TERA PLATFORM

Yuriy Ivanov (Vtools)
01 июня 2019
progr76@gmail.com
(черновик ver: 0.36)
внимание: информация в данном документе устарела

ОГЛАВЛЕНИЕ

Абстрактно

TERA — это платформа децентрализованных приложений. Это своеобразная операционная система. Она состоит из хранилища программ и хранилища данных, интегрированных в сеть Интернет. Механизм публикации программ и данных является свободным от цензуры. Кровеносной системой является Блокчейн.

Рассмотрим следующие слои ИТ:

- Аппаратное Обеспечение;
- Программное Обеспечение;
- Интерфейс пользователя;
- База данных;
- Централизованная сеть;
- Децентрализованная сеть.

В XXI веке почти у каждого человека есть вычислительное устройство (Персональный Компьютер, Ноутбук, Смартфон, Смарт-часы и многое другое). Существование этих устройств было бы бесполезным, если бы для них не производили различное Программное Обеспечение. Процессы и результаты работы данного ПО отображаются через визуальный интерфейс. Часто результат сохраняется в базу данных устройства для возможности повторного обращения. При необходимости доступ к базам данных можно предоставить другим пользователям через сеть, что принесёт гораздо больше пользы пользователю. Каждый подобный шаг увеличивает КПД нужного процесса.

Для связи друг с другом устройства объединяются в сеть, в которой каждое устройство называется **узел**. Наиболее простым способом объединения устройств в сеть является использование одного координирующего сервера. Однако это решение не является надёжным по причине существования единой точки отказа. Существует альтернативное решение, в котором все узлы равны между собой, имеют одинаковый ранг и приоритет. Это решение в дальнейшем обозначается как **децентрализованная сеть**. Важно, чтобы децентрализованная сеть работала как единое целое, представляя собой слаженный организм. Для того, чтобы добиться этой слаженности, используются специальные алгоритмы взаимодействия узлов друг с другом, которые далее будем называть **консенсусами (**консенсус времени, консенсус доставки, консенсус цепочки данных).

TERA — это следующее поколение взаимодействия человека и программного обеспечения.

Введение

Проблемы современных блокчейнов

Низкая производительность. Нет прорывной технологии

К 2017 году была определена основная проблема Блокчейна — низкая скорость работы. В дальнейшем ситуация не поменялась. За исключением централизованных Блокчейнов (к которым мы относим Блокчейны имеющие фиксированное число нод блок продюсеров, например 21) не появилось ни одного масштабируемого решения. Отрасли необходима, применяющая динамическую масштабируемость, технология, позволяющая работать с ней сотням миллионов людей по всему миру. Отсутствие такой технологии приводит к стагнированию отрасли и к потере капитализации криптовалют на биржах.

DApps и централизация

DApp (Decentralized Application) — децентрализованное приложение. Однако на данный момент термин применяется неправильно. Этим термином называют программу, которая взаимодействует со смарт-контрактом в Блокчейне, но фактически расположена на централизованном сервере. Та часть, которая находится на централизованном сервере является ключевой, и без неё работа невозможна. Децентрализованное приложение такого типа может гарантировать только сохранность средств пользователя, так как они находятся на Блокчейне. Такая ситуация сложилась из-за того, что текущие Блокчейны не предоставляют в своей платформе услуг хостинга. Такого понятия как «интерфейс пользователя» нет на существующих Блокчейнах (за исключением Блокчейна TERA).

Нет полной интеграции с Web

Блокчейн остается слишком виртуальным для обычных пользователей, они не видят его перед глазами. Трудно верить в то, что никогда не видел. Добавление в Блокчейны визуальных интерфейсов позволит пользователям наблюдать всю картину в реальном времени и начать работать с ними. Реальному распространению Блокчейна поможет простота разработки приложений. Для этого язык смарт-контракта должен быть максимально простой и максимально знакомый. Необходимо использовать современные распространенные технологии (JavaScript и HTML). Веб-программисты являются самой большой армией IT-индустрии. Они ближе всего к пользователям, они смогут максимально быстро создать востребованные приложения на Блокчейне и сделают их максимально удобными для пользователей.

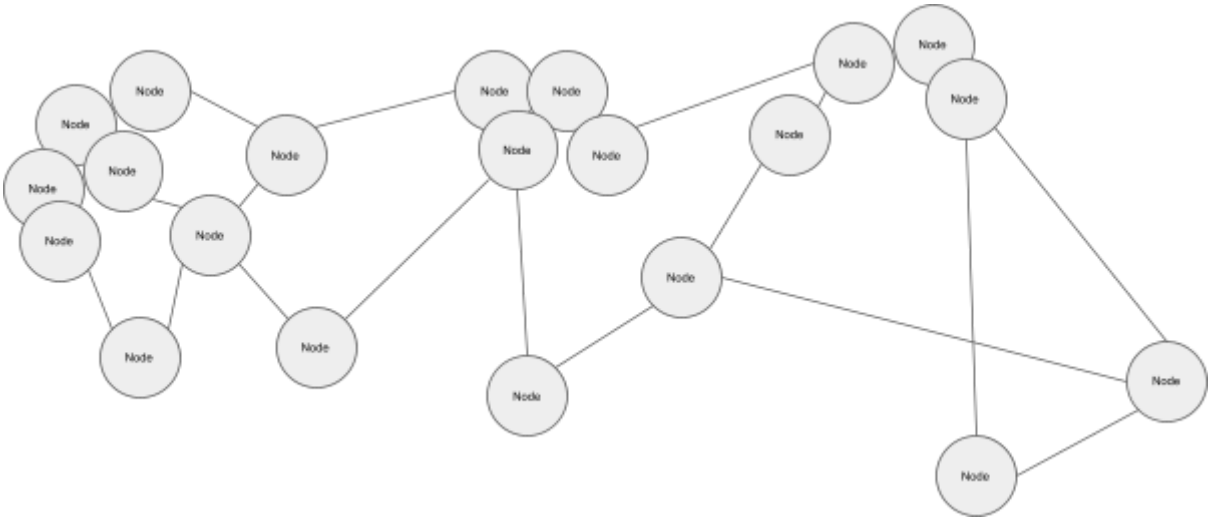
Реализация

Теоретическая часть

Для решения проблемы масштабирования классический подход к построению блокчейна (например тот который используется в Биткоине) не годится, требуется значительная переработка. Практически нужно заново переизобрести блокчейн. Ниже мы показываем какие нужно сделать изменения для построения нового блокчейна. Мы исходим из того что читатель уже прочел WhitePaper Биткоина и полностью понял его принцип.

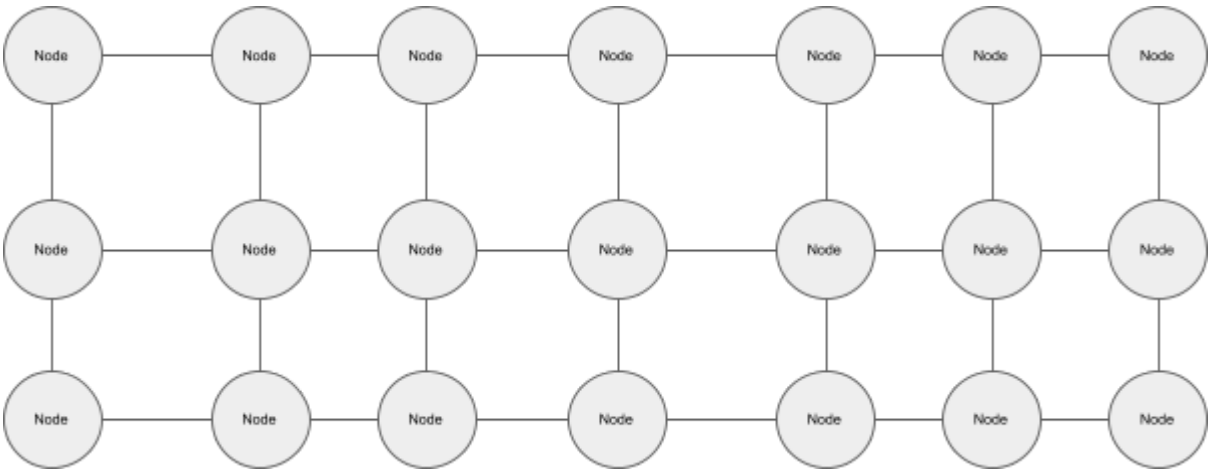
Быстрая маршрутизация сети

В традиционных Блокчейнах не применяется упорядочивание узлов друг с другом, в них применяется устаревший протокол доставки информации Gossip. Общая картина сети выглядит так:



Данная случайная организация связей не гарантирует быструю доставку блоков между всеми узлами.

Поэтому в TERA используется специальный протокол Tera Protocol, по которому узлы самоорганизуются в упорядоченные соединения образуя многомерную регулярную решетку:



Блокчейну для доставки данных от 1-го узла до последнего требуется не более 3 секунд. Узлы образуют соединения между собой, который основывается на подобии их ID. Каждый ID является случайной величиной с длиной 32 байта и не меняются в процессе работы узла. Среднее число связей с другими узлами имеет логарифмическую зависимость от количества узлов в сети, что обеспечивает константное время доставки транзакций. Так, если в сети будет 1 000 000 000 узлов, а время доставки между узлами будет составлять не более 100 миллисекунд, то максимальное время составит: 30 * 100 мс = 3 сек. 30 – это логарифм из 1 миллиарда. Именно столько соединений между узлами и существует. При этом время задержки доставки транзакций между узлами в 100 мс является верхней величиной, на практике оно меньше, так как узлы с меньшей взаимной задержкой имеют приоритет соединения.

Для того чтобы “зацементировать” удачные соединения, каждый узел для себя записывает статистику удачных обменов с другим узлом, с которым обменивается содержимым блоков. Эта статистика влияет на приоритет соединения.

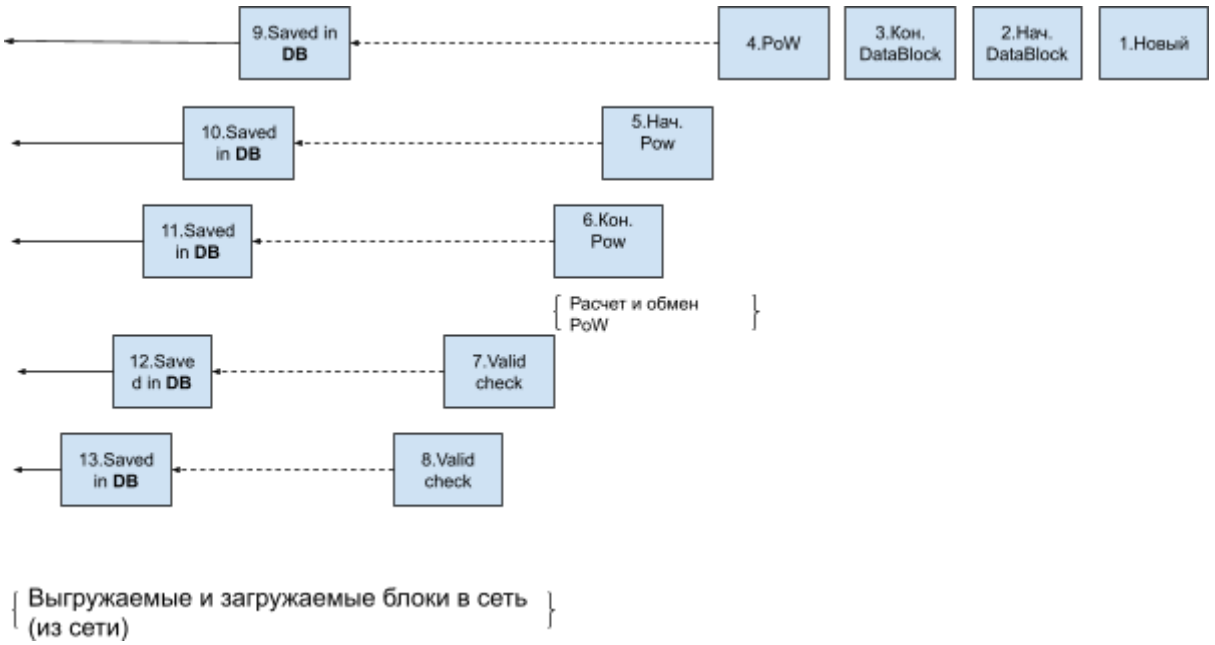
Сетевой протокол

Транзакция отправляется пользователем на N соседних узлов (где N в диапазоне от 5 до 16). Транзакция добавляется в новый формируемый блок (блок текущей секунды). При наступлении этапа обмена транзакция начинает перемещаться с одного узла на другой, накапливаясь в их блоках. В случае если в блоке содержится больше транзакций, чем он может вместить, остаются транзакции с большим PoW (Proof of Work) — таким образом реализуется защита от DDoS-аттак. По окончанию этапа формирования блока выполняется этап подписи и расчет PoW-блока (1 секунда), далее этап поиска блока-лидера с максимальным PoW (3 секунды). Такой блок добавляется в цепочку блоков.

Конвейерная обработка блоков

Блокчейн в TERA формирует блоки один раз в секунду, но время подтверждения блока (т.е. время включения блока в Блокчейн) составляет 8 секунд. Для метода реализации создания блоков в 8 раз быстрее, чем время подтверждения, используется конвейерная обработка блоков. Это можно представить, как 8 отдельных Блокчейнов, с периодом формирования 8 секунд. Каждый такой Блокчейн сдвинут относительно друг друга на одну секунду. Таким образом за одну секунду мы создаем блок 1-го Блокчейна, следующую секунду блок 2-го Блокчейна и так до 8-го Блокчейна. Для того чтобы соединить эти Блокчейны в один, Блокчейны склеиваются. В традиционных Блокчейнах для связи блоков в единую цепочку в заголовке каждого блока включается хеш предыдущего блока. В TERA для этих целей хеш предыдущего блока вычисляется на основании сразу нескольких предыдущих блоков каждого из 8 Блокчейнов. На этом этапе получается логическое связывание 8-ми цепочек в одну.

Параллельно обрабатывается несколько блоков. Порядок этой обработки зависит от текущего времени (текущего блока):

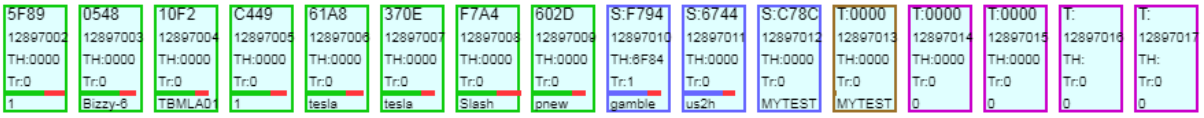


Тайминг:

1. Новый (текущий) блок, загрузка транзакций из Mempool, активация по таймеру.
2. Начало синхронизации блока (распределенное формирование блока).
3. Окончание синхронизации.
4. Связка данных блока с предыдущими блоками, расчет PoW.
5. Начало поиска максимального PoW сети.
6. Окончание поиска максимального PoW.
7. Проверка валидности блока с учетом возможного изменения предыдущих блоков из-за загрузки новой цепочки блоков с большим суммарным PoW.

Из схемы видно, что блок ссылается на предыдущие блоки, но с дельтой 8 блоков. Валидные и сохраненные в БД блоки, начиная с 8-го и далее, участвуют в выгрузке в другие узлы (аналогично они могут быть загружены от других узлов).

Вот так это выглядит в реальном Блокчейне TERA:



Отдельные слои: блокчейн и криптовалюта

Мы разделили понятие блокчейн и криптовалюта. Мы создали два слоя:

1. Слой только блокчейна
2. Слой криптовалюты

Что такое блокчейн: это компьютерная сеть в которой каждый узел является равноправным, их число неограниченно, общение между осуществляется посредством организации единой цепочки данных, в которую информация записывается поблочно в виде команд (транзакций). В классических блокчейнах в блоки записываются только платежные транзакции, при этом не допускается запись в блок транзакции, которая не является валидной (например, не имеет правильную цифровую подпись или не достаточно денег на счете или двойная трата и т.д.).
В блокчейне платформы TERA нет криптовалюты, поэтому допускается запись любой информации, блокчейн используется как транспорт. Каждая запись (далее мы их будем называть транзакциями**)** имеет свою строгую нумерацию и разделены на блоки, блоки связаны с друг другом посредством необратимой криптографической хеш-функции. На первом слое задача блокчейна обеспечить одинаковость информации в каждой ноде сети. Эта задача решается посредством классического консенсуса **PoW**.

Интерпретация правильности информации лежит на следующих слоях. На втором слое реализована поддержка криптовалюты - встроенной монеты **Тера**. На этом же слое реализованы смарт-контракты. Монета Тера важна для сети, так как используется для мотивации майнеров поддерживать сеть.
Т.к. на первом слое гарантирована одинаковость данных, и так как код программы на втором слое одинаков на всех нодах сети, очевидно, что выполняя одни и те же действия все ноды будут иметь одинаковый результат: одинаковые остатки по счетам пользователей, одинаковые состояния смарт-контрактов. Таким образом, если в этих блоках будут невалидные транзакции типа двойных трат, то валидирующий слой одинаково их отклонит на всех узлах сети.

Валидацию можно выполнять в другое время и в другом процессе, не мешая блокчейну. Более того - это можно это делать гораздо быстрее за счет так называемой

пакетной обработки (массовости проверок) — мы можем группировать операции и ускорить работу за счет меньшего количества обращений к Базе Данных.

Зависимость размера базы блокчейна от настроек пользователя

При больших объемах данных, которые неминуемо наступят при 1000 tps (транзакций в секунду), новые пользователи должны иметь возможность быстрого скачивания Блокчейна, чтобы провалидировать его и приступить к работе с ним. Поэтому порядок скачивания меняется — если он раньше был с начала цепочки, то теперь будет загружаться с конца.

Загрузка информации будет зависеть от настроек пользователя — размер памяти диска, которую он выделил для работы Блокчейна. В зависимости от размера будет следующий приоритет загрузки:

1. Таблица счетов
2. Заголовки блоков
3. Содержимое блоков и транзакций

Как это будет работать:

1. Для супертонкого клиента: будет загружаться только часть заголовков и небольшая часть таблицы счетов;
2. Для среднего клиента: вся таблица счетов и заголовков, но только часть содержимого блоков;
3. Для полного клиента — все данные.

Пример:
Пользователь выделяет место под Блокчейн на диске, например, 12 Гб.

Это место на диске делится на три части:

- 1. Регулярная структура блоков (начиная с конца), условно — 5 Гб;
- Другие блоки, не вошедшие в регулярную структуру, но, обязанные храниться на узле (определяется по принципу DHT — степени похожести адреса узла), например 5 Гб;
- Последние часто используемые блоки, например, 2 Гб.

Безопасность

Мы используем консенсус POW для создания необратимой цепочки блоков. На данный момент POW это единственный децентрализованный консенсус и он

предполагает что минимум 51% владельце майнинговых мощностей являются честными.

Защита от replay-атаки

TERA использует Блокчейн с консенсусом PoW. Это позволяет расположить все транзакции последовательно друг за другом. Выполнение транзакций также производится последовательно. При списании со счета проверяется наличие необходимой суммы. В момент списания увеличивается счетчик номера операции ("OperationID"). Каждая последующая платежная транзакция должна иметь следующий номер "OperationID" для предотвращения применения одной и той же транзакции несколько раз.

Защита от двойной траты

Пользователи Bitcoin для защиты от двойной траты ждут минимум 10 минут, а иногда и несколько часов.

В сети TERA блоки создаются раз в секунду, а время первого подтверждения 8 секунд, но, если вы хотите такую же степень надежности, как и в сети Bitcoin, вам нужно ждать аналогичное время. Время ожидания – это степень надежности. Здесь нет магии, в любом алгоритме PoW вы меняете время на надежность. В TEPA мы сделали более гибкую возможность выбора. Можете ждать 8 секунд, 1 минуту, а можете 1 час (если суммы переводов значительны).

Защита от DDoS атак

Ограничение на число отправляемых транзакций

Каждая отправляемая транзакция проверяется от имени какого счета она была отправлена. Это делается путем проверки цифровой подписи по публичному ключу этого счета. Пользователи имеют лимит на число транзакций в течении определенного времени (например 1000 блоков), его значение плавающее - при низкой загруженности сети можно отправить больше транзакций. Реализовано это через механизм приоритета транзакций, транзакции сортируются в порядке приоритета, который зависит от общего числа ранее отправленных транзакций, чем он больше - тем ниже шансы попасть в блок. Таким образом счета с которых часто отправляются транзакции начинают конкурировать только с друг другом, а счета которые редко отправляют - идут вне очереди.
Если предположить что атакующий создал тысячи счетов и начал атаки путем генерации большого количества транзакций по очереди с каждого счета, то уже со второй транзакции они начинают конкурировать с друг другом и канал остается свободным для пользователей, которые не отправили еще ни одной транзакции за последние 1000 сек. При этом каждая следующая транзакция атакующего снижает

эффект от атаки, т.к. она становится все ниже и ниже конкурентоспособна за право включения в блок.

Pow

Для защиты от DDoS-атаки используется алгоритм PoW. Чем больше длина транзакций, тем больше должна быть величина PoW. Величина PoW рассчитывается клиентом перед отправкой транзакции в сеть.
Каждый блок имеет ограничение в 130 Кб, средний размер транзакций составляет 130 байт, таким образом в среднем помещается 1000 транзакций в блок. Каждая транзакция должна иметь поле PoW, в которое записывается проделанная работа по вычислению хеша. Это поле служит для определения возможности включения этой транзакции в блок. Оно должно быть не менее определенной величины и быть достаточным значением чтобы конкурировать с другими транзакциями. В блок включаются только первые ~1000 транзакций, имеющие максимальное значение PoW.

Расчет

Большая пропускная способность Блокчейна и требование на обязательное выполнение PoW в каждой отправляемой транзакции позволяет эффективно организовать защиту от DDoS-атак в следующих границах:

- Атакующий обладает вычислительной мощностью в 1000 раз больше среднего пользователя;
- Средняя загруженность сети составляет 50%, т.е. 500 транзакций в секунду.

В этом случае атакующий может отправить 1000 транзакций в секунду. При первой отправки в сети будет 1000 транзакций атакующего и 500 обычных пользователей, всего 1500 транзакций. Блокчейн примет только 1000 транзакций, значит 500 будут отброшены - по одной трети с каждой стороны. Но при этом будет зафиксировано увеличение средней мощности PoW транзакций и поэтому в следующем блоке обычные пользователи потратят больше вычислительного времени для отправки транзакции. В то же время атакующий не сможет повысить мощность расчета PoW транзакций, т.к. он изначально работает на пределе - на 100% своих мощностей. В итоге средняя мощность PoW транзакции рядового пользователя вырастет в два раза и соотношение в блоке между обычными транзакциями и транзакциями атакующего будет 500 на 500. Т.е. все транзакции пользователей будут приняты.

Из этих рассуждений видно: чем меньше загруженность Блокчейна -- тем труднее нанести DDoS-атаку. Как только средняя загруженность Блокчейна превысит 50%, мы увеличим верхний порог транзакций. На данный момент узел майнеров поддерживает обработку транзакций только одним потоком. Учитывая, что на данный момент многоядерные процессоры являются нормой, не составит труда кратно увеличить производительность каждого узла.

Защита от атаки Сибиллы

В сети все ноды равноправны и анонимны. Они случайным образом соединяются с друг другом для образования многомерной решетки для эффективной передачи данных. Но при этом возможны атаки Сивиллы, когда злоумышленник создает большое количество нод и пытается вести злонамеренные действия:
“Хорошая” нода отличается от “плохой” ноды, тем что она четко следует протоколу.
“Плохая” нода может:

- не передавать информацию когда это нужно
- передавать информацию когда это не нужно
- передавать ложную информацию

Цель каждой ноды в сети корректно передать информацию. Результат корректной передачи это успешно синхронизированный блок, отсутствие орфан цепочек. Этот показатель виден спустя несколько секунд после обмена и он объективен, т.к. защищен консенсусом pow блока, поэтому его подделать нельзя, не имея 51% мощностей (но мы в рассуждениях всегда исходим из того, что 51% мощностей в сети - честные). Таким образом у нас есть в наличии достаточно хороший механизм определения правильности следования протоколу тех нод, с которыми мы обмениваемся. Поэтому для того чтобы “зацементировать” удачные соединения, каждый узел для себя записывает статистику удачных обменов с другим узлом, с которым обменивается содержимым блоков. Эта статистика влияет на приоритет формирования связей при создании сети по типу многомерной регулярной решетки.

Экономическая стимуляция майнеров

Поддержкой сети в Блокчейне занимаются так называемые «майнеры», которые выполняют расчет сложного хеша блока для создания необратимости цепочки блоков. В качестве экономического стимула выступает награда за найденный хеш блока, в размере одной миллиардной части от остатка нераспределенной суммы монет. Изначально общая нераспределенная сумма равнялась 1 000 000 000 (общая эмиссия TERA), поэтому со временем награда будет падать, но это будет компенсироваться реальным курсом на биржах, а также обратным пополнением нераспределенного остатка монет за счет платных транзакций:

- 10 TERA – создание нового счета пользователя вне ограничительной очереди;
- 100 TERA – создание смарт-контракта или децентрализованного приложения;
- 10 000 TERA – создание смарт-токена (т.е. собственной валюты).

Оплата идет на счет #0, т.е. обратно в копилку для майнинга. Цена транзакций будет в дальнейшем меняться через DAO-механизм голосования.

Практическая часть

Спецификация

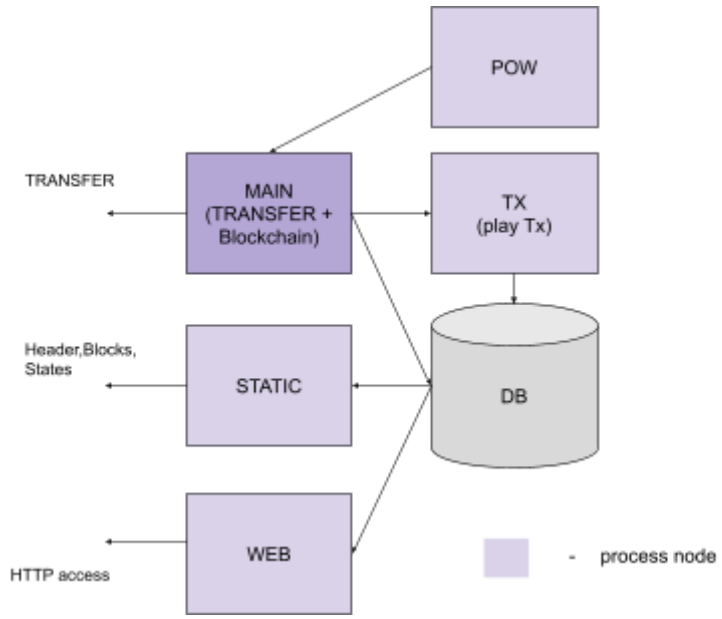
- Консенсус: PoW;
- Алгоритм: TERAHASH (sha3 с оптимизацией на использование памяти);
- Максимальная эмиссия: 1,000,000,000 TERA.
- Награда за блок: 9/1000000000 от остатка нераспределенной суммы монет;
- Премайн: 5%;
- Фонд разработки: 1% от майнинга;
- Время генерации блока: 3 секунда;
- Время подтверждения блока: 8 секунд;
- Размер блока: 350 Кбайт;
- Скорость: 1000 транзакций в секунду;
- Комиссия в транзакциях: бесплатно;
- Криптография: sha3, secp256k1;
- Защита от DDoS-атак: PoW (расчет хеша);
- Платформа: Node.JS;
- Язык смарт-контрактов: JavaScript.

Состав процессорных потоков

Важным аспектом Блокчейна TERA является непрерывная работа сети. Сеть образуется путем создания топологии типа многомерная “решетка” с динамическим поддержанием структуры. Обмен выполняется ежесекундно. Узел должен непрерывно выполнять обмен информацией по новым блокам со своими соседями (эта задача далее будет обозначаться **TRANSFER**). Такой обмен должен выполняться даже если узел находится в режиме загрузки цепочки Блокчейна (т.е. не синхронизирован).

При запуске полного узла создаются следующие процессы (node):

1. **MAIN** — Главный поток программы + TRANSFER. Запись новых блоков в БД. Загрузка истории при рассинхронизации;
2. **STATIC** - Отдача статической информации другим узлам (заголовки, блоки, состояния);
3. **TX** - Выполнение транзакций (изменение таблицы состояний);
4. **WEB** - Отдача данных по протоколу HTTP для полной интеграции с WEB;
5. **POW** - майнинг-процессы. Накачка памяти хешами и быстрый поиск заданного соответствия.



Links

Website: https://terafoundation.org/
Bitcointalk ANN: https://bitcointalk.org/index.php?topic=4573801.0
Repo: https://gitlab.com/terafoundation/tera2

Tools

Tera Decentralized Exchange: http://teraswap.io/
Online Node Map: https://teraexplorer.org/map.html
Web Wallet: https://terawallet.org/
Top Miners: https://teraexplorer.org/dapp/100

API-1: https://gitlab.com/terafoundation/docs/-/blob/master/develop/API.md
API-2: https://gitlab.com/terafoundation/docs/-/blob/master/develop/API2.md
Constants: https://gitlab.com/terafoundation/docs/-/blob/master/develop/CONSTANTS.MD
Release2468:
https://gitlab.com/terafoundation/docs/-/blob/master/develop/release2468.md
Release2600:
https://gitlab.com/terafoundation/docs/-/blob/master/develop/release2600.md

Docs

DApps Paper:
https://docs.google.com/document/d/1PXVBbMKdpsAKPkO9UNB5B-LMwIDjylWoHvAAzzrXjvU/edit?usp=sharing

TERAHASH mining algorithm:
https://docs.google.com/document/d/18DtASGhrbRwXCAkQR1hQG0lVdrStp4CgA-pd6hicwfo/edit

RUS - Обновлённый протокол консенсуса TERA - JINN
https://docs.google.com/document/d/1wV9bFUHeLA-u7y1eM9wQkLkzQ9OJf82rEbCFITXPTg8/edit#heading=h.6wabh3sbxwv5

Social Media

Telegram: https://t.me/terafoundation
Twitter: https://twitter.com/terafoundation
Discord Invite Link: https://discord.gg/CvwrbeG
QQ: https://jq.qq.com/?_wv=1027&k=5KpN5fw
Youtube: https://www.youtube.com/channel/UCMrK6jEqhudlV9XzS2l3rVQ