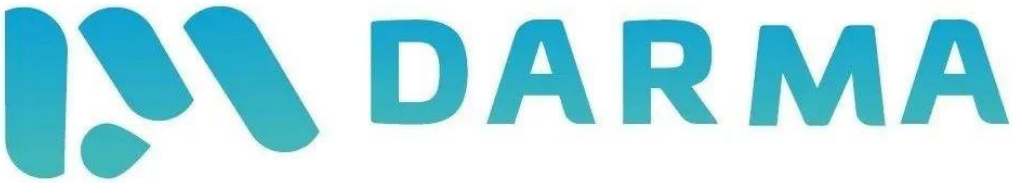

DarmaCash (DMCH) Blockchain

Анонимное, высокопроизводительное, расширяемое децентрализованное финансовое решение с блокчейном

Белый лист

Вводная часть

Утопия подразумевает под собой «воображаемое место», или «идеальное место», также она может относиться к положению вещей, в котором все идеально. DarmaCash(DMCH) - это настоящий финансовый мир, который основан на конфиденциальности и может создавать условия для получения личного стабильного заработка. Благодаря атомному обмену и Oracle, реализуется обмен между величинами личного стабильного заработка и DMCH, который позволяет осуществлять обмен между новым финансовым миром и миром реальным. Мы называем это DMCH-утопия.

Содержание

Глава 1 – Вступление

1.1 Общая информация о проекте

С выпуском белого листа Биткоина Сатоши Накамото, Биткоин установил принципы для всего блокчейн мира: «*Безопасность, понятность и децентрализованность»*. Все эти правила работают по всему блокчейну и никто не может творить злодеяния или вносить изменения в правила. Все эти законы управляются машинами без какого-либо человеческого вмешательства. Принципы блокчейна дают нам представление об утопии, которая не так уж и далека от нас.

ByteCoin и Monero, основанные на протоколе CryptoNote, решили проблему анонимности в системе оплаты биткоина. Однако, в добавок к децентрализованной системе оплаты, мир также нуждается в более сложных децентрализованных анонимных приложениях. К сожалению, из-за низкого уровня пропускной способности, долгого времени ожидания, неподдержанных смарт-контрактов, Oracle и других проблем, препятствовали Bytecoin и Monero дальнейшему развитию децентрализованных приложений. Во имя децентрализации, вышеперечисленные проблемы могли быть решены только путем изменения глобальной верификации, что увеличило бы стоимость разработки.

Кроме того, в современном обществе, наша судьба находится в руках других людей, и многие люди до сих пор не осознали этот факт, даже если и осознали, они не способны освободиться. Безналичное общество приходит без какого-либо предупреждения, а мобильная оплата становится все более популярна. Пока люди наслаждаются приносимым комфортом, они попадают под серьезное наблюдение. В будущем бумажные деньги могут прекратить существование, так как их сложно отслеживать. Безналичное общество, в котором денежное обращение выше и распространен более жесткий надзор, вскоре вытеснит старый мир наличных денег

Но это кошмар для конфиденциальности, так же, как если бы вы жили в мире как в фильме *«Шоу Трумана»*. С момента вашего рождения, деньги будут главной частью вашей жизни, например, ваша еда, одежда, жилье, передвижение, благодаря которым вас будут отслеживать из-за каждого потраченного пенни. The big data будут сортировать ваши хобби и предоставлять обратную связь, предлагая вам их через коммерческую рекламу. Поскольку персональные данные хранятся на централизованном сервере, раскрытие конфиденциальности становится все более частым. Централизованные бюрократические организации могут

присвоить ваше право на использование денег в любое время. Как же это ужасно! А в соответствии с правилами, ориентированными на деньги, люди будут лишены частной жизни и станут все более и более открытыми, и даже основные индивидуальные права человека могут быть скомпрометированы.

1.2 Значимость проекта

Сервисы интернет-приложений, основанные на централизованной архитектуре (включая финансовые услуги), постоянно собирают различного рода информацию о пользователях по разным причинам для расширения бизнеса, но они не обращают внимания на защиту конфиденциальности пользователей, которая является основной работой, даже если и не может стимулировать рост прибыли. Однако, как только информация пользователей просочится через подобные приложения, возможности сотен миллионов пользователей будут скомпрометированы. Утечка информации, если ею злоупотребляют хакеры, приводит к непредсказуемым катастрофам для пользователей, например, к мошенничеству с деньгами или личными данными.

В настоящее время общество остро нуждается в мерах защиты частной жизни, которые управляются технологиями и не зависят от воли человека, поскольку конфиденциальность является самым основным правом человека.

Блокчейн проект DMCH стремится обеспечить анонимность, высокую производительность, и расширение децентрализованного финансового решения, которое основано на Monero. DarmaCash (DMCH) переняло структуру блока Block-DAG, включая персональные адреса, анонимные смарт-контракты, DeFi, и DEX в персональных рамках Monero, и представляет децентрализованные распределённые PPoS, которые не ограничены узлами. Кроме того, оно стремится реализовать высокоскоростную анонимную глобальную SDWAN путем расширения PPoS узлов, и создать децентрализованную распределенную анонимную экосистему сообщества. DarmaCash (DMCH) не только унаследовал Monero в качестве зашифрованной валюты, но и планирует стать децентрализованным выделенным интернетом для защиты личной конфиденциальности.

1.3 Метод реализации

После более десяти лет развития блокчейн индустрии, появились десятки тысяч проектов, и большинство из них были улучшены и оптимизированы на основе Bitcoin, Bytecoin и Ethereum, и постепенно сформировалась спиралевидная эволюционная система. Члены команды блокчейн проекта DarmaCash (DMCH) из разных областей, таких как криптография, экономика, компьютерные технологии и инженерия программного обеспечения, они привержены защите частной жизни под руководством двух циклов – *"учение, исследование, интеграция и оптимизация" и "рынок, спрос и капитал"*, для дальнейшей интеграции и совершенствования блокчейн технологии, это существовало в течение десяти лет

и в конечном итоге предоставило сообществу конкретную практику анонимного, высокопроизводительного, расширяемого децентрализованного финансового решения блокчейна. Цель проекта DarmaCash (DMCH) заключается в формировании монопольного преимущества в конкретной области, а также в постоянном стремлении и внедрении инноваций для достижения децентрализации.

Глава 2 – Техническое решение

В настоящее время базовая структурная декомпозиция основного модуля в блокчейн-проекте показана на рис. 2.1. Вся система стала относительно зрелой. Непрерывная работа системы и постоянно возникающие бизнес требования будут продвигать вперед непрерывную итерацию системы блокчейн-технологии. Кроме того, в итерации будут происходить феноменальные изменения, обусловленные технологическим прогрессом (например, квантовые вычисления, аппаратные прорывы и т. д.) Однако технологические обновления не изменят структуру технологии блокчейна. Это позволит оптимизировать только основные модули в рамках фреймворка. Поэтому структура анонимного, высокопроизводительного и расширяемого блокчейн-децентрализованного финансового решения, развернутого в рамках блокчейн-системы, достаточно стабильна. В качестве базового блокчейна децентрализованных анонимных системных решений, блокчейн проект DMCH продолжит объединять преимущества других проектов в отрасли, обновленных с помощью новейших технологий, а также оптимизировать собственную систему на этой основе, чтобы обеспечить стабильность, продвижение и практичность блокчейна.

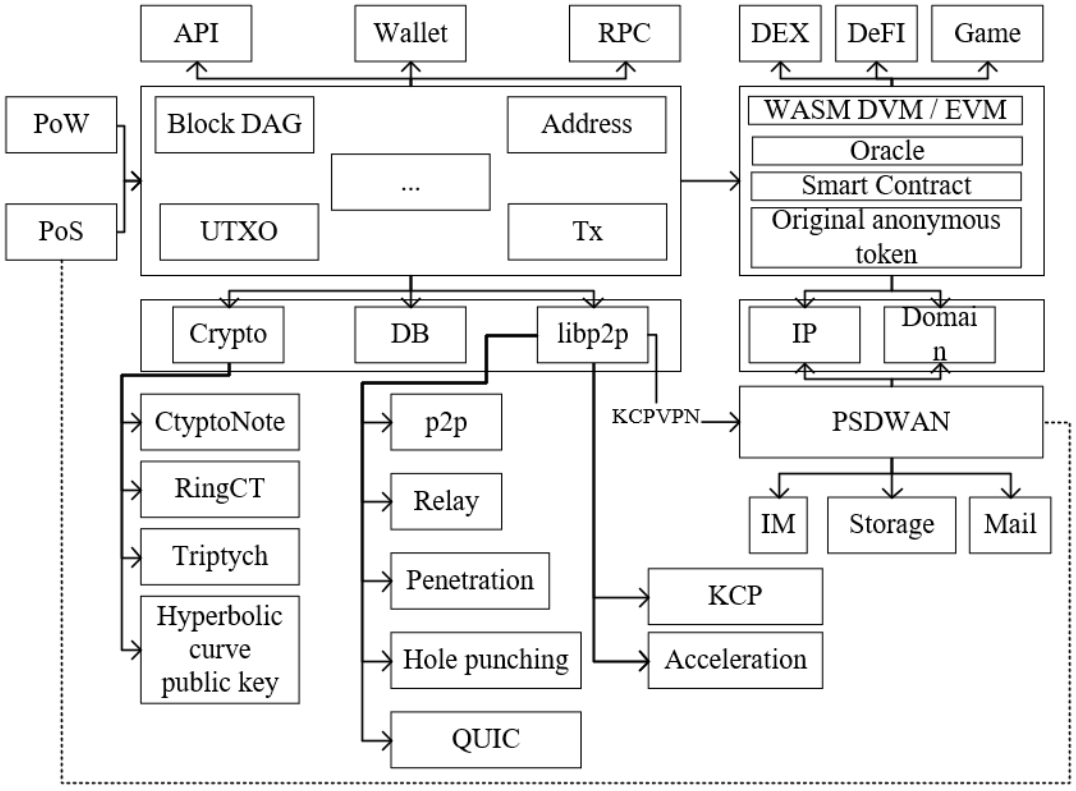

Рисунок 2.1 Системная схема блокчейн проекта DMCH.

2.1 LibP2P

Идея децентрализации блокчейна укоренилась в общественности. На самом деле, блокчейн - это просто распределенная одноранговая (P2P) децентрализованная сеть. Многие люди не имеют четкого представления о P2P. P2P-сеть-это фактически сеть, в которой участники (узлы) могут общаться друг с другом напрямую. Но это не означает, что каждый узел идентичен, так как некоторые узлы играют различную роль в сети. Однако одна из главных особенностей P2P-сети заключается в том, что им не нужен привилегированный “сервер”, который имеет другое “клиентское” поведение, например модель клиент/сервер. Определение P2P-сети очень широкое, поэтому было создано множество различных типов систем, и все они “равны”. Самые распространенные из них это файлообменные файлы, такие как BitTorrent, в то время как блокчейн сети такие как Bitcoin, Ethereum и DMCH тоже P2P сети.

Однако современный Интернет довольно хрупок, и существует множество проблем, большинство из которых связано с адресацией местоположения, но они могут быть решены с помощью адресации контента, более гибкой распределенной одноранговой сетевой модели. Но для достижения адресации контента существует множество препятствий со стороны традиционного интернета, которые в основном отражаются в различных факторах, таких как NAT, брандмауэры, сетевые задержки, надежность сети, роуминг, надзор, различные стандарты в различных устройствах и медленные технологические итерации.

Модуль P2P блокчейн-проекта DarmaCash будет использовать фреймворк LibP2P для решения вышеуказанных проблем. LibP2P первоначально был сетевым уровнем проекта Protocol Lab IPFS, но позже стал независимым проектом из-за его способности трансформировать традиционную интернет-структуру.

Проще говоря, LibP2P-это база данных, которая связывает узлы друг с другом. Любые два узла могут быть соединены LibP2P до тех пор, пока у них есть возможность быть физически связанными, независимо от того, где они находятся, в какой среде они находятся, в какой операционной системе они работают, или находятся ли они за NAT или нет. Кроме того, стоит отметить, что QUIC, принятый LibP2P, возможно, не сможет достичь глобального проникновения в сеть. DMCH будет интегрировать технологию KCP, которая широко используется во всем мире, а блокчейн-интернет, основанный на маршрутизации KCPVPN+BGP, является важной частью системы анонимных, высокопроизводительных, масштабируемых блокчейн-децентрализованных финансовых решений DMCH.

2.2 Block-DAG

Блокчейн, по сути, подобен бухгалтерской книге. Она содержит информацию о сделках между всеми заинтересованными сторонами, как и любая другая база данных. Однако если вы хотите, чтобы база данных была устойчивой для атак и самое главное – поддерживала одно и то же состояние на разных устройствах

одновременно, это будет непросто. Традиционные финансовые платежные системы могут обрабатывать от тысяч до десятков тысяч транзакций каждую секунду. В отличие от этого, производительность обработки транзакций Биткойна отличается на несколько порядков. Производительность обработки транзакций различных известных блокчейн-проектов показана в таблице 2-1 ниже:

Таблица 2-1 Производительность обработки транзакций различных блокчейн - проектов

Name	TPS	Block time
BTC	7	10min
BCH	24	10min
LTC	7~28	2.5min
ETH	20~40	15s

Примечание: Приведенные выше данные взяты из общедоступных данных в Интернете.

Биткойн использует хорошо известную цепную структуру для организации блоков, и транзакции, которые может содержать каждый блок, ограничены. Когда есть несколько майнеров, работающих над блоком, и несколько блоков найдены одновременно, майнерам нужно выбрать "лучшую цепочку", основанную на принципе самой длинной цепи, и временно отбросить другие блоки. Причина, по которой он является "временным", заключается в том, что отброшенный блок будет продолжать расширяться и соответствовать принципу самой длинной цепи, а затем займет место прежней лучшей цепи. В верхней части блокчейна постоянный процесс “отбора, отбрасывания и конвергенции” называется "выбором лучшей цепочки". Например, есть 10 майнеров, которые добыли 10 блоков на одном уровне и в одно и то же время, и в каждом блоке есть 100 транзакций, тогда только один блок будет продлен по лучшей цепочке, а остальные 9 блоков будут отброшены. Таким образом, 900 отброшенных транзакций будут упакованы и подтверждены в следующих блоках. Так что да, если все 10 блоков могут быть подтверждены одновременно, производительность обработки будет увеличена в 10 раз.

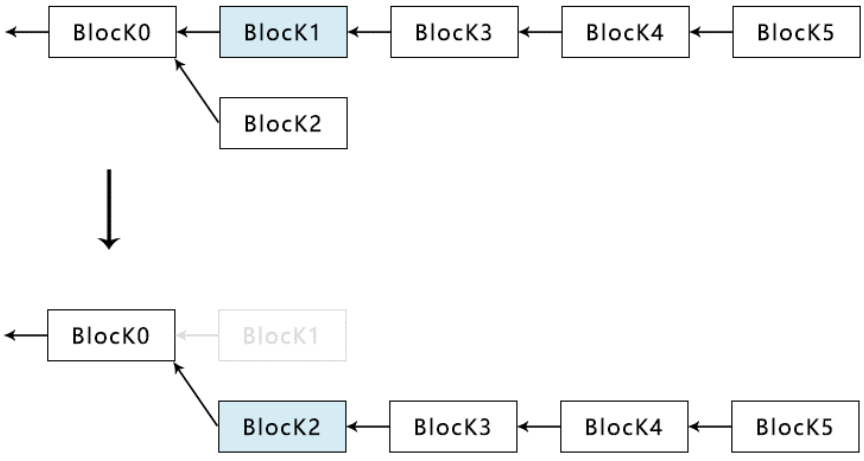

Рисунок 2.2: Выбор лучшей цепи биткоина.

Выбор лучшей цепочки также повлечет за собой еще одну важную проблему безопасности: 51%-ную атаку с хэш-скоростью. Как упоминалось ранее, майнеры, которые контролируют хешрейт, могут фактически манипулировать выбором "лучшей цепочки" и перезаписывать предыдущий блок своими специально подобранными построенными блоками. Так что как предотвратить 51% - ную атаку хешрейта и повысить безопасность блокчейна, стало горячей темой в Биткойне.

2.2.1 Концепция Block-DAG

Block-DAG использует Ориентированный Ациклический Граф (DAG) для организации блоков. DAG относится к ориентированному графу без петель. В неориентированном ациклическом графе, если линия идет из точки A в точку B через C, а затем обратно в точку A, то образуется петля. После изменения направления ребер с “B” на “C”, он превращается в направленный ациклический граф снова. Другими словами, Block-DAG использует "граф" вместо "цепи" для организации блоков, и таким образом избегает проблем производительности и безопасности "лучшего выбора цепочки" биткойна. Проще говоря, разница между Block-DAG и традиционным биткоином заключается в том, что "обработка блоков биткоина является одноядерной и однопоточной, в то время как Block-DAG является многоядерной и многопоточной."

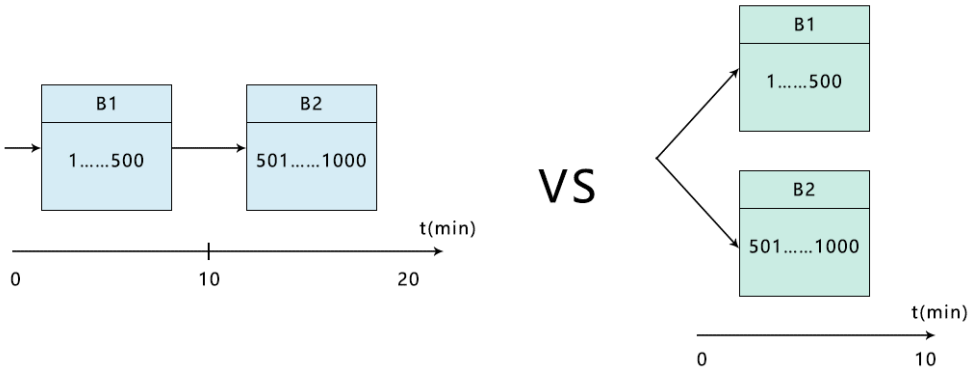

Рисунок 2.3: Параллельная обработка транзакций

Блокчейны, основанные на Block-DAG, больше не являются единой цепной структурой. Весь блок образует сеть, как показано на следующем рисунке:

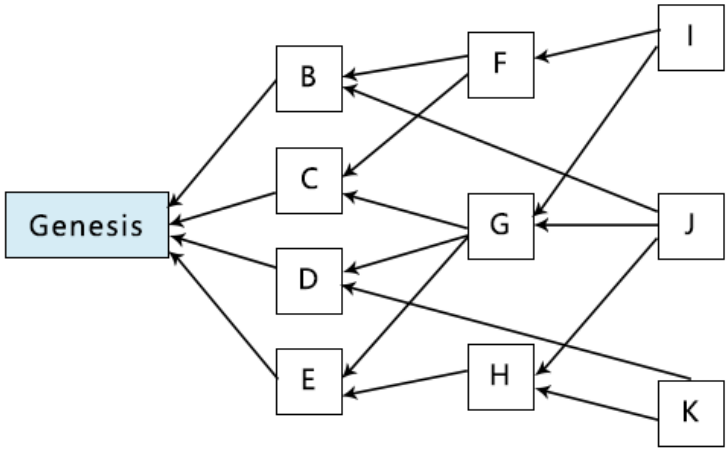

Рисунок 2.4: Организация блоков Block-DAG

Как мы все знаем, в блокчейне блоки постоянно расширяются до более высокого уровня. В Block-DAG, если блок не имеет нового блока, связанного с ним, это означает, что блок находится в "верхнем" положении, и такие блоки называются "наконечниками". Начиная с каждой вершины, блоки генезиса можно проследить только в одном направлении. На наконечник будет ссылаться новый блок, а новый блок может ссылаться на несколько наконечников одновременно. С помощью приведенного выше рисунка давайте посмотрим, как блок block-DIAG расширяется сам по себе:

(1) В самом начале весь блокчейн имеет только один блок – “блок генезиса”, что означает, что есть только 1 наконечник. Если предположить, что одновременно работают 4 майнера, то 4 блока {B, C, D, E} будут расширены на одном и том же наконечнике.

(2) Предположим, что из-за скорости добычи и передачи по сети майнер A и майнер B получили {B, C}, майнер C получил {C, D, E}, а майнер D получил только {E}, который он обнаружил сам. Таким образом, они продолжают добычу на основе наконечника {B, C}, {C, D, E} и {E}. Им не нужно продолжать ждать, пока все блоки узлов будут верифицированы, или выбирать лучшую цепочку из {B, C, D, E}.

(3) Разделите наконечник {B, C, D, E} на три группы: {B, C}, {C, D, E}, {E}, который производит новые блоки {F, H, I}, и майнеры используют их в качестве наконечника и продолжают добывать, а остальное можно сделать тем же способом.

В блоке Block-DIAG, после того как наконечник используется следующим блоком, она называется "отцовской стороной", что аналогично концепции "отцовского блока" в Биткойне. "Сторона" - это концепция алгоритма DAG, которая здесь более подробно не рассматривается. Как видите, из-за различных непредсказуемых факторов не каждый наконечник может быть "отцовской стороной" и продолжать расширяться. Этот вид блока будет отброшен как “сиротский блок” в DMCH. Кроме того, стоит также отметить, что при появлении нового блока, на сколько наконечников можно ссылаться в лучшем случае.

Рассматривая самый крайний случай, если новому блоку разрешено ссылаться на все наконечники, которые он может видеть, это означает, что будет больше параллельных блоков на той же высоте, что приведет к самой высокой производительности обработки транзакций, но побочные эффекты также очень очевидны. Если майнеров будет достаточно, блок будет расширяться без ограничений. Поэтому мы должны найти баланс для максимального количества наконечников, на которые могут ссылаться новые блоки. В настоящее время максимальное количество наконечников, на которые DMCH позволяет ссылаться новым блокам, составляет 3. В версии 3 DMCH это значение может быть динамически скорректировано, и после интеграции с сегментами транзакций оно достигнет огромного улучшения в TPS.

2.2.2 Сортировка Block-DAG

Хотя сортировка блоков перетаскиванием блоков не является обязательной, в большинстве случаев сортировка очень важна. Это объясняется тем, что в большинстве случаев между транзакциями существует своего рода корреляция на основе порядка. Наиболее типичным случаем являются “смарт-контракты”: возникновение определенного условия в одной транзакции основано на конечном исполнительном результате выполнения определенного условия в другой транзакции. Поэтому DMCH необходимо "вычислить" цепочку "логической последовательности" в графическом блоке в соответствии с алгоритмом. За этим стоят две цели:

(1) определить последовательность транзакций, чтобы соответствовать бизнес-требованиям на верхнем уровне;

(2) отбросить сиротские блоки; эта логическая последовательность очень похожа на традиционную цепную структуру биткойна, но между ними также есть существенное различие: Биткойн реализует последовательность через "хэш отцовского блока", в то время как "логическая последовательность" в DMCH-это просто логическое понятие, и между блоками нет никаких физических связей.

Сортированный набор блоков называется "полным порядком". Каждый блок в полном порядке имеет только одну увеличивающуюся высоту Топо. Вот почему вы можете видеть, что для каждого блока в браузере блоков одновременно есть две высоты – высота блока и высота Топо, причем первая является высотой блока в цепочке, и она всегда добавляет 1 к высоте блока своего самого большого наконечника, чтобы гарантировать, что высота цепочки будет продолжать увеличиваться. Под одним и тем же блоком-DAG могут находиться блоки, добываемые несколькими майнерами одновременно.

Что касается сортировки Block-DAG, то многие проекты или команды предложили свои собственные решения. Эти решения имеют свои преимущества и недостатки. Давайте посмотрим, сколько реализовано:

(1) После получения майнером трансляции нового блока, первым шагом является проведение проверки валидности, используя такие методы, как обнаружение двойных расходов, проверка валидности транзакций, PoW

верификация и проверка подписи PoS и т. д. Квалифицированный блок будет помещен в набор блоков.

(2) В соответствии с верифицированным алгоритмом будет найдена начальная точка сортировки. Предположим, что “база” - это отправная точка, тогда “база” - это блок генезиса, который будет расширяться с развитием блокчейна. Блок, выбранный в качестве “базового”, является стабильным блоком (без какого-либо бокового блока, который был оптимизирован в DMCHv2), и его порядок не будет изменен для сортировки в “полном порядке”.

(3) Начиная с “базы”, все последующие блочные транзакции временно помечаются как недействительные.

(4) извлеките последний набор наконечников, включяя недавно добавленный блок, и лучший блок будет выбран в соответствии с верифицированным алгоритмом, который называется “лучшим”. DMCH принял "кумулятивную сумму сложности", чтобы определить лучший выбор наконечника. Так называемая накапливаемая сумма сложности-это сумма сложности всех блоков, которая проходит от блока генезиса до текущего блока.

(5) начиная с “лучшего”, прослеживая назад, чтобы найти его вершину, и, наконец, получить все доступные блоки в диапазоне [“база”, “лучший”], а затем отсортировать их в соответствии с их совокупной сложностью, чтобы получить окончательный сортированный набор блоков. Очевидно, что другие наконечики в наборе не находятся в диапазоне [“базовый”, “лучший”] (так как они являются вершинами, и в блоках нет петли), и они будут временно отброшены. Даже их отцовский край, если на него не ссылается другой блок, будет отброшен в то же самое время. Временный отказ-это нормальный процесс конвергенции в Block-DAG который будет дополнительно проработан.

(6) транзакции всех блоков в диапазоне будут пересчитаны в соответствии с отсортированным порядком блоков (Высота Топо). Повторные транзакции будут автоматически помечены как недействительные. Таким образом, двойные расходы избегаются, и все транзакции имеют последовательность, которая обеспечивает базовую поддержку для работы смарт-протоколов. На той же высоте самым сложным блоком является основной блок, а остальные блоки называются боковыми блоками.

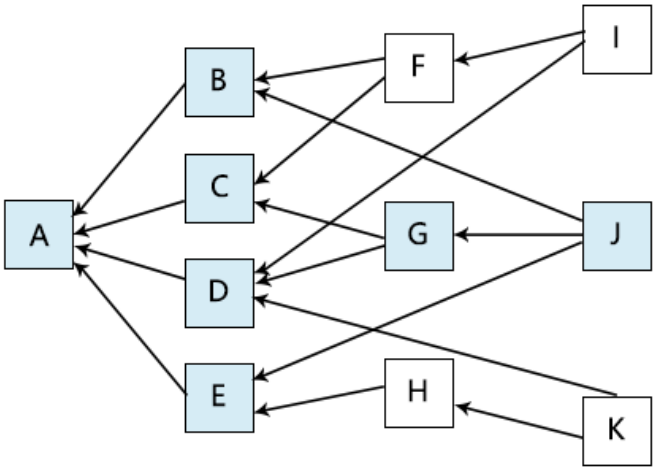

Рисунок 2.5 Сортировка Block-DAG (1)

Как показано на рисунке, набор наконечников-кандидатов равен {I, J, K}, и если предположить, что J - “лучший”, а A - “базовый”, начальная точка (A не имеет бокового блока), то все блоки {A,B,C,D,E, G, J} между [A,J] будут выбраны и отсортированы,а {F,I, H, K} будут временно отброшены.

В сортировке Block-DAG есть два момента, на которые стоит обратить внимание:

(1) в конце Block-DAG всегда есть набор блоков, который ожидает конвергенции и сортировки. DMCH устанавливает минимальное значение высоты цепи равным 8 и продолжает движение вперед до тех пор, пока не будет найдена начальная точка “основания”. DMCHv3 оптимизирует алгоритм, чтобы сократить время подтверждения. Они “нестабильны”, потому что блок может быть отброшен, а, следовательно, и привести к ненадежной транзакции, которая очень похожа на неподтвержденные блоки биткоина. В DMCH текущая "высота стабильности" может быть получена через интерфейс “getinfo”, что означает, что можно различать стабильные и нестабильные блоки.

(2) Что касается "временного отказа", предположим, что текущая Цепочка имеет 10 возможных наконечников и выбран только один блок, то оставшиеся 9 блоков не обязательно могут быть отброшены или, по крайней мере, в большинстве случаев этого не произойдет. Это происходит потому, что следующий новый блок будет выбран в соответствии с верифицированным алгоритмом при выборе "отцовской стороны" (на данный момент допускается до 3 вариантов выбора), поэтому, когда следующий новый блок выбран как “Лучший”, они, естественно, действительны, так как они принадлежат к достижимому блоку в диапазоне [“базовый”, “лучший”]. По аналогии, блоки продолжают расширяться назад, сходятся и сортируются, и большинство блоков будут считаться действительными. Как и в приведенном выше примере, после создания нового блока L и ссылки на {I, J, K} все блоки, предшествующие L, также будут действительны.

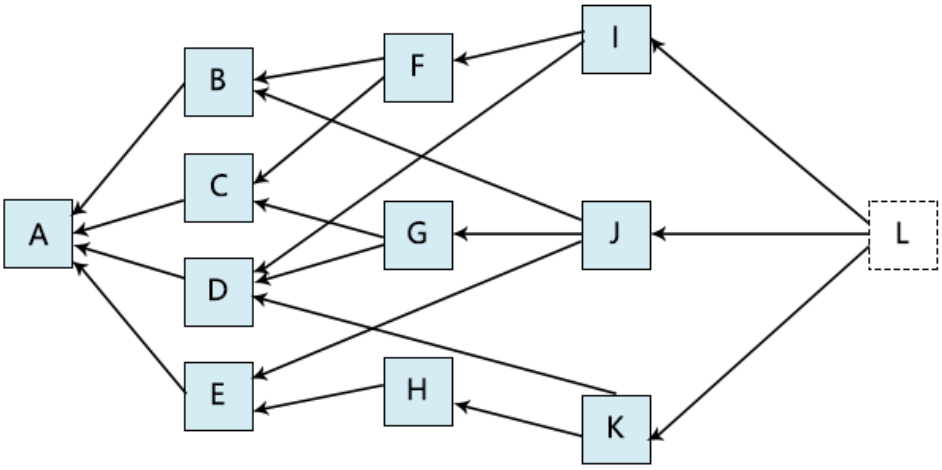

Рисунок 2.5 Сортировка of Block-DAG (2)

Block-DAG-это отличное решение для расширения цепочки, которое эффективно решает проблему низких возможностей обработки биткойн-транзакций. Технология Block-DAG DMCH не конфликтует и эффективно дополняет другие решения для расширения вместимости вне цепочки, такие как Lightning Network. В сочетании с другими технологиями расширения пропускной способности возможности DMCH по обработке транзакций будут значительно улучшены. Между тем, быстрый и простой алгоритм сортировки конвергенции блоков DMCH также заложит прочную основу для следующего приложения смарт-контрактов.

2.3 Анонимность технологии

DMCH-это проект, основанный на Monero, и оба они происходят из протокола CryptoNote. Оригинальнй белый лист CryptoNote появился в 2012 году и был опубликован на сайте Tor. Автор оригинального белого листа использовал псевдоним Николас Ван Саберхаген. Менее чем через год, после того как второе издание белого листа было опубликовано под тем же псевдонимом, личность автора по-прежнему остается неизвестной. Протокол CryptoNote в основном решает две проблемы: одна-это неотслеживаемость, что означает, что для всех входящих транзакций все возможные отправители могут быть источником, но неизвестно, кто их отправил; другая проблема-это несвязанность, что означает, что невозможно доказать, что любые две исходящие транзакции отправлены от одного и того же человека. Конечно, протокол CryptoNote может также решать и другие проблемы. Для получения дополнительной инфорации пожалуйста перейдите по ссылке: https://cryptonote.org/standards/.

2.3.1 Кольцевая подпись

Функция непрослеживаемости использовала технологию кольцевой подписи (Примечание: эта технология может решить проблему анонимности отправителя транзакции). Технология кольцевой подписи основана на концепции групповой подписи предложенной Дэвидом Чаумом и Э. Ван Хейстом (https://www.chaum.com/publications/Group_Signatures.pdf). Кольцевая подпись использует несколько публичных подписей, которые смешиваются вместе, чтобы скрыть реальную подпись транзакции, что не повлияет на возможность проверки действительности транзакции.

И стоит отметить, что позже было доказано, что технология кольцевой подписи может быть прослежена при определенных обстоятельствах (https://eprint.iacr.org/2006/389.pdf). Позже этот вопрос был решен компанией Monero Ring Confidential Transactions (RingCTs).

2.3.2 Одноразовый ключ

Несвязываемая функция использовала технологию одноразового ключа (Примечание: эта технология может решить проблему анонимности получателя транзакции). Поскольку открытый ключ необходим при смене подписи, все входящие транзакции адреса открытого ключа можно наблюдать на блокчейне, поэтому легко разоблачить все стороны, связанные с транзакцией. Таким образом, усовершенствованная технология обмена ключами Диффи-Хеллмана позволит генерировать одноразовый ключ для защиты всех сторон. Общий принцип заключается в том, что отправитель транзакции использует свои собственные данные для хэширования открытого ключа получателя и, таким образом, создает уникальный одноразовый ключ для транзакции, поэтому только получатель может генерировать закрытую часть транзакции. Протокол CryptoNote - это отличный протокол. Для большей информации пожалуйста перейдите по ссылке: https://cryptonote.org/inside.

2.3.3 Достижение анонимности

В процессе достижения анонимности отдельный пользователь имеет два закрытых ключа и два открытых ключа для завершения всего процесса шифрования. Технология Ring Signature гарантирует анонимность отправителя транзакции, технология одноразового адреса (Stealth Address) гарантирует анонимность получателя транзакции, а технология ring confidential transactions (RingCTs) гарантирует анонимность содержимого транзакции.

2.3.4 Суб-адрес

DMCH поддерживает суб-адрес, что похоже на функцию субадресации биткойн-кошельков, которые могут связывать каждый адрес с набором открытых и закрытых ключей (точно так же, как бесчисленные "маленькие кошельки" в большом файле кошелька), но DMCH имеет только один кошелек, сопряженный с набором открытых и закрытых ключей, что превосходит Биткойн-решение с точки зрения производительности и возможности майнинга.

2.3.5 Оптимизация технологии анонимности

Чтобы сохранить технологию анонимности DMCH в лидерах, исследовательская лаборатория Monero Research Laboratory (MRL) и новейшая технология шифрования станут прочной теоретической основой для непрерывной оптимизации проектов DMCH. Например, MRL выпустила триптих и предложила кольцевые сигнатуры, которые не зависят от логарифмического размера. В отличие от MLSAG, Triptych-это новая структура кольцевой подписи, которая объединяет технологии MLSAG, Pedersen and Confidential транзакционных технологий в новые RingCTs, так что анонимность может быть обеспечена более чем в десять раз. Главное новшество триптиха состоит в том, чтобы сделать логарифмическую зависимость, а не линейную зависимость, между размером байта кольцевой сигнатуры и количеством приманок. Таким образом, размер кольца может быть значительно увеличен без серьезных проблем с производительностью. Проект DMCH будет продолжать фокусироваться на таких технологических инновациях. Что касается триптиха, то проект DMCH будет модернизирован из MLSEG в Чикаго и в конечном итоге переведен в триптих.

2.4 Механизм верификации

Механизм верификации можно разделить на классический распределенный механизм верификации и блокчейн-механизм верификации. Начало исследований механизма верификации можно проследить с 1975 года, когда в компьютерной области была поднята "проблема двух армий". Западные ученые исследовали "проблему византийских генералов", которая сосредоточена на том, как небезупречные узлы могут достичь верификации с любыми конкретными данными, когда могут быть неисправные узлы или вредоносные атаки. Исследование механизма верификации основано на этой проблеме. В 2008 году, когда Сатоши Накамото предложил Биткойн, механизм верификации открыл эру верификации блокчейна. В настоящее время механизм верификации блокчейна можно разделить на две категории – один является авторизованным механизмом верификации, а другой-несанкционированным механизмом верификации.

Авторизованный механизм верификации требует от пользователя полной аутентификации личности перед участием в последующем механизме соглашения, в то время как при несанкционированном механизме верификации, который может быть представлен биткоином, узлы могут входить и выходить из блокчейн-цепочки в любое время, а количество узлов подвержено динамическому и непредсказуемому изменению, а процессы выбора производителя блоков, генерации блоков, верификации узлов и обновления блокчейна осуществляются с помощью определенных алгоритмов.

Безусловно, наиболее успешным механизмом верификации по-прежнему является PoW, а именно майнинг. В принципе, все топ-10 блокчейнов в отрасли, где биткойн лидирует, используют механизм верификации PoW. Одна из причин этого явления заключается в том, что для формирования верификации требуется время. Когда все думают, что PoW-это надежный механизм верификации, они будут придерживаться его, и даже если появится лучший механизм верификации, им потребуется много времени, чтобы изменить новый. Вторая причина заключается в том, что PoW эффективно решили проблему византийских генералов с помощью методов шифрования и экономических стимулов. Поэтому справедливые и децентрализованные характеры PoW глубоко укоренились в сердцах широкой общественности. Тем не менее, за десять лет, прошедших с момента создания биткойна, мы должны признать, что в механизме PoW биткойна возникли некоторые производные проблемы.

Механизм верификации блокчейна в основном оценивается по шести аспектам: безопасность, пропускная способность транзакций, масштабируемость, время подтверждения транзакций, децентрализация и занятие ресурсов. Механизм верификации DMCH формируется через три этапа – PoW, PoW+PPoS и PPoS. Его схема трансформации повторяет схему ETH. Кроме того, поскольку DMCH является филиалом проекта Monero, его безопасность, пропускная способность транзакций, масштабируемость и время подтверждения транзакций унаследовали способность Monero. В добавок, с помощью технологии Block-DAG и новейшей технологии шифрования была дополнительно улучшена безопасность (анти-51%двойная атака), пропускная способность (TPS увеличена до 70) и время подтверждения транзакций (около 2 минут) DMCH.

2.4.1 Проблемы механизма верификации PoW

Пока что, механизм верификации PoW имеет некоторые недостатки в области использования ресурсов и децентрализации.

(1)Серьезная пустая трата ресурсов. В данный момент, нужны профессиональные устройства(ASIC) и большое количество электроэнергии для майнинга биткоина, и электричество, которое он потребляет в течение одного года, равно годовому потреблению электроэнергии в небольшой или средней стране, а профессиональные устройства, которые потребляют электричество, выполняют только простую вычислительную работу. Поэтому использование годового

потребления электроэнергии и соответствующего хэш-курса для производства биткоинов с сильно колеблющимися ценами, безусловно, является огромной тратой ресурсов.

(2) Постепенная централизация. Сатоши Накамото сказал “один CPU-один голос”, когда он создал Биткойн. Но великое видение постепенно отклонилось от курса в этом ориентированном на прибыль обществе. Можно заметить, что хеш-курс биткойна во всем мире постепенно стал свидетелем монополизации нескольких крупных майнинговых пулов, и такая тенденция централизации будет становиться все более серьезной.

2.4.2 PoW+PPoS

DMCH’ PoW+PPoS относится к блокам, добытым майнерами, которые должны быть проверены подписью PoS-узлов, прежде чем они будут считаться действительными блоками. 5% блоков DMCH принадлежат PoW майнерам и 95% PoS-узлам и держателям токенов. PPoS-это инновация в проекте DMCH, то есть распределенные PoS-узлы. Проще говоря, в отличие от недостатков централизованного голосования, вызванных суперузлами EOS, все узлы DMCH справедливы, а его механизм гораздо более децентрализован. Фаза PoW+Pos в основном решает следующие проблемы:

a. Быть экофрендли. Поскольку вознаграждение за блок для майнеров составляет всего 5%, механизм стимулирования не поощряет добычу PoW. Это значительно уменьшит затраты огромных вычислительных ресурсов и электроэнергии, а также побудит сторонников держать и блокировать деньги, чтобы заработать проценты. Таким образом, можно сократить затраты на расчет ресурсов и потребление электроэнергии. Вот почему мы называем его настоящим экофрендли механизмом.

b. Быть Децентрализованным. Поскольку 95% вознаграждения за блок приходится на узлы PPoS и пользователей, которые держат и блокируют деньги, люди изменят свое поведение из-за механизма стимулирования. Давайте проведем аналогию: механизм стимулирования PoW биткойна формирует экосистему “майнинг пул + майнинг машина”, в то время как механизм стимулирования PoW+PPoS DMCH формирует механизм “узлы PPoS + удержание и блокировка денег”. Другими словами, майнинг-пулы были преобразованы в узлы PPoS, а майнинговые машины стали деньгами hold & lock. Может ли эта экосистема решить проблему децентрализации? Ответ-да, и существует высокая вероятность формирования децентрализации. Во-первых, он прост в использовании. Работа пулов PoW майнинга и майнинговой машины требует определенной степени IT возможностей, но узлы PPoS-это всего лишь программное обеспечение. Во-вторых, эффективен также механизм стимулирования создания узлов PPoS. Помимо получения вознаграждений при добыче блоков (аналогично сборам за майнинг-пул), существует также коллективное вознаграждение. Это означает, что владельцы узлов PPoS будут

получать не только транзакционные сборы, но и вознаграждение за обслуживание узлов. Это привлечет больше людей к созданию узлов, что, в свою очередь, поможет сделать блокчейн более децентрализованным. Наконец, проект DMCH может скорректировать механизм стимулирования на основе коэффициента децентрализации, который направлен на ускорение строительства децентрализованной сети.

2.5 Смарт-контракты

Основанный на WASM, DMCH smart contract использует PLONK zero-knowledge proof, предоставляет полную среду компиляции языка C/C++ и языка GO, поддерживает "анонимные" контракты и очень легко переносит смарт-контракты Ethereum на платформу смарт-контракта DMCH.

2.5.1 Обзор смарт-контрактов

Смарт-контракты-это свободный от посредников протокол компьютерных транзакций, который может выполнять самоверификацию и автоматическое выполнение условий контракта. В последние годы, с ростом популярности технологии блокчейн, большое внимание уделяется смарт-контрактам. Смарт-контракты на блокчейне децентрализованы, не требуют доверия, программируемы и неизменяемы, могут быть встроены в различные виды данных и активов, чтобы помочь реализовать безопасный и эффективный обмен информацией, передачу величин и управление активами. В конечном счете, ожидается, что она проникнет в реформу традиционных бизнес-моделей и общественных производственных отношений, заложив основу для построения программируемых активов, систем и общества. Обычно существует два свойства смарт-контракта: ценность и статус. Условия “If-Then” и “What-If” в коде задают соответствующие правила триггерного события и ответа. После того как смарт-контракт взаимно верифицирован несколькими сторонами и подписан каждой из них, он отправляется вместе с инициированной пользователем транзакцией (Txn), передается через P2P-сеть и хранится в определенном блоке блокчейна после верификации майнером. Пользователь может применить контракт, инициировав транзакцию после получения возвращенного адреса контракта и информации об интерфейсе контракта. Майнеры мотивированы механизмом стимулирования, заданным системой, и будут вносить свою собственную хэш-мощность для проверки транзакций. После получения контракта или вызова транзакции майнер создаст контракт или выполнит код контракта в локальной среде выполнения (например, EVM). Код контракта будет автоматически судить о том, соответствует ли текущая ситуация условиям запуска контракта, основываясь на доверенных внешних источниках данных (также известных как Oracles) и инспекционной информации мирового государства, чтобы строго соблюдать правила реагирования. Перед упаковкой в новый блок данных, транзакция проверяется.

Новый блок аутентифицируется верифицированным алгоритмом, а затем связывается с основной цепочкой блокчейна, и тогда все обновления вступают в силу.

Ethereum имеет большое сообщество разработчиков, и многие разработчики криптовалют знакомы с виртуальной машиной Ethereum (EVM). С самого начала Ethereum разработал Solidity, язык, ориентированный на EVM, и использовал его в качестве основного языка для смарт-контрактов. Хотя Solidity имеет очевидные ограничения, по сравнению с обычными языками, такими как Go и Rust, в настоящее время она является наиболее широко используемым инструментом разработки в цепочке.

Кроме того, виртуальная машина Web Assembly Virtual Machine (WSM) была принята DMCH, которая является все более популярной технологией в области шифрования и более широком техническом мире. Большинство криптовалют движутся в этом направлении, и есть еще проекты, такие как ETH2 и Polka dot, которые решили использовать WASM.

Хотя Web Assembly обязательно будет успешной, необходимо учитывать переходный период адаптации разработчиков, чтобы убедиться, что EVM работает на DMCH. Поэтому, DarmaCash (DMCH) интегрировал EVM в DMCH, и DMCH будет поддерживать как виртуальную машину WASM, так и виртуальную машину EVM. Поскольку большинство инструментов Ethereum полагаются на web3.js, мы внедрили индивидуального провайдера web3, который позволяет напрямую взаимодействовать с контрактами Ethereum через знакомые интерфейсы в библиотеке web3.

2.5.2 Анонимные смарт-контракты DMCH

Развитие анонимных смарт-контрактов блокчейн индустрии прошло 3 стадии:

Первый этап: Биткоин-это полностью открытый и прозрачный блокчейн-проект. Вам нужно только знать адрес кошелька, чтобы знать доходы и расходы биткоина. Таким образом, легко выяснить отношения между различными счетами. Связывание адресов биткойн-кошельков с реальными пользователями сделает нас “прозрачными”, не оставляя места для конфиденциальности вообще. Чтобы решить проблему конфиденциальности биткойна, разработчики предложили решение, основанное на принципе смешивания денег, которое включает в себя участие многих людей в передаче биткойна, но трудно найти взаимно однозначную связь между различными переводами. Поскольку вход и выход разделены и не могут быть прослежены с одного конца, конфиденциальность пользователя, таким образом, может быть защищена.

Второй этап: чтобы фундаментально решить проблему конфиденциальности, некоторые разработчики разработали блокчейн-проекты, которые защищают конфиденциальность от ее ядра. Основные блокчейны защиты конфиденциальности на рынке можно разделить на четыре категории: смешивание денег, кольцевые подписи, доказательство с нулевым разглашением и серия MimbleWimble, которые представлены Dash, Monero, Zcash и Grin/Beam

соответственно. Однако эти блокчейны, ориентированные на защиту конфиденциальности, не поддерживают смарт-контракты и могут использоваться только в качестве инструментов цифровых активов.

Третий этап: после 2018 года разработчики начали осознавать растущую потребность в защите конфиденциальности в смарт-контрактах, поэтому проект privacy layer начал играть активную роль в различных сценариях. Другими словами, смарт-контракт на блокчейне обеспечивает защиту конфиденциальности. Примечание: соглашение privacy layer может быть построено на блокчейне на первом или втором этапе. В отличие от блокчейн-проекта, который защищает конфиденциальность на втором этапе, проект privacy layer может быть объединен с системой каждого блокчейна для выполнения кросс-цепных операций, что является относительно более гибким и может удовлетворить конкретные потребности пользователей и разработчиков в конфиденциальности. Это так называемые приватные смарт-контракты.

В настоящее время хорошо известные проекты приватных смарт-контрактов на основе Ethereum (ETH) включают NuCypher, Aztec Protocol и Zether. Анонимный проект смарт-контракта на основе Monero (XMR) - это DMCH. DMCH имеет четкое позиционирование для смарт-контрактов, то есть построить простую в использовании, безопасную, частную и эффективную смарт-контрактную платформу на основе Monero, чтобы служить систематическому развитию бизнеса DMCH .

2.5.3 Адаптация UTXO модели DMCH для модели аккаунта

Ethereum

Ethereum, в целом, можно рассматривать как основанный на транзакциях механизм: он берет свое начало из состояния генезиса, а затем, по мере выполнения транзакций, его состояние постепенно меняется на конечное состояние, которое является авторитетной версией в мире Ethereum. Понятие “счет” было введено в Ethereum для замены неизрасходованной модели вывода транзакций (UTXO) биткоина, которые делятся на внешние счета и контрактные счета. Оба типа счетов имеют коррелированный статус счета и адреса счетов, и оба могут хранить Ether (выделенную криптовалюту Ethereum). Разница между этими двумя учетными записями заключается в том, что внешняя учетная запись контролируется закрытым ключом пользователя, и код с ней не связан, в то время как контрактная учетная запись контролируется кодом контракта, и с ней связан код.

Пользователи могут инициировать транзакции в Ethereum только через внешние учетные записи. Транзакции могут включать в себя двоичные данные загрузки транзакций (Payload) и Ether.. Во время транзакции может быть сгенерирована серия сообщений. Когда получателем транзакции или сообщения является конкретный адрес Ø Ethereum, создается контракт. Новый адрес счета контракта вычисляется из адреса создателя контракта и количества транзакций (Nounce),

выданных этим адресом, а Payload транзакции создания контракта формируется в байт-код EVM для выполнения, а выполненные выходные данные постоянно хранятся в виде кода контракта. Когда получатель является контрактным счетом, код в контрактном счете стимулируется для выполнения в локальном EVM. Payload используется в качестве входного параметра контракта, а доверенный источник данных предоставляет необходимую для контракта информацию о внешнем мире. После завершения всех исполнений, результаты выполнения возвращаются, а выполненная транзакция проверяется трансляцией майнера и сохраняется в цепочке блоков вместе с новым мировым состоянием.

Так как транзакции Ethereum сопровождаются потреблением пропускной способности, памяти, затраты на вычисления и т. д., то для того, чтобы стимулировать ввод глобальной вычислительной мощности и рационально распределять права использования, а также предотвратить выход системы из-под контроля из-за вредоносных программ, выполнение всех программ в Ethereum должно нести определенную стоимость. Различные эксплуатационные расходы рассчитываются в “GAS”. Любой фрагмент программы может быть использован для расчета суммы расхода топлива по определенным правилам, и инициатору полной транзакции необходимо оплатить все расходы на исполнение. Когда транзакция будет завершена, оставшееся топливо будет возвращено на счет отправителя транзакции по цене покупки, а необеспеченные сборы будут использованы в качестве вознаграждения для майнера, который добыл блок транзакции. Если во время выполнения транзакции закончится топливо(OOG), переполнение стека, недействительные оказания или другие аномалии, транзакция будет недействительной, но потребленное топливо все равно будет использоваться в качестве вознаграждения для майнеров, которые внесли свои ресурсы.

Для поддержки учетной модели смарт-контрактов, DMCH внедрила дизайн "абстрактного слоя для модели анонимных учетных записей”. Благодаря существованию абстрактного слоя, изменения для любого обычного счета UTXO и смарт-контракта понятны, то есть с точки зрения обычных транзакций создание и вызов смарт-контрактов - это просто другой тип анонимной транзакции, которая не зависит от концепции модели счета. Однако, с точки зрения разработчиков смарт-контрактов, используется модель учетной записи, и существование учетных записей UTXO не заметно. Предположим, пользователь a хочет перевести деньги пользователю с через контракт B, тогда:

(1) пользователь A инициирует транзакцию контракта по адресу контракта B. Функция контрактной транзакции состоит в том, чтобы вызвать трансфертную функцию B и отправить адрес получателя (обычно субадрес C) и перевести в него сумму пользователя C;

(2) после получения транзакции контракт B выполняет код контракта, завершает сопоставление суб-адреса C с контрактным счетом и запускает процесс перевода;

(3) Что касается контрактных счетов, то там будет две транзакции: расходы счета A и доходы счета B, а также расходы счета B и доходы счета C. После этого код контракта обновит баланс контрактного счета;

(4) после запуска кода контракта автоматически запускается обычная транзакция на адрес получателя C.

Таким образом, с точки зрения модели счета UTXO существуют две анонимные транзакции: транзакция от A до B и транзакция от B до C. Однако в смарт-контрактах обновление баланса происходит на трех контрактных счетах, а именно на счетах A, B и C.

Проще говоря, DMCH сопоставляет суб-адрес с одним контрактным счетом, тем самым завершая преобразование из UTXO в модель учетной записи. Таким образом, мы видим, что механизм работы смарт-контракта DMCH точно такой же, как и у Ethereum.

2.5.4 Дизайн анонимных смарт-контрактов DMCH

Когда DMCH реализует модель счета с использованием сопоставления субадресов, смарт-контракты DMCH фактически можно принимать за смарт-контракты Ethereum (ETH). Проект DMCH определяет следующие сценарии в реальной крупномасштабной операции:

(1) содержание договора прозрачно + прозрачный DRC20-токен (валютой контракта ETH является ERC20, а валюта контракта DMCH это DRC20)

(2) понятный контент контракта + анонимный DMNI-токен (все эти понятные активы на BTC, а DMNI имеет анонимные активы на DMCH)

(3) содкржание анонимного контракта (достигается с помощью PLONK, а типы токенов не имеют значения, так как они полностью анонимны)

Вышеприведенные три ситуации охватывают большинство сценариев в приложениях смарт-контрактов. DMCH позволяет своим пользователям выбирать тип смарт-контракта в соответствии с текущей ситуацией. На самом деле, технология гомоморфного шифрования (FHE) может быть использована для обеспечения анонимности содержимого контракта, но нынешняя вычислительная мощность не способна поддерживать этот расчет. В большинстве случаев анонимные контракты направлены на защиту участников и активов, а не всего содержания контракта.

Проще говоря, смарт-контракт DMCH - это необязательный анонимный смарт-контракт. Первая модель "прозрачный контент контракта + прозрачный DRC20-токен" точно такая же, как и контракт Ethereum, то есть полная прозрачность всей информации, которая обеспечивает смарт-контракт DMCH с потенциально большой базой пользователей. Вторая модель “прозрачность содержания контракта + анонимный DMNI-токен” реализует защиту участников на основе первой модели, то есть контрактные активы защищены лежащей в их основе анонимной технологией. Третий тип "анонимности содержания контракта" реализует полную анонимность содержания контракта. Из-за принятия деревьев Меркля и доказательства с нулевым разглашением эта схема защиты конфиденциальности контрактов очень трудоемка, а затраты на топливо довольно высоки, и один блок не может вместить слишком много транзакций такого рода, поэтому он используется только для конкретных сценариев.

2.5.5 Решение Dmni основанное на Bitcoin Omni

Omni protocol-это решение для цифровых активов, основанное на блокчейне Биткойна (самый ранний из них-протокол MasterCoin, как показано на рисунке ниже). Основной принцип заключается в том, чтобы присоединить информацию об операциях, связанных с активами (например, выпуск активов, перевод денег и т. д.), К информации OP_RETURN в протоколе биткойна. В собственном протоколе биткойна информация OP_RETURN может быть произвольной и защищена блокчейном биткойна, поэтому она не может быть изменена. Протокол Omni работает поверх блокчейна Биткойна и поддерживает локальную базу данных. Протокол Omni будет анализировать всю информацию OP_RETURN в биткойн-транзакциях, и если определение протокола будет выполнено, то операции будут выполнены, а информация об активе, записанная в локальной базе данных, будет обновлена. Протокол Omni-это, по сути, схема Colored Coin , и ее можно считать самой успешной схемой Colored Coin на сегодняшний день. Более того, наиболее успешным применением протокола Omni является Omni-USDT.

DMCH использовала существующую анонимную технологическую структуру (кольцевая подпись + одноразовый адрес + RingCT) для абстрагирования набора Omni-подобных технологических рамок. Это означает, что вы можете легко выпускать свои собственные анонимные цифровые активы на DMCH без выпуска своей собственной основной цепочки или смарт-контракта, и вам даже не нужно писать строку кода.

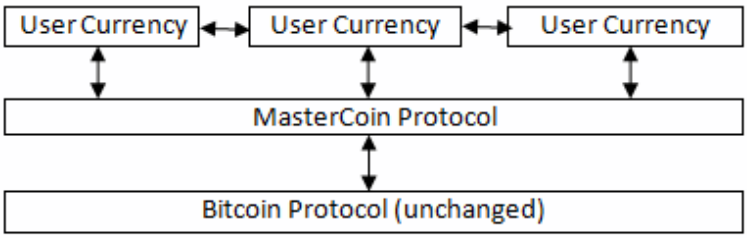

Рисунок 2.7 Протокол Omni

2.5.6 Решение DRC-20

Токен DRC-20-это тип смарт-контракта DMCH, который соответствует стандарту DRC-20. Стандарт DRC-20 определяет ряд широко используемых интерфейсов для операций с цифровыми активами, что облегчает реализацию языков DMCH C и GO (на основе WASM). Обратите внимание, что DRC-20-это всего лишь серия определений интерфейса и не содержит конкретных реализаций. Другими словами, разработчикам цифровых активов необходимо написать свои собственные смарт-контракты для реализации методов, указанных в стандарте DRC-20. Как и другие общие смарт-контракты, окончательное выполнение токена DRC-20-это, по сути, программа смарт-контрактов, работающая в виртуальной

машине DMCH (DVM). Сам протокол DMCH не заботится о бизнес-логике контракта, поэтому производительность конкретного токена DRC-20 полностью зависит от уровня программирования его разработчика.

2.6 Другое

Как показано на системной диаграмме технического плана блокчейн – проекта DMCH на рис. 2.1, технический план проекта DMCH непрерывно оптимизируется и модернизируется в соответствии с принципами двух циклических итераций - "обучение, исследование, интеграция, оптимизация" и "рынок, спрос, капитал". Существует шесть аспектов факторов для оценки модернизации технологий, а именно безопасность, пропускная способность транзакций, расширяемость, время подтверждения транзакций, децентрализация и использование ресурсов. В дополнение к вышеприведенным главам, технологии, находящиеся на экспериментальной стадии, включают в себя комбинацию технологии VRF и технологии Block-DAG, переход между MLSAG, CLSAG и технологией Triptych, а также оптимизацию и отбор баз данных и т.д.

Глава 3 – Core Ecology of DMCH Project

Конкретная практика анонимного, высокопроизводительного и расширяемого децентрализованного финансового решения blockchain требует относительно замкнутой экосистемы (внутренний цикл) и относительно завершенной отраслевой экосистемы (внешний цикл). В настоящее время децентрализованная отраслевая экосистема является относительно полной, а замкнутая экосистема относительно успешна на Ethereum. Однако устойчивое развитие экосистемы Ethereum было ограничено техническими дефектами Ethereum, которые влияют на непрерывное и быстрое развитие системы. Замкнутая экосистема, основанная на DMCH, эффективно дополняет текущую ситуацию, когда экосистема Ethereum недостаточна для удовлетворения рыночного спроса, но в то же время удовлетворяет сильный спрос рынка на конфиденциальность и высокопроизводительные блокчейны.

Блокчейн-проект DarmaCash (DMCH) построит свою собственную базовую экосистему "мгновенных сообщений IM" и "распределенной частной сети", а также финансовую платформу DeFi/DEX, чтобы дать сообществу минимальную систематическую агрегацию, которая сочетает в себе финансовые платежи, безопасные коммуникации и небольшие частные сети в одном, и в конечном итоге развить экосистему DMCH, чтобы даже превзойти экосистему Ethereum.

3.1 Финансовая платформа DarmaCash (DMCH)

Восемьдесят процентов мирового богатства находится в руках двадцати процентов людей. Это социальное явление, которое каждый может почувствовать. Мы называем это "расщеплением на две восьмерки" или "эффектом Мэтью"." Эффект Мэтью отражает поляризацию нашего общества, когда богатые становятся богаче, а бедные-беднее. Двадцать процентов - это те, кто устанавливает правила и получает выгоду от корыстных интересов. Большинство людей в мире попадают в эти самые 80%, но большинство из них хотят быть оставшимися 20%. Интересно, однако, что даже если эти люди успешно трансформируются из низшего класса в высший, баланс не будет нарушен, поскольку люди высшего класса будут формулировать соответствующие правила для защиты своих собственных корыстных интересов, то есть меньшинство всегда будет находиться в доминирующем положении.

"Эффект Мэтью" особенно заметен в финансовом мире. В централизованном финансовом мире власть финансов сконцентрирована, и большинство людей лишены возможности получать средства и могут получать лишь небольшую часть прибыли от проекта. Замкнутый финансовый мир-это те оковы, которые мешают дальнейшему развитию экономики, так как правила защищают интересы небольшого числа людей, а остальные исключают большинство.

3.1.1 Проблемы централизованной финансовой системы(CeFi)

Централизованная финансовая система не является здоровой системой. Это просто инструмент для 20% высшего класса, чтобы собрать деньги с других 80% низшего класса. Высокая концентрация власти позволяет централизованным финансовым учреждениям маркировать, отслеживать и даже блокировать ваши личные активы. Банки являются воплощением централизованных финансовых институтов. Когда обычные люди передают контроль над своими активами банкам или трастовым компаниям, эти финансовые посредники могут легко использовать деньги на рынке для инвестиций, и когда они получают высокую прибыль, они дадут своим клиентам обещанную прибыль. Однако финансовые кризисы низкокачественных ипотечных кредитов часто происходили на протяжении всей истории. Централизованные финансовые институты не могли предвидеть эти риски и были еще более склонны к ошибкам. Эти риски нанесут большой вред централизованной системе. В централизованном финансовом мире существуют пороговые значения для участия в финансовых событиях. Например, частный капитал, венчурный капитал и финансовые слияния и поглощения связаны с частными фондами или некоторыми крупными фигурами на финансовом рынке, и обычные инвесторы никогда не смогут преодолеть разрыв в капитале. Поэтому большинство качественных проектных возможностей контролируются высшим классом. Даже если вы досконально разбираетесь в будущем развитии отрасли, вас все равно могут закрыть из-за недостаточной капиталоемкости.

3.1.2 Децентрализованная система финансов (DeFi) of DarmaCash (DMCH)

Концепции “децентрализованных финансов, распределенных финансов и программируемых финансов”, о которых мы слышим все чаще, могут иметь равную ценность для DeFi, которая имеет несколько выдающихся особенностей:

(1) Основаны на блокчейн технологиях;

(2) Активы контролируются физическими лицами;

(3) Клиринг и расчеты осуществляются в режиме реального времени с помощью смарт контрактов;

(4) Уровень доверия между людьми снижается за счет минимизации зависимости от доверия;

Децентрализованные финансы (DeFi)-это технология с открытым исходным кодом, которая направлена на устранение посредников путем введения децентрализованного слоя, для того, чтобы улучшить текущую финансовую систему во всех аспектах. DarmaCash (DMCH) ожидает, что каждый будет сам себе хозяином, и каждый может свободно планировать свои собственные активы, без угрозы наблюдения, контроля или блокировки централизованных учреждений. DarmaCash (DMCH) построит утопический мир DarmaCash (DMCH)

на основе децентрализации, конфиденциальности и беспристрастности, который обеспечит финансовую безопасность и равенство для каждого участвующего инвестора, чтобы бороться против контроля активов и надзора в реальном мире, и, чтобы устранить вред от централизованной системы финансов, построить по-настоящему децентрализованный финансовый мир.

Утопия подразумевает «воображаемое место», или «идеальное место», также она может относиться к положению вещей, в котором все идеально. DarmaCash(DMCH)- это настоящий финансовый мир, который основан на конфиденциальности и может создавать условия для выдачи персональных стабильных денег. Благодаря атомному обмену и Oracle, реализуется обмен величин между конфиденциальными стабильными деньгами и DMCH, который позволяет обмен между новым финансовым миром и миром реальным. Мы называем это DMCH-утопия.

3.1.3 Логика проектирования DeFi / DEX

Ниже приводится логика проектирования Dharma (DMCH) DeFi / DEX:

(1) Выпуск DMSwap на основе Ethereum. Пожалуйста, обратитесь к 3.1.4 для более подробной информации.

(2) Выпуск DSC (стабильные монеты DarmaCash):

• Maker - это система смарт-контрактов на Ethereum, которая предоставила первую децентрализованную и базовую стабильную валюту DAI (которую можно просто понять как доллары США на Ethereum) и производную финансовую систему. DAI выдается посредством полной ипотечной гарантии цифровых активов, при этом 1 DAI равен 1 доллару США. С момента запуска в 2017 году DAI всегда был привязан к доллару США, и DMCH будет использовать тот же протокол для выпуска стабильной валюты DSC для DMCH.

• Принцип того, что DSC может стать стабильной валютой, аналогичен принципу DAI. DSC всегда имеет избыточное обеспечение, а это означает, что за DSC всегда имеется достаточно активов. Если цены на активы вырастут, то гарантия DSC будет более адекватной. Если стоимость актива упадет до определенного значения (первоначальный участник CDP не выполнил требования о марже или не погасил DSC), контракт будет автоматически ликвидирован. Любой пользователь может ликвидировать активы, не обеспеченные залогом, и получить безрисковый доход в размере 3%. Это побудит многих участников рынка сыграть роль хранителя в Maker. Они могут не только получить выгоду от системы, но и защитить платежеспособность DSC.

• Ликвидность и погашение - важные инфраструктуры для успеха DMCH. DMCH будет распределять 20% от общего объема выбросов среди LP, которые обеспечивают ликвидность для DMCH / DSC.

3.1.4 Основанная на Ethereum DMSwap

В 2020, AMM DEX, которая основана на концепции of DeFi стала свидетелем взрывного роста. Ethereum извлек выгоду из популярности AMM Pool, с дальнейшим развитием ее системы. В теории, основанная на DMCH DeFi/DEX платформа имеет более высокий TPS и более низкий GAS нежели Ethereum, она так же поддерживает защиту конфиденциальности, которая имеет больший потенциал, чем Ethereum. Учитывают, что майнинг породил сифонный эфект, и поставил Ethereum в доминантное положение, DarmaCash (DMCH) запустит проект DMSwap, который основан на Ethereum. Дизайн концепция DMSwap берет свое начало в Uniswap и SushiSwap. Тем не менее, в отличие от Uniswap, SushiSwap и других проектов, DMSwap не только имеет различные механизмы стимулирования, такие как стимулы рекомендаций пользователей, стимулы рекомендаций проектов, стимулы транзакций и выкуп токенов, но и получил анонимную блокчейн-Dharma (DMCH) в качестве поддержки ценности в другом измерении. DMSwap в конечном итоге вернется к системе DEX DarmaCash (DMCH).

Основываясь на общем планировании проекта DarmaCash (DMCH), мы разработали проект DMSwap с следующими целями:

(1) Для проверки реализуемости бизнес-модели на основе платформ DMCH DEX и DeFi s;

(2) Обеспечить более высокую ликвидность для DMCH за счёт AMMPool;

(3) Захватить и зафиксировать долю рынка перед запуском платформ DMCH DEX и DeFis;

(4) Исследовать экосистему ETH, и позволить экосистеме ETH узнать больше о DMCH.

В отличие от Uniswap и SushiSwap, DMSwap ввел следующие аспекты:

(1) Реализован план стимулирования пользователей (реферальные отношения), и рассчитал цену GAS;

(2) Были созданы транзакционные дивиденды;

(3) Транзакция дает создателю гибкость в определении взносов;

(4) В процессе обмена можно указать сторонний адрес;

(5) Участники сделки могут получить DMS (DMS является платформой валюты DMSwap);

(6) Для сделки используется 20% взноса за транзакцию in DMS;

(7) Был реализован план стимулирования проекта и двойной механизм стимулирования токенов, что означает, что если A делает LP для B на DMSwap, то A может получить не только DMS, но и сам токен стимулирования проекта B.

3.1.4.1 DMS

DMS это токен протокала DMSwap. Владение DMS означает обладание всеми правами и интересами платформы DM Swap, а также правом голоса за развитие DMSwap. Все держатели DMS могут голосовать за основные решения по DMSwap. В настоящее время DMS можно получить четырьмя способами: рекомендовать DMSwap другим пользователям, рекомендовать DMSwap другим проектам, стать LP для DMSwap или совершить транзакцию в DMSwap. Часть торгового сбора будет использована для сделки в DMS.

3.1.4.2 DMCHE

DMCHE-это токен ERC 20 на блокчейне Ethereum, поддерживаемый равным количеством нативных DMCH (на блокчейне DarmaCash). Один DMCHE стоит столько же, сколько один локальный DMCH, и пользователи могут передавать данные между DMCH и DMCHE в любое время через DMCH-мост..

3.2 Система моментальной отправки сообщений DarmaCash (DMCH)

Обмен мгновенными сообщениями является частью социальной сети. Являясь самой разветвленной инфраструктурой и открытой платформой интернета, социальные сети значительно повысили эффективность и скорость социального взаимодействия. Мгновенные сообщения, разработанные на базе DMCH сети, станут социальной платформой следующего поколения, основанной на технологии блокчейн, а в сочетании с DeFi IM станет первым социальным финансовым приложением, построенным на блокчейне. Это позволит всем пользователям DMCH иметь чувство принадлежности и общаться в рамках определенной группы.

3.3 Система распределенных частных сетей DarmaCash (DMCH)

Распределенную частную сеть можно понимать, как специфическую форму web3.0. Распределенная частная сеть на базе DMCH, отличающаяся анти-DDoS, антиблокировкой, высокой скоростью и стабильностью, имеет большие преимущества, чем текущая интернет-инфраструктура. Узлы PPoS DMCH полагаются на свой механизм экономического стимулирования для формирования глобально распределенной сети (как показано ниже). Когда DMCH имеет достаточное количество узлов PPoS, формируется децентрализованная распределенная сеть малого мира. Это позволит создать кратчайший путь между любыми двумя клиентскими концами всего в 2-3 узлах и обеспечить наиболее

полную блокчейн-инфраструктуру для децентрализованной прикладной системы DMCH. На этой основе распределенная частная сеть на базе DMCH может управлять всеми текущими интернет-ресурсами, включая IP-ресурсы, ресурсы доменных имен, ресурсы контента и т. д. В этой новой сети малого мира DMCH изменила для нас совершенно новый мир Интернета.

Глава 4 – Механизм реализации токенов

4.1 Технические характеристики

Общее количество монет: Более 460 million (467,440,737)
Верификация: PoW + PPoS
Алгоритм: CryptoNight-R (CNR)
Время блока: 15 seconds
Время подтверждения: 90 seconds
Размер блока: 1.5 MB
Предварительная добыча: 3% (более 14 миллионов), все пожертвованные в сообщество DMCH

4.2 Выпуск майнинга

На начальном этапе, часть DMCH была выпущена через майнинг PoW. С тех пор как PPoS был выпущен в сети, DMCH перенял модель майнинга PoW+PPoS, большая часть DMCH будет сгенерирована майнингом PPoS.

4.3 Кривая дешифрации

DMCHv1 это первая ступень, которая переняла верификацию PoW. В самом начале, каждый блок выпускает 589 DMCH, который один раз в месяц сокращается вдвое, а добыча длится 8 месяцев.

DMCHv2 это вторая ступень, которая переняла верификацию PoW + PPoS. Сначала каждый блок выпускает 7.4 DMCH, и 5% из которых распределяется между майнерами PoW, 65% - между узлами PPoS и пользователями, 30% используется в качестве операционного вознаграждения узла PPoS на ранней стадии, но процент позже снижается до 10%, так как оставшиеся 20% используются в качестве вознаграждения за обслуживание ликвидности DMCH. Вознаграждение за блок будет уменьшаться блок за блоком, а на второй год количество вознаграждений сократится вдвое, а после того, как оно сократится примерно до 1%, оно будет уменьшаться вдвое каждые четыре года, и цикл сокращения производства будет определяться в соответствии с голосами сообщества. DMCHv3 примет верификацию PPoS.

4.4 Принцип дешифрации

Механизм дешифрации и распределения DMCH может быть изменен в соответствии с практическими условиями. Принцип переделки благоприятствует дальнейшему развитию проекта.

Глава 5 – Стратегический план

Time		Plan
2018	**Q1**	Исследование и разработка сети DMCH Технологическое исследование и разработка Block-DAG Оптимизация протокола CryptoNote Оптимизация кольцевой подписи Оптимизация протокола Bulletproof
2018	**Q2**	
2018	**Q3**	
2018	**Q4**	
2019	**Q1**	
2019	**Q2**	
2019	**Q3**	
2019	**Q4**	Выпущена основная сеть DMCH онлайн Выпущен онлайн-обозреватель блоков DMCH Выпущен мобильный кошелек DMCH
2020	**Q1**	Переход верификации от PoW к PoW+PPoS
2020	**Q2**	Исследование и разработка DMCH EVM Анонимная разработка контракта Оптимизация Oracle Технологические исследования и разработки атомного обмена
2020	**Q3**	
2020	**Q4**	VRF+PPoS R&D Анонимная разработка токена Оптимизация смарт-контрактов Разработка децентрализованной биржи DEX
2021	**Q1**	VDF+VRF+PPoS R&D SDWAN R&D IM R&D
2021	**Q2**	
2021	**Q3**	
2021	**Q4**	