ДОПОЛНЕНИЯ ТЕРА ШАРДИНГА (версия 3)

progr76@gmail.com

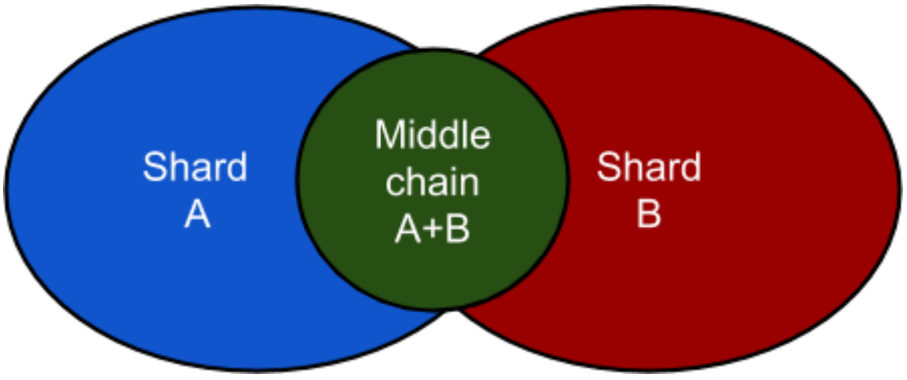
Центральный блокчейн наизнанку

Такое название происходит из того, что логика передачи кросс-транзакций похожа на схему с центральным блокчейном, но с отличиями:

- допустимо несколько таких “центральных” блокчейнов
- в нем нет собственных счетов для хранения монет или состояний
- это чистый лог/журнал кросс-шардинговых транзакций

Сеть представляет собой неограниченный набор блокчейнов. Каждая нода поддерживает два чейна:

- Shard-chain - основная цепочка с собственными внутренними транзакциями (т.е. это обычный блокчейн шарда)
- Middle-chain (платежный канал) - промежуточный блокчейн состоящий из кросс-транзакций. Он предназначен для связи шардов с друг другом. Количество нод/майнеров равно сумме нод блокчейна A и блокчейна B



Атаки:

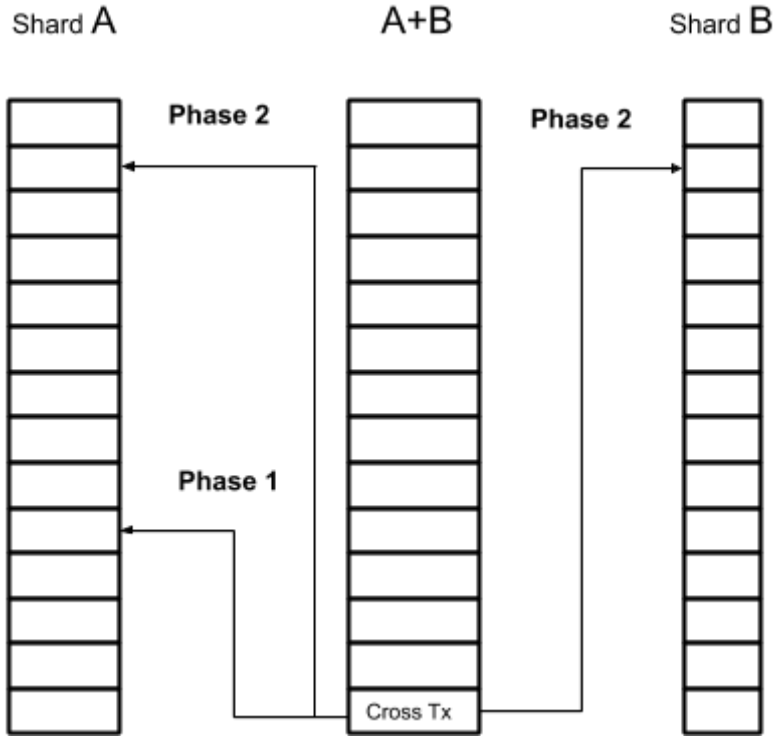
1) **B1.** Больший по мощности блокчейн переписывает историю промежуточного - **невозможно**, т.к. из определения консенсуса pow следует что большинство нод является честными.
2) **B2**. Майнеры меньшего по мощности блокчейн пытается переписать историю промежуточного - **невозможно**, т.к. честных майнеров больше в большем блокчейне.
3) **B3**. Перезапись маленького блокчейна - **все еще возможно**, но без перезаписи промежуточного блокчейна. Из-за этого возможна так называемая “двойная трата” когда плательщик - злоумышленник заплатил одними и теми же монетами два раза. Проблема решается через организацию майнинга таким образом, чтобы каждый майнер на 100% покрывал все шарды, например, через социальную организацию связей майнеров.

M-chain (платежный канал)

Промежуточный блокчейн, предназначен для обмена информацией между шардами, содержит только кросс-транзакции. Валидируется майнерами всех шардов, участвующих в обмене.
В заголовок блока записывается список шардов в виде идентификаторов монет, который валидирует майнер нашедший этот блок (для расчета статистики надежности).

Правила кросс-транзакций

1. Кросс транзакции попадают только в Middle-чейн, но так как его поддерживают все шарды, то они автоматически видны всем.
2. В Кросс-транзакцию записываются названия шардов: имя монеты источника и имя монеты получателя.
3. Исполнение кросс-транзакций идет с задержкой с высотой T1+T2 блоков, где T1 это время выполнения первой фазы (резервирования средств). T2 это время второй фазы (списание и зачисление средств).
4. В Middle-чейн в течении времени T2 в каждый блок записывается голос его создавшего майнера по поводу успешности завершении первой фазы. По истечении времени T2 каждая нода подсчитывает число голосов, в зависимости от числа которых выполняет/не выполняет кросс-транзакцию.
5. В каждой ноде маркер исполнения транзакций является общим между двумя чейнами (шарда и Middle), если один откатывается назад, то все транзакции также откатываются назад.



Линиями со стрелками показан порядок исполнения кросс-транзакций при переводе средств из А в Б

Голосование

Учитываются голоса ЗА и ПРОТИВ
Голос ЗА дает 1 балл
Голос ПРОТИВ отнимает VN баллов, например 8
Порог баллов для принятия решения составляет Vhold. Например если Vhold равно 10 за период в 100 блоков, то это позволит совершать кросс-транзакции между большим и маленьким блокчейнов, когда число майнеров в маленьком блокчейне только 10% от большого, т.к. майнеры из маленького блокчейна будут создавать блоки в среднем в 10% случаев.

Формула голосования (подсчет баллов):

$$Vote = Vyes - VN * Vno$$

Число полученных баллов Vote сравнивается с параметром Vhold, если оно равно или больше его то решение принимается (транзакция считается свершившейся).

Таблица различных вариантов параметров:

Вес голоса ПРОТИВ, Vno	Порог баллов для принятия решения, Vhold	Необходимый % мощностей-для принятия Tx, Vyes	Необходимый % мощностей для блокировки Tx, Vno
1	10	55	45
2	10	70	30
3	10	77	23
4	10	82	18
5	10	85	15
6	10	87	13
7	10	88	12
8	**10**	**90**	**10**

Атаки на платежный канал (компрементация токенов):

1) **P1.** Атака **зачисление без списания**. Ложное голосование ЗА для записи в М-чейн информации о ложном списании монет, для того чтобы во втором блокчейне успешно выполнить операцию их зачисления. Для успешной атаки злоумышленнику требуется контролировать более **90%** мощностей майнинга атакуемого блокчейна.

2) **P2.** Атака - **саботажем**. Ложное голосование ПРОТИВ для предотвращения кросс-транзакций. Для атаки требуется контроль более **10**% мощностей майнинга.

Примечания:

- В результате атаки **P1** токены малого блокчейна обесцениваются в большом блокчейне, т.к. они перестают быть обеспечены соответствующими монетами из-за действия злоумышленника. Но от этой атаки не страдают счета с самими монетами ни в одном блокчейне, т.к. они остаются нетронутыми.
- В результате атаки **P2** невозможно превратить монеты одного блокчейна в токены другого.
- Заметим, что увеличивая обязательный порог для **P1**, мы снижаем порог для **P2**.
- Для преодоления атаки **P1** процент независимых майнеров валидирующих два блокчейна должно превышать в более чем в два раза число необходимое для **P2** и они должны быть равновероятно распределены вместе с майнерами злоумышленниками. В выше рассмотренном примере требуется 20% перекрытия, т.к. в связи с тем что по определению консенсуса pow 51% майнеров честные, то следует что злоумышленник не сможет набрать 90% ни в одном блокчейне для совершения атаки. Каждая нода может вычислить необходимый процент майнеров относительно своего шарда, т.к. при использовании слитного майнинга хэши блоков будут совпадать. Но для гарантии правильности голосования требуется знать процент майнеров блокчейна - корреспондента. Можно потребовать в хэш блока М-чейна записывать идентификатор блокчейна, в этом случае будет достаточно информации для принятия решения: стоит ли начинать голосование или процент майнеров в другом блокчейне недостаточен для кворума.
- Запись в М-чейн параметра, который показывает какой из двух шардов валидирует майнер (допустимы значения: 1-й, 2-й или оба) позволит рассчитывать показатель - процент перекрытия платежного канала майнерами, что позволит своевременно информировать пользователей о его надежности. Мы не можем проконтролировать равномерность распределения честных майнеров во всех блокчейнах. Но зато можно точно сказать, что если процент перекрытия более **60%**, то как минимум 10% честных майнеров есть в обеих блокчейнах (расчет велся так - максимум 50% злоумышленных майнеров и все они находятся в меньшем блокчейне, значит для их блокировки нужно чтобы там было еще 10% честных майнеров из оставшихся, а так как оставшиеся и есть честные, то условие выполнено).
- Так как процент перекрытия и процент голосов - влияют только на платежный канал, а так как он фактически является даппом с собственными токенами, то можно передавать все эти параметры ему для принятия решений.
- Возможно написания таких сценариев Даппов, трансферы транзакций в которых контролируются создателем дапп, т.е. ноды создателя выполняют верификацию и в случае ложной транзакции запрещают перевод средств. Это возможно за счет того что обычная кросс-транзакция требует время T1+T2 блоков, в тоже время как специальная блокирующая транзакция будет

занимать более короткое время для исполнения, т.к. она подписана владельцем дапп и ей не требуется время на голосование.

Порядок создания сети

Каждая нода в своем протоколе рукопожатия указывает собственные параметры, в которых входит название шарда и его хеш, а также список платежных каналов (М-чейнов). Ноды соединяются с друг другом, если у них совпал хоть один из этих параметров: шард или платежный канал.

Согласно степени похожести адреса определяется номер слота (ранее это называлось уровнем) для соединения нод между собой.
При этом если слот не занят - то всегда устанавливается новое соединение.
Если слот занят то он заменяется на новое значение, только если приоритет новой ноды выше (например когда новая это такой же шард как и у нас, а предыдущее значение слота это соединение с нодой из другого шарда).

Алгоритм:

1. Заполняются значения для расчета приоритета:
    - Ранг ноды, если нода из своего шарда, то значение 2, иначе 1
    - Скоринг - логарифм числа успешных обменов
    - Тайминг - среднее время всех выполняемых обменов (макс значение 1000)

2. Выполняется вычисление по формула (в виде конкатенации):

$$\text{Приоритет} = \text{Ранг} \mid \text{Скоринг} \mid (1000\text{-Тайминг})$$

Чем выше число, тем лучше приоритет.

Обмен транзакциями осуществляется по стандартному фазовому (волновому) алгоритму.

Открытие слотов обмена

Открытие Middle-чейн это специальная процедура, которая доступна разработчику шарда. Возможно более одного чейна - фактически такие чейны это каналы обмена транзакциями. При открытии заполняются параметры:

- Хэш генезис блока М-цепи
- Номер блока текущего шарда, с которого будет начинаться исполнение кросс-транзакций
- Описание

Процедура открытия выполняется на каждом шарде.

Каждая нода начинает майнить - загружать цепочки/валидировать столько М-чейнов, сколько у нее прописано.

Системные операции (необходимые на этапе отладки системы):

1. Поддержка М-цепи (добавление слота)
2. Остановка майнинга М-чейна
3. Продолжение майнинга М-чейна
4. Приостановка приема кросс-Тх
5. Продолжение приема кросс-Тх

Операции записываются в блок через спец. транзакцию (кроме операций 4-5, которые возможно делать через сетевые константы).
Отдельная операция - создание М-цепи, выполняется программистом.

Ссылки:
Теория тера-шардинга: https://terafoundation.org/files/TeraSharding-RUS.pdf