Plasma: масштабируемые автономные смарт-контракты

Джозеф Пун
joseph@lightning.network

Виталик Бутерин
vitalik@ethereum.org

11 августа, 2017

РАБОЧИЙ ВАРИАНТ
https://plasma.io/

Выдержка

Plasma – это предлагаемая платформа для стимулируемого и утверждённого выполнения смарт-контрактов, масштабируемых до значительного количества обновления состояний в секунду (потенциально – миллиардов), что позволит блокчейну представлять огромное количество децентрализованных финансовых приложений по всему миру. Такие смарт-контракты стимулируются с целью продолжения автономной работы в рамках существующих комиссионных сборов за сетевые транзакции, которые в конечном счёте базируются на нижестоящих блокчейнах (напр. Эфириум) для проведения транзакционных переходов состояний.

Мы предлагаем метод масштабируемых децентрализованных автономных приложений (*дапсы*) не только для обработки финансовой деятельности, но и для того, чтобы придумать новые экономические стимулы для постоянных служб передачи данных, которые могли бы послужить альтернативой традиционным серверным фермам.

Архитектура Plasma состоит из двух главных блоков: все блокчейн-вычисления будут перемещены в набор функций MapReduce, а поверх существующих блокчейнов будет использоваться опциональный метод Proof-of-Stake привязки токенов с учетом того, что принципы консенсуса Накамото препятствуют удержанию блока.

Эта структура достигается путём составления смарт-контрактов в главном блокчейне с использованием доказательств обмана, таким образом, что переходы состояний могут быть выполнены на основе родительского блокчейна. Блокчейны выстраиваются в древовидной иерархию. Каждая цепочка блоков является отдельной ветвью блокчейна, в которой вычисления осуществляются в MapReduce и передаются с помощью доказательств древовидного хеширования Merkle.

Внося записи журнала операций в дочерний блокчейн, утверждаемый родительской цепочкой, можно достичь невероятного масштабирования с минимальными обязательствами (учитывая доступность и правильность корневого блокчейна)

Самая главная сложность в глобальном управлении неглобальной информацией заключается в доступности информации, а также атаках, удерживающих блоки. В этом случае у Plasma есть смягчающие факторы для решения таких проблем – она позволяет некорректным цепочкам покидать блоки, в то же время создавая механизмы для стимуляции и управления непрерывно продолжающегося выполнения операций.

Обязательства компилируются по принципу древовидного хеширования перед периодической отправкой в корневой блокчейн (как в случае с Эфириум) в стабильном состоянии. Это позволяет проводить невероятно масштабируемые, а также малозатратные транзакции и вычисление. Plasma представляет постоянно функционирующие дапсы на высоком уровне

1 Масштабируемые многопользовательские вычисления

При использовании блокчейнов существовало лишь одно решение, при котором управление корректностью операций требовало личного подтверждения цепочки каждым участником. Для принятия нового блока пользователю было необходимо полностью проверить блок для того, чтобы убедиться в его корректности. Многие иные попытки масштабировать транзакционную ёмкость блокчейнов (напр. Lightning Network) требовали временных обязательств для создания доверительной гарантии (соглашения об подтверждении), так чтобы участники блокчейна имели бы время на обсуждение подтверждённой информации и далее имели бы возможность утвердить состояние. Эта структура подтверждения/критического рассмотрения позволяет подтвердить корректность определённого состояния, в случае же если значение неверно, существует период подтверждения, во время которого другой наблюдатель может предоставить своё доказательство в течении определённого согласованного времени. В случае, если в системе произошёл сбой или была обнаружена попытка мошенничества, блокчейн может непосредственно удалить подозреваемого участника. Это создаёт механизм для участников, побуждающий их утверждению лишь в случае обнаружения неверного состояния. Имея в своём распоряжении такую структуру, заинтересованные участники могут передавать экспериментальные данные не заинтересованным участникам в корневом блокчейне (как в Эфириуме[2][3])

Эта структура может быть использована не только для проведения платежей, но и может быть расширена до выполнения непосредственных вычислений, таким образом превращая блокчейн в оценочную инстанцию для всех контрактов. Однако, при таком раскладе все стороны будут являться участниками, подтверждающими вычисления. В Lightning Network, к примеру, структурафункционирует таким образом, что пользователи могут утверждать обязательства с вычислительными состояниями контракта (напр. с заранее подтверждённым деревом с транзакциями условного состояния, подписанными несколькими лицами)

Эти структуры позволяют выполнять крупномасштабные высокопроизводительные расчёты, однако существует ряд проблем, которые требуют суммирования многих внешних состояний (напр. всецелое суммирование систем/рынков, вычисление больших объёмов информации общего пользования/неполной информации, большое количество участников). Эта форма обязательства к многостороннему состоянию вне цепочки (“каналы состояния”) требует от участников полного подтверждения вычислений, или иначе в самом вычислении накапливается значительное количество обязательств, даже в одноступенчатых сделках. В дополнение к этому, существует понимание “ступеней” , при которых исполнительный путь должен быть полностью развёрнут перед началом контракта, что даёт участникам возможность выходить и инициировать дорогостоящие вычисления в цепочке (поскольку невозможно доказать, какая из сторон служит препятствием).

Вместо этого мы стремимся разработать иную систему, внутри которой вычисления могут осуществляться за пределами блокчейнов, но в конце концов инициироваться внутри цепочек, имея возможность масштабироваться до миллиардов операций в секунду с минимальным обновлением внутри цепочки. Эти обновления состояния происходят в автономном наборе proof-of-stake валидаторов, стимулируемых к правильному поведению, которое обеспечивается доказательством обмана, позволяющих проводить расчёты без легко творимых препятствий вычислительной службе со стороны единичных пользователей. Необходимо, чтобы система могла бы свести к минимуму проблему доступности информации (т.е. удержание блоков), сокращая обновления состояния в корневом блокчейне, которые требуются в случае появления византийских игроков для предотвращения транзакций со сниженным риском в корневой цепочке, а также создание механизма

для приведения в исполнение состояний изменения.

Так же, как и Lightning Network, Plasma – это серия контрактов, выполняемых поверх существующего блокчейна, обеспечивая исполнение, в то же время сохраняя возможность для игроков удерживать средства.

2 Plasma

Plasma – это способ выполнения масштабируемых вычислений в блокчейне со структурой, позволяющей создавать экономические стимулы для автономного и непрерывного управления цепочкой без активного перехода состояния со стороны создателя контракта.

Вдобавок к этому получается возможным добиться значительной масштабируемости путём минимизации средств платежа по контракту до одного бита в битовой карте, так, что одна транзакция и подпись представляет платёж, связанный со многими другими участниками. Мы объединили эту систему со структурой MapReduce для возможности создания масштабируемых вычислений, управляемых обеспеченными смарт-контрактами.

Эта структура позволяет игрокам удерживать средства во внешних источниках и проводить вычисления по контрактам самостоятельно, как майнер, однако Plasma исполняется поверх существующего блокчейна, таким образом, что игроку нет необходимости создавать транзакции в нижестоящей цепочке для каждого изменения состояния (включая записи журнала операций от новых пользователей). Это позволяет сократить объём информации в цепочке до минимума для объединённых изменений состояния.

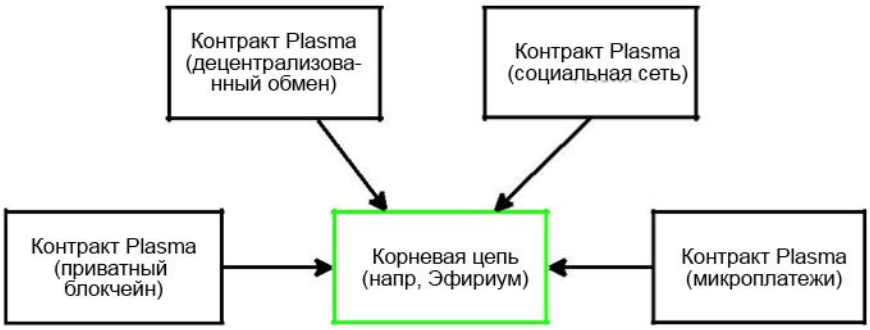

Таблица 1: Кто угодно может создать индивидуальную цепочку Plasma для масштабирования смарт-контрактов для различных условий применения. Plasma – это серия смарт-контрактов, позволяющая многим блокчейнам существовать внутри корневого блокчейна. Корневой блокчейн утверждает состояние в цепочке Plasma. Корневая цепочка – это программа инициации вычислений по всему миру, но она вычисляется или удаляется лишь в случае наличия доказательства обмана. Многие блокчейны Plasma могут сосуществовать со своей собственной бизнес-логикой и условиями смарт-контрактов. Внутри Эфириума, Plasma бы состояла из смарт-контрактов по методу освоенного объёма, которые бы исполнялись непосредственно в Эфириум, но лишь с обработкой крохотных обязательств, которые могут представлять огромный объём вычислений и записей журнала пользователей в случае с невизантийскими игроками.

Plasma состоит из пяти ключевых компонентов: стимулирующего слоя для непрерывной обработки контрактов экономически эффективным способом, структуры организации дочерних цепочек в древовидную структуру для снижения затрат и неттинга транзакций, вычислительная структура MapReduce для создания подтверждений обмана переходов состояния внутри занятых цепочек для совместимости с древовидной структурой, а также для поддержания высокой масштабируемости переходов состояния, далее это механизм консенсуса, который всецело зависит от корневого блокчейна, подобный результатам стимуляторов консенсуса Накамото и в конце концов UTXO-битмаповые структуры обязательств для обеспечения точных переходов состояния на корневом блокчейне с сокращением затрат на массовый выход. Допущение выходов при недоступности информации или иного поведения византийского типа – одна из ключевых особенностей функционирования архитектуры Plasma.

2.1 Блокчейн Plasma или извлечённые многосторонние каналы

Мы предлагаем метод, при котором многосторонние оффчейн каналы могут удерживать состояние в чьих-либо интересах. Мы называем эту структуру блокчейном Plasma. Для средств удерживаемых в блокчейне Plasma, структура позволяет вносить и снимать средства с цепочки Plasma, в которой переходы состояний инициируются доказательством обмана. Это позволяет осуществлять состояние и взаимозаменяемость финансовых инструментов, поскольку пользователю будут доступны внос и снятие средств с учётом того, что блок Plasma будет совпадать со средствами, удерживаемыми в корневой цепочке (Plasma не создана для того, чтобы быть совместимой с частичным банковским резервированием)

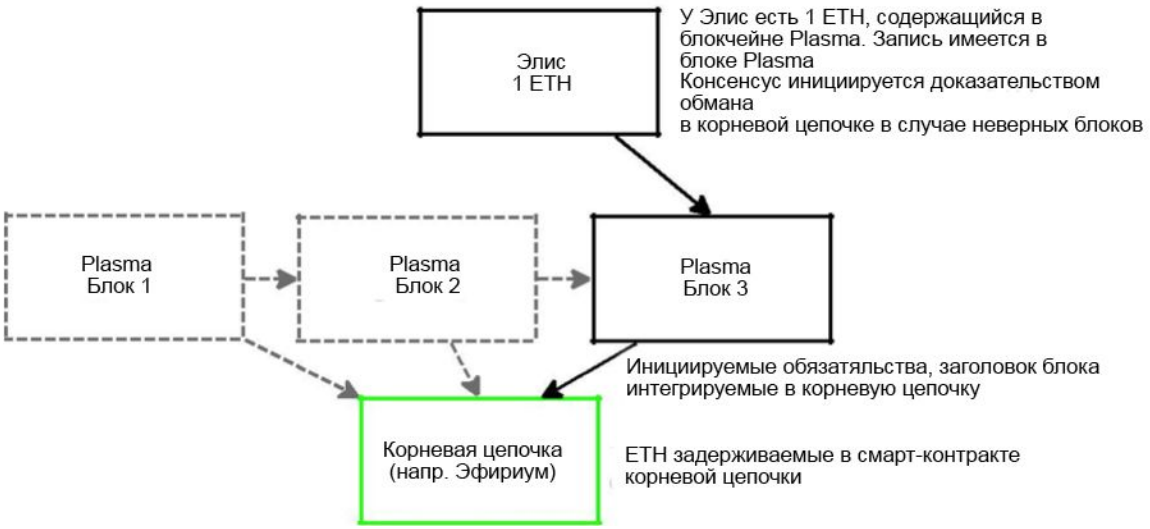

Таблица 2: Блокчейны Plasma – это цепочка внутри определённого блокчейна. Система инициируется консолидированными доказательствами обмана. Блокчейн Plasma не раскрывает содержимого блокчейна корневой цепочки (к примеру Эфириума). Вместо этого, хэши заголовка блока передаются в корневую цепочку и, если в корневую цепочку также передаётся доказательство обмана, то блок откатывается обратно, а его создатель удаляется. Это очень эффективно, поскольку многие изменения состояния представлены лишь одним хэшем (плюс небольшим количеством сопутствующей информации). Такое обновление может представлять

балансы, не представленные в корневом блокчейне (У Элис нет журнала баланса в корневой цепочке, её журнал находится в цепочке Plasma, а баланс в корневой цепочке представляет собой смарт-контракт, инициирующий саму цепочку Plasma). Серые элементы – это старые блоки, чёрные – новейшие блоки: которые были распространены и внедрены в корневую цепочку.

Невероятно большой объём транзакций может проводиться через эту цепочку Plasma с минимальным количеством информации, проходящим через корневой блокчейн. Любой участник может переводить средства кому угодно, включая переводы участникам, находящимся за пределами существующего списка участников. Эти переводы могут добавлять или изымать (с учётом временных задержек и доказательств) средства в нативный коин/токен корневого блокчейна.

Plasma позволяет пользователю (или сети участников в сети proof-of-stake) управлять блокчейном без полного непрерывного журнала записей в корневом блокчейне и без предоставления доверительных фондов ответственного хранения третьей стороне. В худшем случае средства блокируются и срочная стоимость опциона теряется вместе с массовым выходом из блокчейна.

Мы создали серию доказательств обмана в качестве смарт-контрактов на корневом блокчейне, которые инициируют состояние в этом канале, так что любые попытки мошенничества или невизантийского поведения будут пресечены на корню.

Эти доказательства обмана инициируют интерактивный протокол снятия средств. Подобно Lightning Network, снятие средств требует времени на выход. Мы создали интерактивную игру, в которой выходящая сторона подтверждает битовую карту журнала вывода участников, выстроенных по модели UTXO, которая запрашивает снятие. Кто угодно в сети может предоставить альтернативное “консолидированное” доказательство, которое подтверждает были ли потрачены средства или нет. В случае, если информация на выходе не совпадает, кто угодно в сети может подтвердить мошенническое поведение и урезать обязательства, чтобы откатить подтверждение. После определённого периода времени второй консолидированный круг всё же позволит произвести снятие средств, поскольку это будет обязательство в состоянии “до” установки временной отметки. Это позволяет осуществляться массовому снятию средств, таким образом облегчая полный выход из некорректной цепочки Plasma. В координируемых событиях массового снятия, участники могут выйти не более чем с двумя битами объёма блока, поглощаемого на родительском блокчейне (т.е. на корневом Эфириуме внутри цепочки при худшем сценарии)

В случае, если блок переносит атаку, участники могут быстро и дёшево совершить массовый выход со значительным сокращением затрат по сравнению с иными ранее использовавшимися оффчейн предложениями. К тому же это не объединяет доверительные фонды с нод-валидаторами

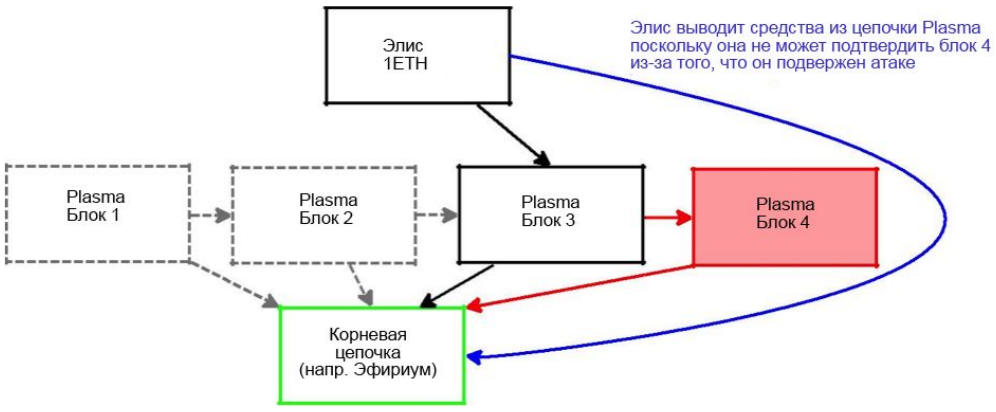

Таблица 3: Выход средств в случае удержания блока. Красный блок (блок 4) – это удерживаемый блок, интегрируемый в корневую цепочку, однако Элис не может получить блок Plasma 4. Она выходит путём передачи доказательства средств в корневом блокчейне, а её выход обрабатывается после задержки, позволяя иметь место обсуждению.

Похоже на то, как закрытие Lightning – это интерактивный механизм между двумя участниками, запускающий инициируемые бесконечные платежи друг между другом, есть возможность запуска интерактивного механизма между участниками. Главное отличие в том, что всем участникам нет необходимости быть всё время онлайн, для того чтобы обновлять состояние, участникам так же не нужно сохранять записи входа в корневой блокчейн для того, чтобы подтверждать своё участие (пользователь может внести средства на Plasma без прямого взаимодействия внутри цепочки с минимальной информацией для подтверждения транзакции при организации этих цепей Plasma в древовидном формате.

2.2 Инициируемые блокчейны в блокчейнах

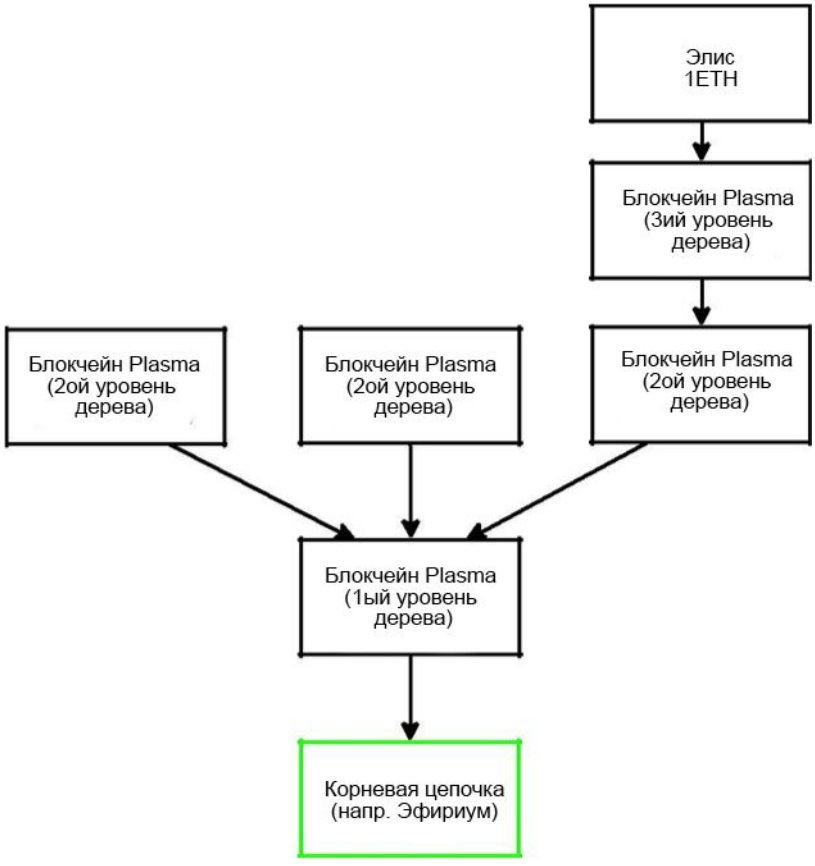

Таблица 4 Plasma составляет дерево из блокчейнов. Блоковые обязательства движутся вниз, а выход можно совершить на любой родительской цепочке, в конце концов интегрировавшись в корневой блокчейн.

Мы создаём механизм подобно судебной системе. В то время как Lightning Network использует оценочную инстанцию для платежей, в конечном счёте инициируемых в корневом блокчейне, мы создаём систему судов более высокой и низкой инстанции для увеличения доступности и снижения затрат на невизантийские состояния. В случае, если в цепь византийского принципа, она может возвращаться к любому из своих родителей (включая корневой блокчейн) для продолжения функционирования или она может выйти в своём текущем подтверждённом состоянии. Вместо инициирования наращиваемого текущего состояния (через аннулирование) мы создаём систему доказательств обмана для инициации балансов и переходов состояния в иерархиях этих цепей.

В итоге, мы можем создать переходы состояния, которые лишь периодически интегрируются в родительские цепочки (которые в свою очередь переходят в корневой блокчейн). Это позволяет добиться невероятного масштабирования вычислений и состояния счетов, поскольку мы можем отправить только необработанные данные родительской (или корневой) цепи в византийских условиях. Траты на восстановление после частичных византийских условий сведены к минимуму, поскольку пользователь может пойти в родительскую цепочку Plasma и инициировать состояние.

Этот дочерний блокчейн исполняется поверх корневого блокчейна (например Эфириума) и с точки зрения корневого блокчейна лишь периодически обнаруживает обязательства с токенам, привязанными к контракту для исполнения правил консенсуса proof-of-stake, а также бизнес-логики блокчейна.

У этого принципа имеются значительные преимущества в увеличении доступности блоков и уменьшении доли для валидации коинов. Однако, поскольку не вся информация распространяется между всеми сторонами (только теми, кто хотел бы подтвердить определённое состояние), стороны отвечают за самостоятельное наблюдение за определённой цепочкой, в которой они сзаинтересованы, чтобы исключить возможность мошенничества, также стороны ответственны за скорый самостоятельный выход из блока, подвергнувшегося атаке.

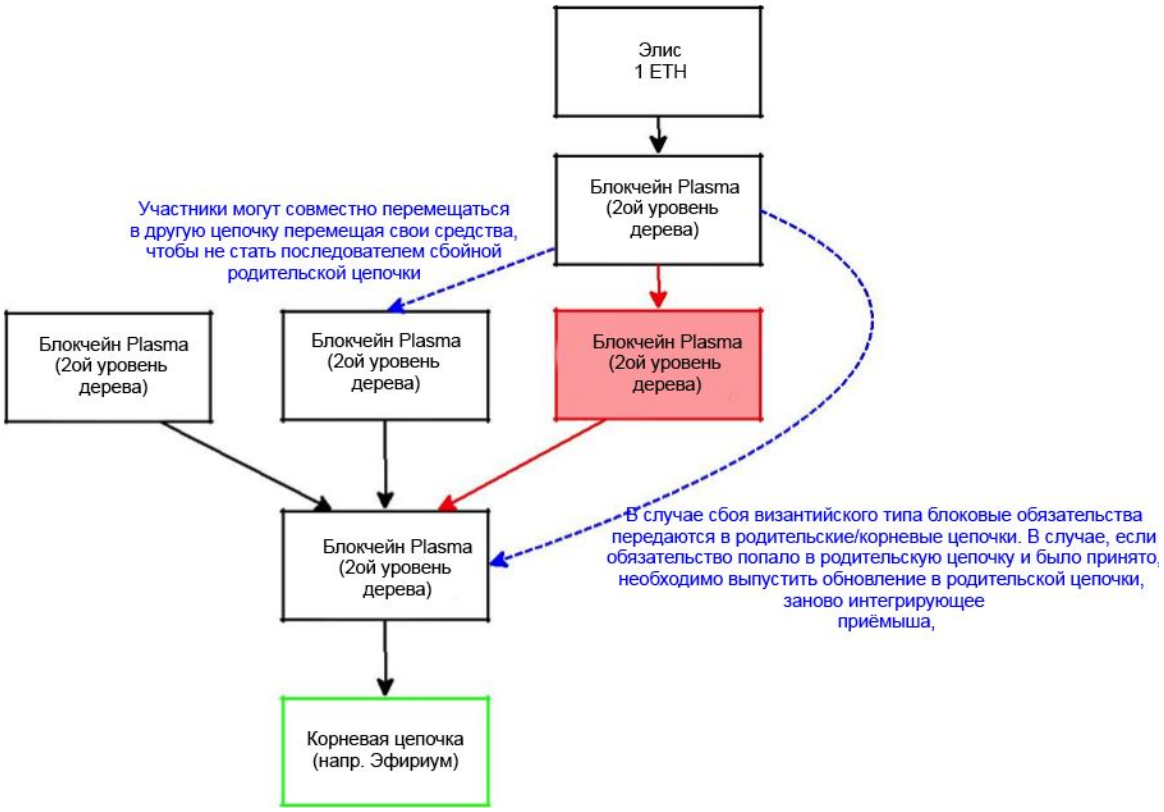

Таблица 5: Доступ через некорректный блокчейн (залитый красным) перемаршрутизован путём передачи обязательств родительской Plasma/корневой цепочке (указана справа пунктирной линией). Участники блокчейна Plasma на 3 уровне дерева совершают массовую миграцию на другую цепочку вместе (указано слева пунктирной линией) после определённого промежутка времени.

Эта конструкция в невизайнтийских окружениях объединяется с деревом состояний блокчейна и обновляет все дочерние Plasma цепочки. Полный набор обновлений по всем цепочкам может быть подтверждён 32-битным хэшем с подписью.

2.3 Plasma Proof-of-Stake (с защитой по методу “подтверждения доли”)

В то время как может быть довольно интересным удерживать средства от имени других с помощью одного единственного валидатора, мы всё же предлагаем метод, при котором одна сторона может инициировать состояние с помощью набора валидаторов, очень часто в структуре proof-of-stake, требующей ETH залог или залог в токене (напр. ERC-20)

Механизмы консенсуса для этой системы proof-of-stake, опять же инициируются во внутриблокчейновом смарт-контракте.

Мы пытаемся создать дубликаты стимуляторов в обход консенсуса Накамото, но с использованием залогов proof-of-stake. Мы верим, что один из более полезных стимулирующих механизмов, созданный, как результат механизма Накамото – это тот, в котором существуют мощные стимуляторы для сведения к минимуму блоков, подвергающихся атакам. Это происходит так, поскольку лидеры выбираются лишь в вероятностном смысле. Лидеры также известны в вероятностном смысле в течение времени (в оригинальной трактовке требовалось 6 подтверждений). Когда пользователь находит блок, он уверен с достаточной долей вероятности, что является лидером, но не имеют в этом прочной уверенности. Чтобы убедиться в своём лидерстве они распространяют свои блоки между всеми участниками в сети, что увеличить свои шансы. Мы верим, что это значительный, если не ключевой вклад в механизм Накамото и достойная попытка продублировать этот стимулятор.

Объединения proof-of-stake могут столкнуться с этой проблемой, если пользователь решит немедленно провести выборы лидера, в этом случае атаки, удерживающие блоки, проводимые более крупными картелями (также описываемые как «проблема доступности информации») становятся более масштабными.

Мы можем смягчить последствия в Plasma Proof-of-Stake, позволяя заинтересованным сторонам публиковаться на корневом блокчейне или родительской цепочке Plasma, которая содержит хэш с обязательствами их нового блока. Валидаторы лишь строят блоки на блоках, которые они полностью подтвердили. Они могут строить блоки на блоках параллельно (для поощрения максимального обмена информацией). Мы создаём стимуляторы для валидаторов для представления последних 100 блоков, которые должны совпадать с соотношением заинтересованных участников (т.е. если пользователь ставит на 3 процента коинов, он должен представлять 3 процента последних 100 блоков), путём выплаты комиссии за транзакцию для точного представления. Нерациональное поведение

участников создаёт лишние расходы, которые затем добавляются в общую кассу в будущем. В каждом блоке существует обязательство, которое включает информацию с последних 100 блоков (с временным значением). Конец корректной цепочки – это цепочка с суммированной массой самых высоких комиссий. После определённого времени блоки завершаются.

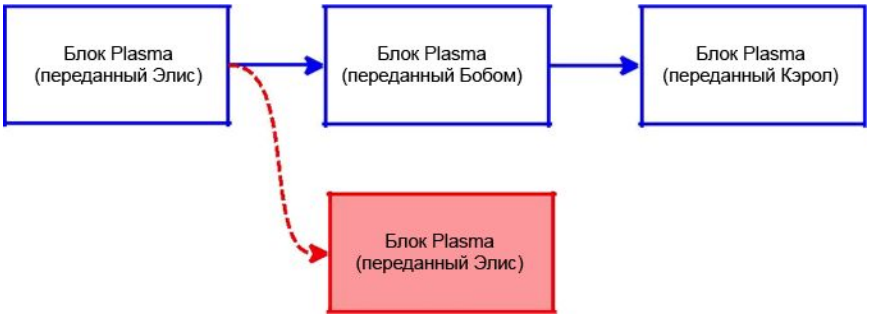

Таблица 6: Представьте себе, что Элис, Боб и Кэрол – 3 валидатора с одинаковым количеством массы. Они совместно стимулируются к созданию круговой структуры для максимальной отдачи. Эти обязательства передаются в родительскую/корневую цепочку. Конец цепочки пропорционален показателю максимальной массы, что достигается корректным распределением блоков по n периодам (синий – текущий кандидат на конец цепочки, красный – приёмыш. Нерациональные концы цепочек содержат лишние комиссионные, идущие в кассу для будущих валидаторов с корректностью, превышающей определённый порог (т.е. 90%) После определённого периода времени можно с точностью утверждать, что конец синей цепочки завершён.

Это поощряет участников принимать больше участия и дублирует 51% выводов об атаках в консенсусе Накамото. В случае, если цепочка атакована удерживающей блок атакой или подвержена византийскому поведению, тогда невизантийские участники совершают массовый вывод из родительского/корневого блокчейна. Если залоги для высшей родительской цепочки Plasma существуют в форме токенов, то скорее всего стоимость токена значительно снизится в результате массового выхода.

2.4 Блокчейны в качестве MapReduce

блокчейн : git :: Plasma : Hadoop (MapReduce)

Создавая вычисление в формате MapReduce так же довольно несложно создать вычисления и переходы состояний в форме иерархического древа.

MapReduce предоставляет структуру для высоко масштабных вычислений через тысячи узлов. У блокчейна возникают такие же проблемы при достижении вычислительного масштаба, однако он также имеет дополнительные требования при создании доказательств вычислений MapReduce.

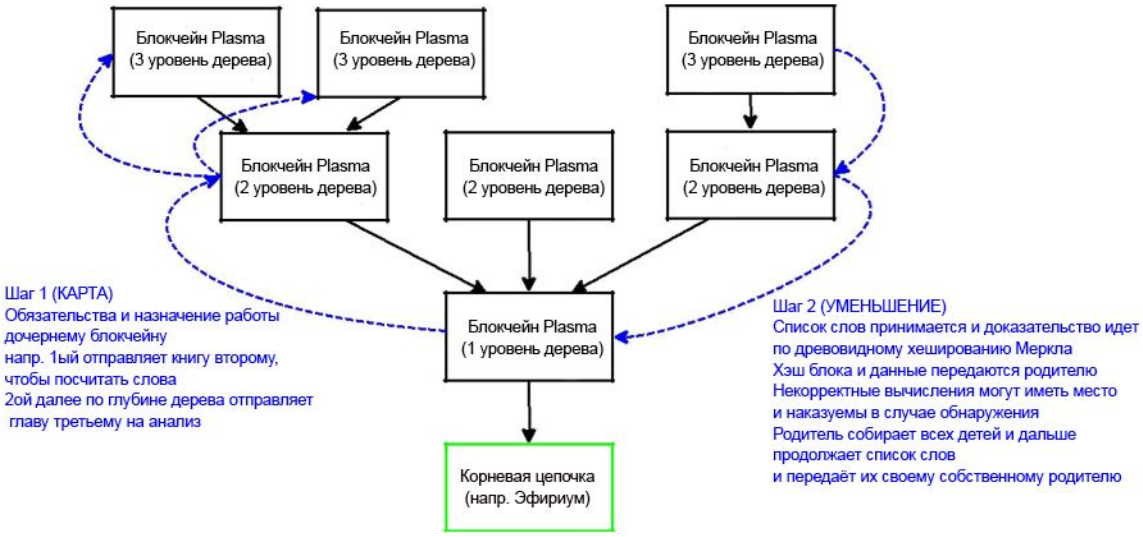

Таблица 7: Синие стрелки – это сообщения, передаваемые из родительского блока в дочерние. Дочерние блоки должны передать обязательства родительскому блоку с каким-то количеством блоков или иначе они столкнутся с удержанием цепи. Информация блока передаёт работу дочерним блокам, которые также участвуют в вычислении. Дочерний блок третьего уровня совершает вычисления и возвращает список слов (напр. 3 случая использования слова «привет», 2 случая использования слова «мир» в главе, за вычисление которой они отвечают). Информация о списке слов затем возвращается к родителю в качестве обязательства, списки слов комбинируются из дочерних блоков и передаются родительскому блоку, в конце концов составляя общий список слов (к примеру сборник всецело содержит 100 случаев использования «привет» и 150 случаев использования «мир»). Это создаёт экономически осуществимое вычисление в масштабе, при котором лишь один заголовок блока/хэша отправляется в корневую цепочку для того, чтобы обслужить очень большой объём информации и работы. Доказательство невыполнимости выпускается только в случае существования некорректного блока, в ином случае периодически в корневую цепочку будут попадать невероятно малые объёмы информации.

Мы предлагаем метод, при котором фаза карты включает обязательства по информации, отправляемой на вычисление на входе, а на шаге уменьшения включает в себя доказательство перехода древовидного хеширования Merkle при возврате результата. Переход древовидного хеширования Меркл осуществляется с помощью доказательств обмана, создаваемых в корневом блокчейне. Для переходов состояния также можно создать доказательство zk-SNARKs. Для некоторых вычислительных конструкций может также потребоваться битовая карта на переходах состояния во время шага Reduce (таким образом на эти случаи может использоваться более, чем один бит на UTXO/профиль)

Наша конструкция делает возможными невероятные высокомасштабные вычисления с временными и скоростными компромиссами. Эти компромиссы создают сеть, в которой узлы утверждают вычисления, а участники отвечают за их подтверждение. Это, однако, не

создаёт систему, в которой пользователь может полностью аутсорсить вычисления без доверительных фондов, но позволяет сжать вычисления в залоговые доказательства. Эти залоговые доказательства поощряют участников утверждать лишь правильные вещи. Опять же это следует концепции Lightning Network, по которой если в лесу падает дерево и никто этого не слышит, то, полагается, не важно, произвело ли падающее дерево звук или нет. Схожим образом, если никто не наблюдает за вычислением или не инициирует его, оно считается верным, а иначе совершенно не важно, каким будет его результат.

Вычисление может наблюдаться любым участником в открытых сетях, но участники, которые удерживают балансы и/или запрашивают корректное вычисление будут иногда наблюдать за цепью, дабы убедиться в её корректности. Преимущество от масштабирования получается в результате устранения требования о наблюдении за цепочками, которые не имеют непосредственного экономического влияния на пользователя, пользователю лишь необходимо следить только за теми цепочками, в которых он хотел бы осуществлять корректное поведение. Поведение на других цепочках Plasma может связываться вместе как часть шага уменьшения, так, что вычисление, имеющее непосредственное влияние на пользователя, выражается в минимальном состоянии. Например, в случае с децентрализованным обменом, пользователю нет нужды как и в каком порядке иные стороны размещают элементы, им лишь необходимо видеть один объединённый журнал заявок, таким образом пользователю необходимо лишь наблюдать за всеми остальными цепочками как единоличной стороне, тогда как собственная цепочка пользователя полностью подтверждается для осуществления транзакций и заказа внесения данных необходимому человеку (включая самого пользователя). Ещё один пример - пользователь может создать блочно-модульную конструкцию на древе цепочек Plasma без необходимости получения обновлений по темам, которые для этого пользователя не представляют интереса.

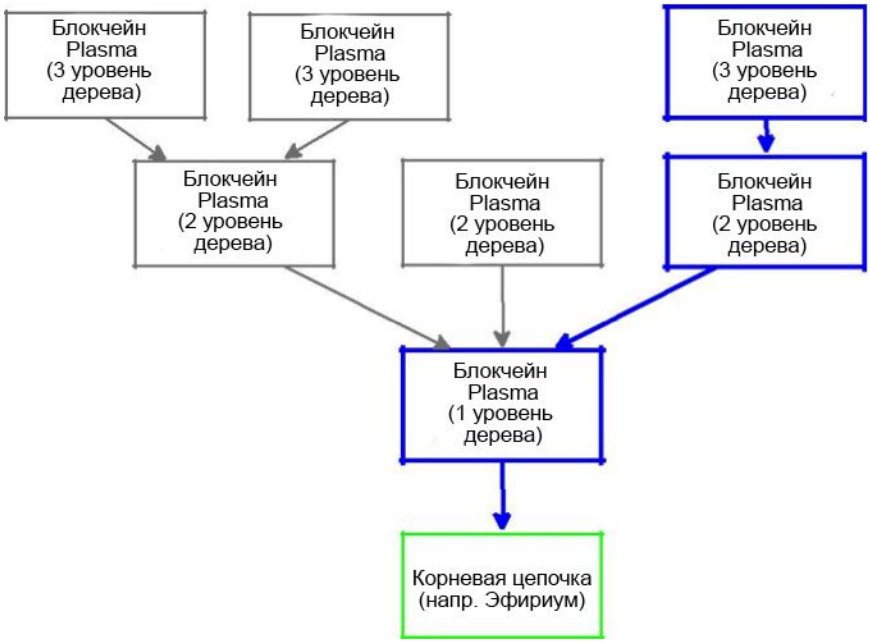

Таблица 8: Пользователю необходимо наблюдать за информацией, которую необходимо инициировать. Если в других цепочках Plasma, которые не требуют инициирования (отмечены серым цветом), возникает экономическая активность или вычисления, пользователь может рассматривать все другие цепочки, как единую противоположную сторону. Например, в случае децентрализованного обмена Plasma, пользователю необходимо наблюдать за цепочками, которые непосредственно влияют на обязательства пользователя (отмечены жирным синим цветом).

2.5 Описание экономических стимуляторов вокруг децентрализованных автономных блокчейнов

Мы предлагаем структуру, в которой пользователю представляется возможным создавать экономические стимуляторы для непрерывного исполнения дочернего блокчейна. Для состояний, не представляющих значительной сложности или не зависящих от переходов состояний, можно использовать нативный токен (ETH для Эфириума). Однако, для более сложных контрактов возможно потребуются более сложные стимуляторы для продолжения исполнения цепочки, поскольку все иные стимуляторы должны поддерживать жизнеобеспечение системы и её корректный порядок. [8][9]

Каждая цепочка Plasma представлена набором контрактов. Эти контракты осуществляют выполнение правил консенсуса цепочки, а мошенничество приведёт к значительным штрафам в случае создания доказательства обмана.

Однако, для того, чтобы скорее избежать появления состояний византийского типа, особенно в отношении жизнеобеспечения и порядка, в идеале необходимо создавать один токен для каждого контракта. Токен представляет эффекты сети при исполнении контракта и создаёт стимулятор для максимального повышения безопасности контракта. Поскольку цепочка Plasma требует от токена защиты сети по структуре proof-of-stake, у игроков снижается мотивация к поведению византийского типа или нарушению гармонии системы, поскольку это приведёт к значительному снижению стоимости токена. Задача токена – обеспечение привязки стоимости к валидаторам, что позволило бы снизить цену токена в случае их нерационального поведения.

С простыми контрактами и бизнес-логикой, такой как расчёт базового контракта, удерживающего средства от имени своих пользователей, залог в Эфириум может представлять ставку в цепочке Plasma.

Ставки, которые устанавливают залоги (токен ли это или ETH) имеют стимуляторы для продолжения управления сетью, поскольку они получают комиссию за транзакции за управление сетью. Эта комиссия за транзакции выплачиваются игрокам в сети, которые поощряют невизантийский тип поведения и обеспечивают долгосрочную ценность токена.

Поскольку у игроков есть стимул продолжать управлять сетью, чтобы собирать комиссию за транзакции, они будут беспрестанно управлять сетью и ограничиваться доказательствами обмана, утверждёнными в контрактах корневого блокчейна.

3 Иерархия архитектуры и смарт-контакты

Исторически многие люди полагают, что блокчейн лучше всего применим по отношению к транзакционным платежам как система расчёта на нетто-основе. Однако следует понимать, что система расчёта на нетто-основе имеет подстройку сложности. Архитектура на нетто-основе, как к примеру Lightning Network, это сеть каналов оплаты, она изменяет структуру для проведения бесконечного числа платежей между её участниками. Транзакционная мощность значительно увеличивается, поскольку каналы имеют нетто-привязку к блокчейну. Платежи можно перенаправлять внутри сети этих каналов.

Такая структура дополнительно позволяет эффективно проводить мгновенные платежи. Это крайне полезно не только для платежей, имеющих высокую степень временной чувствительности, но и также для самих контрактов.

Plasma не создана для скорого достижения утверждённого завершения, даже несмотря на то, что транзакции крайне быстро подтверждаются в дочерних цепочках, им необходимо завершиться в нижележащем корневом блокчейне. Каналы необходимы для того, чтобы иметь скоростную местную функциональность платежей и контрактов (инициируемых внутри цепочки)

В смарт-контрактах существует проблема «свободного выбора», при которой получатель (второй или последний подписавшийся) на предложении смарт-контракте должен подписать контракт и передать его для осуществления – в это время получатель контракта может рассматривать это, как свободный выбор и отказаться подписывать контракт, если деятельность его не интересует. Ситуация ещё более ухудшается, поскольку смарт-контракты работают наиболее эффективно при работе со сторонами без доверительных фондов (так как это снижает риск для противоположной стороны, а также стоимость информации)

Plasma не решает эту проблему сама по себе, поскольку нет гарантий неразрывности с первым и вторым шагами подписи для интерактивных протоколов в блокчейнах.

С помощью Lightning (включая Lightning исполняемый поверх Plasma) можно проводить невероятно быстрые обновления с достаточным ощущением местной завершённости. Вместо одного платежа, который дал бы выбор последней стороне, платёж можно вместо этого разделить на множество малых платежей. Это сводит к минимуму свободный выбор к количеству средств за каждый разделённый кусок. Поскольку вторая сторона смарт-контракта лишь имеет свободный выбор, базирующийся на объёме средств доли, стоимость свободного выбора сводится к минимуму.

Внутри вышеописанных случаев существует возможность того, что Lightning может быть первичным интерфейсным слоем для скоростных финансовых платежей/контрактов поверх Plasma, поскольку Plasma позволяет обновлять учётный журнал с минимальным количеством обязательств корневой цепи.

Таблица 9: В корне расположен блокчейн, который является оценочной инстанцией для контрактов и платежей. Сами контракты расположены в корневом блокчейне. Цепочка Plasma содержит текущее состояние учётного журнала, которое можно установить и возместить на уровне корневого блокчейна. Доказательства обмана существуют для того, чтобы позволить возместить средства. Plasma представляет собой вложенное множество Plasma цепочек для создания площадки для снятия средств в масштабируемом формате с минимальными блокчейновыми транзакциями. На вершине располагается Lightning Network, который позволяет проводить мгновенные платежи внутри Plasma и блокчейнов.

3.1 Самая важная проблема разделения данных – это информация

С наборами разделённых данных существует значительный риск отказа раскрыть информацию в отдельно взятых разделах. С таким раскладом не видится возможным создавать доказательства обмана

Мы попытаемся разрешить эту проблему используя 3 стратегии:

1. Новый механизм proof-of-stake будет стимулировать распространение блоков. Его базовый механизм не полагается всецело на корректную функциональность стимуляторов. Однако, это в любом случае значительно снизит случаи нерационального поведения.

2. Значительные задержи при снятии смогут позволить получить точные доказательства снятия. Пользователям нет необходимости наблюдать за блокчейном так часто, а мошенничество на более высоких цепочках Plasma может быть предотвращено на корневом блокчейне любым честным игроком, являющимся пользователем этой же Plasma цепочки. В случае удержания блока цепочки Plasma могут немедленно заблокировать средства с помощью

доказательства, предотвращая атакующего пользователя от передачи ложных данных о снятии средств. В случае, если атакующий пытается снять больше средств, чем позволяет лимит и блокируются большее количество средств, атакующая цепочка Plasma теряет свой депозит.

Создание дочерних цепочек из которых транзакции могут распространяться в любую родительскую цепочку. По этой причине участники сетей непременно захотят проводить транзакции в удалённых дочерних цепочках. Это создаёт экономическую эффективность для небольших балансов, у которых нет экономической возможности выплачивать большие комиссионные в корневом блокчейне и поэтому таким образом будет можно перемещать средства множеством небольших балансов. Таким образом люди захотят создавать крайне удалённые объединённые дочерние цепочки, которые вкупе будут представлять существенное значение. Стоит обратить внимание, что есть предрассудки касательно репутации выбора цепочек с пользователями, удерживающими очень небольшие балансы, которые не могут попасть в корневой блокчейн из-за транзакционной комиссии, однако этого можно избежать путём создания удалённых объединённых цепочек. Эта модель безопасности является ключевым нововведением цепочек Plasma.

4 Родственные проекты

Некоторые родственные проекты предлагают древовидное хеширование Меркл с шагами уменьшения, как доказательства вычислений, однако это предложение в основном вращается вокруг доступности информации и содействию уменьшению цен и доказательствам обмана, с наличием протокола для управления этими элементами через экономически стимулированную постоянно разделяемую группу цепочек.

Другие схожие проекты предлагают систему дочерних блокчейнов, но не имеют особо заметных отличий в своём подходе.

Plasma использует доказательство древовидного хеширования Меркл для исполнения дочерних цепочек.

4.1 TrueBit

Plasma очень похода в своём подходе к доказательствам обмана на TrueBit. Конструкция её доказательств обмана похожа на TrueBit, и практически вся работа TrueBit непосредственно применима к Plasma, особенно работа вокруг доказательсta древовидного хеширования переходов состояния.

Архитектура TrueBit позволяет создавать компактные доказательства для дальнейшей передачи в блокчейн Эфириум, что требуется для Plasma, поэтому практически вся тяжёлая работа проводится TrueBit, в чём заслуга её разработчиков. Использование игры подтверждения, которая генерирует доказательства древовидного хеширования является несомненным преимуществом, позволяющим уменьшить масштаб вычислений. Иные похожие выводы также применимы к TrueBit, в частности состояние вычисления должно

быть вычислимо и передаваемо через Интернет (большие куски данных необходимо разделить на несколько частей). Также необходимо смягчить последствия проблемы доступности данных, любые неудачные попытки следует придать публичной огласке. Мы также стараемся устранить эти проблемы, особенно последние две.

Главный аспект, который Plasma пытается построить на TrueBit – это значение участников с разных сторон, которым необходимо проводить вычисления на общем состоянии. Например, определённое количество участников лишь волнуются о подразделе данных и вычислении и лишь желает вычислять интересующие их аспекты (напр. BBS или обмен). Мы также пытаемся уменьшить воздействие проблемы осуществления вычислительных раундов на площадках вне цепочек.

4.2 Разделение блокчейнов.

Текущая работа над разделением блокчейнов использует схожие техники и имеет схожие цели, например предложение разделения Эфириума. Эта конструкция может быть совместима в качестве высшего слоя. Если же разделён корневой блокчейн, тогда цепочка Plasma может исполняться поверх него для ещё большей масштабируемости и иных преимуществ. Это может быть и тестовой площадкой для различных техник разделения, поскольку в консенсус Эфириума и других обширных блокчейнов не нужно будет вносить изменений для начала базовых операций.

4.3 Интегрированные сайдчейны

Драйвчейны имеют много общего с интегрированными сайдчейнами, кроме того, что отсутствует информация о валидаторах, а также присутствует изменяющийся список участников (майнеров) с ещё большей децентрализацией.

Plasma – это не интегрированный сайдчейн, поскольку она не опирается на интеграцию для честной деятельности, и не зависит от доверенных игроков для воплощения состояния внутри цепочки. Plasma также реализует состояние учётного журнала в других блокчейнах, позволяя использование тех же коинов/токенов, однако она также осуществляет подтверждение в случае наличия доказательства обмана. Plasma не полагается на сильную лигу игроков, что подразумевает значительный риск в зависимости от корректности таких игроков, поэтому и не является привязанной интегрированным сайдчейном.

4.4 Блокчейн совместного майнинга

Среди премеров можно отметить Namecoin, который создаёт пересекающиеся блоки с родительским блокчейном. Это подразумевает полное подтверждение блокчейна, однако не предоставляет преимуществ масштабируемости. Блоки расширения – это живописный пример цепочек совместного майнинга, которые позволяют средствам перемещаться между первичным блокчейном и цепочной совместного майнинга (с механизмом исполнения полного набора майнеров – по правилу консенсуса корневой цепочки). Цепочки совместного майнинга позволяют вводить новые правила консенсуса и выбирать пользователей для подтверждения только тех цепочек, что представляют для них интерес, однако майнеры и валидаторы должны подтверждать всё. Целью Plasma является обеспечение возможностей для пользователей и майнеров подтверждать только те

цепочки, которые представляют для них интерес.

4.5 Тричейны

Тричейны предлагают блокчейны древовидной структуры, которые подтверждаются в дочерних блоках с использованием доказательства выполнения работы. Корневая цепочка содержит суммируемое доказательство работы от всех дочерних блокчейнов. Далее вниз по схеме безопасность ещё выше, но выше она не столь высока, всё зависит от уровня подтверждения и работы. В то время как топология тричейна тождественна древесной структуре, сама его структура зависит от безопасности майнинга, который суммируется по ветвям. Модель безопасности становится менее безопасной ближе к листьям, поскольку она защищена доказательством выполнения работы. Plasma прямо противоположна этой структуре, в ней майнинг выполняется с учётом полной безопасности только в корне, все иные средства безопасности и доказательства исходят из корня. Похожая работа – построение доказательств блоков, расположенных в древовидной структуре.

4.6 zk-SNARK и zk-STARK

Неинтерактивные доказательства вычислений позволяют пользователю получить значительные преимущества в масштабируемых вычислениях. zk-SNARK/STARK и другие формы неинтерактивных компактных доказательств являются отличным подспорьем для Plasma. Доказательство может быть предоставлено вместе с результатом вычисления с древовидным хешированием Меркла. К тому же есть определённые преимущества в сокращении общесистемных атак при удержании небольших балансов в дочерней цепочке Plasma. SNARK уже проводит исследование на предмет совмещения функциональности с MapReduce и мы надеемся результаты этого исследования позволят повысить прибыть, а Plasma может расшириться, сделав доказательства упорядочиваемыми и исполняемыми внутри набора блокчейнов.

Дальнейшие преимущества заключаются в доказательствах вычислений, которые позволяют осуществлять более быструю синхронизацию и подтверждение самих цепочек. Заметьте, что zk-SNARK не решает проблему доступности данных, она лишь уменьшает количество требований к данным и вычисления. Это особенно полезно в качестве замены или дополнения к любым временным механизмам аутентификации «вызов-ответ». zk-SNARK может быть использована в качестве защиты в глубине схемы. Если последняя линия обороны использует блокчейн без вычурной криптографии, вторая линия обороны как раз может быть zk-SNARK, а первой линией обороны будет проверенное вычислительное оборудование.

Снятие средств с цепочек Plasma можно было бы дополнительно защитить с помощью zk-SNARK, что позволило бы не запрашивать битовую карту, которая в свою очередь позволила бы переводить очень небольшие балансы.

4.7 Cosmos/Tendermint

Cosmos выстраивает блокчейны в структуру «хаб» Cosmos и подтверждает дочерние блокчейны с помощью доказательств системы ставок. Существует значительное сходство

между конструкцией дочерних блокчейнов, однако Plasma опирается на создание доказательств обмана для исполнения состояний в дочерних цепочках и уже практически стала нарицательной и применима ко многим цепочкам. Конструкция с защитой по методу «подтверждение доли» для Cosmos предполагает наличие как минимум 2/3 честного количества валидаторов, включая валидаторов её собственной Cosmos Zone.

4.8 Polkadot

Polkadot также выстраивает структуру для иерархии блокчейнов. Существует схожесть с архитектурой Polkadot. Вместо структуры с валидаторами-рыбаками, обеспечивающими точность блоков, мы создали серию дочерних блокчейнов, которые исполняют состояния с помощью доказательств древовидной иерархии Меркл. Конструкция Polkadot опирается на состояния дочерних блокчейнов (парачейнов) и доступность информации, осуществляемую валидаторами-рыбаками.

4.9 Lumino

Lumino – это архитектура для контрактов по методу освоенного объёма со сжатыми обновлениями в блокчейне. Она позволяет участникам обновлять только минимальные исполняемые состояния. Архитектура управления выходом в Plasma продвигает эту идею ещё дальше, позволяя лишь одному биту обозначать определённый выход. Это создаёт скоростную и низкозатратную координацию при массовом снятии средств в случае сбоя в дочерней цепочке Plasma.

5 Многостороннее состояние оффчейн

Целью является создать метод, при котором участники могли бы удерживать средства в нативных коинах/токенах блокчейна, без значительных ончейн состояний. Plasma начинает стирать границу между ончейном и оффчейном (к примеру являются ли разделы ончейн или оффчейн?)

Существует две распространённых проблемы при попытке установления многосторонних оффчейновых каналов. Первая – это необходимость выполнять синхронизированное обновление состояния среди всех участников, где также будет необходимо обновление системы (или в противном случае идти на уступки в зависимости от доступности глобальных обновлений состояния), а это значит постоянное нахождение онлайн. Вторая проблема состоит в том, что добавление и удаление участников в канал требует большого обновления ончейн, перечисляющего всех участников, которые добавляются и удаляются.

Было бы вместо этого гораздо разумнее создать механизм, в который многие участники могли бы добавляться или из которого удаляться без значительных обновлений корневой цепочки, а обновления внутреннего состояния могли бы осуществляться без участия всех сторон, им лишь необходимо участвовать если их балансы регулируются или если замечено поведение византийского типа.

Общая конструкция - это дочерний блокчейн, который позволяет удерживать балансы, представленные в смарт-контракте корневого блокчейна (напр. Эфириума). Балансы

смарт-контрактов представлены и расположены в балансах завершенных блоков в дочерней цепочке Plasma. Это позволяет пользователям удерживать нативный токен в дочернем блокчейне с развёрнутым представлением балансов корневого блокчейна, также позволяя снятие средств после периода обсуждения.

Для того, чтобы этого достичь мы создали модель UTXO (выход непотраченных транзакций) для журнала операций. Хотя это и не является острой необходимостью, гораздо проще работать со скоростным снятием средств. Логическое объяснение модели UTXO – легко представлять в компактном виде, было ли использовано определённое состояние или нет. Это может представляться в виде TRIE для доказательств древовидного хеширования Меркл или в качестве битовой карты для компактного представления, представляемого всем для анализа. Другими словами, смарт-контракты удерживаются на счетах корневой цепочки, но цепочка Plasma сохраняет набор балансов UTXO для распределения балансов, находящихся в счёте корневой цепочки. Для дочерних цепочек, у которых нет значительных требований касательно переходов состояния представляется возможным использовать модель счёта для более сложных и частых переходов состояния, однако возникает больше зависимости от доступности блокового пространства в родительском блокчейне.

На текущий момент пользователь может полагать, что единичный лидер блока выбирает блок дочерней цепочки Plasma. Возможно составить набор proof-of-stake или именованную заготовку валидаторов, однако в этих примерах мы для простоты используем лишь один именованный валидатор. Роль валидатора заключается в предложении блоков, которые служат в качестве упорядочивателя транзакций. Валидатор/предлагающий ограничен доказательствами обмана, построенными в контракте корневого блокчейна. Если они распространяют блок с неверным переходом состояния, любой другой участник, получающий блок, может отправить доказательство обмана древовидного хеширования Меркл в родительский блокчейн и неверный блок будет откачен обратно и оштрафован.

Блоки распространяются среди участников, которые хотели бы за ними наблюдать, включая участников, держащих балансы или желающих наблюдать за вычислениями или их инициировать в индивидуальной цепочке Plasma.

В то время как существует минимальная сложность в управлении депозитами в состоянии оффчейн, переходы состояний и снятие средств представляют собой большую сложность.

5.1 Доказательства обмана

Все состояния внутри этого дочернего блокчейна исполняются с помощью доказательств обмана: которые позволяют любой стороне запускать некорректные блоки, принимая во внимание доступность данных блока.

Однако, самой большой трудностью в этой конструкции является отсутствие явных гарантий, касающихся доступности данных/блока.

В корневом блокчейне (напр. Эфириуме) существует набор доказательств обмана, которые обеспечивают правильность всех переходов состояний в случае, если доступны данные блока. Для сложных вычислений переходы состояний надо представить в виде

древовидного хеширования Меркл для эффективного подтверждения.

К тому же переходы состояний также могут запускаться с помощью zk-SNARK/STARK, которые обеспечивают невозможность неверных выходов. Конструкции zk-SNARK могут потребовать рекурсивные SNARK для большей эффективности и, таким образом, могут потребовать дальнейших исследований касательно их возможностей. Однако в текущий момент система разработана на успешное функционирование без SNARK.

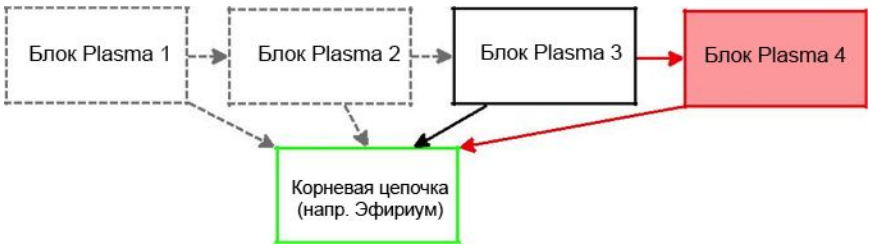

Таблица 10: У всех есть информация о блоках 1-4. Запущенный переход состояния блока 4 - доказуемо мошеннический с помощью доказательств древовидного хеширования Меркл в блоке 4 и данных из предыдущего блока.

Доказательства обмана обеспечивают подтверждение всех переходов состояния. Примерные доказательства обмана являются доказательством транзакционного объёма трат (средства доступны в текущей UTXO), доказательства перехода состояния (включая проверку подписи на подлинность на выходе, доказательство включения/исключения среди блоков, а также доказательства внесения/снятия. Некоторые другие более сложные доказательства требуют наличия интерактивной игры. Общая конструкция будет нацелена на функциональный подход к подтверждению блоков.
Если кто-то напишет механизм консенсуса в Solidity, будет требоваться дополнительный вход для каждой функции с доказательством древовидного хеширования Меркл блока, которому потребуется подтверждение, а выход сможет вернуться лишь если подтверждение прошло успешно. Затем необходимо просто дублировать код подтверждения консенсуса чтобы обработать его в форме компактного доказательства древовидного хеширования Меркл (так чтобы не потребовалось обрабатывать блок целиком для создания доказательств обмана)

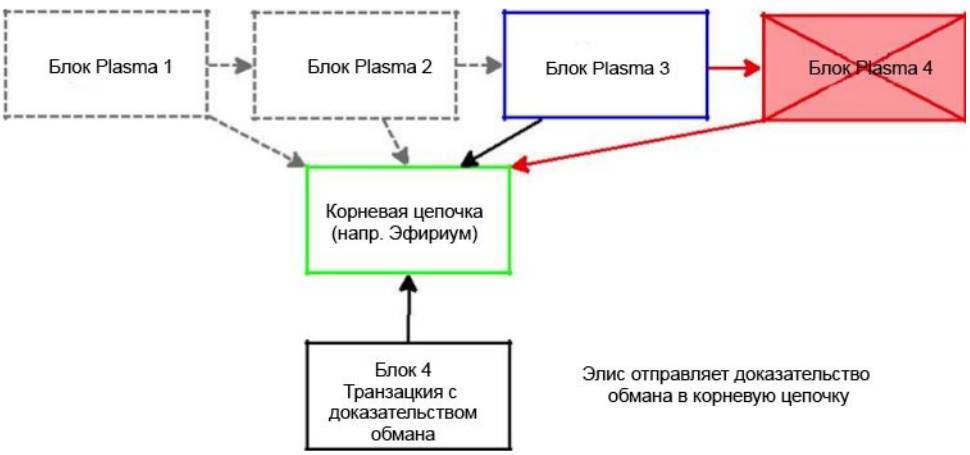

Таблица 11: У Элис есть копия всех данных блока, поэтому она отправляет доказательство обмана в корневую цепочку. Блок 4 теряет подтверждение и откатывается назад. Пользователь, подавший блок 4 наказывается, он теряет залог, хранящийся в смарт-контракте. Текущий блок сейчас – блок 3 (синий). После определённого времени блоки завершаются и подавать доказательства обмана уже станет нельзя. Пользователям следуем строить только на блоках, которые не признаны мошенническими путём полного подтверждения блоков.

Для того, чтобы у этой конструкции было минимальное количество доказательств, однако, следует помнить, что все блоки должны предоставить обязательство TRIE-структуры древовидного хеширования Меркл, TRIE-структуру потраченных выходов, древо Меркл для транзакций и ссылку на предыдущее изменяемое состояние.

Доказательства обмана гарантируют, что коалиция участников не сможет создать мошеннические блока и избежать наказания. В случае, если мошеннический блок обнаруживается и подтверждается на корневом блокчейне (или родительских цепочках Plasma) некорректный блок откатывается назад. Это позволяет отдельным участникам создавать стимуляторы против поведения византийского типа, что решает проблему уязвимости перехода состояний в интегрируемых привязанных биткоин сайдчейнах.

Результатом являются высокомасштабируемые переходы состояния, способные существовать в блокчейне Plasma, в то же время обеспечивающие наблюдателям, имеющим доступ к данным блока, подтверждать (и таким образом разоблачать) некорректные переходы состояний. Другими словами, платежи могут проводиться в этой цепочке только с временными обязательствами на корневой цепочке.

5.2 Депозиты

Депозиты из корневой цепочки отправляются непосредственно в главный контракт. Контракт же уже отвечает за отслеживание обязательств по текущему состоянию, за наказание некорректных обязательств с использованием доказательств обмана и за обработку снятия средств. Поскольку дочерний блокчейн Plasma является полным валидатором корневого блокчейна, то входящие транзакции должны обрабатываться с использованием двухфазной привязки.

Депозиты должны включать в себя блокхэш цепочки направления, чтобы определить направление дочерней цепочки. Это достигается путём использования мультишагового процесса для обеспечения возможного возврата коинов.

Таблица 12: У Элис есть счёт ETH с один эфир на счету. Она хочет отправить его в блокчейн Plasma. Она отправляет его в контракт Plasma.

1. Коины или токены (напр. Эфир или токены ERC-20) отправляются в контракт Plasma в корневом блокчейне. Эти коины можно вернуть в течение определённого периода времени в качестве ответа.

2. В блокчейн Plasma включено доказательство входящей транзакции. В этом случае блокчейн Plasma подтверждает обязательства по факту входящей транзакции и будет доступна для траты в случае фиксированной транзакции или траты, инициируемой вносителем. Когда этот фактор включён в блокчейн, он начинает обрабатывать обязательства по рассмотрению запроса на снятие средств. Однако не существует подтверждения того, что вноситель обладает достаточной информацией для создания доказательства обмана, значит у нас всё ещё нет обязательств со стороны вносителя. Этот блок включает добавление в древо состояния, битовую карту, и древо транзакций, так, чтобы могло иметься компактное доказательство корректного включения.

3. Вноситель подписывает транзакцию в дочернем блокчейне Plasma, запуская транзакцию, что включает в себя обязательство в том, что они видели блок с обязательством цепочки в фазе 2. Роль этой фазы заключается в том, что вноситель подтверждает факт того, что он обладает достаточной информацией для снятия средств.

После завершения этого процесса, цепочка принимает обязательства по факту того, что они обработают эти коины и дадут распределение, так, что снятие средств может быть всецело подтверждено. С помощью третьей фазы пользователь подтверждает факт того, что он может снимать средства.

Таблица 13: У Элис теперь есть один эфир в блоке Plasma. Она взяла обязательство в том, что она видела средства и теперь зафиксировала их. Средства содержатся в смарт-контракте корневой цепочки, но записи учетного журнала находится в этом конкретном блокчейне Plasma (отсюда и переходы состояний, то есть отправка средств другим пользователям или смарт-контрактам)

В случае, если вноситель не прошёл через фазу 3, он может попытаться провести снятие средств на корневом блокчейне. Вноситель подаёт неподтверждённый запрос на снятие средств и должен будет ожидать в течение довольно длительного периода времени какого-то пользователя в сети, который бы создал доказательство обмана о том, что вноситель закончил передачу и зафиксировал средства в блокчейне Plasma. В случае, если доказательство отсутствует, вноситель может снять свои неподтверждённые средства. Такое снятие требует мощной связки с корневой цепочкой, чтобы убедиться в отсутствии поведения византийского типа.

5.3 Массовое снятие средств и битовое состояние

Самое важное, о чём стоит позаботиться в этой системе – это её невозможность подтвердить состояние.

Для того, чтобы проводить максимальное сжатие транзакции состояния, выходы можно добавочно представить в битовом состоянии. Это необходимо для доказательств снятия средств, которые могут быть слишком дорогостоящими, чтобы проводить их на корневой цепочке. Целью этой конструкции является предоставление возможности удерживать небольшие балансы в цепочке Plasma. Эти балансы удерживаются в стопроцентном резерве в контракте на корневом блокчейне, но главный журнал целиком находится за пределами блокчейна. Первичный удар, который необходимо смягчить – это удерживаемые некорректные блоки (с обязательствами корневой цепочке). В случае, если система обнаруживает некорректные переходы состояний, участникам будет необходимо провести массовый вывод транзакций.

С битовой конструкцией снятие средств включает в себя битовую карту подписанных транзакций, которые хотели бы выйти. Затем создаётся игра/протокол, которые запускаются смарт-контрактом для обеспечения корректной информации. Битовая карта

обеспечивает возможность всем рассуждать о тратящихся выходах.

Поскольку это битовая карта, она делает необходимым представление состояния в структуре непотраченного транзакционного выхода (UTXO) для максимальной эффективности небольших балансов. Объём трат компактно доказуем: а большой набор переходов состояний может быть выполнен безотказно. А после предопределённого периода времени биты снова можно использовать заново.

Существует шкала плавного перехода от дорогой с высокими гарантиями до дешёвой с низкими гарантиями.

1. Состояние журнала учёта на корневом блокчейне

2. Состояние журнала учёта в Plasma, экономически жизнеспособное для проведения единичной транзакции ончейн

3. Состояние журнала учёта в Plasma, экономически жизнеспособное для проведения с использованием битовой карты (стоимость 1-2 бита)

4. Состояние журнала учёта в Plasma, экономически нежизнеспособное для проведения с использованием битовой карты на корневом блокчейне. Массовое снятие со стоимостью 1-2 бита обойдётся слишком дорого.

Для пользователей, удерживающих балансы, которые можно было бы запустить на корневой цепочке, требование работать в UTXO-битовом формате не является необходимым. Однако для тех, кто удерживает балансы и может осуществлять операции, только 1-2 битная транзакционная комиссия на корневом блокчейне будет достаточно низкой.

Для четвёртого типа (1-2 битная ончейн стоимость слишком высока для массового снятия) система всё равно будет устойчива к отказам (пусть даже и с предположением о то, что именованные сущности будут достаточно надёжными). Следующие разделы этой статьи описывают иерархическую блокчейновую структуру, служащую для создания многих площадок, на которых было бы экономически возможным провести массовое снятие средств. В дополнение к этому, если общее значение транзакций в четвёртой категории значительно ниже стоимости токена, тогда теоретически было бы слишком дорого нападать на такие балансы, поскольку в первую очередь пострадает репутация держателей токенов.

5.4 Переходы состояний

По умолчанию, переходы состояния в цепочке Plasma исполняются внутри схожего многофазного процесса, как и в случае с внесением. Это необходимо для обеспечения пользователей информацией, необходимой для проведения переходов состояний. Однако, в отличие от конструкции внесения, в данном случае, как только транзакция подписана и добавлена в блок, существует связующее обязательство. Для этой цели переходы состояний должны включать подпись, обновления состояния (напр. точку назначения, количество, токен и любые другие данные о состоянии), а также TTL с истекающим сроком и обязательство для каждого блока. В то время, когда этот TTL не требуется, он не должен занимать больше времени, необходимого для создания доказательств выхода, чтобы

убедиться, что нам известны негативные условия выхода. Заранее подписанные транзакции, конечно же, не должны содержать TTL. Не следует ожидать от этой конструкции высокой жизнеспособности, поскольку уже существуют предположения о жизнеспособности системы снятия средств с учётом глубокой реорганизации. Обязательство к блоку – это обязательство тратящего средства в том, что сущность, передающая транзакцию в цепочку Plasma имела возможность наблюдать за блоками по цепочке вверх до той точки, где она могла бы применять доказательства. Она также должна находиться за блоком, в котором произошёл потраченный выход.

Для скорого завершения многостороннее обязательство происходит следующим образом:

1. Элис хотела бы потратить свой выход в цепочке Plasma Бобу, который находится в этой же самой цепочке Plasma (без записи о полной транзакции, который надо бы было отправить в блокчейн). Она создаёт транзакцию, которая тратит один из её выходов в цепочке Plasma, подписывает её и отправляет транзакцию

2. Транзакция включается в блок валидаторами цепочки Plasma. Заголовок включается в часть блока в родительской цепочке Plasma или корневом блокчейне, в конце-концов попадая в корневой блокчейн и оставаясь там.

3. Элис и Боб наблюдают за транзакцией и подписывают подтверждение того, что он видел транзакцию и блок. Это подтверждение подписывается и включается в другой блок Plasma.

Для медленного завершения должен произойти только первый шаг.

После получения подтверждения транзакция может считаться завершённой. Необходимостью третьего шага является обеспечение доступности блока для участников (Элис и Боба). Третий шаг мог бы быть пропущен, однако в связи к этим возникли бы задержки при завершении. Логическим обоснованием является факт того, что транзакция не должна признаваться завершённой пока все стороны, относящиеся к транзакции, не подтвердят корректность блока и доступность информации.

В случае удержания блоков после шага 1, Элис не может определить, была ли потрачена её транзакция. Если транзакция была включена в блок (удерживается он или нет), то она рассматривается, как неподтверждённая, в случае, если не завершён шаг 3. Таким образом Элис всё ещё может совершить снятие этих средств, если она не подписалась под обязательством, принимая, однако, во внимание то, что её сообщение о снятии средств появилось в корневом/родительском блокчейне до того, как блок был завершён. Элис не может снять средства после завершения блока, и, считается, что блоки были отправлена Бобу. Если блоки удерживаются до завершения (между шагами 1 и 2), а Элис и/или Боб за этим наблюдают, тогда Элис может вывести свои незавершённые средства. Если блоки удерживаются после шага 2, но до шага 3, тогда считается, что у Боба имеется достаточная информация для вывода средств, но по сколько ни у Элис, ни у Боба нет полных обязательств по платежу, он считается незавершённым; в зависимости от доступности информации любая из сторон может забрать средства. Если обе стороны

подписались в шаге 3, то транзакция считается полностью завершённой. Исполнение хэша pay-to-contract начинается после завершения этого шага, особенно в случае, когда подписи были доказуемо поставлены на цепочке. В случае, если одна из сторон отказывается ставить подпись или если происходит удержание блоков, исполнение не является обязательным до получения доказательства о возмещении. Поскольку все состояния в конце-концов отправляются в цепочку с помощью доказательств древовидного хеширования Меркла, существует меньшая зависимость от хэша pay-to-contract, поскольку платежи могут быть подтверждены и исполнены после завершения.

Стоит обратить внимание, что шаг 3 является необязательным для смарт-контракта вместе подписи обеими сторонами, т.е. состояние является условным на момент HTLC выпуска прообраза. Это позволяет добиться многоцепочной и многотранзакционной неразрывности. Сложность создания контракта может повыситься, поэтому при желании добавить такие функции необходимо иметь высокий навык работы с языками программирования/инструментами.

5.5 Периодические обязательства в корневую цепочку

Цепочка Plasma должна быть способна создавать упорядоченность в блокчейне. В цепочке Plasma существует упорядоченность между блоками, но блоки не проверяются и могут сами располагать себя где угодно. В результате этого существует необходимость создавать обязательства в корневом блокчейне. Цепочка Plasma отправляет заголовок своего блока в корневую цепочку и её заголовок проходит через доказательства обмана. В случае отправки мошеннического заголовка с доступностью данных для других пользователей любой другой участник может отправить доказательство обмана и в таком случае обязательство и блок будут откачены обратно со штрафами для отправителя.

Эти обязательства позволяют создать чёткий порядок без каких-либо дальнейших неопределённостей. Если же наблюдаются попытки внести неопределённость или двусмысленность в систему, то доказательства обмана помогут эффективно наказать злоумышленника. После определённого периода времени блоки завершаются и, как результат, не могут быть реорганизованы, с учётом того, что корневой блокчейн также достигает достаточной завершённости.

5.6 Выведение средств

Plasma позволяет пользователям вносить средства нативных коинов и токенов (напр. ETH и токенов ERC-20). Она также позволяет переходы состояний внутри блокчейна Plasma, состояние которого исполняется корневым блокчейном, опять же при условии достаточной доступности информации. В случае нарушения доступности информации необходимо совершить массовый выход с цепочки Plasma. В конце концов также есть возможность совершить простой вывод средств, удерживаемых в цепочке Plasma.

Однако при нормальном функционировании системы пользователи могут совершать простые выводы средств.

5.6.1 Простой вывод средств

При простом выводе средств пользователям лишь разрешается снимать средства, которые были отправлены в корневой блокчейн и были в конечном счёте завершены в цепочке Plasma.

Мы ранее описали архитектуру внесения, компактного представления состояния журнала операций и переходы состояний. До текущего момента, кроме как с помощью доказательств обмана, не существовало иного способа отправки состояния журнала операций текущей цепочки Plasma в корневом блокчейне. При работе с выводом средств, однако, требуется особое доказательство удержания средств в цепочке Plasma и их актуальность.

Выводы – это самый критически важный компонент системы, поскольку они обеспечивают взаимозаменяемость коинов между корневым блокчейном и дочерними цепочками Plasma. Если пользователю удастся внести средства в цепочку Plasma, выполнить переходы состояний (иными словами отправить коины другим сторонам), а у сторон имеется возможность выводить средства, то значение должно быть приближено к стоимости коинов в корневой цепочке. В некоторых случаях средства на цепочке Plasma могут быть более полезными, поскольку они обладают большей транзакционной мощностью, а безопасность в конце-концов зависит от корневой цепочки.

Для простого вывода средства все средства требуют большой залог, а все запросы на выведение средств должны включать большой залог, использующийся в качестве доказательства обмана. В случае, если доступны текущие данные блока, то у третьей стороны существует возможность предоставить это доказательство по невероятно низкой стоимости, поскольку службы третьих сторон могут подтверждать блокчейны Plasma в режиме реального времени и подтверждать корректность доказательств вывода средств.

Все участники цепочка Plasma ДОЛЖНЫ подтверждать все родительские цепочки Plasma и корневой блокчейн для того, чтобы убедиться, что в текущий момент не происходит текущих выводов средств с определённых счетов/выходов во время обновления состояния. В случае, если происходит вывод средств, то соответствующий блок не сможет тратить коины/токены, а поведение византийского типа в данном случае нарушает консенсус и подлежит доказательству обмана, наказанию и откату блока по каждому контракту Plasma в корневом блокчейне.

Вывод средств проводится таким образом:

1. В корневой блокчейн или родительскую цепочку Plasma подаётся подписанная транзакция вывода. Выводимый объём должен представлять целостные выходы (без частичных выводов). Могут выводиться несколько выходов, но им всем необходимо быть в одной и той же цепочки Plasma. Также как часть вывода раскрывается расположение выходной битовой карты. Дополнительный залог размещается в качестве части вывода для предотвращения и наказания фальшивых запросов на вывод.

2. Для всех обсуждений существует предопределённый период времени, очень схожий с тем же периодом в Lightning Network. В таком случае, если кто-либо сможет

подтвердить то, что выход уже был потрачен в цепочке, из которой совершается вывод (во многих случая это корневой блокчейн), тогда вывод средств отменяется, а залоговый запрос на вывод пропадает.

3. Также существует и вторичная задержка для рассмотрения времени ожидания всех других запросов на вывод с БОЛЕЕ НИЗКОЙ высотой подтверждения блоков. Это необходимо для запуска упорядоченного вывода в определённой цепочке Plasma или корневой цепочке.

4. В случае, если утверждённый в смарт-контракте Plasma согласованный период времени на обсуждение истёк, и не были предоставлены доказательства обмана в корневой или родительской цепочке, тогда предполагается, что вывод средств был проведён корректно, а выводящий пользователь может извлечь свои средства в корневой или родительской цепочке. Выводы средств обрабатываются в порядке от старых к новым когда речь касается возраста счёта/UTXO.

Необходимо заметить, что это возможно, если это экономически оправдано, совершить вывод в случае проводимой на блок атаки в цепочке Plasma.

Доказательства обмана лишь требуют того, что кто угодно в сети может предоставить копию подписанного сертификата оплаты из того выхода, чему можно представить компактные доказательства. Для Lightning и других каналов состояния также существует дополнительное требование для подтверждения более высокого временного вывода средств. Что же касается каналов, в случае, если осуществляется попытка более низкого временного вывода средств, средства остаются в цепочке Plasma, доступные для вывода при предоставлении правильной подписи. Другие конструкции также возможны, но архитектура может потребовать иметь фронтальную нагрузку, как часть создания доказательств обмана смарт-контрактов для цепочки Plasma.

Поскольку стандартные процедуры вывода – это довольно медленный и дорогостоящий процесс, они скорее всего могут быть объединены в единую процедуру вывода, а иначе все остальные захотят обменять коины на другие цепочки с использованием Lightning или атомной мультичейновой торговли

5.6.2 Быстрое снятие средств

Быстрый вывод средств использует ту же конструкцию, что и простой вывод средств, однако средства отправляются в контракт, управляющий атомной мультичейновой торговлей. Средства обмениваются на средства в корневой/родительской цепочке с коротким временным замком на другие средства с высоким временным замком, выходящие из цепочки Plasma.

Быстрый вывод, несмотря на название, не является мгновенным. Однако он значительно сокращает время ожидания вывода до времени подтверждения завершения транзакции, конечно при условии того, что цепочка Plasma не подвержена поведению византийского типа (включая удержание проводящих блоков). По этой причине быстрый обмен выводов невозможен во время удерживающих блок атак, а вместо этого потребуется запрос на медленный массовый вывод.

Быстрый вывод средств происходит следующим способом:

1. Элис хочет вывести средства в корневой блокчейн, но не хочет ждать. Она хочет заплатить срочную стоимость за это удобство. Ларри (поставщик ликвидности) желает оказать ей эту услугу. Элис и Ларри договариваются организовать вывод средств в корневой блокчейн. Блокчейн Plasma в данном случае не должен быть подверженным поведению византийского типа.

2. Средства фиксируются внутри контракта на определённом выходе в цепочке Plasma. Всё это происходит практически таким же способом, как и при обычном переводе, то есть обе стороны передают транзакцию, а затем берут обязательства в том, что видели эту транзакцию в блоке Plasma. Условия этого контракта заключаются в том, что если контракт передаётся на корневой блокчейн и там завершается, тогда платёж пройдёт через цепочку Plasma. Если нет возможности предоставить доказательство транзакции, Элис может вернуть средства. Также представляется возможным сконструировать эту схему как HTLC и Элис будет необходимо сгенерировать прообраз и выпускать его только тогда, когда она посчитает нужным, и когда средства будут переведены.

3. После того, как верхний блок Plasma будет завершён и Ларри уверен, что он может вывести средства в случае соблюдения условий контракта, он создаёт ончейн контракт, который способен совершить платёж в пользу Элис с указанным объёмом средств (чем меньше объём, который он получит, тем меньше будет составлять комиссия за эту услугу).

В нашем примере поставщик ликвидности Ларри должен работать в режиме реального времени и полностью подтверждать блокчейн Plasma перед принятием этого обмена. Если Ларри неспособен полностью подтвердить цепочку Plasma (или если он не видел доказательства обмана смарт-контракта, утверждённые в корневой цепочке), ему не следует проводить вывод средств. Если Ларри не хочет, чтобы средства попали в эту цепочку, а желает перенаправить их в блокчейн, то он может инициировать вывод после завершения этой операции или же провести атомный обмен, как непосредственную часть вывода средств.

Во многих случаях может быть гораздо выгодным совершать переводы между блокчейнами Plasma с оговоренной нетто-стоимостью с поставщиками ликвидности. Переводы могут осуществляться между цепочками Plasma с помощью Lightning или атомных обменов, которые позволяют быстро достичь завершения.

Поскольку это атомный межчейновый обмен, Элис и Ларри не предоставляют друг другу расписок по средствам. Средства Элис находятся на корневой/родительской цепочке, а Ларри сможет получить полный доступ к корневой/родительской цепочке немного позднее. Принимая во внимание низкозатратную доступность блока и завершённое невизантийское поведение корневого блокчейна, Ларри может быть точно уверен, что получит свои средства, даже если он не доверяет самому блокчейну Plasma.

5.7 Неблагоприятный массовый вывод средств

В то время как неблагоприятная массовая транзакция существует в пределах системы Plasma, для протокола она не требуется, её архитектура в первую очередь предназначена для поддержания экономической стабильности состояния (низкий газ/комиссия) в случае удержания блоков. Если пользователь желает использовать состояние счёта внутри цепочки Plasma, тогда ему необходимо положиться на иные архитектуры, а также на иерархию платежей. Вдобавок, заметьте, что здесь используется модель UTXO, но эта система лишь работает хорошо в случае, если корневая цепочка использует модель счёта. К тому же, если массовые выводы средств не являются необходимым или желаемым средством, то возможно использовать модель счёта для удержания средств в цепочке Plasma и позволять только простой вывод средств (с увеличивающимся числом последовательности).

Поскольку первичная задача архитектура Plasma связана с атаками, удерживающими блоки, целью которых является дискредитирование доказательств обмана (и других вопросов, связанных со снижением доступности данных), необходимо смягчить последствия эпизодов снижения доступности данных. Если пользователи на цепочке Plasma обнаружили недоступный блок, крайне важно, чтобы участники вышли из цепи к определённой дате. В случае, если участники не вышли из сети вовремя, результатом может быть то же самое, что и необсуждение некорректного вывода средств в Lightning. Этот механизм – ключ к корректному функционированию блокчейна Plasma. Plasma полагается на то, что если пользователи будут обнаруживать византийское поведение, заключающееся в удержании блоков, то сами же пользователи и будут ответственны за выход из блокчейна Plasma.

Логическая составляющая здесь заключается в том, что не представляется возможным обнаружить удержание блоков на корневом блокчейне (или пользователь сам поймёт, что никогда не получал блоки, или же цепочка Plasma сделает вывод, что пользователь отказывается принимать во внимание доступность блока и фальшивит) Как результат, платой за недоступность заявленного блока становится раскрытие текущего состояния ончейн (как так то, что делает Lightning) Однако для больших блоков и переходов состояния это может оказаться невероятно дорогостоящим выбором, и Plasma не использует эту конструкцию, поскольку неизвестно, кто отвечает за эти выплаты. Вместо этого Plasma предполагает, что если пользователь думает, что блокчейн Plasma удерживает блоки и может повлиять на способность проводить переходы состояний в будущем, тогда ему следует выйти из этой цепочки Plasma и присоединиться к другой как можно скорее.

Таким образом, массовый вывод средств считается негативным поскольку блок становится недоступным, конечно это при учёте того, что цепочка Plasma повреждена или подвержена византийскому поведению. Массовый выход гарантирует, что византийское поведение цепочки Plasma не влияет на средства пользователя больше, чем задержка времени или удержание цепи.

Считается, что в будущем будут использованы дополнительные смягчающие факторы безопасности со SNARK, но архитектура таких систем всё ещё остаётся открытым

вопросом. Эта конструкция не полагается на SNARK для вывода, считая, что на корневой цепи изредка наблюдаются поползновения наблюдателей. Однако, запуская состояния перехода внутри цепочки Plasma, можно свести к минимуму и подвергнуть воздействию защитных функций схемы SNARK способность атакующей или византийской Plasma совершать негативное удержание блоков для кражи средств у тех, кто не наблюдает периодически за цепочкой Plasma.
В этом случае потребуется доказательство SNARK для совершения переходов состояния и доказательно SNARK для проведения вывода средств, что позволит получить большую уверенность в переходах состояний. Однако Plasma не ставит своей задачей всецело полагаться на SNARK для правильного поведения перехода состояния, с учётом того, что пользователь наблюдает за цепочкой, а смарт-контракты корректно шифруют механизмы и могут выводить средства на корневом блокчейне. Схожие преимущества применимы и к Lightning Network, а именно то, что касается обеспечения корректного текущего состояния, запуская оффченовые состояния, только возможные в рекурсивных доказательствах SNARK, переданных третьей стороной на цепочки, поддерживающие смарт-контракты.

Цепочки Plasma можно обезопасить с помощью защиты на глубине схемы с помощью первой линии обороны с помощью элементов безопасности или оборудования, вторая линия - SNARK и STARK, а последняя линия обороны обеспечивает безопасность существуя в качестве интерактивной игры внутри внутри цепочки. Первую линию обороны можно прорвать, но вторая линия защитит систему баснописной криптографической схемой, в то время как последняя линия представляет из себя открытую прозрачную интерактивную игру. Изначально мы представляли Plasma, как систему, использующую последнюю линию обороны.

Массовое снятие средств достигается путём создания интерактивной игры, в которой выходы осуществляются следующим способом:

1. Элис договаривается с другими участниками цепочки Plasma совершить массовый выход. Несколько массовых выходов могут происходить одновременно, но у них не должно быть дублирующихся выводов средств. В случае, если таковые имеются, массовый выход по порядку обновит их балансы, и пользователь, создавший дубликат, будет оштрафован. Все стороны должны согласовывать действия, чтобы отправить свои средства непосредственно в другую цепочку Plasma.

2. Пэт, инициатор выхода, желает организовать этот выход. Пэт связывается с цепочкой Plasma назначения, чтобы отправить средства и обязывается автоматически распознавать средства, как доступные в новой цепочке, когда завершится массовый выход.

3. Пэт подтверждает цепочку Plasma вверх до точки доступности информации. Эта точка должна находиться между допустимым обсуждением и периодом завершения Plasma (отдельно от завершения корневого блокчейна) и в соответствии с условиями смарт-контракта. Пэт указывает журнал операций ожидающего местоположения участникам в новой цепочке Plasma. Пэт собирает подписи участников, желающих выйти (включая, как в нашем случае, Элис). Пэт подтверждает в блокчейне, что все

участники имеют право выхода вплоть до самой высокой точки доступности данных. Пэт создаёт транзакцию выхода с массивным залогом (как утверждено в смарт-контракте корневого блокчейна). Пэт также может взять комиссию с выходящих участников.

4. После скачивания всех подписей пользователи заново расписываются под массовым выводом. Это позволяет пользователям наверняка знать, что Пэт не будет оштрафован, и что операция готова к исполнению. Биты пользователей, не подавших вторичную подпись, включены не будут.

5. Затем Пэт наблюдает, не совершались ли ещё какие-либо транзакции выхода и удаляет дубликаты в случае необходимости, затем подписывает транзакцию выхода и передаёт её на корневой блокчейн или родительскую Plasma цепочку. В случае наличия дубликатов родительские цепочки расставляют приоритеты (вверх до корневого блокчейна, как до высшего приоритета). Более ранние транзакции составляют больший приоритет. На момент передачи транзакции инициации массового выхода (MEIT), Пэт оставляет залог, подтверждающий правильность его информации: проверенности блоков, установки UTXO на высоте блока, незавершённость, а также планирование битовой карты с древовидным хешированием Меркл в UTXO, обязательства счёта (в сумме древа Меркл для скоростных доказательств). Подписи Элис и остальных пользователей доступны до момента запроса. Являясь одним из частников MEIT, Пэт публикует полную битовую карту выходного состояния. Таким образом и другие участники, наблюдающие за корневыми/родительскими цепочками, способны подтвердить, откуда осуществляется выход и вмешаться, если данные некорректны. Завершение транзакции инициации массового выхода требует довольно долгого времени и может занять несколько недель, поскольку MEIT это транзакция, служащая крайней мерой (но этот процесс можно будет ускорить в будущем после интеграции SNARK).

6. В случае наличия дублирующих выводов Пэт может обновить битовую карту и баланс будет выведен после небольшого периода отсрочки.

7. Любой из участников сети может вмешаться в данные MEIT со своей обсуждаемой транзакцией массового выхода. Однако, поскольку Пэт не может знать, заменит ли блок выход в будущем, он не может быть оштрафован, если транзакция была потрачена на будущий блок (но пользователя могут за это оштрафовать). Если предоставлено возражение, тогда средства блокируются, пока не закончится дискурс. Вмешательства должны возникать во время начала периода отсрочки, и, если возражение небеспочвенно, тогда Пэт должен обновить баланс, который предстоит вывести.

8. Если возражений не возникает, то после утверждённого периода завершения для MEIT пользователи получают свои средства.

Время окна завершения для цепочки Plasma – это время, в которое пользователю необходимо хотя бы периодически наблюдать за цепочкой. После закрытия окна завершения считается, что для всех присутствует доступность данных блока блокчейна

Plasma.

Также, когда Пэт создаёт MEIT, он подтверждает корректные записи вверх до определённой высота блока Plasma, а также подтверждает факт того, что у него имеются подписи для вывода с каждым выходом. Пэт не штрафуется в случае двойной траты выхода после периода подтверждения (Пэт также не штрафуется за удерживание блока)

5.7.1 Обсуждение массового вывода: возражение против некорректного вывода

В случае, если пользователь (такой как Элис) замечает, что Пэт пытается провести массовый вывод без её разрешения, она может вмешаться в процесс вывода, создав возражение.

1. Элис видит, что Пэт пытается провести массовый вывод через один из её выходов в блокчейне Plasma. Элис передаёт возражение с массивным залогом. Этот бонд гарантирует тот факт, что возражение не будет оставлено. Она передаёт его в блокчейн.

2. Если возражение не обсуждается в течение определённого периода времени, то Элис получает свой залог обратно, а MEIT отменяется целиком. Если же возражение подвергается дискуссии, а Пэт или любая другая сторона создаёт доказательство обмана для её возражения о некорректном выводе, тогда MEIT продолжает свой процесс, а залог Элис сгорает.

Участники должны быть уверены, что их подписи доступны для доказательства, поскольку в MEIT есть вторая фаза (шаг 4), так что у них имеется достаточная информация для обсуждения возражения, особенно, если это возражение носит мошеннический характер. Стимуляторы работают против создания возражений мошеннического характера, поскольку такие возражения будут исключены, учитывая доступность блоков и отсутствие цензуры в корневой цепочке.

5.7.2 Обсуждаемая транзакция массового выхода.

В случае, если выход был потрачен при MEIT в более дальнем блоке, Пэт может об этом не знать, поэтому его нельзя оштрафовать, поскольку нельзя доказать удержание блока.

Может существовать несколько обсуждений, которые подвергают сомнению похожие битовые карты, но к ним всем должны прилагаться крупные залоги.

Любой участник может подать битовую карту/разброс тратимости с помощью большого залога. Большой залог – это подтверждение того, что коин был потрачен в более дальнем блоке, с обязательством к заголовку блока.

Однако, это обсуждение нельзя доказать компактно, поэтому требуется как минимум ещё одно повторное возражение, для того, чтобы выпустить возражение по поводу подвергаемой сомнению транзакции массового выхода (CDMET)

Возражение в этом обсуждении выглядит следующим образом:

1. Элис замечает, как кто-то (напр. оператор цепочки, выполняющей удержание блока) пытается воспрепятствовать её массовому выходу, в котором она участвует. Она направляет возражение в это обсуждение с большим залогом, подтверждающим факт того, что инициатор обсуждения не может предложить корректных расходов.

   Инициатор обсуждения должен ответить на возражение в течение периода времени. Если инициатор не способен предоставить доказательство расходов, а, проще говоря, подпись следующей транзакции, тогда Элис оправдывается и всё обсуждение удаляется (вот почему разрешаются дублирующие обсуждения). Если инициатор может доказать факт траты коина, Элис теряет свой залог и обсуждение продолжается.

5.8 Переработка UTXO

После того, как выход был завершён, возможно заново использовать битовую карту UTXO для компактности.

5.9 Заключение

В результате этой игры с массовым выводом средств возможно совершить массовый вывод, который потребит 1-2 бита информации за вывод при самом оптимистичном сценарии для многих выходящих участников.

Массовые выходы – это нечто, что является необходимой вещью при удержании блоков. Однако, этот процесс может быть крайне дорогостоящим. Именно поэтому нам могут потребоваться альтернативные стратегии, которые не зависят от перегрузки корневой цепочки.

Эта конструкция позволяет многим участникам удерживать свои средства в дочерних блокчейнах, аннулирование состояния происходит в помощью доказательства обмана в случае, если доступна информация блока, могут проводиться переходы состояний (т.е. платежи), возможен вывод средств, а массовые выходы (хоть и с некоторой задержкой) возможны и при удержании блока.

6 Блокчейны внутри блокчейнов

Как мы и описывали ранее, Plasma в своём естестве создает метод для выполнения масштабируемых вычислений, однако нам также необходимо справляться с проблемами, такими как удержание блоков для создания доказательств обмана или доступность блокового пространства. Решением для удержания блоков в Plasma является создание системы, в которой пользователи могут инициировать массовые выходы в случае удержания цепочки или удержания блока Plasma.

Однако транзакция массового вывода в блокчейне может быть очень дорогостоящей, особенно если набор UTXO достаточно велик, и также требуется отправка битовой карты.

К тому же использование одного выхода может быть более желаемым решением. Транзакции массового выхода требуют сложных интерактивных игр, включающих многих участников. Этот процесс можно использовать только лишь как самую крайнюю меру.

Вместо этого мы создаём систему судов более высокой и низкой инстанций, где могут существовать отдельные площадки для доказательства состояния. Можно рассматривать корневой блокчейн как суд высшей инстанции, из которого все подчиняющиеся суды черпают свою власть. Именно закон корневого блокчейна, позволяет всем нижестоящим судам почерпать свою законную власть. Это позволяет масштабировать площадки, пользователям необходимо обращаться в суды высшей инстанции для более представительной площадки лишь в случае, если состояние более низкого суда подвергается сомнению или приостанавливается. Передача подтверждений состояния в высших судах всегда возможна, но стоит дороже.

Все состояния проходят древовидное хеширование Меркла и отправляются в корневой блокчейн. При самом оптимистичном сценарии заголовки блоков отправляются в прямую родительскую цепочку, а родительская цепочка отправляется к своему родителю и так далее, пока движение не достигнет корневой цепочки. Внутри заголовка есть обязательство по Мерклу к блокам, которые были замечены у родителей.

Транзакции можно передавать в цепочку Plasma и любую родительскую цепочку Plasma, а также и в корневой блокчейн. Целью этой меры является обеспечение взаимозаменяемости и противодействия цензуре. К тому же в случае удержания блока и нераскрытия его движения, у пользователя всё равно будет возможность снять средства.

Как только обязательство по блоку отправляется, ему требуется подождать, пока закончится определённый период подтверждений, отражаемых в корневом блокчейне перед подтверждением. В течение этого времени доказательства обмана могут передаваться в корневой блокчейн или в любую посредническую цепочку Plasma (которая затем отправляется в корневую цепочку через корень блока)

Каждая индивидуальная цепочка Plasma исполняет машину состояний, которая собирает обязательства в блок Plasma. Отдельно взятая цепочка Plasma может или не может иметь возможность вникнуть в детали дочерних цепочек Plasma. Вместо этого у них есть подтверждённый баланс значения цепочки Plasma. Когда дочерняя цепочка Plasma обновляет своё состояние, она отправляет хэш заголовка своего блока в любую из родительских цепочек Plasma или в корневой блокчейн.

Это означает, что состояние определённых блоков можно отправлять в несколько родительских цепочек одновременно. В случае наличия дубликата он может и не иметь сбоя (но может быть оштрафован по определённым правилам консенсуса в зависимости от приложения). С другой стороны, если существует двухсмысленность в состоянии, напр. состояние отправленное родителю 1 отличается от родителя 2, это значит, что вносители залогов в Plasma цепочку потеряют внесённые средства.

Новые обновления состояния дочернего элемента могут производиться с использованием следующих устройств электронного входа в своём сообщении обновления состояния: выплачиваемая комиссия (и обозначение), запускаемый корневой блокхэш,

предыдущий блокхэш, принимающий родительский блокхэш, доказательство внесения и доказательство вывода средств.

В какой бы родительский блокчейн ни отправлялись бы данные, дочерняя цепочка должна видеть всё до этой точки, рекурсивно включая всех родителей над этой точкой. Это нужно для того, чтобы доказать, что он не допустит двусмысленности и двойной траты транзакций (и в случае наличия двусмысленности раскроет путь к дочерней цепочке для её устранения)

В случае появления двусмысленности родительская цепочка должна всегда соблюдать приоритет. Стимуляторы создаются для раскрытия двусмысленности любой стороной, которой о них известно.

Внесение и вывод средств возможны на обеих родительских цепочках, так же, как и на корневом блокчейне.

Выводы так же возможны между цепочками Plasma, учитывая, что присутствует достаточная ликвидность и другая сторона желает перенести средства куда-то либо ещё.

Если пользователь желает удались записи с использованием главного блокчейна, то возможно необходимо построить HTLC между цепочками, которые выглядят как ончейн платежи Lightning.

Все доказательства обмана должны предоставлять доказательства древовидного хеширования Меркл для обязательств цепочки. Фальшивые доказательства дискредитируют определённую цепочку Plasma, которая отвечает за мошеннический блок.

Главнейшая сложность в архитектуре – это представление состояния транзакции, отправляемое по нескольким родительским цепочкам в интересах борьбы с цензурой. Ранние циклы могут предположить, что переходы/транзакции состояний лишь могут проводиться в индивидуальной цепочке Plasma, и что единственное взаимодействие с другими цепочками – это передаваемое сообщение, переходящее к родителю/дочернему элементу и внесение/вывод средств. Таким образом, самая главная сложность это только доказательства, относящиеся к внесению и выводу средств.

Обязательства к данным считаются частью доказательств включения.

6.1 Получение средств внутри цепочки

В этой иерархической системе блокчейнов в блокчейнах получение средств от другого пользователя выглядит как следующий процесс (если Элис хочет отправить средства Бобу в цепочке Plasma третьего уровня глубины):

1. Элис связывается с Бобом касательно средств, которые она хотела ему отправить. Элис раскрывает Бобу цепочку Plasma, в которой Боб получит средства. Боб решает, получать ли платёж, а важнее всего то, что он должен убедиться, что смарт-контракт в корневом блокчейне – именно тот, в котором он хотел получить платёж (следует проверить коды/механизмы смарт-контракта, а также приемлемые задержки выхода консенсуса)

2. Если платёж всех устраивает, они ставят предварительные подписи на положении, утверждающем условия платежа, во многих случаях это будет доказательство платежа путём включения блока в блокчейн с достаточно долгим существованием, однако в некоторых случаях это может быть хэш pay-to-contract. Это не происходит ончейн, а лишь едва для того, чтобы прикрепить условия соглашения для предоставления остальным.

3. Элис совершает платёж внутри цепочки Plasma. Блок подписывается валидаторами и обязательство заголовку блока отправляется в родительские блоки. Обязательства по Мерклу в дочерние цепочки Plasma включены в каждый родительский блок и затем в конце концов включены в корневой блокчейн.

4. Боб полностью синхронизируется с корневым блокчейном, а затем подтверждает цепочку, в которую должны прийти средства и любого её родителя. Бобу нет нужды подтверждать другие цепочки Plasma, в которые не попадают его средства. В худшем случае Боб может полностью подтвердить, что Элис провела платёж в Plasma цепочке с достаточно долгим существованием. Однако, если оба желают быстрого завершения, Элис может подписаться под подтверждением заполнения платежа в новый блок (см. предыдущее высказывание касательно получения платежей внутри цепочки Plasma). Если Элис желает подписаться под платежом и Боба это устраивает (так как он может подтвердить вывод средств), тогда считается, что достигнуто завершение. Боб теперь может вывести средства из этой цепочки Plasma.

Ключевой аспект архитектуры заключается в том, что пользователь полностью отвечает за подтверждение дочерних блокчейнов. Если Боб не подтвердит цепочку Plasma и всех родителей (в конце-концов периодически отправляется обязательство в корневую цепочку), тогда она не признаётся выполненной. Также, как и в констукции Lightning Network, Бобу не нужно думать о том, что происходит в других блокчейнах Plasma. Он лишь наблюдает за корректностью цепей, которые для него важны. Когда у него появляется возможность использовать коины, он уверен в том, что он может их потратить.

6.2 Получение средств из родительской цепочки

Получение средств из родительской цепочки похоже на внесение из корневого блокчейна, с единственной разницей в том, что получателю будет необходимо подтвердить все родительские цепочки Plasma (а не просто саму цепочку Plasma). Внесение средств в дочернюю цепочку Plasma происходит быстро.

6.3 От древа – в сеть

В то время как вышеуказанное описание применимо к одной родительской цепочке, для цепочек Plasma есть возможность наблюдать за несколькими корневыми блокчейнами. Это позволяет пользователю обновлять балансы с помощью дочерних цепочек. Следует, однако, уделить внимание, поскольку сбой в одном из родителей может не быть замечен всеми участниками сразу, а каскадные системные сбои нужно смягчать с помощью временных задержек и минимизации предположений кроссчейновой ликвидности. Создание наиболее правильной конструкции для этого – всё ещё насущная проблема.

6.4 Смягчение проблемы удержания блоков.

Создавая многие площадки, где пользователи могли бы передавать транзакции вывода, можно утверждать, что сегодня существует множество возможных площадок в которых можно выйти из удерживаемой цепочки или содержащей удерживаемые блоки. Если происходит сбой в дочерней цепочке, можно провести простой индивидуальный выход на родительских цепочках, даже если на корневой цепочке транзакции становятся слишком дорогостоящими.

Это позволяет пользователям иметь определённую толику уверенности в удержании выходов микроплатежей на цепочке Plasma, учитывая, что у них есть подтверждение того, что родительские цепочки Plasma функционируют должным образом. Эта цель является этому первопричиной, также как и смягчение удара каскадных сбоев.

Если пользователь удерживает достаточно большой баланс на выходе, ему не следует увлекаться перестраховкой, если нет значительного значения времени, однако, если у пользователя лишь один выход с низким значением (при котором уплата комиссии за транзакцию становится непосильной), ему стоит позаботиться о мерах предосторожности, а именно предусмотреть, доступна ли одна из родительских цепочек Plasma. В случае, если пользователь хотел бы большей уверенности, ему нужно пошерстить глубоко спрятанные цепочки с многими независимыми сторонами, исполняющими цепочку Plasma на каждом уровне. Тут конечно тоже могут появиться негативные побочные эффекты, однако если определённая цепочка Plasma будет заподозрена в византийском поведении, то всем будет необходимо совершить массовый вывод на новую цепочку. Если же имеется родитель, не имеющий византийского поведения, есть возможность продолжить работу и облегчить быстрые переходы в другую цепочку если родители отказываются обрабатывать обязательства византийской цепочки.

Конечно могут появиться сервисы, которые не делают ничего, кроме как обрабатывают транзакции в случае сбоя на дочерней цепочке. Оператор такого сервиса не должен делать ничего до того момента, как произойдёт сбой на дочерней цепочке (в точке, где он может быть достаточно неактивным, даже выключить серверы, пока не произойдёт сбой, заголовки блоков автоматически пропустят их чтобы передать на цепочку уровнем выше пассивного оператора) Мы полагаем, что многие выводы в родительских цепочках будут простыми, а не массовыми, поскольку родительская цепочка имеет невероятно высокий объём транзакций. (лимит размера блока/газа)

6.5 Выход

Массовые выходы возможны в родительскую цепочку или в корневую цепочку. Если дочерняя цепочка начинает действовать по принципам византийского поведения, то любое состояние в ней признаётся некорректным, так же, как и в цепочке Plasma без интегрированных друг в друга родительских цепочек. Похожим образом, массовые выходы – это быстрый способ выйти из византийской родительской цепочки. Возможно даже пропустить родительскую цепочку (или саму дочернюю цепочку) вплоть до её родителя или корневой цепочки.

В то время как может показаться, что в архитектуре содержится неясность, есть чёткое предопределение – если одна из цепочек заподозрена в византийском поведении, должны действовать все дочерние элементы. Существуют варианта оптимизации, которые позволяют выходам осуществляться без координации со стороны центрального узла (выходы по умолчанию без подписи переносятся на сторону пользователей, а цепочка Plasma сама создаёт обязательство о получении, но такая оптимизация требует значительной доработки)

Конструкция практически такая же, как и в простом выходе или массовом выходе, однако существуют незначительные изменения в архитектуре, направленные на поддержку интегрированных цепочек. Выходы могут дублироваться, но выходы на родительской цепочке всегда будут оставаться приоритетными. Если родительская цепочка начинает проявлять византийское поведение, тогда можно совершать выходы и на корневой цепочке. Цепочка обязана (если её идентифицируют, как византийскую) отражать и обновлять состояние продублированного выхода своей родительской/корневой цепочки и удалять этот выход в своей собственной цепочке. Однако, если она этого не сделает, средства пользователей окажутся в корневой цепочке.

Если родитель подвержен византийскому поведению, а дочерний элемент, удерживающий средства, функционирует корректно, то возможно избежать совершения транзакции массового выхода. Участники находят новую цепочку для перехода и совершают простой выход, при котором поставщик ликвидности получает средства в этой дочерней цепочке, а другие пользователи получают средства в новой цепочке (уже без византийского родителя). Целью этого шага является возможность быстрого переноса средств в новую цепочку и обеспечения быстрого выхода.

6.6 Масштабируемость

Эта функция позволяет масштабируемость битовой карты UTXO, в случае если карта становится слишком большой, пользователю лишь необходимо разбить её на множество дочерних цепочек. Считается, что для дочерних цепочек это представляется в качестве баланса счёта с данным значением высоты блока (и концов цепочек) вместо вывода средств. Схожим образом, для состояний, которые предпочитают использовать счета вместо UTXO, это также представляется возможным, считая, что пользователь желает совершить обмен только поддерживающих простых выводов.

Конечный результат этого процесса – это отличная масштабируемость, доступная пользователям. Им лишь необходимо наблюдать за цепочками Plasma, в которых удерживаются их средства (а также их родителями). Это эффективно разделяет набор данных в подтверждение, воздействующее на пользователя.

7 Plasma с защитой по методу “подтверждение доли”

Мы предлагаем простую конструкцию proof-of-stake. Это скорее всего не самая оптимальная конструкция proof-of-stake, однако она может отлично продемонстрировать, на может произойти в цепочках Plasma.

До сих пор мы полагали, что оператор цепочки Plasma – это одно лицо, ответственное за подпись блоков. Если создаётся некорректный блок, кто угодно, кто обладает данными блока, может создать доказательство обмана и откатить блок обратно, оштрафовав оператора. Это доказательство возможно, как только оператор поставит на блоке свою подпись. Передача обязательства древовидного хеширования Меркла в блок Plasma происходит в корневую цепочку (и так как высший родительский блок Plasma включает обязательства для обновлений состояния дочерних элементов), а корректное поведение обновлений состояния обеспечено упорядочиванием и залогами.

Однако во многих случаях желательно создать цепочку proof-of-stake вместе односторонней цепочки proof-of-authority (подтверждение полномочий). Это снижает риски, связанные с удержанием блоков (получается возможным получить лучшее от обоих слов, интегрируя цепочку в proof-of-authority одной стороны, или также представить её в качестве открытой многосторонней цепочки proof-of-stake) Обеспеченная токеном цепочка proof-of-stake также даёт держателям токенов стимул к корректной работе, поскольку потенциальная стоимость токенов снижается при наличии византийского поведения. Больше информации о потенциальной стоимости токенов будет предоставлено в следующем разделе.

Конструкцию proof-of-stake гораздо легче создать в Plasma, поскольку она всё ещё опирается на твёрдость нижележащего корневого блокчейна. Проблемы, связанные с удержанием, завершением и другими факторами дают толчок к усовершенствованию надёжности корневой цепочки. В своём лучшем состоянии Plasma будет так же безопасна, как и корневая цепочка. Если корневая цепочка исполняет proof-of-work (доказательство выполнения работы) тогда схема выглядит как proof-of-stake на proof-of-work (или Plasma на корневом блокчейне соответственно). Если корневой блокчейн – proof-of-stake, тогда конструкция выглядит, как proof-of-stake на proof-of-stake, однако механизмы proof-of-stake могут выглядеть проще или отличаться от того, который исполняется в корневом блокчейне.

7.1 Стимуляторы консенсуса Накамото

Мы пытаемся дублировать первичные стимуляторы консенсуса Накамото (доказательство майнинга). Один из самых важных стимуляторов, который необходимо дублировать – этот стимулятор, поощряющий распространение блоков другим майнерам.

Многие существующие механизмы proof-of-stake полагаются на выбор лидера, когда во время t_0 выбирается лидер, а во время t_1 у него есть право на создание блока. Это действие не повторяет стимуляторы консенсуса Накамото касательно распространения блоков. Консенсус Накамото предполагает выбор лидера, но этот выбор несколько вероятностен. Если пользователь находит блок, то он считает себя лидеров, но не уверен до конца. Кто-то другой мог майнить этот же блок в тот же самый момент. Лучший способ увеличить шансы лидера – это быстро передать блок настолько далеко, насколько это возможно, чтобы другие могли начать строиться на нём. Это создаёт стимуляторы для доступности информации.

Конструкции proof-of-stake в Plasma требуется нечто схожее.

Мы создали ситуации выбора, которыми хотим поощрить всех распространять свои

блоки настолько далеко, насколько это возможно. Могут тут быть и другие конструкции (особенно те, в которых существует сильная зависимость от случайного выбора и вероятностного выбора лидера с помощью размещения случайных множеств в определённые ветви и определение конца цепочек, как ветви с самым большим множеством)

7.2 Пример простого доказательства модели proof-of-stake

В то время, как это лишь простое предложение создать модель proof-of-stake, вероятно, оно явно не самое оптимальное. Целью является создать нечто простое, что может использоваться в Plasma.

Вместо создания механизмов запуска, наш подход заключается в простом создании стимуляторов для точной координации и корректного поведения (распространение блоков).

Комиссии расположены в корневом контракте и им же распространяются и выплачиваются в случае необходимости, но вся бухгалтерия происходит внутри самой цепочки.

Как часть контракта-ставки, размещённые средства игроков приписываются уполномоченному игроку. Он отвечает за действия от лица пользователя, и именно пользователя штрафуют, если игрок совершает недобросовестные действия. Ставки проводятся в течение отведённого времени (напр. 3 месяцев). Минимальное количество на одного игрока – один процент от всех токенов, с максимальным порогом в 5 процентов. Если требуется разместить более 5 процентов, то необходимо использовать несколько профилей (целью этого шага является увеличение распространения данных и уменьшение эффективности картелей меньше 51%)

Средства размещаются в зависимости от того, были ли последние 100 блоков Plasma представлены всем участникам. Например, если кто-то поставил на 3 процента игроков, у них должно быть 3 процента предыдущих 100 блоков. Если число оказывается больше, отдельный игрок не получает дополнительных вознаграждений за передачу дополнительных обязательств в блок. Если среди последних 100 блоков имеется меньше 3 процентов, то создатель текущего блока получает меньше вознаграждений. В корневой цепочке на блок можно разместить только один блок.

Это стимулирует всех участников согласовать свои действия и включать все блоки равномерно. Идея в том, что пользователям нет нужды создавать механизмы запуска, они ведь могут согласовать и исполнять какую-то схему (круговую) для обеспечения крупнейших вознаграждений.

Если они не получают максимальной транзакционной комиссии из-за некорректного количества блоков, средства располагаются в ячейке и выплачиваются в будущие блоки.

Результатом является экономическое стимулирование, которое мотивирует всех к участию.

Однако этот процесс ещё не завершён, мы ещё только мотивируем игроков к участию. В каждом блоке есть обязательство по Меркле для данных в различных частях блоков из

последних 100 блоков. Этот заставляет игрока иметь полные данные блока и постоянно заставляет создателя блока распространять его среди всех игроков.

Конец цепочки определяется наивысшей наградой, а если существуют параллельные ветви, тогда побеждает та, у которой есть наибольший объём комиссии за максимальную координацию.

Эта конструкция не разработана для того, чтобы остановить 51% атак, она существует для мотивирования пользователей распространять блоки (поскольку удержание блоков – не меньшая угроза). В дополнение, эта конструкция полагается на доступность информации и беспристрастность при включении блоков в корневую цепочку, ведь невозможно создать такой proof-of-stake на корневой цепочке из-за предположений о доступности данных и стимуляторов цензуры.

8 Экономические стимуляторы

С моделью подтверждения proof-of-stake возможно создавать стимуляторы, которые бы синхронизировались бы с корректным функционированием условий контрактов. В то время как доверительные гарантии обеспечивают точность по отношению к цепочке, нам необходимо создавать дальнейшие стимуляторы для доступности данных и дискредитации удержания блоков. Только разрешив ставки с использованием токена, характерного для цепочки Plasma, можно убедиться, что существует стимулятор для продолжения функционирования, поскольку стоимость токена определяется нетто-текущей/дисконтированной стоимостью всех будущих доходов от ставок. Следовательно, сбои сети снижают стоимость имеющихся токенов и отдельные игроки будут значительно мотивированы работать в интересах постоянно продолжающегося функционирования сети.

Операторы цепочек Plasma получают комиссию за передачу ончейн транзакций. Вычисление также может собирать комиссию для разных операторов и комиссия может каскадно спускаться вниз, особенно при сложных операциях. Пока существует стимулятор для дальнейших транзакций в дочерних цепочках на глубине, возможно создавать обязательства для передаваемых средств или для вычислений в дочерних цепочках, а в случае, если обязательство некорректно, данные блока становятся недействительными и неисполнимыми. Это не всегда необходимо, и во многих случаях пользователь может выбрать больше вычислений в дочерних цепочках с меньшей необходимостью для распространения комиссии вверх до родительских цепочек.

Для обновлений системы возможно создать другой контракт, который принимает этот же токен и объявить о периоде перехода (или же сообщество коллективно решит этот вопрос в децентрализованных системах)

Это может создать самоисполняемые системы. Тогда как есть необходимость платить за клауд-сервисы и управлять ими на хостах, которые предоставляют хранение и вычисление данных, теперь возникает возможность создавать набор смарт-контрактов (с доказательствами обмана), токен, и с достаточным количеством участников, уплачивающих комиссию система сможет функционировать сама с набором игроков,

которые будут корректно управлять сетью и вычислительной инфраструктурой, в самом деле осуществляя вычисления в бесформенном облаке.

8.1 Токены vs. Коины и экономическая безопасность

Эти доказательства обмана и залоги, хранящиеся в корневом блокчейне могут быть нативным токеном, напр. эфир (ETH) для Эфириума, или это может быть отдельный токен, определяющий правила консенсуса для нижележащего блокчейна.

На первый взгляд использование нативного токена корневого блокчейна выглядит проще простого, однако существуют интересные последствия для экономической безопасности.

Если целью стоит предотвратить удержание цепочки или некорректного поведения, в зависимости от применения блокчейна, тогда скорее всего не будет иметься достаточного количества стимуляторов для предотвращения некорректного поведения при использовании одного лишь ETH. Стоимость токена упадёт если в цепь удерживается или подвержена византийскому поведению. К тому же стоимость токена – это приблизительно чистая текущая стоимость будущей комиссии транзакции, которая может добавить токену ценности. Если ставить на ETH, то ставка происходит со значением, происходящим от значения времени залога, относящегося к получаемому объёму комиссии. Ожидается, что залоговое значение будет значительно ниже, чем нетто текущая/дисконтированная стоимость токена. Вдобавок, довольно сложно доказать и дискредитировать задержки цепочки и удержание блоков если залог оставляют в ETH и получают деньги обратно после периода ставок. Здесь не хватает стимуляторов, мотивирующих пользователей не действовать по византийскому типу, в то время как при работе с токенами стоимость токена будет снижаться при распространении случаев поведения византийского типа.

9 MapReduce для блокчейна

Практически всё, что вычислимо на MapReduce может также быть вычислено и на этой цепочке. Конечно это потребует глубокой реструктуризации нашего понимания вычислений и программирования на блокчейне. Это и есть MapReduce, но с доказательствами обмана. Каждый узел представляет собой блокчейн. Это прекрасно совместимо с древовидной структурой блокчейна Plasma, описанной в предыдущих разделах.

Если пользователь хочет выполнить стандартный счёт слов, то он может создать древо Меркла из цепочек, управляющих функцией уменьшения. Если имеется доказательство обмана, тогда узел, его выпустивший, штрафуется. Если вы можете создать функцию уменьшения на суммировании, тогда вы можете создать среднее арифметическое. Например средние цены и так далее. Функция карты лишь отправляет вычисления по индивидуальным цепочкам и затем принимает результаты. Очевидно существует препятствие, касающееся проводимых данных, вот почему требуются доказательства обмана уменьшения. Не видится возможным провести выборочное вычисление всех типов, но возможно решить многие проблемы; обычно проблемы памяти можно решить, запуская упорядочивающие алгоритмы, которые создадут компромиссы движения внутри цепочки Plasma.

Если узлы не могут произвести блоки для подтверждения вычислений, тогда их результаты дискредитируются и откатываются назад. Обратите внимание, что это не гарантирует вычислительной выборочности, которую осуществляет MapReduce (поскольку вам нужно наблюдать за цепочкой для соблюдения консенсуса), однако это даёт толчок началу деятельности и возможности масштабировать для игроков. Как результат, первичные ограничения заключаются в том, что стороны, которые затронуты определённым вычислением должны наблюдать за этим набором вычислений. Если требуется наблюдать лишь за малой частью, тогда всё в порядке, но если же необходимо наблюдать за всеми вычислениями, тогда масштабируемость здесь не будет столь полезной. Таким образом, многие проблемы можно быть решить именно таким способом, напр. децентрализованный обмен (ваш набор в карте сам наблюдает за вашими продажами, если все остальные запустили нетто-исполнение, вам не нужно думать о подробностях) и т.д.

Формат блока должен быть совместим с данными, которые могут быть вычислены в конструкции TrueBit. Здесь нет обязательств к состояниям (возможность создания UTXO TRIE, которое позволяет доказательствам переходов состояний включаться/исключаться), TRIE счёта (для дочерних цепочек и сложных переходов состояний), также обязательство по комиссии (древо, отправляющее переходы состояний по комиссиям), транзакции по Мерклу, обязательства по данным, передаваемым из родительских/дочерних блоков, обязательства по увиденным родительским/дочерним блокам (для предотвращения изменения порядка), а также любая другая бизнес-логика (напр. пример счёта слов будет иметь отсортированное обязательство по Мерклу к словам и точкам, где его видели). Создавая обязательства по Мерклу, можно создавать смарт-контракты, доказуемые на корневой или родительской цепочке, которые могут подтвердить некорректные переходы состояний. Есть несколько проблемных наборов, которые могут быть несовместимы с этим форматом, но подойдёт требование случайного вычисления без значительного количества памяти. Мысленной схемой для этого будет – относиться к максимальному объёму памяти для вычислений, как к эквиваленту максимального количества данных, допускаемых в доказательстве обмана.

Определённые функции карты и reduce позволяют блокчейну функционировать таким образом, что на нём существует обязательство по обработке данных. Это требует от родителя и дочерних элементов создания обязательства обработки. Дочерние элементы должны включать родителя, передающего данные, а иначе цепочка будет задержана. Родитель может запустить вычисление в дочерних элементах, и если дочерний элемент задерживается, запуск вычислений может произойти после передачи данных в родительскую цепочку и получения там доказательства. Первоочередной угрозой в конструкциях TrueBit является проблема удержания, необходимо быть начеку при продолжительной работе если дочерняя цепочка задерживается, даже несмотря на то, что это трудноосуществимая процедура, особенно со времени (наборы данных могут измениться и при временной последовательности становится сложнее разбираться с проблемами)

Составляя блокчейновое вычисление в системе MapReduce с дочерними цепочками,

есть возможность взять существующую компьютерную науку и напрямую применить её к наборам проблем распространяемых систем, которые существуют для блокчейнов. Возможно создать контракты Solidity, которые могут найти множество применений в бизнесе благодаря масштабируемости. Необходимо лишь провести вычисления и подтверждения для интересующего вида деятельности.

10 Примеры применения

Децентрализованные приложения (дапсы) могут быть реформированы, как проблема MapReduce с заложенным токеном экономическими стимуляторами для корректной деятельности.

10.1 Клон Reddit на блокчейне.

В первую очередь это касается хранения данных (CRUD). В первую очередь вычисления и доказательства вращаются вокруг контроля доступом, идентификации (голосование и посты) и модерации. Многие веб-приложения на самом деле просто делают CRUD с хвоста.

Корневой блокчейн содержит правила консенсуса смарт-контракта и доказательства обмана. Высший по цепи родитель содержит аккаунты подфорумов на reddit. Каждый субфорум – это дочерний блокчейн Plasma от самого высокого родителя. В каждом субфоруме есть цепочка постов Plasma. Дочерняя цепочка постов также содержит комментарии. Механизмы консенсуса поддерживают контроль доступа. Случайные обязательства данным предыдущих блоков (со случайными значениями, даваемыми родительской цепочкой) передаются на заголовок каждого блока. Функция reduce периодически вычисляется для топ-постов и другой статистики.

Компьютер отдельно взятого пользователя скачивает данные и ПО, подходящих под машинные форматы данных. Отправка данных требует уплаты комиссии за транзакцию для стимуляции включения данных, также может потребовать комиссию за скачивание данных старых блоков в зависимости от доступности.

Чтобы просмотреть определённый пост, пользователь подтверждает обязательство на корневой цепочке, затем идёт в конец цепочки к самому высокому родителю (обратно на какое-то количество блоков, чтобы попасть в период завершения, возможно длящийся около недели), находит TRIE аккаунта состояния для необходимого субфорума. Затем он подключается к сети DHT, чтобы найти узлы по субфоруму, скачивает конец цепочки (и какое-то количество блоков назад для подтверждения) субфорума и просматривает список постов, скачивает TRIE состояния, и как лёгкий клиент - также сырые данные необходимого поста с комментариями. Пользователям лишь необходимо наблюдать за цепочками Plasma, которые относятся к ним (только скачивать посты и субфорумы, относящиеся к ним).

Это простой пример хранения данных с некоторыми вычислениями в блокчейне. Возможно, что валидаторы могут полностью подтвердить все узлы, однако, также возможно их разделить. Как только разделение зашло слишком далеко, может возникнуть обеспокоенность доступностью информации. Отличным способом это исправить будет

предоставление полного контроля к дочерней цепочке владельцу субфорума reddit.

10.2 Децентрализованный обмен

Клон reddit в блокчейне, который делает очевидными последствия для CRUD веб-приложений, не получает больших преимуществ от операций MapReduce, за исключением статистики сайта.

Децентрализованный обмен показывает, что есть возможность обменять низкое время ожидания на высокую вычислительную мощность. Поскольку существует множество состояний, есть возможность того, что вместе UTXO в аккаунтах будут определены возможные выходы или же для каждого шага в машине состояний, так что более крупная битовая карта используется для представления каждого состояния вместо одного логического значения, представляющего объём расходов в битовой карте.

Почти так же, как и в случае с reddit, существует дерево дочерних цепочек, представляющее торговую пару. В каждой будет дерево цепочек для увеличения масштабируемости (для пар с низкой активностью возможна только одна цепочка Plasma, но для цепочек с высокой активностью возможно наличие большего числа дочерних элементов) Каждая из этих цепочек имеет залоговую активность и количество, которое может быть передано за раз ограничивается объёмом залога.

Первым шагом будет наличие балансов в дочерней цепочке, так что это будто бы платёжная цепочка Plasma в основании.

Затем заказы поступают непосредственно в дочернюю цепочку. Как часть обязательства к родителю, все заказы объединяются в обязательство древовидного хеширования Меркл одного журнала заказов, представленного в качестве одного заказа в самой цепочке. Этот шаг рекурсивно уменьшает все журналы заказов дочерних элементов до единого журнала заказов, представляемого этой цепью, пока он не достигнет высшего родителя в цепочке Plasma. После того, как заказы получены, окно заказов закрывается и торговля завершается по принципу группы.

После этого завершается шаг reduce и передаётся в корневой блокчейн, а индивидуальным цепочкам сообщается об их расположении с помощью шага map. Родитель передаёт дочернему элементу расположение заказов в обусловленном порядке. Учитывая, что дочерний элемент мог видеть другие заказы (что подразумевает, что он может наблюдать за родительской цепочкой во время этого шага), они смогут доказать корректное выполнение расположения на этом шаге map. После получения расположения, шаг map продолжается рекурсивно по отношению к дочерним элементам это цепочки.

По завершению этого процесса совершается последний шаг reduce путём передачи всех обновлений по средствам в блок и затем передачу заголовка блока родителю.

Конечно, требуются дальнейшая оптимизация, позволяющая несколько циклов MapReduce в случае значительных изменений цены (позволяя сохранять высокую точность цен), однако эта общая конструкция требует невероятно высокого объёма. Теоретически возможно проводить всю мировую торговлю через эту сеть с компромиссами по скорости

путём превращения её в биржу исполнения пакетов данных, полностью обязавшуюся и гарантированную корневым блокчейном.

Такой тип конструкции подходит для многих типов финансовой деятельности и вычислений.

10.3 Децентрализованная почта (D-Mail)

Чтобы создать D-Mail, необходимо представить свой аккаунт в цепочке Plasma и запросить платёж, чтобы получить почту (вставить сообщение в цепочку). Все отправления зашифрованы одним публичным ключом. Запуск возможен для того, чтобы убедиться, что выполняются платежи неизвестными лицами, также возможна дальнейшая оптимизация с использованием zk-SNARK. Родительская цепочка содержит директорию цепочек и запускает платёж. Всё очень просто.

10.4 Децентрализованная сеть доставки содержимого (CDN)

Есть возможность создать децентрализованный CDN. Это схожая с разделением Эфириума конструкция. Относиться к каждому дочернему блокчейну, как к разделу. Иметь навигационный знак (это может быть корневой блокхэш или что-то ещё). Перемешать данные между разделами через сколько-то блоков. Родительские цепочки отвечают за обязательства к перемешиванию. Другие могут неспешно вести архив. Объявляется потеря данных и те, кто держит архив, получают вознаграждение. Стимулируется распространение, поскольку пользователи получают вознаграждение только в том случае, если данные имеются в другом разделе. Прочность конструкции зависит от требования длины потока, чем выше прочность, тем больше разделов должны иметь копию в любое время. Ключевой момент здесь в том, что у хранилища есть функция пропускной способности. Данные не рассматриваются, как стационарные данные на диске. Все данные находятся в потоке и движении к их следующему направлению, надо заметить, очень даосистский подход.

Чтобы скачать данные, пользователю нужно подтвердить раздел родительской цепочки и случайный навигационный знак, чтобы знать, какие разделы содержат данные, затем подключиться к ней через DHT, определяя пиров и скачивая данные.

10.5 Приватные цепочки

Участников никто не заставляет раскрывать данные цепочек другим участникам (хотя и ничто не останавливает их от публичности). Как результат, при желании участники цепочки могут создать сеть приватных блокчейнов, управляемых корневой цепочкой. Это подобно разделению Интернет/Интранет. Транзакции будут проводиться в местной приватной цепочке, но также и связываться и иметь финансовую активность, гарантированную публичной цепочкой.

11 Атаки, риски и смягчение

11.1 Код смарт-контракта

. Написать код для хорошего смарт-контракта непросто. Безопасность будет целиком зависеть от корректного исполнения доказательств обмана. Возможно, что некоторые доказательства обмана не будут включены, а некорректные переходы состояний смогут подтвердиться в корневой цепочке.

11.2 Закрытие транзакции в главной цепочке – слишком дорогая процедура

Существует риск, при котором транзакция может быть закрыта в главной цепочке, но это совершенно экономически неоправданный шаг. Это может создать жульнические схемы выхода, в которых мошенники могут координировать большой объём малых значений и добавлять его к большому значению.

Этого можно избежать, имея предоставление выхода, сортируя все транзакции по предоставлению выхода и предоставляя выход из целой цепочки сразу после периода обсуждения. Это также позволяет наблюдателю третьей стороны наблюдать от чьего-то лица. Однако эта конструкция значительно всё усложняет. Эти заранее подписанные объединённые транзакции могут распространяться в другие родительские сети в зависимости от того, в какой части цепи происходит сбой, в конце-концов даже в корневой сети. Однако этот процесс полагается на то, что стороны будут вести себя корректно, вот почему пользователям стоит объединять все непотраченные платежи в один выход или серию выходов, при которые выходящие транзакции будут экономически обоснованными.

К тому же есть возможность оставлять миктоплатежи в цепочках, которые гарантируются дорогостоящим токеном, и перемещаться с этим значением (поскольку есть демотивация от полного уничтожения цепочки Plasma)

Если обобщённые рекурсивные SNARK/STARK становятся оправданными, теоретически можно ограничить неавторизованный выход выводящему пользователю, даже с удерживаемыми блоками.

11.3 Завершение

Это окно обсуждения для выхода на самом деле создаёт предположения для завершения. Если в нижележащей цепочке имеются значительные залоговые ресурсы на реорганизацию, чтобы принудительно начать завершение, тогда это может значительно снизить риски, касающиеся реорганизации глубоких цепочек, создавая недостаток синхронности между цепочками. Примером смягчения отрицательных последствий является запланированный гаджет завершения Эфириум CASPER.

11.4 Недостаток мощности корневой цепочки или увеличение расходов

Без смягчающих мероприятий в случае если комиссионные или газ повысятся в цене слишком сильно, не будет возможности выйти из транзакции в течение определённого периода времени. Напр. если комиссия транзакции или газа увеличится в 50 раз или если не будет достаточно места для выходящих транзакций и майнеры не будут увеличивать мощность или лимит газа.

Существует несколько видов смягчающих шагов задержки выхода, а именно приостановка механизма счёта выхода, который производит выходы надлежащим образом. Это можно сделать, приостанавливая выходы так долго, чтобы появилась транзакция выхода из последнего числа блоков. Это позволит всем выйти вовремя с учётом того, что недавно осуществилась как минимум одна транзакция выхода. Если выход происходит перед выходом пользователя, то счётчик обнуляется. Результатом будет неопределённость ожидания перед получением средств обратно, что увеличивает расценки на расходы на поставщиков ликвидности. Простой механизм мог бы просто приостанавливать часы во время вывода, если среднестатические расценки газа/комиссии в блокчейне находятся на высокой отметке (ограничиваемые резонной верхней границей времени, в течение которой может существовать эта пауза)

Пользователи удерживающие средства должны убедиться, что как минимум у одного родительского блокчейна Plasma есть высокий уровень уверенности касательно доступности информации (в идеале несколько независимых родителей)

11.5 Root Chain Censorship Цензура корневой цепочки

Архитектура предполагает, что около 51% корневой цепочки являются честными. Если участники в корневой цепочке сговариваются атаковать сеть цензурируемыми блоками, могут возникнуть серьёзные трудности при проведении транзакций выхода или обновлений состояния, потенциально приводя к потере значительных средств. Цензура – первоочередный фактор безопасности и оценки рисковой стоимости и её, также, как и уловки завершения (например CASPER) будет необходимо ограничить в будущих цепочках.

Этого можно избежать, добавив в zk-SNARK/zk-SNARK доказательства наличия средств, но потребует новых исследований и программирования.

Использование огромных залогов как части каждой выходящей транзакции поощряет доказательства обмана, поскольку майнеры скорее всего будут вознаграждены значительным количеством от этих доказательств обмана и цензура будет дискредитирована.

Безопасность, позволяемая для этой сети – это функция честности и корректности родительских цепочек Plasma, корневого блокчейна и размера баланса.

Системные ограничения глобального масштаба на переводимые объёмы (ограниченая скорости на выходах из блока) и обеспечение более низкого его объёма, чем на CASPER может также быть одним из вероятных смягчающих механизмов

11.6 Задержка цепи

Если цепочка останавливается, то после определённого периода времени может получить предложение о переходе состояния. Поглощающая цепочка, получающая контроль над транзакциями может передавать подтверждение и затем вся цепочка сдвигается. Это разрешается только после того, как цепь (игнорирующая передачу транзакций на родителях) не движется вперёд в течение определённого периода времени.

Доказательства обмана могут воспрепятствовать воплощению кончику цепочки.

Может существовать и большая стимуляция для остановки цепочки для финансовой деятельности, включающей в себя сложные переходы состояний.

11.7 Невозможность изменить правила консенсуса.

Поскольку архитектура фронтального типа, не видится возможным поменять правила консенсуса без предварительного программирования этой способности. Можно этого избежать путём создания путей обновления, как части системы (например ручная остановка после определённой даты) Невозможность это сделать также имеет социальные последствия касательно невозможности остановить цепочки, поскольку у держателей токенов есть стимул к постоянному движению системы, поэтому остановить цепочку Plasma после запуска будет довольно сложно.

12 Будущие исследования

Существуют дополнительные области для будущих исследований, включая преимущества для безопасности цепочек. Текущая область исследований – это обобщённые рекурсивные SNARK/STARK, которые могли бы значительно увеличить безопасность выходных транзакций. Конечно было бы замечательно иметь защиту в глубине структуры, поскольку последняя линия обороны была бы прямым децентрализованным механизмом выхода, дозволяющим обсуждаемые доказательства, а первые линии обороны были бы продвинутая криптография и оборудование для защиты. Дальнейшие разработки для инновационной защиты –криптографии или гомоморфного шифрования также были бы крайне полезны.

Требуется более продвинутая стратегия по разработке способности наблюдать за несколькими корневыми цепочками одновременно, оставаясь синхронизированным (за пределами ручного запуска синхронизации)

Также необходимы будущие исследования касательно завершения и его работы сразу с несколькими цепочками, а также минимизации рисков выхода на блокчейне (тут тоже могут помощь SNARK/STARK)

13 Заключение и обобщение

Plasma – это архитектура с первичным фокусом на обеспечение доступности информации (особенно в свете удерживающих блок атак) со сжатием данных.

Мы предлагаем механизм, в котором пользователи могли бы передавать исполняемые обязательства, позволяющие им держать средства в блокчейне, состояние которого контролируется корневым блокчейном.

Это позволяет значительно увеличить вычисления и хранилища по широкой бесформенной сети компьютеров. Деятельность связана экономическими игроками, выполняющими обязательства, которые в конце концов выполнимы на всех родительских цепочках и потоках, идущих в корневой блокчейн, который содержит смарт-контракт с

истиной. Эта конструкция позволяет пользователям совершать переходы состояний, которые иначе не были бы эффективными в корневой цепочке.

Из этой конструкции для блокчейна также возможна обработка обязательств почта на всех финансовых вычислений в мире (если это не занимает слишком много исполнительной памяти одновременно) Доказательства используются только в случае неверных вычислений и тогда обязательства откатываются обратно. Операторам в цепочке не требуется доверительный фонд работы.

Для уменьшения стимуляторов, касающихся остановки цепочки и другого византийского поведения, комиссионные создают новые стимуляторы для цепочки, поддерживающие работу. Остановка дискредитируется, если на цепочке Plasma есть деятельность с токеном, характерным для этой цепочки. Если цепь останавливается, её стоимость снижается, что создаёт дополнительный стимул для постоянной работы.

Этот стимулятор и архитектура позволяют создавать дапсы, которые постоянно работают, существуя за счёт комиссий за транзакции. Эти дапсы могут создать клаудную систему, в которой данные постоянно обрабатываются и подтверждаются, но члены которой постоянно меняются и не имеют чётких очертаний. Plasma позволяет блокчейнам поднимать масштаб, чтобы помогать обобщённым приложениям для числа пользователей без каких-либо ограничений. Создатель приложения может просто написать код смарт-контракта, затем отправить код в блокчейн, а стимуляторы будут продолжать исполнять вычисления этих контрактов, так долго, как люди платят комиссионные в цепочке Plasma.

14 Благодарность

Большое спасибо авторам TrueBit за архитектуру и воплощение доказательств по Мерклу, включая Кристиана Райтвиснера. Спасибо Влад Зам за вдохновение и его помощь в формулировке и формализации идей. Спасибо Томасу Греко, Петру Добашевски и Паве и Перегуд за помощь и поддержку.

СДЕЛАТЬ: Объявить ещё больше благодарности
СДЕЛАТЬ: Улучшить библиографию
СДЕЛАТЬ: Закончить таблицы и диаграммы

Список литературы

1. [1] Джозеф Пун и Тэдж Дрейджа. Lightning Network.https://lightning.network/lightning-network-paper.pdf, Март 2015.
2. [2] Эфириум. Эфириум. https://ethereum.org.
3. [3] Гэвин Вуд. ЭФИРИУМ: ПЛАТФОРМА ДЛЯ СОЗДАНИЯ ОНЛАЙН СЕРВИСОВ НА БАЗЕ БЛОКЧЕЙНА http://gavwood.com/paper.pdf, Февраль 2015.
4. [4] Райден. Сеть Райдена. https://raiden.network/.
5. [5] Джеффри Дин и Санджай Гемават. MapReduce: упрощенная обработка данных

на больших кластерах. В OSDI, стр. 137–150. Ассоциация USENIX, 2004.

6. [6] Сатоши Накамото. Биткойн: электронная денежная система одноранговой сети. https:// bitcoin.org/bitcoin.pdf, Октябрь 2008.

7. [7] Ник Сабо. Формализация и защита отношений в публичных сетях. http:// szabo.best.vwh.net/formalize.html, Сентябрь 1997.

8. [8] Fred Erhsam. Блокчейн Токенса и рассвет децентрализованной бизнес-модели. https://blog.coinbase.com/ app-coins-and-the-dawn-of-the-decentralized-business-model-8b8c951e734f.

9. [9] Нэйвэл Равикант. Модель биткойнов для краудфандинга https://startupboy.com/ 2014/03/09/the-bitcoin-model-for-crowdfunding/.

10. [10] Джейсон Теутш и Кристиан Рейтвисснер. Масштабируемое решение для проверки блокчейна. https://people.cs.uchicago.edu/~teutsch/papers/truebit.pdf, Март 2017.

[11] Виталик Бутерин. Часто задаваемые вопросы об Эфириуме. https://github.com/ethereum/wiki/ wiki/Sharding-FAQ.

1. [12] Адам Бэк, Мэт Коралло, Люк Дашир, Марк Фриденбах, Грегори Максвэл, Эндрю Миллер, Эндрю Поэлстра, Джорж Тимн и Питер Вюлле. Введение блокчейновых инноваций и фиксированные сайдчейны https://blockstream.com/sidechains.pdf, Октябрь 2014.

2. [13] Пол Шторц. Драйвчейн http://www.truthcoin.info/ blog/drivechain/.

3. [14]Биткойн-Wiki. Объединенная спецификация добычи. https://en.bitcoin.it/wiki/Merged_ mining_specification.

4. [15] Питер Тодд. Тричейн https://github.com/petertodd/tree-chains-paper.

5. [16] Илай Бен-Сассон, Алессандро Кьеза, Эран Тромер и Мардас Вирза.Неинтерактивное нулевое разглашение для архитектуры фон Ньюмана. https://eprint.iacr. org/2013/879.pdf, Май 2015.

6. [17] Алессандро Кьеза, Эран Тромер и Мадарс Вирза .Кластерное программирование в нулевом разглашении https://eprint.iacr.org/2015/377.pdf, Апрель 2015.

7. [18] Джей Квон. Cosmos: сеть распределенных регистров https://github.com/cosmos/ cosmos/blob/master/WHITEPAPER.md, Сентябрь 2016.

8. [19] Гэвин Вуд. POLKADOT: ВИДЕНИЕ ГЕТЕРОГЕННОЙ МУЛЬТИЧЕЙНОВОЙ СИСТЕМА. https://github.com/w3f/polkadot-white-paper/raw/master/ PolkaDotPaper.pdf, Ноябрь 2016.

9. [20] Серджио Демьян Лернер. Протокол сжатия транзакций lumino (ltcp). https: //uploads.strikinglycdn.com/files/9dcb08c5-f5a9-430e-b7ba-6c35550a4e67/ LuminoTransactionCompressionProtocolLTCP.pdf, Февраль 2017.

10. [21] Илья Герхардт и Тимо Ханке. Гомоморфные адреса оплаты и протокол оплаты по договору. http://arxiv.org/abs/1212.3257, Декабрь 2012.

11. [22] Тир Нолан. Alt-цепи и атомные передачи https://bitcointalk.org/index.

php?topic=193281.msg2224949#msg2224949.