FEBRUARY, 2018

POSITION PAPER

V. 2.1

ENECUUM

Оглавление

1. Abstract

Валюта для экономики — то же, что язык для речи. Есть и историческая конкуренция, и заимствования, и потери при переводе. Язык растет и развивается пропорционально количеству говорящих и объему произнесенного/написанного/прочитанного, то есть количеству проведенных на нем “транзакций”. Языки держатся на плаву и сопротивляются вымиранию самим своим использованием и благодаря дарвинистской способности к адаптации. Большинство традиционных валют развивались естественным путем, как говоры и диалекты. У искусственно сконструированных языков всегда было мало, а то и никаких шансов выжить, несмотря на их притязания на всемирный охват, тщательно продуманные элементы и отсутствие, например, неправильных глаголов.

Теперь, когда мы вступили в эпоху криптовалют и блокчейна, своего рода искусственных языков, становится очевидно, что же необходимо любой платформе, чтобы при проведении транзакций выбор пал именно на нее. Та самая способность меняться. В то время, как у многих блокчейнов жесткие и даже неуклюжие системы, система Enecuum высоко адаптивна и по-настоящему децентрализована, поскольку ее участники могут голосовать за введение новых свойств для улучшения функционала без изменений протокола. Кроме того могут вноситься изменения в параметры блокчейна и путем представления варианта измененного протокола. Ниже представлены все технические объяснения, но ключевой момент прост и ясен: мы уверенны, что с усиленными конфиденциальностью, безопасностью и масштабированием, но, прежде всего, способностью меняться и адаптироваться Enecuum - это блокчейн будущего, который приходит надолго.

Он СКОНСТРУИРОВАН ДЛЯ ЖИЗНИ.

2. Disclaimer

<Получить от юристов>

3. Введение

С момента создания Bitcoin в 2009 году лежащая в его основе технология блокчейн открыла новые перспективы развития мировой экономики. Последующее появление смарт контрактов[1], позволяющих заключать и автоматически исполнять сделки по заранее определенным условиям, значительно расширила потенциал ее применения. Мы считаем, что блокчейн способен по-настоящему реформировать многие из областей финансово-хозяйственной деятельности, такие как торговлю, финансовые рынки, голосование и даже логистику.

На сегодняшний день разработки в этой области ведут практически все ведущие институты – крупнейшие банки и корпорации объединяются в консорциумы, а государства ищут пути для создания правового поля вокруг технологии.

Существующие решения, одним из самых ярких представителей которых является Ethereum, уже предоставляют широкие возможности для их применения в различных сферах. Тем не менее, для дальнейшего развития и массового распространения технологии блокчейн необходимо преодолеть ряд проблем, которые можно условно объединить в три категории – масштабируемость, безопасность и конфиденциальность.

3.1 Масштабируемость

Обратной стороной всех преимуществ децентрализованной структуры блокчейна является его ограниченная пропускная способность. По факту, большинство существующих механизмов достижения консенсуса в распределенном реестре – это компромисс между высоким числом транзакций и степенью централизации сети [1]. Это означает, что стремление к увеличению количества обрабатываемых транзакций зачастую ведет к возрастанию рисков, связанных с надежностью работы системы. Кроме того, по мере роста размера блокчейна будут увеличиваться требования к дисковому пространству, ширине Интернет-соединения и вычислительным мощностям, в результате чего количество полных нод может снизиться, что также негативно скажется на безопасности всей сети.

3.2 Безопасность

Помимо проблем, связанных с вопросами масштабирования блокчейнов, существует ряд угроз, возникающих в результате различных особенностей их архитектуры. Так, механизм подтверждения транзакций, основанный на алгоритме Proof of Work, привел к высокой концентрации майнинговых мощностей в Китае, поскольку цена на электричество в этой стране является одной из самых низких в мире. Этот факт значительно увеличивает

[1] Смарт-контракт (англ. Smart contract — умный контракт) — компьютерный алгоритм, предназначенный для заключения и поддержания коммерческих контрактов в технологии блокчейн.

различные риски, связанные с централизацией системы, например, такие, как возможность провести «Атаку 51%»[2].

Другим источником опасностей являются смарт контракты, которые, в отличие от самого блокчейна, в значительной степени подвержены уязвимостям и багам, уже принесшим пользователям многомиллионный ущерб и нанесшим непоправимый вред репутации всей отрасли. Количество используемых смарт контрактов будет неизменно расти, а существующие способы выявления их слабых мест пока неэффективны.

Кроме того, в последнее время все большую актуальность получает проблема управления децентрализованной сетью, возникающая в результате сосредоточения власти над процедурой внесения изменений в протокол в руках узкой группы лиц [2]. В случае, если взгляды этой группы противоречат интересам остальной части сообщества, возникает конфликт, способный полностью парализовать процесс модернизации системы, необходимый для её стабильного развития, и привести к расколу сообщества.

3.3 Конфиденциальность

Большинство существующих блокчейнов предполагают открытость всех транзакций, что ограничивает их коммерческую привлекательность, а также нарушает приватность частных лиц. Прозрачность является одним из основных преимуществ распределенного реестра, но это свойство далеко не всегда является желаемым, особенно, когда речь идет о переводах между бизнес контрагентами, различных финансовых операциях или других транзакциях, которые пользователи предпочли бы оставить в тайне.

[2] А т а к а 51% – гипотетическая атака на блокчейн, исполняемая группой майнеров, контролирующий больше 50% всей вычислительной мощности системы.

4. Описание продукта

Enecuum представляет собой децентрализованную платформу нового поколения, обладающую уникальными характеристиками, позволяющими реализовать неограниченное количество безопасных и масштабируемых блокчейн сервисов и приложений.

Одним из ключевых преимуществ Enecuum является разработанный нами механизм хранения и записи транзакций HyperDAG[3], который обладает высокой гибкостью настроек, открывающих новые возможности применения технологии блокчейн в бизнес среде. HyperDAG дает возможность создавать на базе системы отдельные цепочки блоков, правила работы которых можно подстраивать под решение любых задач, в том числе задачу быстро и дешево обрабатывать большое количество транзакций.

Более того, данное решение позволяет интегрировать технологию шардинга[4], успешно решающую проблему масштабирования блокчейна.

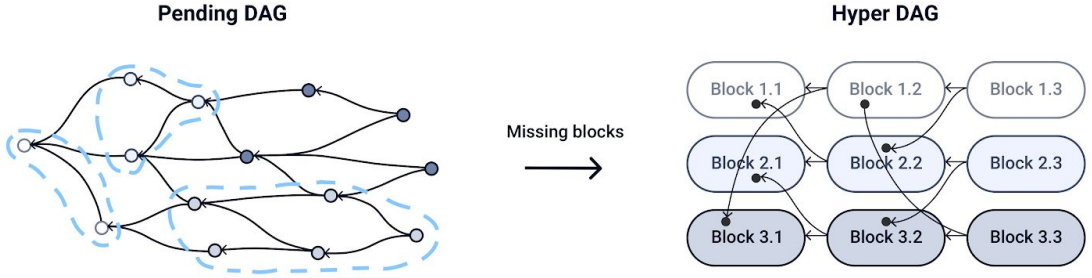

Figure 1. DAG с транзакциями, ожидающими подтверждения, как часть HyperDAG

В Enecuum используется гибридный алгоритм консенсуса, комбинирующий в себе методы Proof of Work (PoW) [3], Proof of Stake (PoS) [4] и Proof of Activity (PoA) [5], последний из которых применяется на практике впервые. Такое сочетание обеспечивает возможность подтверждать транзакции практически с любого устройства, подключенного к сети, что ведет к максимально возможной децентрализации системы и её высокой устойчивости к атакам различного типа.

[3] HyperDAG (Directed Acyclic Hypergraph) - граф, в котором каждым ребром могут соединяться не только две вершины, но и любые подмножества вершин.

[4] Sharding - процесс распределения данных между множеством устройств в сети, при этом сохраняя связность этих данных.

Высокая безопасность Enecuum также достигается за счет использования линейной логики при реализации смарт-контрактов SHARNELL[5]. Линейная логика позволяет проводить надежную автоматическую сертификацию смарт-контрактов перед их публикацией в блокчейн, гарантирующую отсутствие потенциальных уязвимостей, небезопасных вариантов срабатывания, зависаний и прочих нежелательных исходов.

Кроме того, Enecuum является высокоадаптивной системой, что выражается в имеющейся у пользователей возможности принимать участие в её развитии и голосовать за выдвигаемые другими участниками предложения по улучшению её функционала. В целом, повлиять на изменение параметров блокчейна можно будет двумя способами – либо представить конкретный вариант измененного протокола в открытый репозиторий проекта на GitHub[6], чем, вероятно, будут пользоваться опытные разработчики, либо проголосовать за коррекцию каких-либо параметров сети, для внедрения которых внесения модификаций в протокол не требуется. Последний вариант предусмотрен архитектурой системы, и воспользоваться им смогут все держатели криптовалюты ENQ (после завершения тестового периода наладки сети, когда будет открыт для общего доступа алгоритм голосования за параметры консенсуса; во время тестового периода технический контроль сохраняется у команды Enecuum в целях улучшения и работы над протоколом).

Enecuum реализован с использованием функционального языка программирования Haskell, одними из главных характеристик которого являются стабильность выполнения и минимальная возможность появления побочных эффектов. В качестве основного криптографического протокола выбран Cryptonight, с собственными модификациями, имеющий высокую стойкость к ASIC устройствам.

«Топливом» всей системы являются монеты ENQ, которые будут генерироваться системой согласно заданным параметрам и выплачиваться майнерам в качестве вознаграждения за выполняемые ими вычисления. Кроме того, ENQ будут необходимы для проведения транзакций и создания новых токенов и «веток».

[5] SHARNELL - Shared Noncommutative Linear Logic, авторская разработка Enecuum. Эти смарт контракты состоят из математических формул и бизнес-ориентированной логики.

[6] GitHub-аккаунт Enecuum - https://github.com/Enecuum

4.1 Транзакции

На сегодняшний день сложилось два основных подхода к хранению транзакций в распределенных реестрах - в виде блоков (Bitcoin [6], Ethereum [7] и многие другие) и в виде Directed Acyclic Graph[7] (IOTA [8], Byteball [9], Universa [10]). Преимуществом первого метода является его высокая надежность, которая достигается за счет 100% дупликации реестра среди всех подключенных к сети нод. С другой стороны, такой механизм накладывает определенные ограничения на скорость работы сети и потенциал её масштабирования. В Directed Acyclic Graph (далее - DAG) нет блоков, а все поступающие транзакции ссылаются на одну или несколько предыдущих, таким образом подтверждая их. В результате, реестры подобного типа способны очень быстро обрабатывать большой поток транзакций, однако безопасность их работы вызывает некоторые опасения в сообществе [11].

Мы объединили два этих подхода и создали принципиально новый метод записи транзакций, который называется HyperDAG. Его ключевое отличие от оригинального DAG состоит в том, что транзакции, поступающие в систему, могут ссылаться не только на одну из предыдущих транзакций, но также и на их группу (которая входит в блок) (см. Рисунок 2, подробнее см. раздел Блоки). В результате, HyperDAG успешно совмещает в себе преимущества обоих методов и одновременно решает их недостатки – обрабатывает тысячи транзакций в секунду и имеет высокую степень защиты от атак.

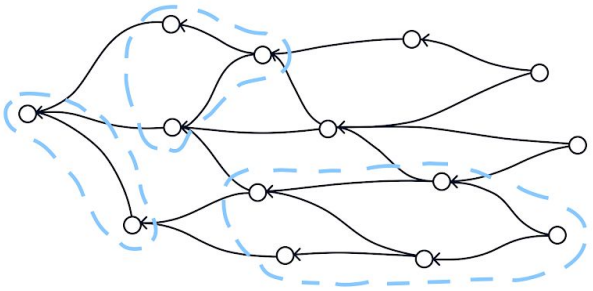

Рисунок 2. Принцип работы HyperDAG

Подобный метод представления транзакций обладает большими возможностями по их сортировке, анализу и выборке. Так, появляется возможность создавать различные ветки (цепочки блоков) в рамках одной сети, а также применить технологию шардинга, увеличивающую скорость работы сети и избавляющую её от необходимости 100% дупликации всей содержащейся в блокчейне информации среди подключенных нод.

[7] Directed acyclic graph (DAG) - ориентированный граф, в котором отсутствуют направленные циклы, но могут быть «параллельные» пути, выходящие из одного узла и разными путями приходящие в конечный узел.

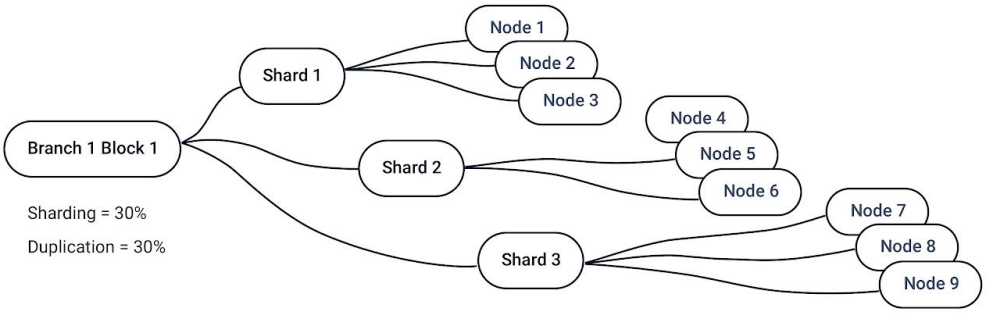

Рисунок 3. Шардинг

Транзакции в Enecuum имеют несколько параметров - дупликация[8], шардинг и quality of service (QS), последняя из которых по сути является скоростью исполнения транзакции. Дупликация увеличивает безопасность блокчейна, но сдерживает скорость его работы, шардинг - наоборот. По умолчанию настройки выставлены следующим образом: дупликация - 30%, шардинг – 30%, QS - нет. Возможность изменения этих параметров позволяет масштабировать сеть, а также создавать уникальные сервисы в рамках отдельных веток системы.

4.2 Блоки

По мере накопления в HyperDAG достаточного количества транзакций для создания блока, происходит его сборка. Анализируя заданные параметры транзакций, майнеры определяют их ценность для системы и объединяют в соответствующие блоки. Благодаря внедрению двойных хэш-ссылок на предыдущие транзакции [MD1] , параллельно могут майниться до N блоков, содержащих в себе разные транзакции, что по сути ускоряет их прохождение в N раз. Предел N динамический и может быть например 1000, что дает скорость транзакции рассчитанную как 1000 x 62 x 40 = 2 480 000 транзакций в секунду, где 40 - максимальное число транзакций самого маленького блока, 62 – количество устройств в команде PoA, проверяющих транзакции (из 64 участников команды), 1000 – число параллельно майнящихся макроблоков.

Размер блока в Enecuum не имеет фиксированного значения и варьируется от 4 Кб до 4 Мб. Блоки минимального размера могут создаваться для проведения операций с минимальной задержкой, а при увеличении нагрузки на сеть их размер будет возрастать. В случае, если потребуется блок больше 4 Мб, система также позволяет объединять их в любом количестве в макроблоки, позволяющие записывать в блокчейн неограниченные объемы данных.

[8] Дубликация - повтор данных (транзакций и т.д.) на всех нодах в сети. Такой подход позволяет достигнуть высокой надёжности системы.

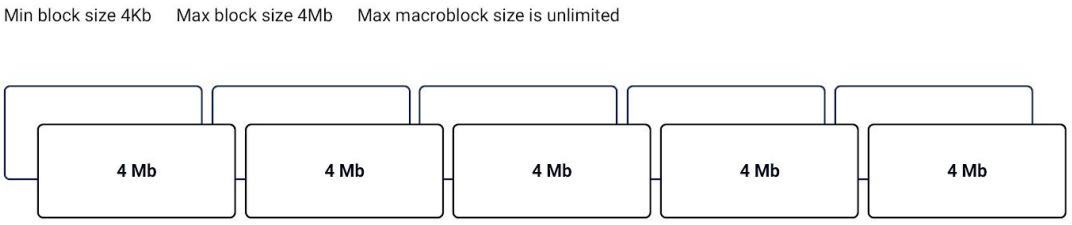

Рисунок 4. Блоки в Enecuum

Для снижения времени между созданием блоков (Latency) в макроблоки Enecuum внедрен протокол Bitcoin-NG [12]. Суть его работы заключается в том, что каждый микроблок внутри макроблока создается в реальном времени, добавляя в блокчейн транзакции сразу в момент их поступления. Это позволяет не ждать пока сформируется весь большой блок, найдётся его хэш и блок будет синхронизирован между всеми нодами сети.

Структура блоков состоит из 3 основных разделов, представленных на следующей схеме:

Рисунок 5. Структура блоков в Enecuum

4.3 Ветки

Использование HyperDAG для хранения транзакций позволяет формировать «ветки», представляющие из себя цепочки блоков, содержащие только однородные транзакции. По сути, каждая из веток – это отдельный блокчейн, являющийся составной частью всей системы. В каждой из веток могут быть установлены свои правила создания блоков и их подтверждения. При этом, нодам не обязательно скачивать и хранить у себя все неосновные ветки Enecuum.

Схематически процесс распределения блоков по веткам представлен на Рисунке 6. Разным цветом представлены транзакции различного типа, которые попадают в соответствующие ветки.

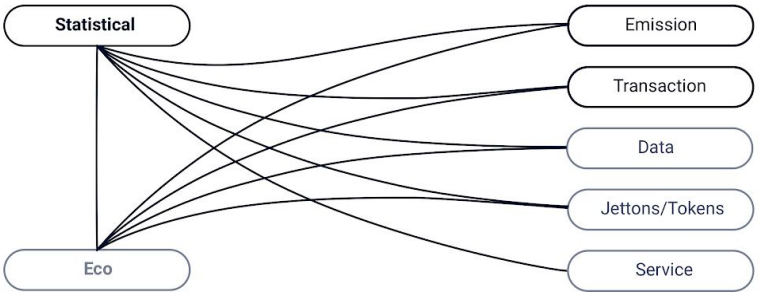

Рисунок 6. Пример распределения блоков по веткам

Ключевыми ветками системы являются:

1. **Транзакционная ветвь**, в которую попадают все обычные транзакции между пользователями с использованием ENQ.
2. **Эмиссионная ветвь**, которая содержит транзакции, генерирующие новые монеты ENQ в качестве вознаграждения за майнинг.
3. **Статистическая ветвь**, накапливающая и анализирующая статистику о работе системы. В неё попадают данные о количестве нод, полученных рекордах в майнинге, размерах блока и многие другие параметры, в том числе и размеры вознаграждений за PoA майнинг (что включает в себя подтверждения транзакций).

Кроме того, в системе Enecuum может быть создано неограниченное количество других веток следующего типа:

4. **Экологические ветки**, служащие «фильтром» от подозрительных операций и транзакций, не прошедших валидацию. Например, если с недавно созданного кошелька в сеть отправляется нехарактерно большое количество транзакций, они попадут сначала в экологическую ветку для более тщательного анализа.

5. **Жетонные ветки**, предоставляющие широкие возможности для реализации различных сценариев. Если в системе Enecuum создать жетон (см. пункт 1.6.) и выпустить под ним токены, все операции с таким жетоном и этими токенами могут быть зашифрованы и храниться в отдельных ветках. Кроме того, в жетонных ветках возможны свои правила работы. Например, все ноды могут признаваться валидными и поступающие от них транзакции будут проводиться гораздо быстрее из-за отсутствия необходимости достижения консенсуса между всеми участниками сети.

6. **Сервисные ветки**, позволяющие создавать всевозможные децентрализованные сервисы, такие, как голосования, опросы, мессенджеры и приложения для документооборота. В транзакции таких веток может быть добавлена дополнительная информация, что позволит создать гибкие условия для решения практически любой задачи на блокчейне.

7. **Дата ветки**, представляющие из себя децентрализованные хранилища. Принцип работы дата веток схож с протоколом BitTorrent, однако вместо традиционного хеширования в Enecuum применяется собственный алгоритм бесшовного хеша[9]. В результате, авторизованные пользователи смогут получить доступ даже к части зашифрованного файла, чего нельзя сделать в BitTorrent.

4.4 Три типа майнинга

Консенсус в блокчейне Enecuum достигается в результате взаимодействия трех алгоритмов майнинга – Proof of Work, Proof of Stake и Proof of Activity. Использование данной комбинации позволяет достичь максимально возможной децентрализации сети, значительно повысить безопасность и ускорить её быстродействие.

Условно процесс подтверждения транзакций в Enecuum можно разделить на 3 этапа. На первом из них подключенные к сети PoW майнеры анализируют HyperDAG и собирают транзакции для сборки блока. После нахождения удовлетворяющего текущей сложности хеша блок еще не считается валидным, а распространяется по сети для подтверждения PoA майнерами.

[9] Бесшовный хеш -

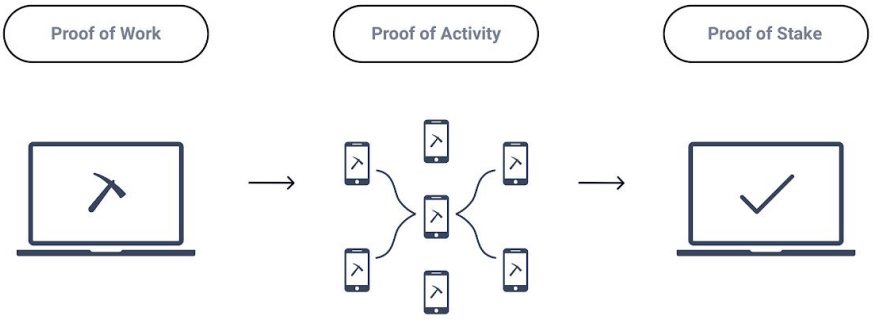

Рисунок 7. Консенсус в Enecuum

Далее PoA майнеры, объединенные в команды по несколько участников, проверяют полученный хэш и, в зависимости от того, какие транзакции включены в блок, прикрепляют его к одной из веток системы. Проверка хэша блока на корректность не требует больших вычислительных мощностей, поэтому данную операцию можно будет производить даже с самых простых устройств, включая мобильные телефоны. Кроме того, формирование команд будет происходить на основе анализа нескольких факторов, включающих географическое положение ноды, степень её участия в системе и многих других, с целью достижения наивысшего уровня безопасности консенсуса.

Роль PoS майнеров будет заключаться в постоянной перепроверке достоверности транзакций в системе и полученных в их результате балансов кошельков. За эту активность они будут получать часть предназначенного за майнинг вознаграждения в виде процентов на остаток. При этом, системой будут определены минимальный уровень баланса, при недостижении которого деятельность PoS майнеров учитываться не будет, и максимальный уровень, превышение которого не будет приносить дополнительную прибыль.

В отличие от существующих методов вознаграждения, при которых сеть генерирует новые монеты сразу после нахождения валидного блока, в Enecuum в этот момент происходит только начисление баланса (кошелек получает так называемые марки, которые подробнее описаны в разделе 1.6.), а непосредственная выплата за майнинг

происходит в среднем 1 раз в день. Это сделано для защиты сети от взлома её алгоритма майнинга или получения контроля над большинством вычислительных мощностей.

Согласно первоначальным настройкам вознаграждение за майнинг между его участниками будет распределяться следующим образом: PoW – 70%, PoA – 20%, PoS – 10%. Однако, наличие статистической ветки позволяет системе контролировать эту пропорцию, защищая интересы системы от возможных злоупотреблений.

4.5 Смарт-контракты SHARNELL

Для написания смарт-контрактов в блокчейне Enecuum используется язык JavaScript, а виртуальной машиной для их выполнения будет V8 от Google. Система будет поддерживать два типа контрактов:

1. «Легкие» смарт-контракты, состоящие исключительно из математических формул, и основанные на бизнес-ориентированной линейной логике SHARNELL. Линейная логика является полностью предсказуемой, что позволяет свести к минимуму вероятность выявления уязвимостей.

Логические смарт-контракты состоят из формуляра, содержащего описание значений в формуле, и самой формулы, учитывающей любые поставленные условия и вероятности, с возможностью полного или частичного достижения и срабатывания. Каждое условие логического контракта размещается в формуляре и получает соответствующий символ, после чего составляется математическая формула, полностью отображающая условия контракта. Также применяется система π-исчислений[10] для параллельного выполнения расчетов.

Контракты данного типа идеально подходят для выполнения наиболее распространенных операций – таких как multsig, escrow и подобных. В первой версии блокчейна они будут создаваться с помощью графического редактора на основе сетей Петри[11].

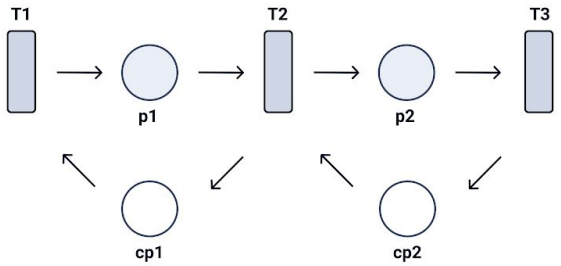

Рисунок 8. Смарт-контракты в Enecuum

[10] π-исчисления
[11] Petri Net Editor

2. «Тяжелые» смарты-контракты, содержащие код, предназначенный для решения более сложных задач, таких как ведение научных расчетов и обучение нейронных сетей.

Данный функционал будет выполнен в выделенной зоне блокчейна, доступ к которому будет оплачиваться криптовалютой ENQ по специально определенной ставке. Так же будет применена система π-исчислений и система каналов с сессионными типами.

4.6 Жетоны и марки

Как было отмечено ранее, в системе есть понятие жетон. Жетон - это криптографический суррогат, такой же, как и токен, который может быть создан любым пользователем системы. Жетон служит для создания выделенной зоны (собственной ветки), в которой обращение основной валюты блокчейна ENQ недоступно. При этом, жетон одновременно является доступом и ключом для расшифровки транзакций в соответствующей ему жетонной зоне и может быть свободно передан между пользователями системы.

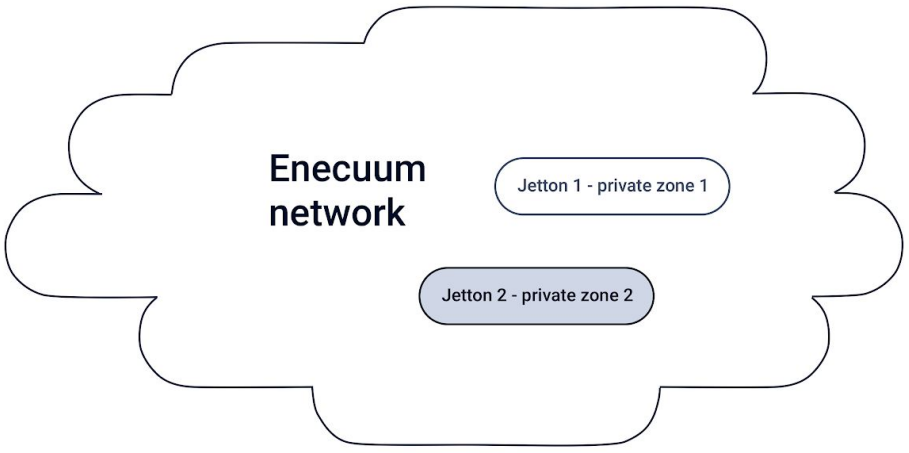

Рисунок 9. Жетоны и жетонные зоны

Жетоны могут включать в себя токены, принятые к обращению в соответствующей жетонной зоне. Конвертация таких токенов в основную валюту блокчейна будет происходить через соответствующий им жетон.

Ключевым назначением жетонов и жетонных зон является возможность создания гибкой среды для удобного взаимодействия бизнеса и их клиентов на базе блокчейн технологии.

Еще одним инструментом, расширяющим функционал блокчейна Enecuum, являются марки. Марки применяются для маркировки токенов, транзакций или кошельков и не могут существовать как отдельная единица, а только в паре с платежной единицей.

Марки используются для обозначения конкретных функций помеченных объектов и обеспечивают строгое выполнение поставленных условий или определенных задач. Предназначение марок не может быть изменено и определяется до их выпуска.

Системой предусмотрены следующие виды марок:

- Марки ускорения транзакций.
- Марки вознаграждений за подтверждения транзакций, которые при накоплении данных в статистической ветке конвертируются в ENQ.
- Марки пометки токенов. Например, владелец помеченных маркой токенов сможет произвести с ними строго ограниченный список действий и перевести их только на помеченные соответствующей маркой кошельки. Такой функционал создает условия, при которых можно эффективно управлять распределением государственного и корпоративного бюджетов, контролировать закупки или выдавать целевые кредиты.

5. Проблемы и решения

5.1. Масштабируемость

Способность дешево и безопасно обрабатывать большое количество транзакций в открытых блокчейнах является одной из самых важных задач, которые необходимо решить для широкого распространения технологии и её адаптации под нужды современного общества. Наиболее часто пропускную способность сетей Bitcoin и Ethereum сравнивают с платежной системой Visa, которая способна обрабатывать более 50`000 операций в секунду [13], что в тысячи раз превышает текущие возможности самых распространенных криптовалют. А учитывая тот факт, что количество пользователей криптовалют в мире растет огромными темпами, в моменты пиковой нагрузки комиссии за транзакции в децентрализованных системах достигают таких величин, при которых их использование в реальных бизнес моделях также становится нецелесообразным.

Простое увеличение размера блока способно повысить количество обрабатываемых транзакций, однако данное решение является частичным и временным. В связи с тем, что записанные в блокчейн данные остаются в нем навсегда, размер блокчейна неуклонно растет. Более того, с увеличением пропускной способности его объем будет расти еще большими темпами, по причине чего в будущем только крупные компании смогут выделить ресурсы, необходимые для хранения и обновления такого массива данных, что вероятно приведет к увеличению централизации сети.

Благодаря использованию HyperDAG для записи и хранения транзакций, Enecuum идеально подходит для реализации шардинга, позволяющего разделить блокчейн на несколько более мелких частей, представленных отдельными ветками или их частями и обрабатываемых параллельно. Таким образом, в комбинации с переменным размером блоков, Enecuum сможет эффективно обрабатывать десятки и сотни тысяч транзакций в секунду без ущерба для безопасности системы, в результате чего комиссии за транзакции в большинстве случаев будут равны нулю или иметь минимальные значения.

Кроме того, возможность создания неограниченного количества веток в системе позволит создавать на их основе различные коммерческие приложения, не требующие создания собственного блокчейна и не нагружающие основную ветку Enecuum. Параметры каждой ветки могут настроены индивидуально, отражая потребности конкретного сервиса. Это могут быть как открытые сети, стать пользователем которых сможет любой желающий, так и закрытые системы, работающие среди заданного круга участников. В случае необходимости увеличения скорости транзакций или размера блоков в определенной ветке, можно изменить правила консенсуса соответствующим образом, создав свои ноды. Единственным ограничением будет мощность поддерживающих конкретную ветку нод и их пропускная способность.

На сегодняшний день архитектура блокчейна Enecuum уже позволяет создавать макроблоки неограниченного размера, что является уникальным решением, позволяющим масштабировать скорость работы протокола за счет постоянного роста вычислительных мощностей современных процессоров.

5.2. Безопасность

Низкая децентрализация

В первом поколении блокчейнов транзакции подтверждаются с помощью алгоритма майнинга Proof of Work. Это надежный механизм, доказавший свою эффективность в защите сети от атак различного типа, таких как DoS и спам. С ростом популярности и курса криптовалют PoW майнинг превратился в масштабный бизнес с инвестициями в сотни миллионов долларов США. В результате, низкая стоимость электричества и дешевая рабочая сила в Китае привела к серьезной концентрации майнинговых мощностей в этом регионе, что ставит под угрозу безопасность систем из-за потенциальных картельных сговоров между крупными пулами и возможности проведения «Атаки 51». Появление ASIC устройств еще больше усугубило эту проблему, поскольку майнинг на обычных компьютерах потерял всякий экономический смысл, а централизация власти в руках крупных инвесторов только усилилась [14].

Комбинация трех типов майнинга в блокчейне Enecuum и использование криптографического протокола Cryptonight позволяют достичь максимальной децентрализации системы не только в географическом плане, но также и среди различных типов устройств и социальных слоев населения, что делает его одним из наиболее безопасных распределенных реестров.

Кроме того, наличие статистической ветки, собирающей и анализирующей информацию о состоянии блокчейна, дополнительно защищает систему от потенциальных угроз различного типа, равномерно распределяя степень влияния на консенсус среди всех участников майнинга.

Уязвимости смарт контрактов.

Изобретение смарт-контрактов дало мощнейший толчок развитию всей криптовалютной индустрии, однако на сегодняшний день технология их реализации содержит множество слабых мест. Поскольку после записи в блокчейн смарт-контракт уже нельзя скорректировать, ошибка при его создании может впоследствии обернуться многомиллионными потерями для пользователей, что уже не раз происходило с различными криптовалютными проектами [15].

Существующие методы оценки безопасности смарт контрактов, заключающиеся по большей части в ручном аудите их кода сообществом программистов, крайне неэффективны, поскольку число создаваемых смарт контрактов растет опережающими темпами, а их сложность значительно увеличивается. Кроме того, в наиболее популярной платформе для смарт контрактов Ethereum используется специально спроектированный язык программирования Solidity [16], еще не получивший широкого распространения в среде разработчиков, в связи с чем в этой области наблюдается острая нехватка опытных профессионалов, что также не способствует решению обозначенных проблем.

Линейная логика, используемая при реализации смарт контрактов SHARNELL, выводит безопасность этой технологии на новый уровень. Она позволит проводить надежное автоматическое тестирование смарт контрактов перед записью в блокчейн, что снизит к минимуму вероятность наличия в них ошибок и уязвимостей. Вдобавок, JavaScript является одним из самых популярных языков программирования, в результате чего созданием смарт контрактов сможет заниматься большой круг специалистов.

Централизация власти над блокчейном.

Несостоявшийся апгрейд сети Биткоина Segwit2x и его хардфорк, результатом которого стало появление Bitcoin Cash, свидетельствуют о наличии разногласий в сообществе относительно дальнейшего пути развития первой криптовалюты [17]. К сожалению, архитектура Биткоина устроена таким образом, что его майнеры, разработчики и обычные пользователи имеют различные мотивы, формирующие их взгляды на необходимость внесения тех или иных изменений в протокол [2]. В результате, происходит раскол сообщества на отдельные группы, действующие исключительно в своих интересах, что замедляет эволюционный процесс адаптации системы к изменяющимся условиям рынка и может привести к её устареванию.

Блокчейн Enecuum решает эту проблему, предоставляя всем пользователям равноценную возможность влияния на процесс усовершенствования платформы посредством проведения on-chain голосования за выдвигаемые предложения по оптимизации каких-либо существующих параметров или внедрения новых инструментов.

Более того, внесение требуемых изменений в работу блокчейна Enecuum будет максимально безопасным процессом, поскольку они могут быть заранее протестированы на наличие потенциальных сбоев в одной из вспомогательных веток системы.

5.3. Приватность

Существует расхожее мнение, что криптовалюты анонимны и тем самым предоставляют широкие возможности для осуществления незаконной деятельности. Действительно, несмотря на то, что все транзакции внутри сети прозрачны и открыты, реальные личности и компании, осуществляющие эти переводы, неизвестны. Тем не менее, эта точка зрения является неверной, поскольку за каждой операцией в открытом блокчейне навсегда сохраняются цифровые следы, анализ которых позволяет с высокой степенью

точности определить её настоящих контрагентов. В случае, если злоумышленникам удастся ассоциировать публичный адрес с реально стоящим за ним человеком или компанией, они смогут заполучить о них важную конфиденциальную информацию и нанести непоправимый ущерб [14] [18].

Наличие жетонных зон позволит пользователям Enecuum производить транзакции в приватном режиме, сведя к минимуму риски раскрытия реальных личностей. Жетон является ключом шифрования транзакций, и только его владельцы смогут видеть операции, проведенные в соответствующей жетонной зоне. Если же внутри приватной зоны необходимо применение основной криптовалюты ENQ, то жетоны становятся еще и средством обмена, выступая в качестве разменного инструмента между выпущенными в жетонной зоне токенами и ENQ. Таким образом, ключ шифрования в виде жетона надежно защищает транзакции внутри жетонной зоны от постороннего внимания, а использование всей мощности сети для подтверждения таких транзакции гарантирует, что они будут проходить без задержек.

6. Use cases

6.1. Платформа для проведения ICO

Высокая пропускная способность блокчейна Enecuum позволит стартапам проводить привлечение средств любого масштаба без рисков зависания сети, в результате чего все инвесторы смогут быть уверены, что примут участие в ICO и быстро получат свои токены. Поскольку смарт-контракты в Enecuum будут работать на JavaScript, разобраться с их написанием сможет любой веб-программист, что приведет к значительному удешевлению их создания. Кроме того, использование линейной логики позволит исключить уязвимости в контракте и снизит риски их взлома.

Применение модели отмен позволит реализовать сложные краудсейлы с поэтапным сбором и возвратом средств вкладчиков на любом этапе. Собственная нотация токенов по аналогии с ERC-20 упростит вывод токенов, созданных на блокчейне Enecuum, на биржу после ICO.

6.2. Банковский сектор, крупный и средний бизнес, страховые компании

С помощью жетонов и марок банки и государственные учреждения смогут надежно контролировать целевое расходование выданных кредитных и бюджетных средств, а различные компании проводить между собой безопасные расчеты, не опасаясь раскрытия коммерческой тайны. Например, Банк А выпускает свой жетон и под ним выпускает токены USD, EUR. Договорившись с Банком Б о совместном проведении взаиморасчетов через эти токены он передает Банку Б свой жетон. Теперь никто кроме банка А и Б не может прочесть транзакции с этими токенами.

Другой пример - Банк А владеет базой клиентов, ведущих в нем обслуживание своего бизнеса. Таким клиентам присвоены различные марки – признаки их бизнеса (строительная компания, поставщик промышленного оборудования и прочие). В этом случае банк может выдавать токены в целевой кредит бизнесу на строительство нового цеха, помечая токены соответствующими признаками. В результате, компания, получившая эти токены, сможет рассчитаться ими только с определенными организациями, потратив их в соответствии с целью выданного кредита.

Кроме того, возможность добавления аннотации к транзакциям позволяет сделать страховой сервис на блокчейне, учитывающий историю клиента. Так, появится возможность хранить прямо в блокчейне рейтинги пользователей и определять их страховые суммы, проводя автоматические расчеты в смарт контрактах.

6.3. Распределенные вычисления

Возможность исполнения «тяжелых» смарт контрактов в выделенных зонах позволит выполнять сложные вычисления, требующие большой мощности, без нагрузки на основные ветки Enecuum (любые JS библиотеки, нейронные сети, научные расчеты, рендеринг графики и так далее). Оплата таких смарт контрактов будет происходить с помощью ENQ, а её размер будет устанавливаться пользователем, подобно цене транзакции в блокчейне Ethereum. В момент создания заявки заказчик сам устанавливает цену, а майнеры решают, выгодно им предоставлять свои вычислительные мощности или нет. В случае, если исполнители согласны на условия сделки, смарт контракт блокирует средства заказчика для оплаты до выполнения задачи и предоставления валидных результатов, после чего средства автоматически переводятся майнерам.

6.4. Децентрализованное хранение

Применение технологии шардинга и возможность изменения параметра дупликации транзакций позволит эффективно использовать предоставленное пользователями место на их дисках. Например, если 4 пользователя предоставят по 5 Гб пространства, то при установленных параметрах дупликации и шардинга по 50% эффективный объем для хранения файлов будет равен 10 Гб.

Экстраполируя данные выводы на всю сеть, размер «глобального децентрализованного диска» будет расти пропорционально, сохраняя доступность данных и достаточно высокую скорость доступа к ним. В результате, это позволит реализовать на блокчейне Enecuum такие сервисы, как децентрализованные хостинги, облачные сервисы хранения данных и CDN.

Кроме того, применение поверх дата ветки смарт контрактов и жетонов для шифрования даст возможность создавать сложные платные услуги доступа к децентрализовано размещенному (и не изменяемому) контенту, которые можно будет оплатить токенами.

6.5. Микроплатежи, fintech сервисы и IoT

В базовом сценарии развития комиссия за обычные переводы между пользователями в системе равна нулю. Безусловно, с увеличением количества пользователей и появлением приложений, работающих на основе блокчейна Enecuum, нагрузка на него будет возрастать, однако возможность создания отдельных веток с собственными правилами консенсуса, стимулирующего деятельность майнеров, позволит создать условия для работы микро-транзакционных сервисов.

Если такой сервис не станет централизованным, то комиссия за его операции не будет браться вообще. Если такой сервис станет делать множество микротранзакций с одного кошелька, то комиссия появится, но будет взиматься в небольшом размере. Например, в случае работы сервиса по выдаче микрокредитов, совершающего по 10`000`000 транзакции в сутки, все его транзакции могут быть легко записаны в несколько больших макроблоков по 10 Мб. Комиссия будет считаться за весь блок и в расчете на 1 транзакцию будет иметь крайне низкие значения.

В результате, функционал блокчейна Enecuum также может получить применение в области интернета вещей. Реализация простого клиента для майнинга PoA на различных устройствах, подключенных к сети, позволит окупать стоимость производимых ими транзакций. Кроме того, собственный сетевой протокол Enecuum обеспечивает высокую доступность таких устройств посредством установления между ними mesh сети[12].

[12] Mesh сеть -

7. Список литературы

[1] P. Kasireddy, «Blockchains don’t scale. Not today, at least. But there’s hope.,» 2017. [В Интернете]. Available: https://hackernoon.com/blockchains-dont-scale-not-today-at-least-but-there-s-hope-2cb43946551a.

[2] F. Ehrsam, «Blockchain Governance: Programming Our Future,» 2017. [В Интернете]. Available: https://medium.com/@FEhrsam/blockchain-governance-programming-our-future-c3bfe30f2d74.

[3] A. J. Markus Jakobsson, «Proofs of Work and Bread Pudding Protocols (Extended Abstract),» 1999. [В Интернете]. Available: http://www.hashcash.org/papers/bread-pudding.pdf.

[4] V. Buterin, «What Proof of Stake Is And Why It Matters,» 2013. [В Интернете]. Available: https://bitcoinmagazine.com/articles/what-proof-of-stake-is-and-why-it-matters-1377531463/.

[5] C. L. A. M. M. R. Iddo Bentov, «Proof of Activity: Extending Bitcoin’s Proof of Work via Proof of Stake,» 2014. [В Интернете]. Available: https://eprint.iacr.org/2014/452.pdf.

[6] S. Nakamoto, «Bitcoin: A Peer-to-Peer Electronic Cash System,» 2008. [В Интернете]. Available: https://bitcoin.org/bitcoin.pdf.

[7] Ethereum Foundation, «Ethereum Homestead Documentation,» 2018. [В Интернете]. Available: http://www.ethdocs.org/en/latest/.

[8] IOTA Foundation, «The IOTA Developer Hub,» 2018. [В Интернете]. Available: https://iota.readme.io/.

[9] A. Churyumov, «Byteball: A Decentralized System for Storage and Transfer of Value,» 2016. [В Интернете]. Available: https://byteball.org/Byteball.pdf.

[10] Universa Corporation LTD, «Universa Blockchain Platform Whitepaper,» 2017. [В Интернете]. Available: https://universa.io/files/whitepaper.pdf?v=1.3.

[11] N. N. T. D. a. M. V. Ethan Heilman, «IOTA Vulnerability Report: Cryptanalysis of the Curl Hash Function Enabling Practical Signature Forgery Attacks on the IOTA Cryptocurrency,» 2017. [В Интернете]. Available: https://github.com/mit-dci/tangled-curl/blob/master/vuln-iota.md.

[12] A. E. G. E. G. S. R. v. R. Ittay Eyal, «Bitcoin-NG: A Scalable Blockchain Protocol,» 2015. [В Интернете]. Available: https://arxiv.org/pdf/1510.02037.pdf.

[13] J. Vermeulen, «VisaNet – handling 100,000 transactions per minute,» 2016. [В Интернете]. Available:

https://mybroadband.co.za/news/security/190348-visanet-handling-100000-transactions-per-minute.html.

[14] P. Kasireddy, «Fundamental challenges with public blockchains,» 2017. [В Интернете]. Available: https://medium.com/@preethikasireddy/fundamental-challenges-with-public-blockchains-253c800e9428.

[15] M. B. a. T. C. Nicola Atzei, «A Survey of Attacks on Ethereum Smart Contracts,» 2016. [В Интернете]. Available: https://eprint.iacr.org/2016/1007.pdf.

[16] «Solidity,» 2017. [В Интернете]. Available: http://solidity.readthedocs.io/en/develop/.

[17] J. J, «No SegWit2x Makes Bitcoin Cash Shine Amidst Crypto Bloodbath,» 2017. [В Интернете]. Available: https://cointelegraph.com/news/no-segwit2x-makes-bitcoin-cash-shine-amidst-crypto-blood bath.

[18] J. Clifford, «Privacy on the blockchain,» 2017. [В Интернете]. Available: https://hackernoon.com/privacy-on-the-blockchain-7549b50160ec.

[19] "Deep Inference," 2018. [В Интернете]

Available at: http://alessio.guglielmi.name/res/cos/

Глоссарий

https://bits.media/news/kapitalizatsiya-proekta-cardano-uzhe-na-starte-prevysila-polmilliarda-dollarov/

- про управление до 2020 года