AERGO
Technical White Paper

Последнее обновление 17 июля 2018 г.
Перевод: icoinzzz.pro (@coinzzzpro)

AERGO — это новый планируемый блокчейн-протокол, который нацелен на то, чтобы обеспечивать функционирование как публичных, так и частных блокчейн-внедрений. Основываясь на опыте BlockoInc (Blocko) в предоставлении крупномасштабных частных блокчейнов производственного уровня солидным корпоративным клиентам, AERGO станет системой, специально разработанной для того, чтобы создавать условия для корпоративной архитектуры на основе блокчейна путем применения как инновационных, так и проверенных технических подходов к процессу создания масштабируемых систем распределенных баз данных.

Заявление об отказе от ответственности

Данная бумага связана с проектом AERGO и предназначена для ознакомления вместе с белой бумагой, доступной по ссылке https://AERGO.io. Этот и другой документы могут быть в любое время изменены или удалены без предварительного уведомления об изменениях или доступе к какой-либо дополнительной информации.

Данная бумага описывает будущий проект

Данная бумага содержит прогнозные заявления, которые основываются на убеждениях AERGO Limited, частной компании из Гонконга, ограниченной внесенным капиталом (Реестр юридических лиц, №2713137) (AERGO Limited), а также определенных допущениях AERGO Limited и доступной AERGO Limited информации.

AERGO, в соответствии с данной технической белой бумагой, находится в разработке и постоянно обновляется, включая ключевые управленческие и технические функции, но не ограничиваясь ими. Нативный токен AERGO задействуется в разработке и использовании экспериментальных платформ (программного обеспечения) и технологий, которые могут не принести плодов или не привести к достижению целей, описанных в данной белой бумаге. Когда и если AERGO будет завершена, она может существенно отличаться от сети, описанной в данной белой бумаге. Никаких заверений или гарантий в отношении осуществления любых планов, будущих прогнозов и перспектив или их рациональности не дается, и ничто в данном документе не следует рассматривать как обещание или заверение относительно будущего.

Возможные покупатели

Информация в данной белой бумаге предоставляется частным образом определенным возможным покупателям и не предназначена для получения или прочтения кем бы то ни было еще. Право на возможность покупки не гарантировано и может подлежать ограничениям.

Никаких предложений регулируемых продуктов

Платформа AERGO, токен AERGO и любой другой токен, функционирующий на этой платформе, не является ценной бумагой или любым другим регулируемым продуктом в любой юрисдикции. Данный документ не является предложением или попыткой привлечения к приобретению любых ценных бумаг или любых других регулируемых продуктов, как не является рекламой, приглашением или попыткой привлечения к

процессу инвестирования. Условия покупки не являются документом о предложении финансовых услуг или рекламным проспектом любого рода.

Токен AERGO не является долей, акцией, организационной единицей или роялти и не обеспечивает никаких прав на капитал, прибыль, доходы или поступления от платформы или программного обеспечения в AERGO Limited или в любой другой компании, а также на интеллектуальную собственность, связанную с платформой или любыми другими публичными или частными учреждениями, корпорациями, фондами или другими объединениями в любой юрисдикции.

Данная белая бумага не является рекомендацией

Данная белая бумага не является рекомендацией к покупке токена AERGO. Не следует ссылаться на нее при принятии каких-либо решений относительно покупки или заключения контрактов.

Предупреждение о рисках

Покупка токена AERGO и участие в распродаже токена AERGO несет в себе значительные риски. Прежде чем покупать токен AERGO, следует тщательно взвесить и принять во внимание эти риски, включая те, что перечислены в любых других документах.

Мнения, приводимые в данной технической белой бумаге

Мнения и суждения, приводимые в данной технической белой бумаге принадлежат AERGO и не отражают официальную политику или позицию какого-либо правительства, квазиправительства, органа власти или общественного органа (включая любые регулирующие органы любой юрисдикции, но не ограничиваясь ими) в любой юрисдикции. Источники, на которых основана информация, содержащаяся в данной технической белой бумаге, считаются надежными, однако гарантий их точности или полноты нет.

Официальным языком данной белой бумаги является английский

Данная техническая белая бумага и связанные с ней материалы выпускаются только на английском языке. Любые переводы предоставляются исключительно в ознакомительных целях и не заверяются AERGO Limited или любым другим лицом. Никаких гарантий в отношении точности и полноты любых переводов не дается. При возникновении каких-либо несоответствий между переводом и англоязычной версией данной технической белой бумаги правильной считается англоязычная версия.

Никакой принадлежности к третьим сторонам

Ссылки на определенные компании и платформы в данной технической белой бумаге приводятся исключительно в демонстрационных целях. Использование названий и торговых знаков любой компании и/или платформы не указывает на какую-либо поддержку любой из этих сторон или принадлежность к ней.

Вам следует получить профессиональную консультацию

Вам необходимо проконсультироваться у юриста, бухгалтера, специалиста по налогам и/или любого другого профессионального консультанта, прежде чем определяться с покупкой токена AERGO или другим образом участвовать в проекте AERGO.

Данная техническая белая бумага не согласовывалась ни с одним регулирующим органом ни в одной юрисдикции. Ссылки на определенные компании, сети и/или потенциальные варианты применения в данной бумаге приводятся исключительно в демонстрационных целях. За исключением напрямую упомянутых партнеров или провайдеров, таких как Blocko, использование названий и торговых знаков любых других компаний и/или платформ не указывает на принадлежность к любой из этих сторон или их поддержку.

Предпосылки
Blocko обеспечила своей собственной частной блокчейн-имплементацией «Coinstack» более 20 корпоративных клиентов. Coinstack основана на модифицированой архитектуре Bitcoin и исполняющей смарт-контракты Виртуальной машине Ethereum и имеет сходство с QTUM2 и RSK. Хотя Coinstack работала достаточно хорошо даже для крупномасштабных вариантов использования, таких как обеспечение функционирования процесса аутентификации для целой клиентской базы провайдера кредитных карт с миллионами пользователей в день, она также позволила получить представление о верхнем пределе производительности протокола Bitcoin и несовместимости Виртуальной машины Ethereum с корпоративной архитектурой и стоящими за ней разработчиками.

Чтобы лучше использовать цепь инструментов и прикладную архитектуру Coinstack, поддерживая актуальные варианты использования, Blocko начала работать над AERGOSQL и AERGO. AERGOSQL — это инновационная система для смарт-контрактов, способная задействовать реляционную модель данных и позволяющая разрабатывать смарт-контракты, используя инструменты и языки, знакомые корпоративным разработчикам. Детальное описание AERGOSQL приводится в технической белой бумаге AERGOSQL, доступной по ссылке https://AERGO.io/paper/.

В данной бумаге описываются проблемы, препятствующие корпоративным блокчейн-внедрениям, а также новые требования и архитектура, способные решить эти проблемы.

Требования к корпоративным блокчейнам
Мы считаем, что среда и условия работы корпоративных блокчейнов и публичных, универсальных блокчейнов отличаются. Благодаря развертыванию Coinstack, Blocko удалось на своем опыте познакомиться с реальностью освоения корпоративных блокчейнов.

Ниже приводится ряд наиболее общих обстоятельств этого процесса:

- В отличие от пользователей публичных блокчейнов, которые обычно управляют узлами блокчейна на недорогом, стандартном аппаратном обеспечении, компании чаше запускают блокчейны на аппаратном обеспечении серверного уровня, с обширными вычислительными возможностями и хранилищем.
- Компании хотят управлять блокчейном не просто на облаке, а на частом облаке, а также на машинах без предустановленной операционной системы. Функционал, обеспечиваемый частным облаком и средами без предустановленной операционной системы существенно отличается от функционала публичных облачных сервисов.
- Тогда как пользователи публичных блокчейнов управляют узлами блокчейна в небольшом количестве, компании хотят управлять большим числом блокчейн-узлов,

чтобы пользоваться преимуществами горизонтальной масштабируемости и доступности.

- Компании нуждаются в большем контроле и расширенном функционале в отношении администрирования блокчейна, чем пользователи публичных блокчейнов.
- Тогда как большинство приложений, работающих на публичных блокчейнах являются автономными или зависимыми только от активов на самом блокчейне, компании хотят объединять работающие на блокчейне приложения со множеством внешних и внутренних систем, таких как электронная почта, СМС, базы данных, LDAP и общедоступные данные.

Далее рассматривается ряд других ключевых атрибутов, которые, по нашему мнению, являются неотъемлемыми для корпоративных блокчейнов.

МАСШТАБИРУЕМОСТЬ

Поскольку пользователи блокчейна в большинстве случаев имеют доступ к лучшим, как по количеству, так и по качеству, аппаратным средствам, компании должны внедрять свои блокчейн-разработки с масштабированием и по горизонтали, и по вертикали.

ОПЕРАЦИОННАЯ СОВМЕСТИМОСТЬ

Корпоративные системы, как правило, зависят от объема различных технологий, накопленных за годы собственной работы, и при этом блокчейн-проекты компаний должны работать как с современными стандартными интерфейсами, такими как OAuth, так и с подходящими старыми интерфейсами, такими как Active Directory.

СРЕДА РАЗРАБОТОК

Поскольку основная сторона развития предприятия, как правило, ориентирована на проект, разработчикам остается совсем мало возможностей для экспериментов и изучения новых языков и инструментов программирования. Вместо того, чтобы заставлять их изучать новые языки для создания смарт-контрактов, корпоративные проекты должны позволять программистам применять имеющиеся знания и опыт работы со знакомыми инструментами.

В то же время некоторые ресурсы, которые уже считаются само собой разумеющимися, например, неограниченный интернет, остаются недоступными для корпоративных веб-программистов. Следовательно, компании должны обеспечивать более полную, по сравнению с «любительскими» блокчейн-проектами, среду разработки со всеми средствами программирования и интеграции и аппаратными платформами.

КОНФИДЕНЦИАЛЬНОСТЬ ДАННЫХ

Компании сталкиваются с проблемами при обеспечении строгой защиты данных и конфиденциальности информации, а также защиты персональных данных клиентов и сотрудников. Часто безопасность данных является более важным вопросом, чем неизменность и целостность данных в блокчейне. В настоящее время одним из способов обеспечения безопасности данных в частных блокчейн-системах является внедрение шифрования и дешифрования на уровне приложения, однако, корпоративные проекты должны обеспечивать более надежный и целостный подход к обеспечению безопасности данных.

ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

В то время как веб-разработчики с удовольствием используют Vagrant или Docker на своих ноутбуках, для компаний скорее подходят ИТ с более крупными инструментами, такими как Tivoli Provisioning Manager, OpenStack или Kubernetes. Для компаний, работающих с блокчейном, необходимо поддерживать интеграцию с существующими технологиями для управления ИТ-подразделениями предприятия и предоставлять гораздо более богатый набор функциональных возможностей при их администрировании. Экспорт и импорт, резервное копирование данных, мониторинг, протоколирование и миграция данных – это типичные функции, которые игнорируются при реализации частных блокчейн-проектов, но важны в корпоративной среде.

СТРУКТУРИРОВАННОЕ И НЕСТРУКТУРИРОВАННОЕ ХРАНЕНИЕ ДАННЫХ

Смарт-контракты обеспечивают функциональную основу как для общественных блокчейн-проектов, так и для корпоративных. В отличие от децентрализованных приложений, построенных на частных блокчейнах с доступом к облачным хранилищам и агентам в сети доставки содержимого, приложения на корпоративных блокчейнах должны быть более самодостаточнымИ, а сами компании – снабжать их обширными функциональными возможностями как для структурированного, так и для неструктурированного хранения данных.

БАЗОВАЯ АРХИТЕКТУРА

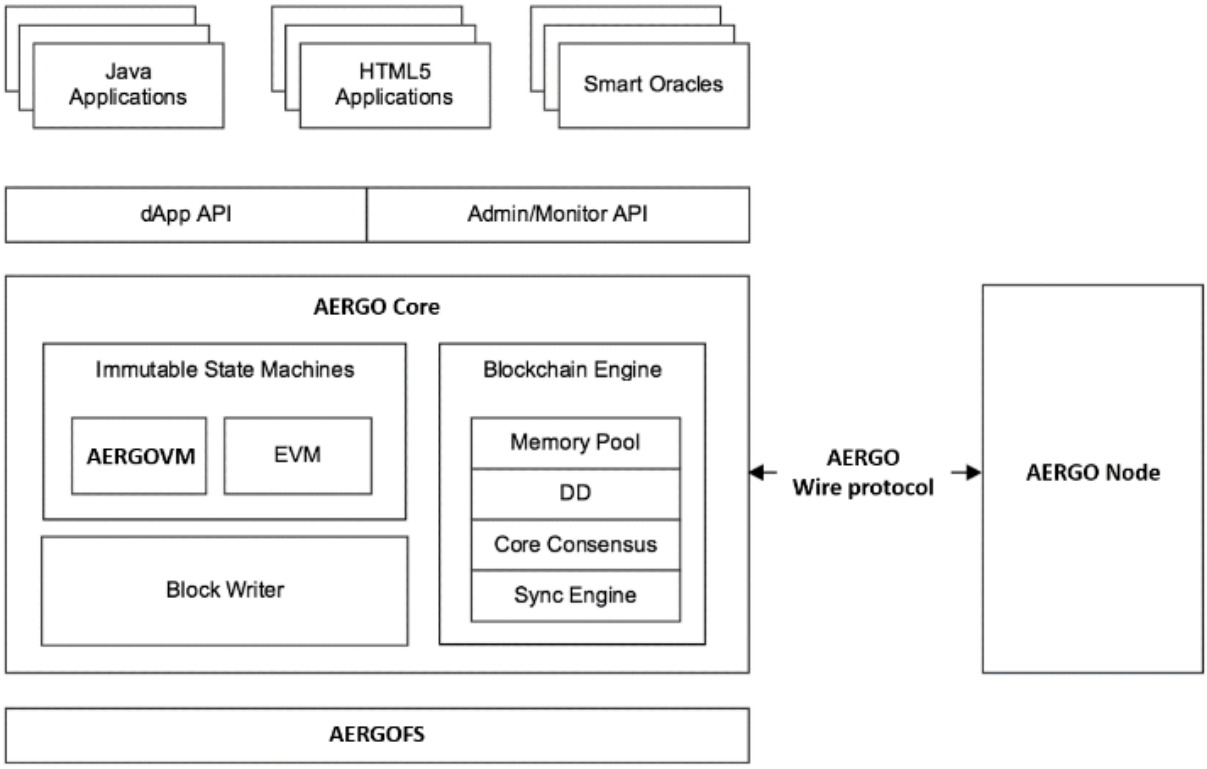

Рисунок 1. Архитектура AERGO

AERGO намерена стать комплексной и универсальной платформой, которая устранит пробел между общедоступным блокчейном и закрытым. Проекту необходимо эффективно работать в обеих средах, следовательно, AERGO должна быть компактной, но гибкой в дизайне.

Для того, чтобы выдерживать рабочие нагрузки с потенциалом в миллионы пользователей, одновременно обращающихся к одной и той же сети узлов, AERGO намерен заимствовать многие концепции как от традиционных разработок по базам данных, так и от проектов по распределенной обработке данных.

РАСПРЕДЕЛЕННЫЙ КАТАЛОГ

Распределенный каталог **(DD)** - это базовое функциональное средство, используемое как отдельный блок при построении всей системы AERGO.

Каждый DD в репозитории управляет независимым изолированным пространством имен. Каждое пространство имен содержит информацию о разных ветвях и тегах в хранилище, а также действительность различных идентификаторов на блокчейне.

Каждый DD сам по себе является блокчейном, со своим первичным блоком и оптимальным блоком. В отличие от обычных, блоки DD ограничены по размеру с относительно долгим интервалом создания между ними; поскольку DD используются для управления метаданными, они должны быть компактными.

DD по своей роли и функциональности сопоставим со словарями данных в базах данных, zookeeper для Hadoop или etcd для CoreOS.

а. Структура (ToL)

Предлагается использовать структурное пространство имен в DD для хранения информации по всем ветвям в репозитории, включая первичные, или корневые, блоки. Информация о тегах управляется внутри структурного пространства имен. В итоге, структурное пространство имен содержит информацию об оптимальном блоке каждой ветви; поскольку HEAD-тег постоянно отслеживает его.

б. Служба распределенных каталогов (DDS)

Пространство имен DDS содержит записи по разным объектам на блокчейне; их открытые ключи и действительность, а также соответствующие функции и разрешения. Пространство имен DDS служит основой контроля доступа к репозиториям AERGO.

Каждый объект может представлять либо клиента-агента, либо сертификат сервера. Причем, для объектов, имеющих сертификаты сервера, DDS может служить как списком отзыва сертификатов, так и DNS с информацией о маршрутизации.

AERGOFS, предлагаемый компонент распределенной файловой системы AERGO, должен зависеть от DDS, поскольку DDS отслеживает объемы данных, состоящие из каждого виртуального узла AERGOFS. В свою очередь, AERGOFS можно использовать для хранения блоков и индексов для разных ветвей в репозитории.

Пространство имен DDS также формирует основу идентифицируемости узлов для участия в базовом процессе согласования.

КОНСЕНСУСНЫЙ АЛГОРИТМ

a. Внутренний консенсус
Внутренний консенсусный алгоритм предназначен для использования его при создании DDS. Внутренний консенсусный алгоритм и DDS взаимозависимы, поскольку Внутренний консенсусный алгоритм должен получить доступ к DDS в рамках распределенного каталога для задействования новых блоков.

Предлагаемый базовый консенсусный алгоритм AERGO является делегированным доказательством доли участия (DPOS). A DPOS является предпочтительной моделью консенсуса, поскольку в целом:

- По мнению разработчиков, он обеспечивает масштабируемость и простоту операций, требуемых внутренним консенсусом; а также
- DPOS работает с допущением, что могут произойти перестройки блоков, и, следовательно, это оптимальный алгоритм для поддержания базовой инфраструктуры AERGO.

б. Пользовательский консенсус
По умолчанию каждый репозиторий использует внутренний консенсус. Поскольку AERGO намеревается обеспечивать подключаемую архитектуру для консенсусного алгоритма, то можно будет использовать различные его схемы вместо базового консенсуса. Примечательно, что RAFT (для разработки) и PBFT (для соблюдения строгого порядка) полезны при разработке и запуске различных сервисов.

Используя один и тот же порядок инструментов при создании смарт-контрактов, в каждом репозитории может применяться и пользовательский консенсусный алгоритм. Заданная пользователем логика может определять, как именно происходят и управляются события в блокчейне.

- Создание блока и его разрешения
- Передача блока и приоритеты

Поскольку разветвление и слияние блоков можно воспринимать также как события реорганизации блоков, для управления распределенной версией применяется все та же политика реорганизации блоков. С точки зрения управления версиями политика реорганизации блоков называется «Согласованное слияние».

СМАРТ-КОНТРАКТЫ
AERGO поддерживает многоагентную парадигму и инфраструктуру, основанную на плагинах смарт-контрактов.

Каждый контракт может быть выполнен или запрошен клиентом-агентом, либо другим смарт-контрактом. Поскольку AERGO предоставляет разрешающий многое интерфейс и максимальную совместимость при реализации смарт-контрактов, то контракты, написанные для виртуальной машины Ethereum, Fabric Chaincode или AERGOSQL, могут применяться друг с другом.

b. AERGOSQL

AERGOSQL представляет собой классический способ написания смарт-контракта для AERGO и реляционную модель данных для хранения и доступа к данным и SQL-подобному скрипту при написании смарт-контрактов.

Используя AERGOSQL, смарт-контракты могут быть написаны с помощью знакомого синтаксиса SQL.

```
CREATE TABLE IF NOT EXISTS accounts   (
        owner VARCHAR NOT NULL PRIMARY KEY,
        balance NUMERIC (15, 2)
);

CREATE OR REPLAE FUNCTION
transfer (sender text, to text, amount numeric (15, 2))
RETURNS text
AS
$$
DECLARE
        sender_bal numeric ;
BEGIN
        SELECT balance INTO sender_bal FROM accounts WHERE owner = sender ;
        IF NOT FOUND THEN
            RETURN 'Sender not found' ;
        END IF
        IF sender_bal < amount THEN
            RETURN 'Not enough balance' ;
        END IF
        UPDATE accounts SET balance = balance + amount WHERE owner = to ;
        IF NOT FOUND THEN
            RETURN 'Receiver not found' ;
        END IF;
        UPDATE accounts SET balance = balance - amount WHERE owner = sender ;
        RETURN 'OK' ;
END
$$
```

Рисунок 2. Пример модели кодирования AERGOSQL

Для максимальной производительности AERGOSQL задействует такие технологии как LLVM для оперативной компиляции и высокой производительности Б-дерева и такие как WiredTiger для хранения данных.

c. Совместимость

Благодаря своей подключаемой архитектуре AERGO способен поддерживать различные вариации смарт-контрактов. AERGO наследует совместимость виртуальной машины Ethereum от BlockoCoinstack по умолчанию. Fabric Chaincode поддерживается благодаря легкой виртуализации, такой как у Docker.

Первоначальная запускаемая версия AERGO будет зависеть от работы виртуальной машины Ethereum. В будущем планируется использование оперативной компиляции виртмашины Ethereum для повышения производительности.

СМАРТ-ОРАКУЛЫ

AERGO, посредством внедрения смарт-оракулов, поддерживает интеграцию смарт-контрактов внутри закрытой экосистемы на блокчейне, а также смарт-контрактов, учитывающих внешние события и факторы. Смарт-оракулы смогут обеспечить следующие функциональные возможности:

- Разрешать смарт-контрактам брать данные из устаревших систем, таких как Active Directory
- Разрешать смарт-контрактам запускать события на внешних сервисах, таких как электронная почта или SMS

С точки зрения смарт-контракта: смарт-оракулы являются внешними факторами, которые связаны с конкретным смарт-контрактом; смарт-оракулы реагируют на изменения соответствующего смарт-контракта и вводят данные в качестве ответа. В некоторых случаях они способны запускать смарт-контракты автономно.

С точки зрения децентрализованного приложения: смарт-оракулы реализуют микросервисы, которые задействуют внешние функции, требуемые этим приложением. Поскольку смарт-оракулы и децентрализованные приложения могут обмениваться данными вне сети, то микросервисы смарт-оракулов могут использоваться для внешней связи, требуемой смарт-контрактом; а обычный пользовательский сценарий включает в себя обмен аутентификационным маркером между смарт-оракулом и децентрализованным приложением.

Изоморфные контракты

Набор инструментальных средств разработки AERGO намерен поддерживать изоморфное выполнение смарт-контракта посредством автоматической генерации кода. Такой изоморфный код, созданный с помощью смарт-контракта, может быть доступен как децентрализованным приложениям, так и смарт-оракулам, что обеспечивает прозрачный доступ к смарт-контракту и базовой структуре данных. Изоморфное выполнение смарт-контракта имеет решающее значение для эффективности разработки смарт-контракта, приложений и сервисов на его основе.

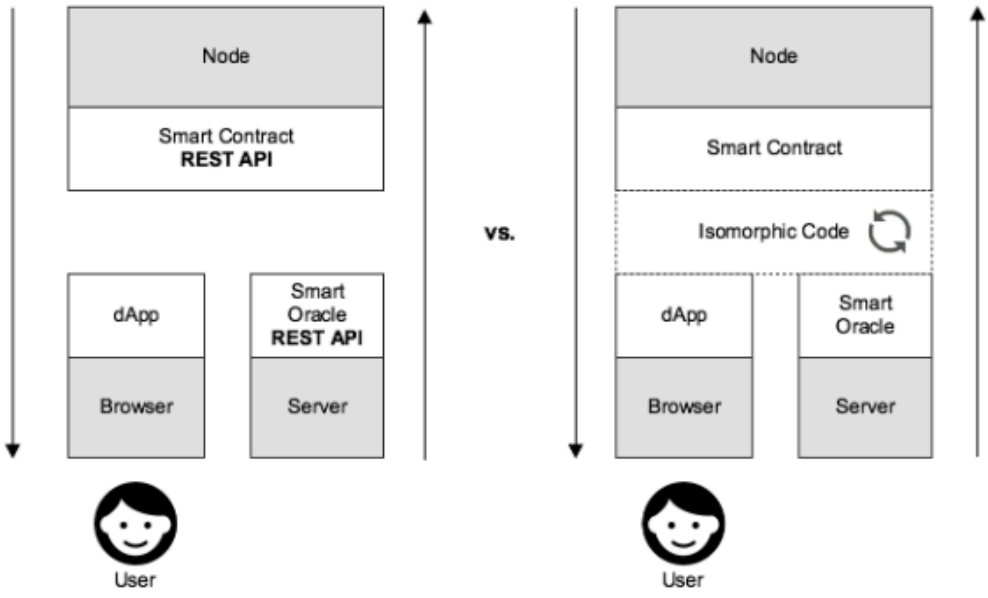

Рисунок 3. Обычное dApp против изоморфной архитектуры dApp

Не все языки смарт-контрактов поддерживают изоморфные контракты; поддержка изоморфных контрактов ограничивается контрактами, написанными для AERGOSQL.

РАСПРЕДЕЛЕННАЯ ФАЙЛОВАЯ СИСТЕМА
AERGOFS является главным компонентом платформы AERGO, предоставляя функции распределенной файловой системы.

AERGOFS зависит от распределенного каталога (DD) при управлении метаданными, которые относятся к нужным файлам. Метаданные о каждом файле, включая его физическое местоположение, хеш-значение и различные статистические данные, хранятся в DD.

Хотя смарт-контракты обеспечивают структурированное хранение информации с помощью схем данных и индексов для более быстрого запроса, AERGOFS намерен предоставить возможность неструктурированного хранения данных AERGO.

AERGOFS предоставляет простой HTTP-интерфейс, дающий доступ как через смарт-оракулов, работающих на серверной платформе, так и через децентрализованные приложения, работающие в веб-браузерах.

РАСПРЕДЕЛЕННЫЙ КОНТРОЛЬ ВЕРСИЙ

В отличие от традиционных систем на блокчейне, AERGO рассматривает ветвление цепи и реорганизацию блоков как основные функции блокчейна, а не как бессмысленные побочные эффекты. Принимая Git-подобные модели данных и структуру команд, AERGO стремится обеспечивать совместное использование данных так же просто, как и при совместном использовании исходного кода.

РЕПОЗИТОРИИ

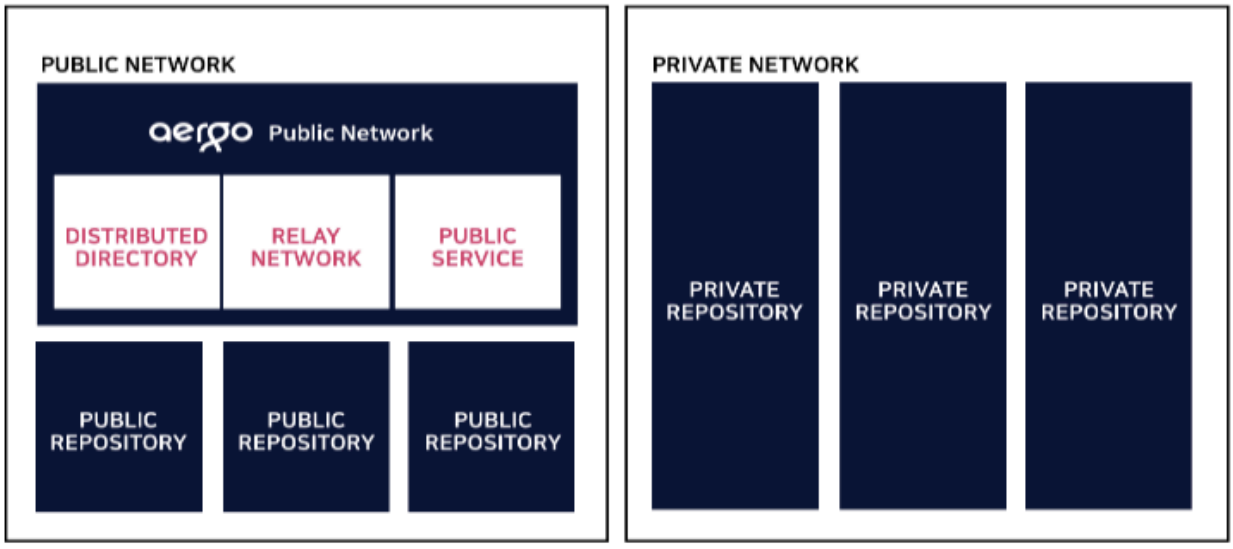

Рисунок 4. Открытые и приватные репозитории

AERGO поддерживает создание открытых и закрытых репозиториев. Каждое из хранилищ может либо иметь имя, либо нет. Именованный репозиторий имеет соответствующий общедоступный объект в распределенном каталоге AERGO Public Network. У репозитория без имени такой ассоциации нет.

Открытый репозиторий AERGO, во многом схожий с публичным репозиторием Git, предназначен для прозрачности чтения и записи или выборочного разрешения для анонимных пользователей. Общая конфигурация заключается в создании открытого репозитория AERGO с анонимным доступом только для чтения.

Закрытый репозиторий AERGO подразумевает полный контроль доступа, как для чтения, так и для записи хранилища. Открытый или приватный репозиторий - это, по сути, закрытый блокчейн, т.е. он работает независимо от AERGO Public Network. В результате токен AERGO никак не применяется в публичных или приватных репозиториях.

ВЕТВИ

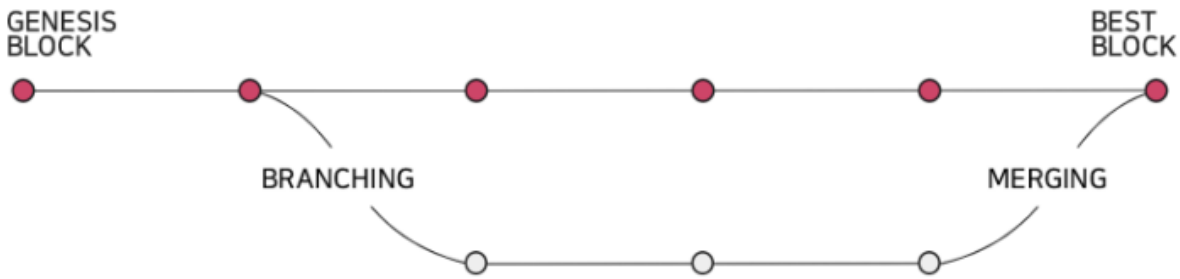

Рисунок 5. Ветвление и слияние блоков

Внутри каждого репозитория могут быть созданы разные ветви, указывающие на отдельный снепшот состояния блокчейна. По сути, понятие «оптимальной цепи» AERGO аналогично «главной ветви».

СИНТАКСИС И СЕМАНТИКА

AERGO стремится обеспечить понятный синтаксис и семантику для пользователей, привыкших к таким системам контроля версий, как Git. К таким функциям можно обращаться через клиента AERGO CLI, а также пользовательские интерфейсы RPC.

a. Основные команды

Ниже приведены примеры базового использования AERGO при распределенном контроле версий.

```
aergo branch <new branch> [--block=<block hash>]
```

Эта команда создает новую ветвь. Поскольку нет нечетко определенного блок-хеша в качестве параметра, оптимальный блок текущей ветви используется как корневой блок для новой ветви. Новая ветвь функционирует как независимая цепочка, с возможностью добавления новых блоков. Без созданных пользователем ветвей по умолчанию существует лишь главная ветвь.

```
aergo tag <block hash> [--block=<block hash>]
```

Данная команда создает новый именованный тег. Поскольку нет нечетко определенного блок-хеша в качестве параметра, оптимальный блок текущей ветви используется как корневой блок для нового тега. В отличие от ветви, тег не может включать в себя новые блоки.

```
aergo checkout <branch | tag>
```

Данная команда извлекает копию существующей ветви или тега для проверки или манипуляции.

```
aergo pull <repository:branch>
```

Эта команда осуществляет слияние изменений в удаленной ветви в ветвь локального репозитория. В результате удаленные операции применяются также и к локальному хранилищу. В этом процессе также синхронизируются именованные теги.

```
aergo push <repository:branch>
```

Этой командой осуществляется попытка слияния изменений в локальной ветви в ветвь удаленного репозитория. В результате локальные операции применяются также и к удаленному репозиторию. В данном процессе также синхронизируются именованные теги.

б. Ветвление и слияние
Одним из наиболее сложных понятий в распределенных системах управления версиями является процесс объединения ветвей, а для блокчейна с данными в режиме реального времени слияние еще более сложно. Благодаря тому, что данный процесс не нарушает структуру, ветвление представляется простым и понятным.

Однако слияние требует два разных подхода.

Автоматическое слияние
По умолчанию автоматическое слияние - это планируемый процесс объединения двух ветвей. Автоматическое слияние схоже с процессом реорганизации блоков в блокчейне. В этом случае блоки источника, предназначенные для слияния, растворяются в операциях и поглощаются специальным пулом объекта слияния. В конечном счете, пул слияния ведет к созданию нового блока, прикрепленного к оптимальному блоку объекта слияния. В этом процессе операции, несовместимые с целевой ветвью слияния, автоматически исключаются из нового блока.

Согласованное слияние
Согласованное слияние происходит только тогда, когда ветвь создается с определенной логикой согласованного слияния. Оно аналогично функциям объединения в таких системах контроля версий, как Git. В отличие от автоматического объединения, которое исключает несовместимые операции по умолчанию, согласованное слияние опирается на заранее определенную логику разрешения конфликтов при управлении несовместимыми операциями. Логика разрешения конфликтов реализуется как смарт-контракт системного уровня.

МАСШТАБИРУЕМОСТЬ

AERGO применяет три различных подхода для достижения масштабируемости.

- Разбиение на области
- Вертикальное масштабирование
- Горизонтальное масштабирование

РАЗБИЕНИЕ НА ОСНОВЕ ДОМЕНА

Разделение на основе доменов является самой базовой стратегией масштабирования, используемой AERGO. Разбиение по доменам достигается на AERGO с помощью функции распределенного контроля версий (DVC).

В отличие от обычных проектов на блокчейне, AERGO может свободно разделять и объединять свои данные по ветвям. В итоге распределенный реестр может быть разбит как логически, так и физически через разные репозитории.

Такой подход уже успешно используется такими распределенными системами контроля версий, как Git и Mercurial. Например, такой гигантский сервис, как GitHub, может размещать у себя десятки миллионов репозиториев.

Однако эффективность разбиения на основе доменов зависит от конкретной структуры и принципа использования данных. Когда отдельный репозиторий сталкивается с необходимостью обработать неограниченно расширенный объем данных, то разделить данные с помощью ветвления очень сложно. Поэтому AERGO предлагает два дополнительных подхода к масштабируемости при обработке огромного для одного хранилища объема данных.

ГОРИЗОНТАЛЬНОЕ МАСШТАБИРОВАНИЕ

Стратегия горизонтального масштабирования AERGO зависит от функциональности, предоставляемой AERGOFS, который, в свою очередь, выполняет две задачи для достижения масштабируемости:

1) AERGOFS может служить уровнем хранения для блоков и индексов каждого из узлов. Способ использования AERGOFS узлами AERGO очень похож на то, как HBase использует HDFS. С помощью AERGOFS каждый узел может хранить неограниченное количество блоков и индексов и функционировать как гигантский суперузел.

2) AERGOFS также может функционировать как хранилище объектов, подобное S3. В данной конфигурации AERGOFS обеспечивает неизменный и долговечный доступ к двоичным данным. В этом случае смарт-контракты AERGO должны сохранять локаторы для доступа к файлам, хранящимся на AERGOFS.

ВЕРТИКАЛЬНОЕ МАСШТАБИРОВАНИЕ

Наиболее простой и прямой подход, который AERGOFS старается использовать для масштабируемости, - это оптимизация одного узла.

Хотя горизонтальное масштабирование хорошо показывает себя при работе с большим объемом данных, оно все же не соответствует реалистичным критериям. С появлением

дешевой памяти и быстрого сохранения как на SSD, и ограниченной пропускной способностью сети, оптимизация отдельного узла очень эффективна для работы повседневных систем. Blocko хорошо усвоил это, представляя реалистичные блокчейн-разработки для компаний, и AERGO, используя помощь Blocko, стремится заимствовать многие идеи и приемы от Blocko'sCoinstack в этом направлении.

Чтобы сделать каждый узел максимально эффективным, AERGO обеспечит свои узлы эффективным сетевым стеком и оптимизированным механизмом хранения для расширенного ввода/вывода данных.

- Сетевой стек AERGO обеспечивает нестандартную, высокопараллельную сетевую структуру, способную обслуживать большое количество узлов со сложной топологией и в среде без ОС, и в облачной среде.
- AERGOSQL является базисом для высокопроизводительного механизма хранения, которого требует AERGO.
- В узлах AERGO применяется многопоточная архитектура, дающая возможность использования многоядерной системы.

КОНТРОЛЬ МНОГОПОТОЧНОСТИ

AERGO стремится предоставить два механизма для сериализации операций.

СЕРИАЛИЗАЦИЯ НА УРОВНЕ БЛОКОВ

Поскольку каждая ветвь блокчейна состоит из серии блоков, операции могут быть сериализованы путем размещения друг за другом.

AERGO намерен обеспечить многоверсионность данных для контроля параллельных транзакций (MVCC), основываясь на высоте блока. То есть, имея конкретную ветвь и высоту блока, можно обеспечить [согласованное считывание] через различные узлы репозитория.

Функциональность MVCC от AERGO обеспечит как изоляцию отдельных снепшотов для согласованного считывания, так и форму оптимистической блокировки путем управления версиями строк или документов. Однако MVCC применим только для сериализации на уровне блоков.

СЕРИАЛИЗАЦИЯ НА УРОВНЕ ПУЛА

Клиенты, получающие доступ к узлам AERGO, могут воспользоваться детерминированным планируемым созданием блоков делегатами, характеристикой DPOS и внутренним консенсусом и выполнять операции синхронно, с надежной гарантией завершения транзакции.

Поскольку каждый делегированный узел может применять единый порядок сериализации для обработки новых транзакций в пуле памяти и для создания новых блоков, клиентам не нужно ждать, пока интервал блоков не получит результат транзакций. Таким образом, время ожидания выполнения транзакции уменьшается с секунд до миллисекунд.

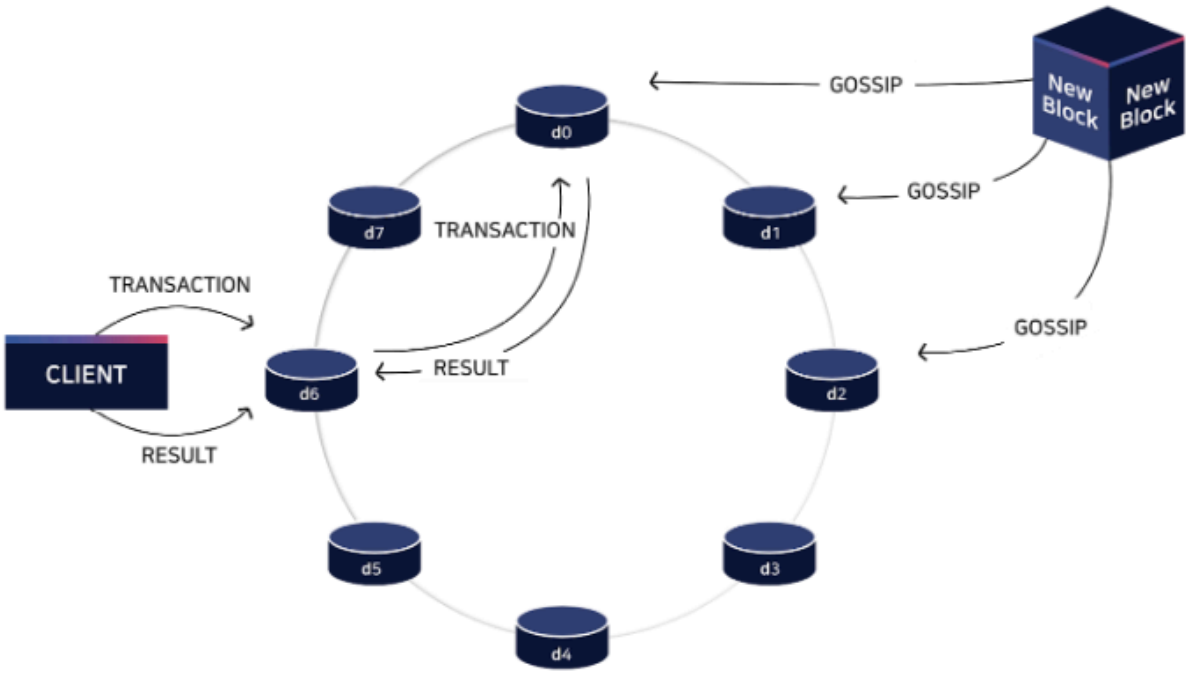

Рисунок 6. Сериализация уровня пула

Однако задействование реорганизации блоков и разбиения цепи, а также присутствие злонамеренных клиентов делают сериализацию уровня пула обеспечивающей лишь вероятностный уровень согласованности. С другой стороны, имея оптимистичные рабочие нагрузки, сериализация уровня пула показывает себя хорошо при работе над решением проблем реальной жизни.

КОНФИДЕНЦИАЛЬНОСТЬ

ИЗОЛЯЦИЯ ДАННЫХ

AERGO намерен давать пользователям достаточный доступ к данным регистра, предоставляя закрытые git-подобные репозитории.

Создавая новую ветвь из удаленной родительской, пользователи могут сохранять заново созданные блоки в закрытой ветке, изолируя их от общественности. Доступ к блокам можно получить, только имея разрешение этих пользователей на доступ к конкретному хранилищу, содержащему данную ветвь.

СОВМЕСТНЫЙ ДОСТУП К ДАННЫМ

Для обмена данными конкретная ветка может быть синхронизирована с удаленными репозиториями. В этом случае закрытые ветви хранилища могут либо отбирать из общего репозитория соответствующие объекты фиксации изменений, либо автоматически сбрасывать весь набор изменений.

ПАРАЛЛЕЛЬНОСТЬ

Производительность конкретного блокчейна зависит от точности создания новых блоков и точности обмена ими, а также времени, которое требуется каждому узлу для проверки новых блоков.

Процесс создания блока включает в себя рассмотрение всего распределенного консенсусного протокола блокчейна. Известно, что процесс проверки блока, используемый как часть различных распределенных консенсусных протоколов, иногда плохо разработан и реализован.

Несмотря на то, что слабые узлы приемлемы при запуске блокчейнов потребительского класса, таких как bitcoin или Ethereum, блокчейн корпоративного уровня, такой как AERGO, требует очень высокой производительности почти в режиме реального времени. Иными словами, каждый узел должен быть реализован с такой же точностью, как сам консенсусный протокол.

Для того, чтобы максимизировать производительность, AERGO намерен ввести концепцию параллельности на различных этапах обработки блоков.

Параллельность подразумевает тщательный анализ зависимостей между транзакциями, содержащихся в каждом блоке, и эффективной архитектурой, вдохновленной проектом SEDA.

АНАЛИЗ ЗАВИСИМОСТИ
Чтобы гарантировать согласованность между узлами, при реализации блокчейна обычно используется политика сериализации выполнения всех транзакций и доступных блоков.

В результате скорость обрабатываемых узлом блоков зависит от времени, которое тратится на обработку каждой операции, независимо от количества обрабатывающих единиц или объема доступной памяти.

Чтобы обеспечить параллельную проверку транзакций и блоков, AERGO будет осуществлять анализ зависимостей между транзакциями и блоками и создаст структуру данных, известную как Детерминированное дерево транзакций.

Детерминированное дерево транзакций (DTT)
DTT можно рассматривать как формальное представление порядка выполнения транзакций с целью подвести к детерминированным результатам для машин состояний, на которые влияют эти транзакции.
По сути, для набора транзакций может существовать более одного подходящего и правильного DTT.

Каждая ветвь DTT может обрабатываться и применяться к базовым машинам состояний, которые связаны с конкретными транзакциями, будучи при этом параллельно в детерминированном результирующем состоянии. Типичное DTT будет иметь несколько ветвей различной длины.

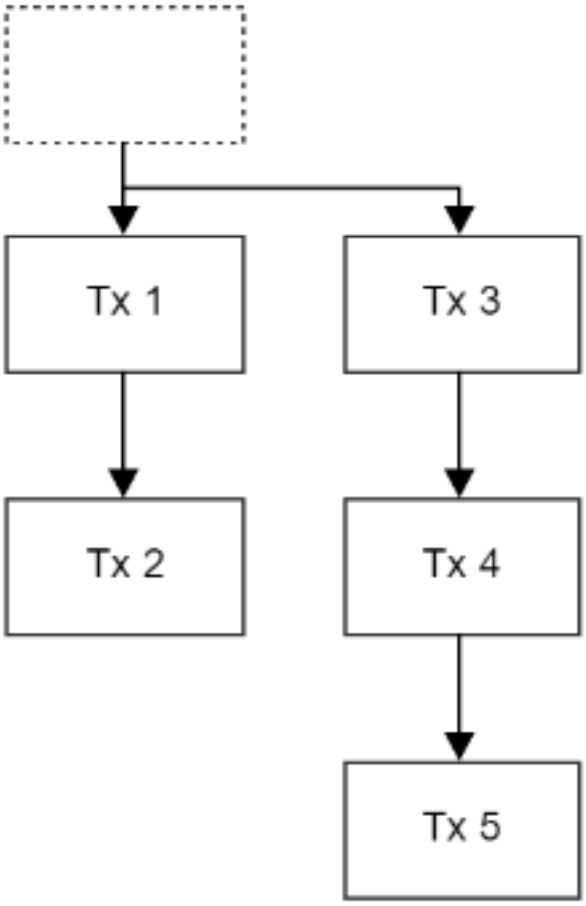

Рисунок 7. Дерево детерминированных транзакций

В зависимости от размера блоков каждое DTT может иметь ветви длиной от нескольких транзакций до нескольких тысяч транзакций. Аналогичным образом, разные DTT могут иметь различное количество ветвей.

Действительность DTT может быть проверена только путем фактического выполнения DTT несколькими машинами состояний. Версия DTT также может быть оптимизирована в другую версию путем преобразования этого дерева.

Чтобы создать DTT для отдельного пакета транзакций в реальные временные рамки, AERGO опирается на определенные правила анализа транзакций. Более сложный подход, включая машинное обучение, планируется протестировать в будущих релизах AERGO.