

# TERA PLATFORM

Yuriy Ivanov (Vtools)

19 марта 2019

[progr76@gmail.com](mailto:progr76@gmail.com)

(черновик ver: 0.31)

## ОГЛАВЛЕНИЕ

<b>Абстрактно</b>	<b>2</b>
<b>Введение</b>	<b>3</b>
Проблемы современных блокчейнов	3
Низкая производительность. Нет прорывной технологии	3
Даппы и централизация	3
Нет полной интеграции с Вебом	3
<b>Реализация</b>	<b>4</b>
Теоретическая часть	4
Быстрая маршрутизация сети	4
Сетевой протокол	5
Конвейерная обработка блоков	5
Разделение доставки и валидации данных	6
Река данных	7
Зависимость размера базы блокчейна от настроек пользователя	7
Безопасность	8
Защита от двойных трат	8
Расчет числа подтверждений блоков	9
Экономическая стимуляция майнеров	9
Защита от DDOS атак	9
Практическая часть	10
Спецификация	10
Состав процессорных потоков	11
<b>Ссылки</b>	<b>12</b>

# 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 на консенсусе POS и его производных) 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

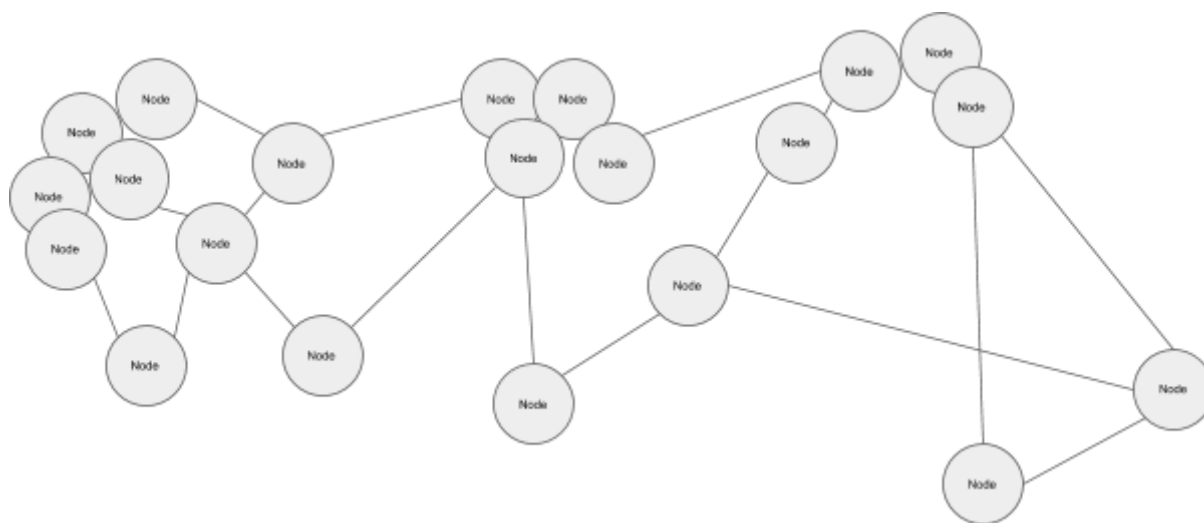
Блокчейн остается слишком виртуальным для обычных пользователей, они не видят его перед глазами. Трудно верить в то, что никогда не видел. Добавление в Блокчейны визуальных интерфейсов позволит пользователям наблюдать всю картину в реальном времени и начать работать с ними. Реальному распространению 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

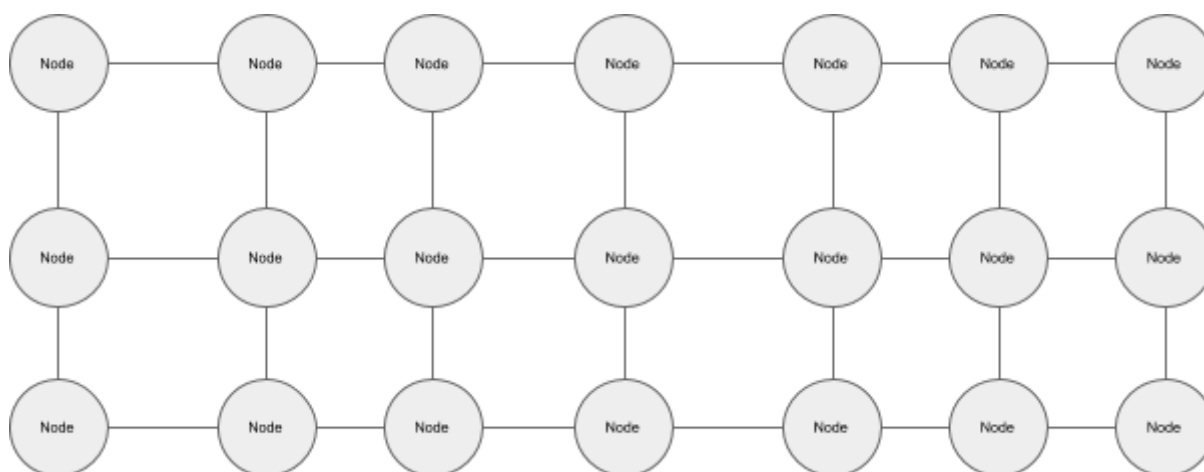
### Быстрая маршрутизация сети

В традиционных Блокчейнах не применяется упорядочивание узлов друг с другом. Общая картина сети выглядит так:



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

В TERA узлы самоорганизуются в упорядоченные соединения:



Блокчейну для доставки данных от 1-го узла до последнего требуется не более 3 секунд. Для достижения этого узлы соединяются между собой в специальные связи,

основанные на подобию адресов узлов. Адреса узлов являются случайными величинами (32 байта) и не меняются в процессе работы узла. Число связей с другими узлами имеет логарифмическую зависимость от количества узлов в сети, благодаря этому достигается 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:  $30 * 100 \text{ мс} = 3 \text{ сек}$ . 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.

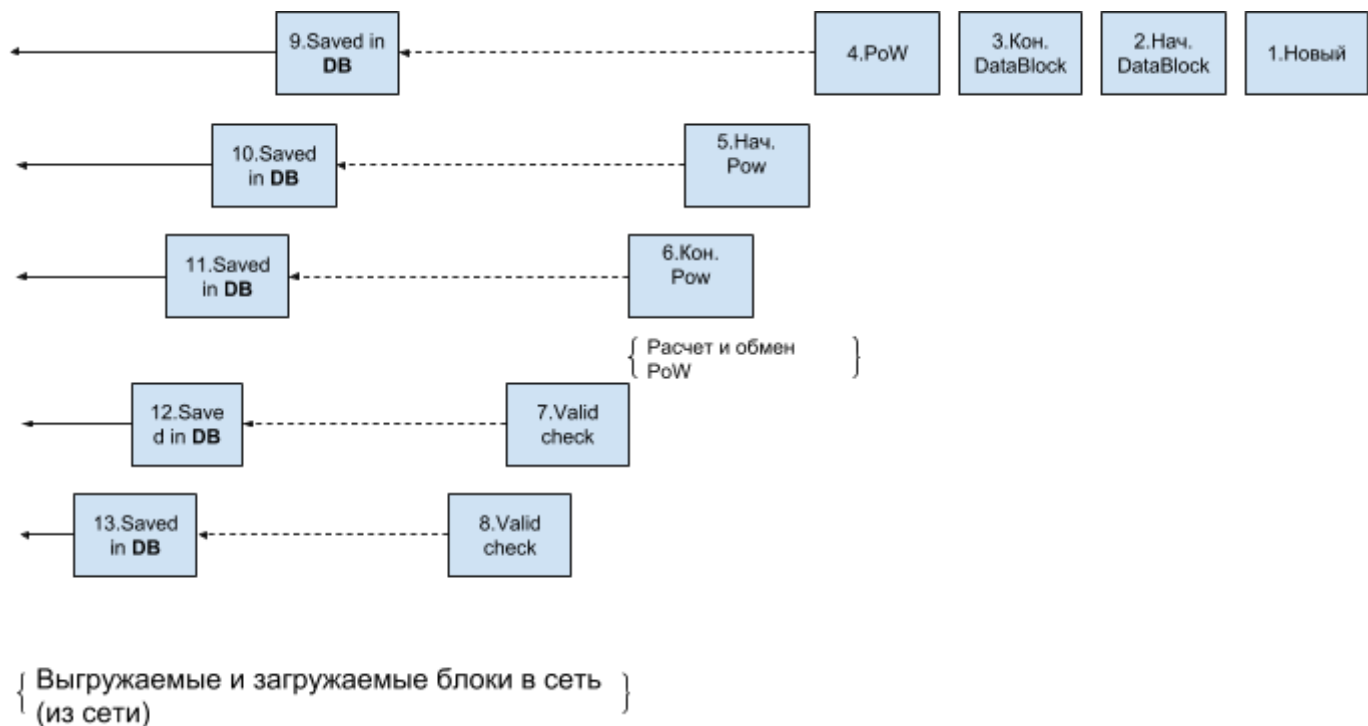
## Сетевой протокол

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-атак. По окончании 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:

5F89	0548	10F2	C449	61A8	370E	F7A4	602D	S:F794	S:6744	S:C78C	T:0000	T:0000	T:0000	T:	T:
12897002	12897003	12897004	12897005	12897006	12897007	12897008	12897009	12897010	12897011	12897012	12897013	12897014	12897015	12897016	12897017
TH:0000	TH:0000	TH:0000	TH:0000	TH:0000	TH:0000	TH:0000	TH:0000	TH:8F84	TH:0000	TH:0000	TH:0000	TH:0000	TH:0000	TH:	TH:
Tr:0	Tr:0	Tr:0	Tr:0	Tr:0	Tr:0	Tr:0	Tr:0	Tr:1	Tr:0	Tr:0	Tr:0	Tr:0	Tr:0	Tr:0	Tr:0
1	Bizzy-8	TBMLA01	1	tesla	tesla	Slash	onew	gamble	us2h	MYTEST	MYTEST	0	0	0	0

**Разделение доставки и валидации данных**

Каждый узел сети является равноправным. Число узлов неограниченно. Общение между узлами осуществляется посредством организации единой цепочки данных, в которую информация записывается в виде команд (транзакций). Часто такую цепочку называют Блокчейном, но в данной платформе ее применение расширено.

Традиционно в блоки записываются транзакции, при этом не допускается запись в блок транзакции, которая не является валидной (например, не имеет правильную цифровую подпись, не достаточно денег на счете, двойная трата и т.д.). В платформе TERA Блокчейн используется как транспорт, поэтому в блоки может записываться произвольная информация (далее мы будем называть ее **транзакция**). Интерпретация правильности информации лежит на приложениях более высокого уровня.

Блокчейн имеет механизм консенсуса, который определяет какая цепочка данных является истиной, но этот консенсус не содержит правил интерпретации транзакций внутри блока. Данные блока являются черным ящиком — все операции производятся как с набором байтов. 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.

## Река данных

Платформу TERA можно абстрактно представить в виде водного канала, который гарантирует непрерывность и нумерологический порядок прохождения судов с грузовыми контейнерами. Канал не отвечает за юрисдикцию судов и грузов. Полезность от судов получают порты, рыболовные заводы, склады и т.д. Они нагружают корабли полезной работой. Как этим пользоваться? Допустим, вам нужно доставить груз из порта А в порт Б. В порту А поместите груз в контейнер и отправьте его. В порту Б проверяйте все контейнеры на нужное содержимое и заберите груз, когда его найдете. Канал доставляет корабли сразу во все порты назначения всего за 8 секунд.

Важный аспект — это нумерологический порядок. Цель Блокчейна сделать так, чтобы на каждом устройстве мира был единый порядок и состав блоков. Если это обеспечить, то программа, которая их читает будет всегда выдавать один и тот же результат на всех компьютерах мира. Таким образом, даже если в этих блоках будут неправильные транзакции, двойные траты и так далее, то программа на стороне пользователя это увидит и отклонит ее выполнение. Это называется процесс валидации транзакции. Для ускорения всей системы мы разделили его от процесса доставки блоков. Таким образом валидацию мы можем выполнять в другое время и в другом процессе, не мешая Блокчейну, а также гораздо быстрее за счет 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

### Защита от двойных трат

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.



## Расчет числа подтверждений блоков

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

В сети TERA блоки создаются раз в секунду, 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 TERA мы сделали более гибкую возможность выбора. Можете ждать 8 секунд, 1 минуту, а можете 1 час (если суммы переводов значительны).

## 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.

## Защита от DDoS атак

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.

### Расчеты:

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 отправке 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 трудакратно увеличить производительность каждого узла.

## Практическая часть

### Спецификация

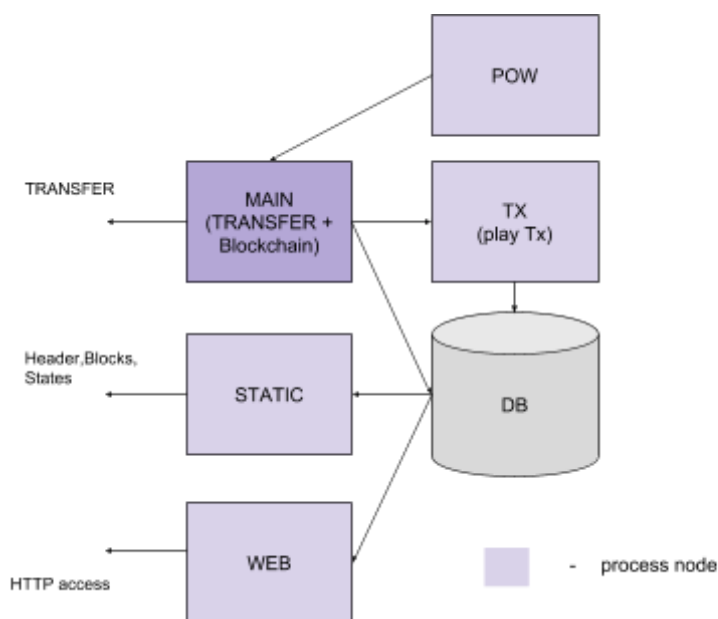
- Консенсус: PoW;
- Алгоритм: TERAHASH (sha3 с оптимизацией на использование памяти);
- Максимальная эмиссия: 1,000,000,000 TERA.
- Награда за блок: 1/1000000000 от остатка нераспределенной суммы монет;
- Премайн: 5%;
- Фонд разработки: 1% от майнинга;
- Время генерации блока: 1 секунда;
- Время подтверждения блока: 8 секунд;
- Размер блока: 130 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.



## ССЫЛКИ

Веб-сайт: <https://terafoundation.org/>

Анонс на BitcoinTalk: <https://bitcointalk.org/index.php?topic=4573801.0>

Twitter: <https://twitter.com/terafoundation>

Reddit: <https://www.reddit.com/user/Terafoundation>

Discord: <https://discord.gg/CvwrbeG>

Source Code: <https://sourceforge.net/p/tera/code/ci/master/tree/>

Telegram-канал: <https://web.telegram.org/#/im?p=@terafoundation>

QQ: [https://jq.qq.com/?\\_wv=1027&k=58VsQxc](https://jq.qq.com/?_wv=1027&k=58VsQxc)