Теория TEPA-шардинга

Yuriy Ivanov (Vtools)
29 июня 2019
progr76@gmail.com
(ver: 0.01)

upd 01.09.2020: детали имплементации устарели

Абстрактно

Понятие блокчейна как философии децентрализованной передачи ценностей глубоко впиталось в общество и в нем появилась потребность создания такой глобальной сети, которая полностью децентрализована и не имеет проблем с масштабируемостью.

На основе нового протокола шардинга можно создать сеть с миллионами нод и общей производительностью измеряемой миллионами транзакций в секунду. Основной принцип: в сети создается неограниченное количество равноправных блокчейнов, объединенных с друг другом через общий хеш сети. Блокчейны коммуницируют с друг другом напрямую через кросс-шардинговые транзакции. Так как в сети нет главного чейна через который осуществляются такие транзакции, то и нет узкого места, что позволяет обеспечить практически бесконечную масштабируемость. Безопасность сети осуществляется внешним контуром легкого блокчейна, он состоит только из заголовков общих хешей. Майнеры сети выполняют работу по подбору такого общего хеша сети и занимаются валидацией дочерних блокчейнов.

Введение

Обеспечить максимальную децентрализацию в виде практически неограниченного количества блок-продюсеров возможно на консенсусе PoW. Но простое разбиение нод сети на шарды в виде отдельных блокчейнов хоть и приводит к кратному росту общей производительности, но также приводит к кратной потери безопасности. Становится проще провести атаку 51% на каждый блокчейн в отдельности. Действительно если мы всю сеть разбили на 100 равных по мощности майнинга шардов, то для атаки на отдельный блокчейн достаточно 0,51% мощности майнинг-оборудования всей сети. Чтобы предотвратить такую угрозу можно применить совместный (merged) майнинг. В этом случае майнеры рассчитывают только общий хеш сети, сложность хеша остается такой же и таким образом безопасность сети не ухудшается. Но возникает проблема как правильно организовать валидацию шардов, т.к. ресурсы одной ноды ограничены (для гарантии децентрализованности майнинга будем исходить из того что одна нода может валидировать не более одного шарда).
Центральная идея решения этой проблемы это использование социального аспекта майнеров - использование “теории шести рукопожатий”. Майнеры могут иметь несколько нод, майнеры могут иметь связи (друзей которым доверяют).

Анализ механики шардинга

На практике возникает простой вопрос - что делать обычному рядовому пользователю, который скачал программу майнинга, у которого только один компьютер и соответственно ресурсов для валидации хватает только на один шард?

В консенсусе PoW существует интересная зависимость между безопасностью сети и временем. Чем больше времени затрачиваем на создание хеша, тем больше безопасность сети и наоборот. Это что-то вроде закона, который нельзя обойти, но который нужно использовать. Отсюда очевидный вывод: если нет достаточного количества майнеров поддерживающий валидацию шарда, то значит этот шард будет реже по времени иметь подтверждающий блок. Шарды которые имеют достаточно редкое количество подтверждений будут менее предпочтительны для пользователей, это будет отражаться на их рыночной капитализации (т.к. каждый шард это самостоятельный блокчейн со своей криптовалютой).

Выглядеть это будет так: майнер указывает связь между своими нодами и шардами, которые эти ноды валидирует. При майнинге в меркл-дерево блока победителя включаются **только** хеши провалидированных шардов. Пользователи будут считать блок шарда подтвержденным только если он включен в общий хеш сети.
Таким образом у майнера у которого только одна нода будет провалидированным только один шард, а у майнера у которого много нод - практически все шарды. Т.к. вероятность нахождения блоков будет у майнера, у которого больше ресурсов (нод), то:

- Если в сети будут превалировать ноды профессиональных майнеров у которых много нод, то в сети большинство блоков будут иметь все провалидированные шарды.
- Если количество нод (с условно равными мощностями) будет равно, то в среднем все шарды будут провалидированы через один блок.
- Если будет больше одиночных майнеров, то вероятность валидации шарда будет находиться в прямой зависимости от его популярности (и в обратной от общего количества шардов).

Таким образом:

- Новый майнер с единичной нодой сможет достаточно просто участвовать в майнинге, при этом он мотивирован для валидации других шардов в любой момент когда пожелает нужным.
- Для введения нового шарда достаточно чтобы его провалидировал хотя бы один майнер. Время подтверждения блоков шардов зависит от популярности и рыночной эффективности шарда.

Все это вместе обеспечивает плавный и органичный механизм образования и поддержания шард, который будет регулироваться рыночными методами - путем изменения курса встроенной криптовалюты шарда.

Техническая реализация

Термины

Сеть - под этим термином понимается виртуальная (релейная) сеть в виде связи нод (компьютеров) с друг другом в определенной последовательности, сгруппированных по разным шардам (блокчейнам) и работающих под одним протоколом передачи данных.
Шард - в данной версии документа под шардом понимается отдельный блокчейн, особенностью которого является то что его валидацию выполняют майнеры общего блокчейна.

Монеты

Каждый шард имеет собственную встроенную монету (криптовалюту), кросс-шардинговые транзакции - это фактически кросс-шардинговые свопы. Нет глобальной криптовалюты. Обмен криптовалют из разных шард возможно только при

создании смарт-контрактов в виде децентрализованных бирж, курс в которых зависит от спроса и предложения.
Для хождения единой криптовалюты, например Теры, каждый шард может имплементировать платежные каналы в виде смарт-контрактов, который меняет один токен Теры из одного шарда на другой токен Теры в другом шарде (ид токена зависит от самого смарт-контакта, что он считает Терой). Общий баланс монет и токенов внутри шарда остается постоянным.
Такой подход обеспечивают финансовую безопасность для пользователей шардов, если предположить что один шард скомпрометирован, то остальные шарды не пострадают.

Нода

Нода это основная единица сети. Все ноды равноправны. Они объединяются с друг другом по определенным правилам и образуют так называемую релейную сеть, которая позволяет оптимально обмениваться информацией в сети. Ноды не соединены напрямую с друг другом, каждая нода имеет ограниченное число связей - оно пропорционально логарифму количества нод во всей сети.

Функции ноды как участника сети:

1. Общая информацией сети:
    a. Расчет (майнинг) и обмен данными общего хеша сети
    b. Синхронизация времени
    c. Синхронизация версий кода
2. Валидация и обмен данными шарда (блокчейна). Стандартно нода может валидировать только один шард.
3. Валидация и обмен данными кросс-шардинговых транзакционных буферов (максимальное число ограничено)

Правило создания сети

Для того чтобы эффективно передавать как общую так и внутиршардинговую информацию внутри сети создаются несколько контуров обмена. Такие контуры имеют вид многомерной решетки. Так как работа каждой ноды в сети не гарантирована, то соединения имеют динамическую природу - они постоянно поддерживаются путем соединения с другими нодами и имеют резерв.

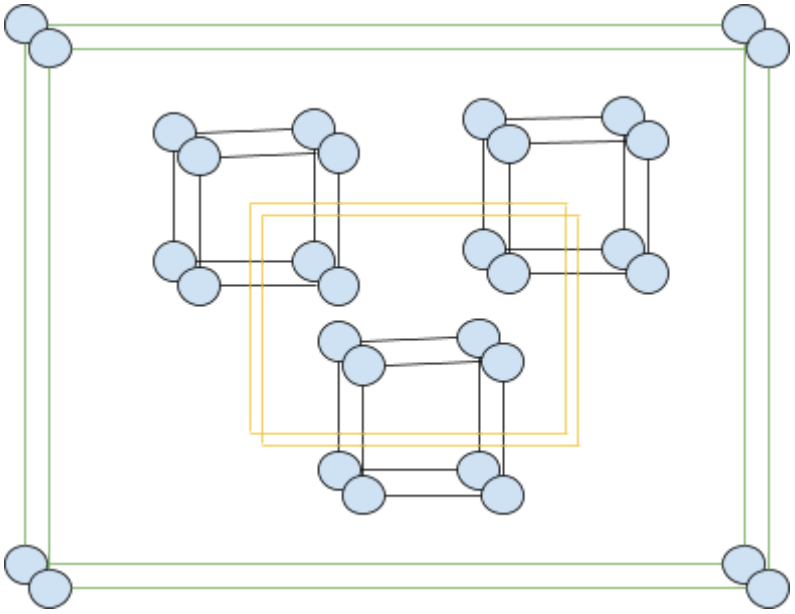
Динамическая структура в виде многомерной регулярной решетки строится на основе похожести идентификаторов нод - в зависимости от степени такого подобия определяется его номер измерения в многомерном кубе, этот номер далее будем называть уровнем обмена информацией. Так как много нод могут претендовать на один и тот же уровень, то существует следующий порядок:

1. На каждом уровне в порядке приоритета сначала добавляются ноды текущего шарда для обмена транзакциями шарда.
2. Параллельно на каждом уровне добавляются ноды других шардов для обмена буферами кросс-шардинговых транзакций.

3. Если уровень пуст (или нод недостаточно), то добавляются ноды из общего списка для обмена общей информацией сети.

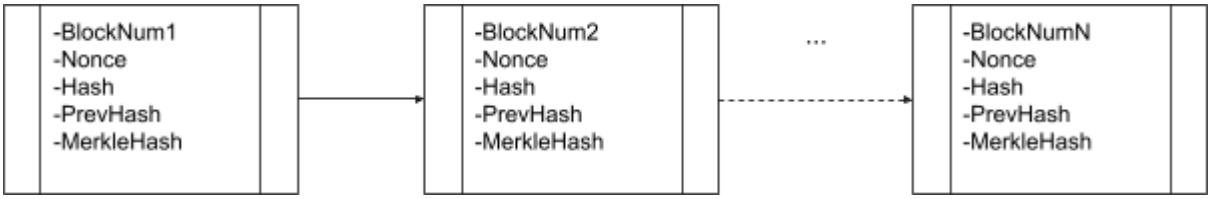
Общая информация содержится во всех нодах, поэтому в правилах указано сначала заполнение уровней нодами с уникальной информацией, а затем с более общей.

Таким образом ноды будут соединены во внешний многомерный куб для обмена общей информацией сети и внутренние кубы - для обмена информацией внутри каждого шарда.



Структура общих блоков сети (**устарело**)

Сеть представляет собой блокчейн блокчейнов. Верхнеуровневый блокчейн состоит только из хешей шардов. Его цель цементирование состояний хешей шардов - невозможность отката блоков назад. Построение этого блокчейна классическое: хеши шардов сгруппированы в блоки, майнеры должны вычислить хеш нового блока который зависит от предыдущего хеша блока (PrevHash), числа Nonce и хешей входящих в него шардов (MerkleHash).

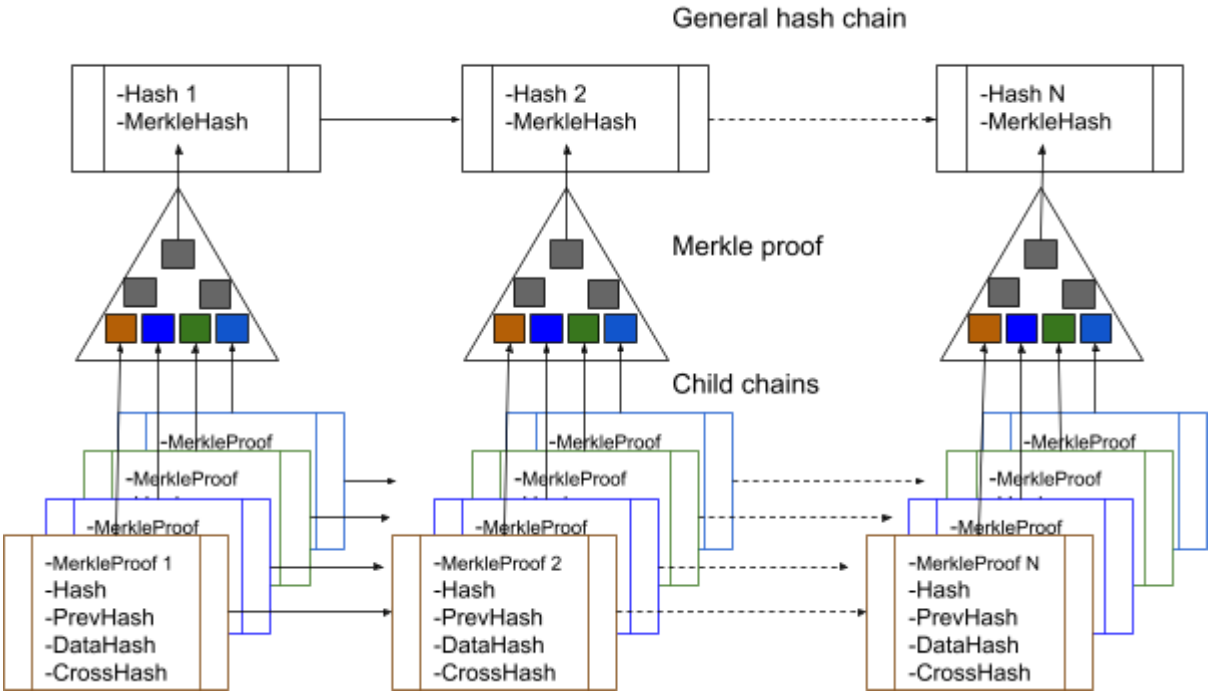


Заголовок общего блока занимает 128 байт, размер за год составит 4 Гбайта.

Майнеры нашедшие общий блок должны разослать в те шарды, которые они поддерживают доказательство Меркла - информацию по связи хеша шарда с общим

хешем сети. Технически это просто реализуется за счет того, что у майнера есть точный список/дерево шардов, которые он поддерживает.

Схема соединения дочерних блокчейнов с общим (**устарело)**



Скорость формирования блоков

Консенсус базируется на алгоритме PoW, но так как блоки формируются раз в секунду, то не применяется понятие *target*, которое используется в классическом блокчейне Биткоин и его копий. Вместо этого работа по поиску подходящего хеша выполняется ровно одну секунду, хеш с наибольшей сложностью отправляется в сеть. В сети при поиске хеша-лидера происходит сравнение хешей между собой и отбирается с наименьшим количеством слева нулей т.е. численно меньший.

Горизонтальное масштабирование при совместном майнинге

При большом количестве шардов (например тысяч и сотни тысяч) валидация всех шардов одним обычным майнером практически невозможна - одна нода может провалидировать только один шард, а число нод у обычного майнера ограничено. Горизонтальное масштабирование позволяет увеличить эти возможности следующим образом:

1. Первый способ - создать кластер из собственных нод. Для этого в настройках каждой ноды задается принадлежность к одному кластеру путем ввода общего секретного пароля. В этом варианте число поддерживаемых шардов ограничено числом собственных нод майнера.

2. Второй способ - включение внешнего кластера нод, которому майнер доверяет (например своего друга) в дерево доверительных кластеров. Это делается путем добавления публичного ключа внешнего кластера и указания уровня иерархии доверия (можно ли доверять в свою очередь его дочерним узлам). При таком варианте число поддерживаемых шардов может многократно превышать число собственных нод майнера. Причем можно указывать степень

Майнер может комбинировать оба варианта для достижения максимальной надежности и прибыли.

Вариант стратегии пользователя:

1. добавить свои ноды (5 штук по одному шарду)
2. добавить кластер нод друзей (2 кластера с одним уровнем иерархии, т.е. только ноды друзей)
3. добавить кластер из 100 шардов известной компании типа VISA/MasterCard

Мотивация майнера

Мотивация майнера - это получение наград в каждом шарде, таким образом он стимулирован чтобы провалидировать и включить в состав заголовка хотя бы один шард. Алгоритмом допускается возможность включения ноль шардов в этом случае хеш шардов (ShardsHash) имеет нулевое значение.
Для того чтобы максимизировать прибыль майнер должен стремиться провалидировать как можно больше шардов, т.к. награды он получает независимо в каждом из них. Так как нода может валидировать только один шард, то майнер может запускать несколько нод с настройкой на валидацию разных шард, а чтобы в блок включать информацию по нескольким шардам он может объединить свои ноды в доверенный кластер.
Оптимальная стратегия майнера будет заключаться поиск кластеров, которым он может доверять для включения их в свой майнинг лист. В идеале он будет стремиться к 100% охвату шард сети Тера.

Алгоритм выбора цепочки

1. При начальном старте полная нода, а также легкий клиент загружает заголовки цепочек общей сети, определяет цепь с максимальной суммой сложности хеша и далее считает ее главной.
2. После этого ищутся ноды требуемого шарда и закачиваются заголовки блоков шарда. По ним определяется цепь требуемого шарда с максимальной суммой сложности хеша (таким образом идет защита от форка). Сложность берется из общих хешей сети и складываются только те блоки, в которых хеш блока был включен в общий заголовок блока сети (проверяется через меркл дерево)

Кросс-шардинг

Кросс-шардинговый буфер

Для обеспечения кросс-шардинговых транзакций в каждой ноде существует специальный буфер, который представляет собой массив элементов высотой 1000 блоков. Для возможности быстрой валидации от этого массива рассчитывается хеш (CrossHash), который записывается в заголовок блока шарда. Элементы массива представляют собой хеши успешных кросс-шардинговых транзакций. Таким образом внешний шард может быстро проверить завершилась ли с успехом кросс-шардинговая транзакция в другом шарде. Если транзакция появилась одновременно во всех требуемых буферах, то она фиксируется как успешная.

Буфер двух шард, жирным текстом выделены совпадающие транзакции:

Shard A

	12017:1323DEF123449394324 12017:**A342423F12344432489** 12017:**ABCDEF185476345345** 12015:**2ABCDEF95348348344** 12015:**1AFDDE640963545417** 12015:**FACDEF893856769620** 12015:DDEF08937783444CC5 12015:**CCDEF1234434923449** 12014:**DFCD8237832F833331** 12013:**EE98237423982390619** 12013:**2383423534534347609** 12013:**2398445EF1234489543** 12013:**234E212F12313123255** 12013:**F32842F233483464544** 12013:**F89BA5454EF4353454** 12013:1A42002234493938DE 12012:**43433441242349DE38** 12012:**F2CDEF131233853DE3** 12012:**E45345EF45534545789** 12012:**A4F8334A5345436791** 12011:3B4DEF120328945812 12011:**1BC2EF123449393889**

Shard B

	12017:**A342423F12344432489** 12017:**ABCDEF185476345345** 12015:**2ABCDEF95348348344** 12015:**1AFDDE640963545417** 12015:**FACDEF893856769620** 12015:**CCDEF1234434923449** 12014:**DFCD8237832F833331** 12013:**EE98237423982390619** 12013:**2383423534534347609** 12013:**2398445EF1234489543** 12013:**234E212F12313123255** 12013:**F32842F233483464544** 12013:**F89BA5454EF4353454** 12012:**43433441242349DE38** 12012:**F2CDEF131233853DE3** 12012:**E45345EF45534545789** 12012:**A4F8334A5345436791** 12011:8543985AFE453534532 12011:**1BC2EF123449393889** 12010:ED89534098356701001 12010:F19234AE765923904C 12010:C934ED0935456789A7

Кросс-шардинговые транзакции

Для передачи ценностей между блокчейнами служат транзакции, которые являются вызовами функций смарт-контрактов с признаком кросс-шардинга. Такая транзакция вызывает функцию сразу в двух шардах.
Для обеспечения атомарности вызова сразу в двух шардах существует специальный протокол, а каждая функция в смарт-контрактах имеет дополнительный параметр - Флаг вызова, который системно заполняется в зависимости от ситуации (0 - начальный вызов, 1- транзакция успешно выполнена в обоих шардах, -1 - транзакция отменена).

Порядок работы таков:

1. Формируется кросс-шардинговая транзакция и отправляется сразу в два шарда
2. В каждом шарде выполняется вызов функции с параметром флага = 0. В этом режиме смарт-контракт должен зарезервировать передаваемые ценности.
3. В случае успеха выполнения хеш от транзакции отправляется в буфер кросс-шардинговых транзакций. Успехом выполнения считается если в коде не было вызвано исключение.
4. Через 100 блоков в каждом шарде выполняется проверка хеша в обоих буферах (своего и корреспондента), если транзакция присутствует там и там, то выполняется повторный вызов функции с флагом 1. По этому флагу в коде должно выполниться снятие резерва и передача ценности.
5. Если хеша транзакции нет в обоих буферах, то выполняется вызов функции с флагом -1, но только в том блокчейне где хеш присутствует в буфере. По этому флагу должно выполнится только снятие резерва (т.е. возвращение в блокчейна в первоначальное значение которое было до транзакции).

Варианты создания кросс-шардинговых связей

Из-за того что ресурсы одной ноды ограничены количество шардов для обмена в один и тот же момент времени также ограничены фиксированным значением.
Как ноде определить с какими шардами нужно выстраивать обмен данными?
Для этого можно применить такие правила:

1. Динамическое связывание. Нода следит за составом кросс-шардинговых транзакций, если встретилась транзакция с шардом с которым нет связи, то такая связь создается. При создании связи учитывается приоритет как обмена, так и принадлежности к доверительному кластеру.
2. Список кросс-шардов зависит от депозита
3. Список кросс-шардов зависит от голосования майнеров

Работа пользователей из кошелька с разными шардами.

Пользователь будет иметь один кошелек для работы со всеми шардами.
При создании нового счета помимо прочего он вводит название шарда, которое всегда совпадает с названием криптовалюты.
Если он хочет отправить средства в другой шард он перед номером счета получателя пишет название шарда и двоеточие. Например BNB:198678. Это означает что кошелек должен автоматически отправить средства на специальный смарт-контракт, который является шлюзом с шардом BNB.

Выводы

Возможно достижение бесконечной масштабируемости путем опционального использования доверия при валидации шард. Но в отличии от других блокчейнов такая доверительная система не имеет проблем с децентрализацией, т.к. по умолчанию она отключена, а если майнер задал группу доверия и при этом ошибся, то в целом сеть от этого не пострадает, т.к. другие майнеры имеют отличные от него группы доверий.