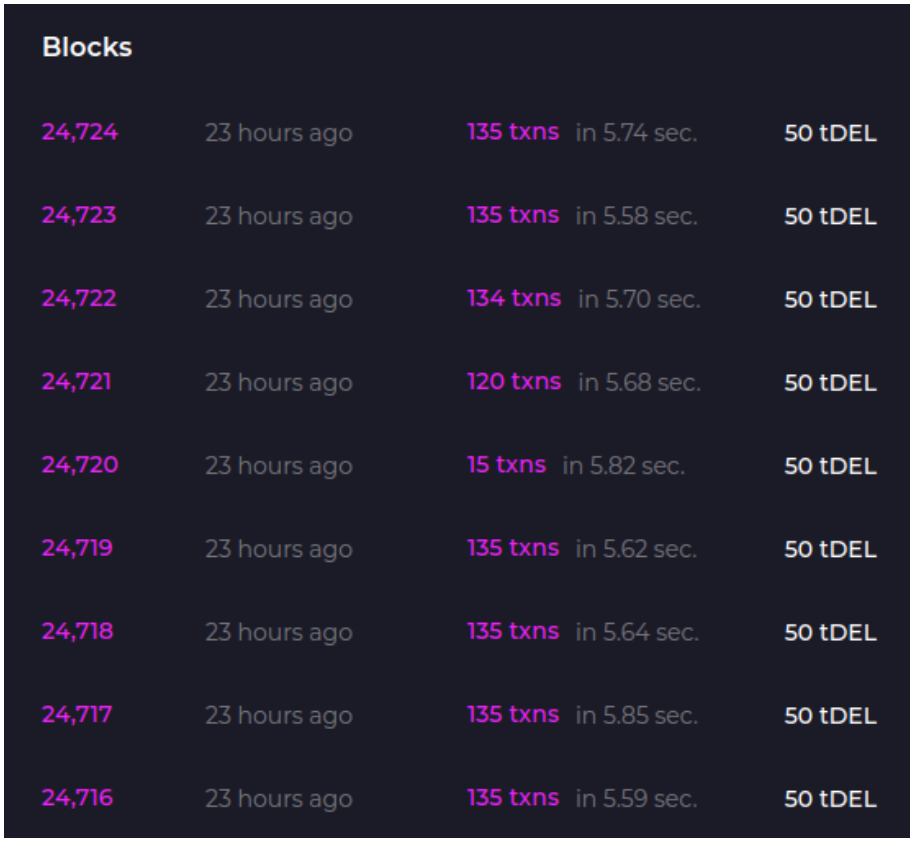


Рисунок - блоки Decimal в Обозревателе.

В основе Decimal лежит движок Tendermint. Более подробно об устройстве блока можно узнать из его спецификации (https://github.com/tendermint/spec/blob/953523c3cb99fdb8c8f7a2d21e3a99094279e9de/spec/blockchain/blockchain.md)

Здесь же приведём выдержки из документации.

23.1. Структура данных

Блок включает в себя следующий список основных типов данных:

- Блок (Block)
- Заголовок (Header)
- Версия (Version)
- Идентификатор блока (BlockID)
- Время (Time)
- Данные транзакции (Data (for transactions))
- Подтверждения и голоса (Commit and Vote)
- Доказательства (EvidenceData and Evidence)

23.2. Блок

Блок состоит из заголовка, транзакций, голосов и списка доказательств нарушений (например, двойная подпись).

```
type Block struct {
  Header  Header
  Txs     Data
  Evidence    EvidenceData
  LastCommit  Commit
}
```

Заметьте, что **LastCommit** является набором подписей валидаторов, которые подписали последний блок.

23.3. Заголовок

Заголовок блока включает в себя метаданные о блоке и о консенсусе, а также подтверждения данных в текущем блоке, предыдущем блоке и результат, возвращенный приложением:

```
   type Header struct {
// основная информация о блоке
Version  Version
ChainID  string
Height   int64
Time     Time

// информация о предыдущем блоке
LastBlockID BlockID

// хэши данных блока
        LastCommitHash  []byte // подтверждения от валидаторов из предыдущего блока
        DataHash  []byte  // Дерево Меркла хэшей транзакций

// хеши данных от приложений из предыдущего блока
ValidatorsHash  []byte // валидаторы текущего блока
```

NextValidatorsHash []byte // валидаторы следующего блока

ConsensusHash []byte // параметры консенсуса для текущего блока

AppHash []byte // состояние приложения после транзакций из предыдущего блока

LastResultsHash []byte // корневой хеш всех данных транзакций из предыдущего блока

// информация для достижения консенсуса

EvidenceHash []byte // конфликты в данном блоке

ProposerAddress []byte // создатель данного блока

23.4. Транзакции

Данные - это обёртка списка транзакций, которые являются байтовыми массивами произвольной длины:

```
type Data struct {
  Txs [][]byte
}
```

24. Ссылки

1. Jae Kwon, Tendermint: Consensus without Mining Draft v.0.6 (outdated), 2014.
https://tendermint.com/static/docs/tendermint.pdf

2. Practical Byzantine Fault Tolerance Miguel Castro and Barbara Liskov Laboratory for Computer Science, Massachusetts Institute of Technology, 545 Technology Square, Cambridge, MA02139
http://www.pmg.csail.mit.edu/papers/osdi99.pdf

3. Vitalik Buterin A Proof of Stake Design Philosophy
https://medium.com/@VitalikButerin/a-proof-of-stake-design-philosophy-506585978d51

4. Cosmos SDK
https://docs.cosmos.network/

5. Tendermint
https://docs.tendermint.com/

6. Хайек, Фридрих Август фон
https://ru.wikipedia.org/wiki/%D0%A5%D0%B0%D0%B9%D0%B5%D0%BA,_%D0%A4%D1%80%D0%B8%D0%B4%D1%80%D0%B8%D1%85_%D0%90%D0%B2%D0%B3%D1%83%D1%81%D1%82_%D1%84%D0%BE%D0%BD

7. Кейнс, Джон Мейнард
https://ru.wikipedia.org/wiki/%D0%9A%D0%B5%D0%B9%D0%BD%D1%81,_%D0%94%D0%B6%D0%BE%D0%BD_%D0%9C%D0%B5%D0%B9%D0%BD%D0%B0%D1%80%D0%B4

8. BIP: 173 or bc1 addresses
https://github.com/bitcoin/bips/blob/master/bip-0173.mediawiki

9. Pieter Wuille lecture on new bech32 address format
https://www.reddit.com/r/Bitcoin/comments/62fydd/pieter_wuille_lecture_on_new_bech32_address_format/

10. Bech32, native SegWit address already used on the mainnet
https://www.reddit.com/r/Bitcoin/comments/74tonn/bech32_native_segwit_address_already_used_on_the/dqlogru/

11. Enterprise-class open source distributed monitoring solution. https://www.zabbix.com/ru/manuals