

mytime

Technical Paper 1.0

Русская версия
31 Октября, 2017

mytc.io

Содержание

Глоссарий	4
Введение	5
Бизнес-задачи	6
Технологические вызовы	7
Архитектура mytime	9
Full Node	10
Connector	11
Master Controller	11
Money BlockChain Controller	11
Time BlockChain Controller	12
Virtual Machine / Smart-Contract Executor	12
Light Client	12
Connector	13
Light BlockChain Controller	13
Decentralized File System	14
Applications / Services	14
Public API	16
Blockchain	17
Получение депонированной криптовалюты	19
Разрешение конфликтов при регистрации времени	21
Алгоритм консенсуса Proof-of-Time	22
Сеть	23
Эпоха	24
Процесс выбора майнеров	25
Награда за майнинг	26
Влияние депонированной криптовалюты на голос	26
Распределение голосующих адресов	27
Репутация и портрет пользователя	28
Smart-контракты	31
Криптовалюта MYTC	32
Эмиссия MYTC	33
Конституция платформы	34
Зачем нужна конституция	34
Реализация конституции	35

Интеграция с платформой	36
Приложения	36
Базовые приложения	37
Chronos Foundation	39
Защита от атак	40
Экономика mytime	41
Депонированная криптовалюта	41
Мотивация участников системы	42
Мотивация пользователей	42
Мотивация сервисов	43
Мотивация валидаторов	44
Мотивация нод	44
Мотивация хранения данных	45
Выводы	46
Отказ от ответственности	47
Риски проекта	49

Глоссарий

Депонированная криптовалюта — переходное состояние прав на криптовалюту, когда контрагент А уже не обладает криптовалютой, а контрагент В имеет права на ее получение, но еще не получил.

Сервис — бизнес, взаимодействующий с пользователями через приложения.

Приложение — программный продукт, предоставляющий услуги клиенту и содержащий функциональность для автоматизации обмена данными и начисления депонированной криптовалюты.

Proof-of-time — алгоритм на базе DPoS, в котором депонированная криптовалюта значительно повышает вес голоса.

Принцип подтверждения времени — потраченный интервал времени валидируется депонированием криптовалюты.

Протокол Chronos — правила функционирования двух блокчейнов Time и Money согласно принципу подтверждения времени с алгоритмом консенсуса Proof-of-Time.

Блокчейн Time — публичный реестр подтвержденного времени.

Блокчейн Money — публичный реестр финансовых транзакций.

mytime — открытая децентрализованная блокчейн-платформа для подтверждения стоимости времени, основанная на протоколе Chronos, протоколе Money, смарт-контрактах и сервисах.

MYTC — криптовалюта, платежное средство внутри платформы **mytime**.

Эмиссия MYTC — динамический выпуск MYTC при появлении новых блоков, зависящий от объемов подтвержденного времени. Эмиссия распределяется среди пользователей пропорционально голосам за ноды, по алгоритму Proof-of-Time.

1. Введение

mytime — децентрализованная платформа с новой блокчейн-архитектурой с точки зрения социального и экономического аспектов. Новизна архитектуры определяется следующими факторами:

- Базовая функция платформы — присвоение стоимости времени пользователя.
- Криптовалюта в депонированном состоянии является модификацией эскроу-транзакции.
- Принцип подтверждения времени и алгоритм Proof-of-Time поощряют передачу права собственности на криптовалюту другим участникам платформы.
- Эмиссия MYTC зависит от внутреннего состояния Chronos в любой момент времени.
- Репутация — это производная характеристика транзакционной активности участников платформы.
- Метаданные в транзакциях позволяют придать ценность криптовалюте по правилам работы, определяемым приложениями.

mytime будет поддерживать смарт-контракты на уровне протокола. Смарт-контракты обеспечат сложную логику взаимодействия сервисов и пользователей друг с другом. Простейший пример такого взаимодействия — разделение вознаграждения, полученного с депонированной криптовалюты, между сервисом и пользователями.

При разработке **mytime** мы опираемся на лучшие принципы и практики проектов: Cardano, Plasma, EOS, NEM, а также на различные модификации Graphene.

mytime разрабатывается по принципу business first. Мы думаем в первую очередь о снижении издержек в бизнес-процессах и массовом привлечении пользователей через интеграцию с крупными B2C бизнесами.

Краткосрочной метрикой проекта **mytime** является быстрый рост количества подключенных сервисов и количества пользователей.

Среднесрочной метрикой проекта является увеличение количества транзакций между сервисами и пользователями.

Долгосрочной ключевой метрикой развития **mytime** станет снижение транзакционных издержек внутри сети при увеличении объема транзакций. Следование этой метрике обеспечит устойчивость протокола при остановке роста или падении криптовалютного рынка.

1.1. Бизнес-задачи

В современном мире количество сервисов, требующих внимания человека, увеличивается с каждым днем.

Время каждого пользователя конечно. Этого времени не хватает даже на повседневные сервисы, в которых у пользователя есть потребность.

Сервисы взаимодействуют с пользователями при отсутствии эффективных и измеримых критериев оценки времени.

Мы предлагаем конвертировать время в ликвидную ценность, предоставив всем платформу для монетизации взаимодействия на базе подтвержденной стоимости времени. Время пользователей подтверждается мгновенным переводом права собственности на MYTC от сервиса к пользователю.

Эмиссия MYTC дополнительно мотивирует сервис подтверждать время пользователя. Чем крупнее вознаграждение пользователя, чем больше пользователей в сервисе, чем выше их репутация и чем чаще происходит вознаграждение, тем больше MYTC получает сервис.

Подтверждение времени пользователей и защиту от злоупотреблений и фальсификации обеспечивает протокол Chronos на основе алгоритма Proof-of-Time.

В **mytime** все взаимодействия между участниками строится на взаимовыгодном удовлетворении потребностей сервисов и пользователей.

Примеры:

- Программы лояльности, в которых компания оплачивает пользователям время, проведенное в сервисе.
- Оплата времени, потраченного на просмотр видео и компьютерные игры.
- Рекламные модели через вознаграждение за внимание.
- Оплата времени всех участников дистанционного образовательного процесса.
- Учет рабочего времени.
- Поминутные авторские отчисления.

Ценность **mytime** определяется низкими транзакционными издержками и выражением бизнес-процессов через нефальсифицируемую стоимость времени. Все экономические процессы могут быть рассчитаны и верифицированы временными характеристиками взаимодействий между объектами. Это позволяет конвертировать друг в друга любой вклад, затраты, долевое участие и иные показатели взаимодействия.

Протокол позволяет рассчитать вклад каждого участника во взаимосвязанные процессы создания добавочной стоимости в глобальной экономической модели.

1.2. Технологические вызовы

Работа платформы **mytime** предполагает большое количество участников и огромное количество транзакций, содержащих произвольные метаданные. Это создает следующие технологические вызовы перед командой и комьюнити **mytime**:

1. Как сделать **mytime** экономически устойчивой системой с мотивацией всех участников системы?

2. Как обеспечить хранение и неизменность информации о стоимости времени и сопутствующих метаданных для сотен миллионов пользователей?
3. Как правильно разрешить противоречия между сервисами, конкурирующими за одну и ту же минуту пользователя?
4. Как обеспечить обработку данных пользователей без возможности копирования данных потенциальным приложением (или нодой) злоумышленником?
5. Как выстроить эффективную систему репутации пользователей и приложений?
6. Как обеспечить консенсус сети при важных обновлениях протокола **mytime**?
7. Как защитить платформу от потенциальных атак?

В этом документе мы описываем стратегию решения обозначенных технологических вызовов.

2. Архитектура mytime

Архитектура платформы **mytime** включает в себя следующие компоненты:

1. Full mytime Node.

A. Connector.

I. Peer 2 Peer Public Interface.

II. RPC Public/Private Interface.

C. Master Controller.

D. Money BlockChain Controller.

E. Time BlockChain Controller.

F. Virtual Machine / Smart-Contract Executor.

2. Light mytime Node.

A. Connector.

I. Peer 2 Peer Public Interface.

II. RPC Public/Private Interface.

C. Light BlockChain Controller.

3. Decentralized File System.

4. Applications.

5. Public API.

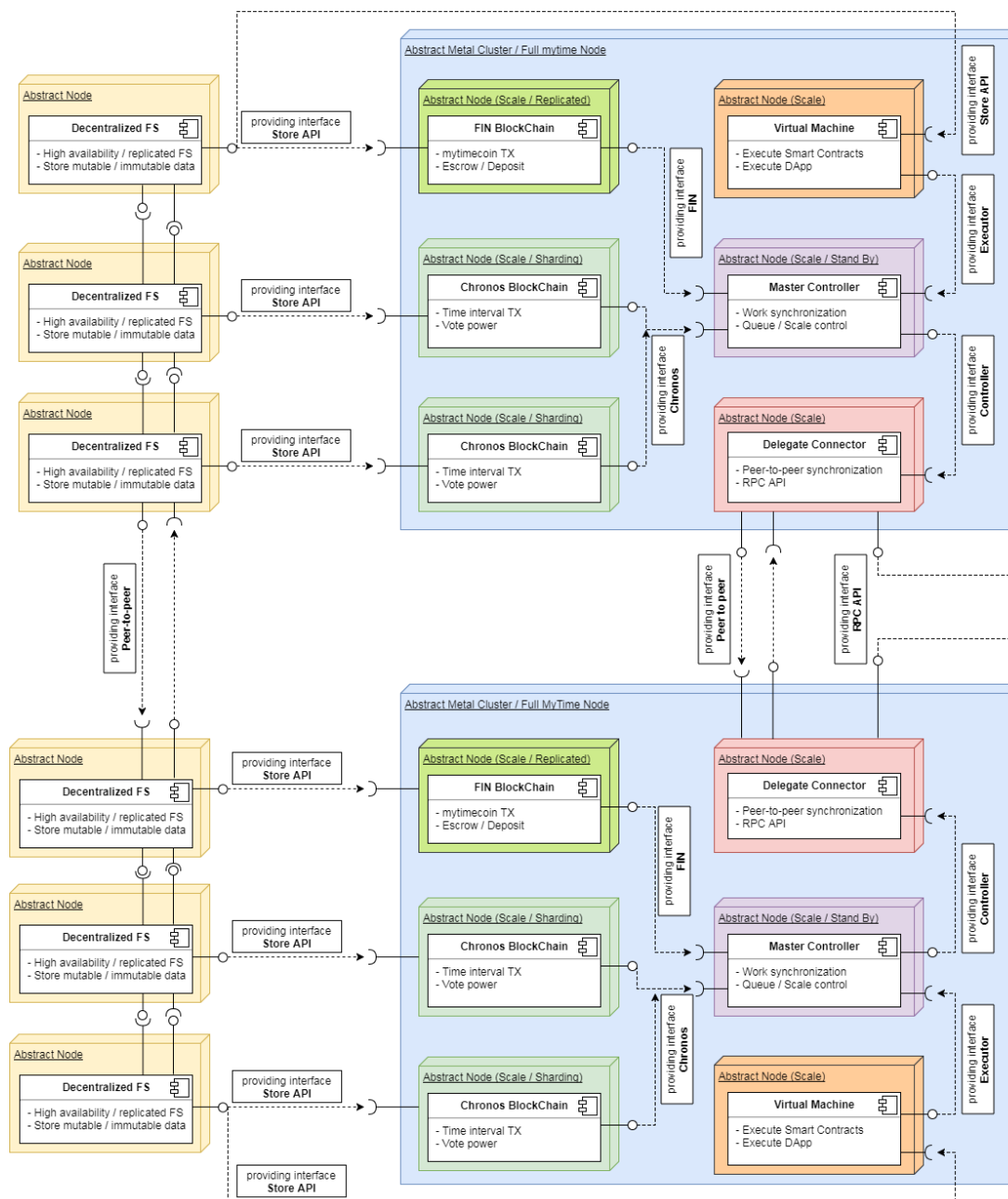
6. Zero Application.

A. Wallet.

B. BlockChain Explorer.

C. Marketplace.

Взаимосвязь компонентов отражена на следующей схеме:



2.1. Full Node

Полные узлы сети (делегаты) — центральный компонент всей платформы **mytime**. Этот компонент обеспечивает бесперебойную работу упаковки блоков и голосования, а также участвует в обеспечении консенсуса сети.

Полные узлы обрабатывают весь объем транзакций параллельных блокчейнов платформы **mytime**, обеспечивая целостность и неизменность данных.

2.1.2. Connector

Внутренний компонент полного узла, обеспечивающий интерфейс пирингового обмена данными с другими узлами сети. Помимо обмена данными, компонент обеспечивает возможность подключения к узлу по технологии RPC. Он может быть масштабирован горизонтально для увеличения пропускной способности.

2.1.3. Master Controller

Внутренний компонент полного узла. Обеспечивает управление остальными компонентами, формирует очередь задач и контролирует их состояние. Может масштабировать другие компоненты узла для повышения производительности, если для этого хватает ресурсов. Основная функция — связывание компонентов в одно целое. Компонент контролирует выполнения распределенных приложений и смарт-контрактов, создавая для выполнения изолированные виртуальные среды и виртуальные машины. Компонент имеет состояние, которое может храниться во внешней оперативной памяти узла (Redis / Memcached). Отказоустойчивость обеспечивается за счет создания StandBy-реплик компонента. Во время критической ситуации происходит автоматическое переключение на живой экземпляр компонента.

2.1.4. Money Blockchain Controller

Внутренний компонент полного узла, обеспечивает работу блокчейна с финансовыми транзакциями. Компонент верифицирует и контролирует состояние блоков, содержащих финансовую информацию. Может использовать для хранения децентрализованную файловую систему. Может использовать для хранения еще не включенных в блок транзакций внешнюю оперативную память (например, транзакций депонированного времени Escrow). Компонент может быть реплицирован для повышения производительности упаковки блоков и верификации состояния блокчейна.

2.1.5. Time Blockchain Controller

Внутренний компонент полного узла. Обеспечивает работу блокчейна регистрации времени. Компонент верифицирует и контролирует состояние блоков, содержащих временные интервалы. В случае критического отключения приложения он может принудительно завершить сессию регистрации времени. Компонент может использовать для хранения децентрализованную файловую систему. Компонент может быть шардирован по идентификаторам пользователя для повышения производительности упаковки блоков и верификации состояния блокчейна.

2.1.6. Virtual Machine / Smart-Contract Executor

Внутренний компонент полного узла. Обеспечивает виртуальную среду для выполнения произвольного кода, например для выполнения кода смарт-контракта. Один полный узел может содержать разные виды виртуальных машин, включая изолированную среду выполнения контейнеризированных приложений.

2.2. Light Client

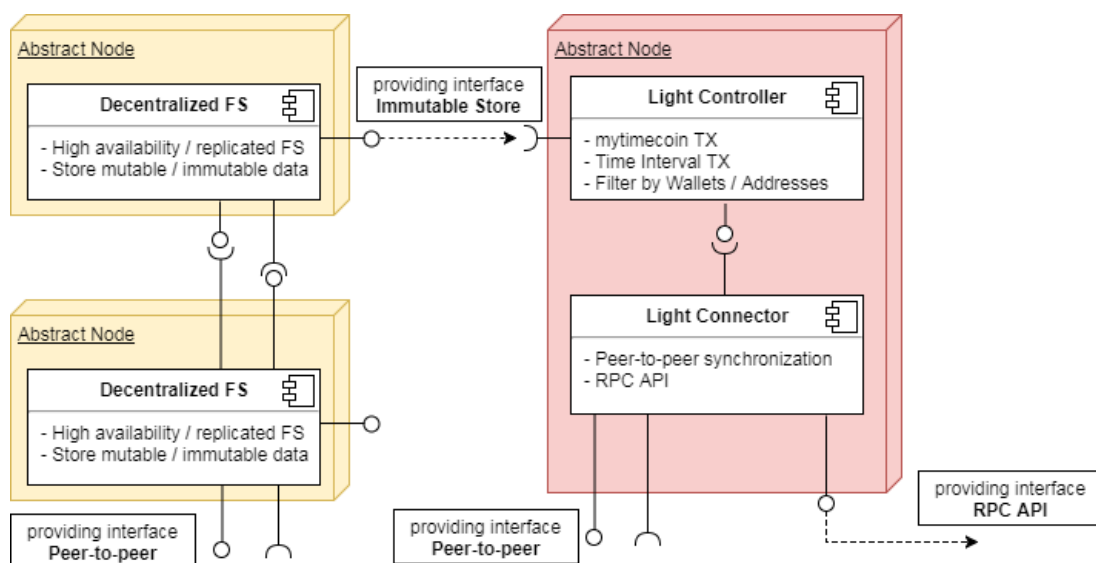
Легкие клиенты служат основой для связи с блокчейном клиентских приложений, например, кошельков или приложений, которые регистрируют время пользователей в автоматическом режиме. Данный компонент спроектирован специально для запуска в среде с ограниченными ресурсами. Легкий клиент контролирует не всё состояние блокчейна, а только то, что связано непосредственно с участником платформы, например, цепочки финансовых транзакций, относящиеся к определенному кошельку, или временные интервалы, которые относятся к конкретному приложению. Компонент может использовать децентрализованную файловую систему для хранения своего состояния. Легкие клиенты не могут участвовать в прямом производстве новых блоков, но при этом могут выполнять проверку валидности отдельных цепей.

2.2.1 Connector

Внутренний компонент узла, обеспечивающий интерфейс пирингового обмена данными с другими узлами сети. Кроме этого, компонент обеспечивает возможность подключения к узлу по технологии RPC. Узел дает ограниченную возможность использования интерфейса RPC. Через интерфейс можно управлять только той информацией, которая касается узла (была добавлена в него ранее).

2.2.2 Light Blockchain Controller

Внутренний компонент узла, обеспечивающий интерфейс пирингового обмена данными с другими узлами сети. Кроме этого, компонент обеспечивает возможность подключения к узлу по технологии RPC. Узел дает ограниченную возможность использования интерфейса RPC. Через интерфейс можно управлять только той информацией, которая касается узла (была добавлена в него ранее).

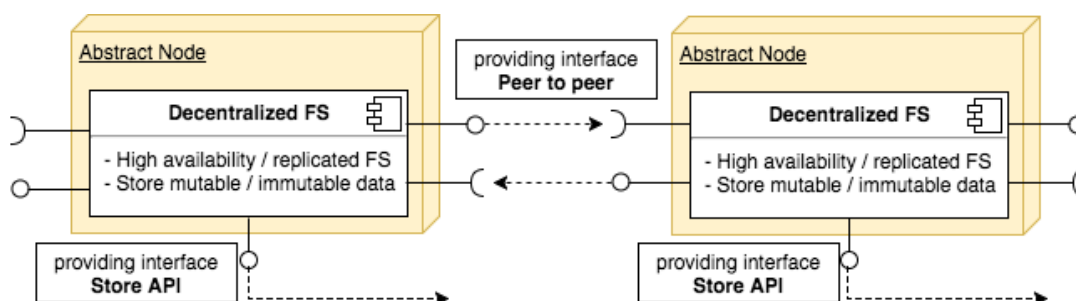


2.3. Decentralized File System

Для хранения информации о финансовых транзакциях и зарегистрированном времени, а также условиях, при котором происходила подобная регистрация, платформа **mytime** будет использовать децентрализованную файловую систему. Такая файловая система должна обладать должной степенью надежности и доступности.

Высокая надежность может обеспечиваться за счет избыточного реплицирования данных и поддержания необходимого минимального количества реплик, а также их постоянной проверки. Высокая доступность может обеспечиваться за счет правильного гео-позиционирования узлов файловой системы. Также необходимо, чтобы такая файловая система обладала должным уровнем доверия.

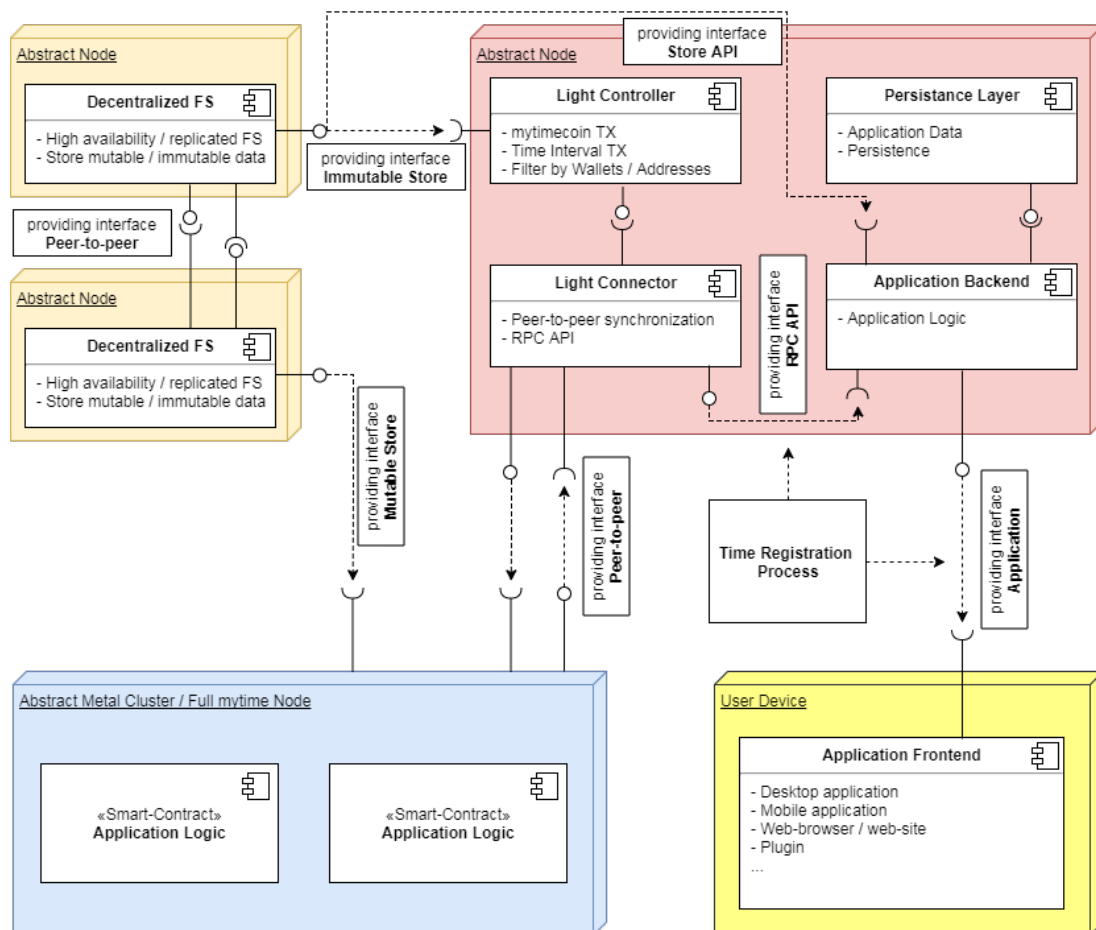
Мы рассматриваем как возможность использования уже существующих подобных файловых систем наподобие Storj, FileCoin, Maidsafe, Siacoin, EOS, так и возможность разработки собственной реализации децентрализованной файловой системы в рамках платформы **mytime** на базе IPFS.



2.4. Applications / Services

В рамках платформы **mytime** приложения и сервисы выполняют автоматизированную регистрацию времени и депонирование криптовалюты. Приложения мотивированы раскрывать информацию о себе в обмен на увеличение степени участия в эмиссии и регулировании платформы **mytime** за счёт дополнительного повышения собственной репутации.

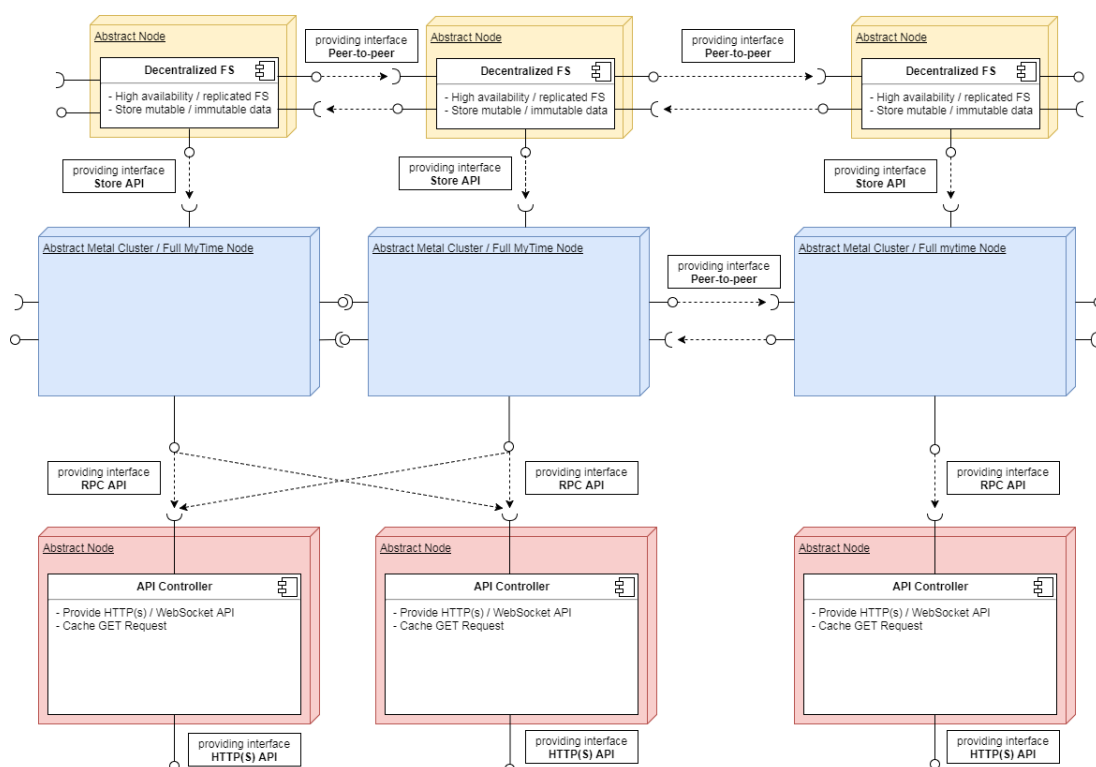
Став участником платформы, любое приложение получает свой уникальный адрес. Любой пользователь платформы может дать приложению разрешение регистрировать его время, проведенное в приложении. Приложение может быть программой для настольного компьютера, мобильным приложением под любую платформу, веб-сайтом, плагином для браузера и т.д. Пользователь может оценить приложение, выставив ему рейтинг. Для этого пользователь должен отправить в сеть специальную транзакцию. Приложение может быть связано с набором смарт-контрактов для того, чтобы реализовывать особые механики по вознаграждению пользователя за определенные действия. Для хранения своего состояния и данных приложение может использовать децентрализованную файловую систему.



2.5. Public API

Для упрощения взаимодействия с платформой **mytime** будет представлено децентрализованное высокопроизводительное публичное API, позволяющее выполнять любые операции с блокчейнами Time и Money. API призвано решить проблему быстрого подключения к сети, когда нет возможности запустить свой узел или запуск такого узла не целесообразен, будь то полный или легкий узел. API будет реализовывать стандартные интерфейсы подключения HTTP / HTTPS, WebHooks, WebSockets.

Стандартные запросы на чтение данных (типа GET) не будут ограничены по количеству и будут бесплатными. Остальные запросы, требующие больших вычислительных ресурсов и изменяющие состояния данных, могут иметь тарификацию и ограничение по количеству.



3. Blockchain

Платформа **mytime** базируется на двух связанных блокчейнах Time и Money, выполняющих взаимодополняющие функции.

Блокчейн Time позволяет фиксировать сессии пользователей и осуществлять депонирование MYTC со стороны приложений или сервисов. Блокчейн Money используется для проведения финансовых транзакций.

Алгоритм Proof-of-Time обеспечивает работу репутационных метрик и систему голосования по алгоритму консенсуса типа Delegated Proof-of-Stake.

На рисунке ниже схематично изображены блокчейны **mytime**. Задача ноды при работе с протоколом Chronos заключается в следующих действиях:

1. Фиксирование отрезков времени участия пользователей и одновременного депонирования MYTC, сохранение произвольного набора данных в записи.
2. Контроль сессии. Под этим понимается фиксация первого депозита и запись завершения сессии.
3. Определение «пересекающихся» сессий, алгоритмизированное разрешение конфликтов, если это не регламентировано кодом смарт-контракта.
4. Контроль сумм и подпись последней эскроу-транзакции финансового приложения.

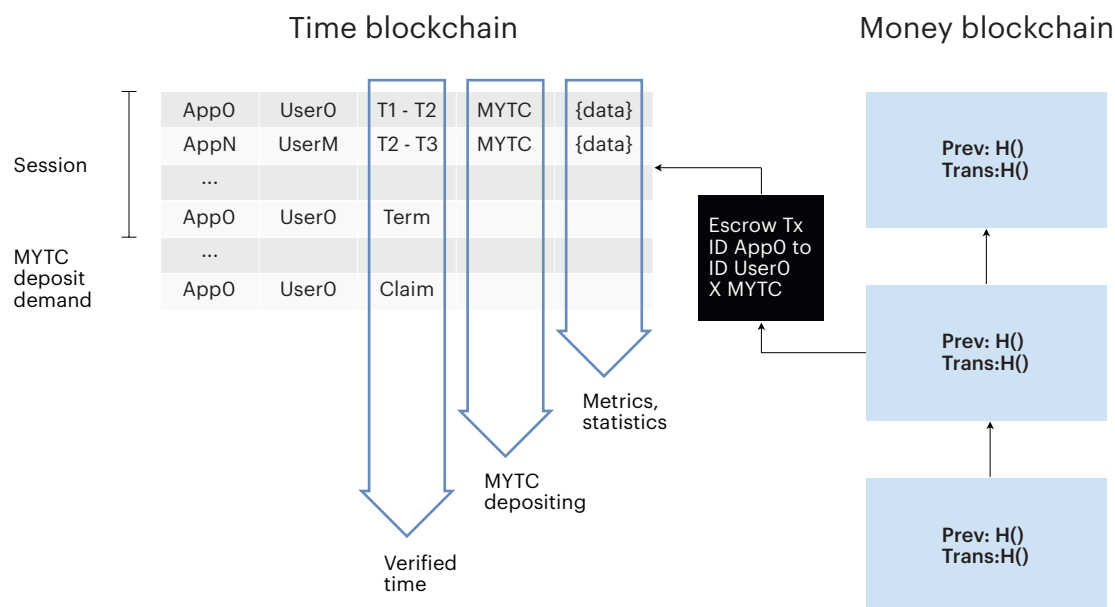


Схема связи блокчейна Chronos и финансового блокчейна MYTC

Блоки обоих блокчейнов, Time и Money, формируются на одной и той же ноде в рамках самого «медленного» блокчейна. При этом, очевидно, что технические параметры всей системы будут определяться наиболее нагруженным блокчейном Time, чьи характеристики будут полностью определены в процессе дальнейшей разработки протокола, определении экономически целесообразных объемов дополнительных данных в записи депонирования времени. Кроме того, возможно формирование ссылок в блоке данных записи блокчейна Time для децентрализованного хранения информации различного характера, релевантной приложениям и сервисам, формирующим запись.

Рассмотрим более подробно механизм связи блокчейна Time и финансового блокчейна Money на примере осуществления транзакции со стороны пользователя для востребования депозита MYTC в обмен на подтверждённое время.

3.1. Получение депонированной криптовалюты

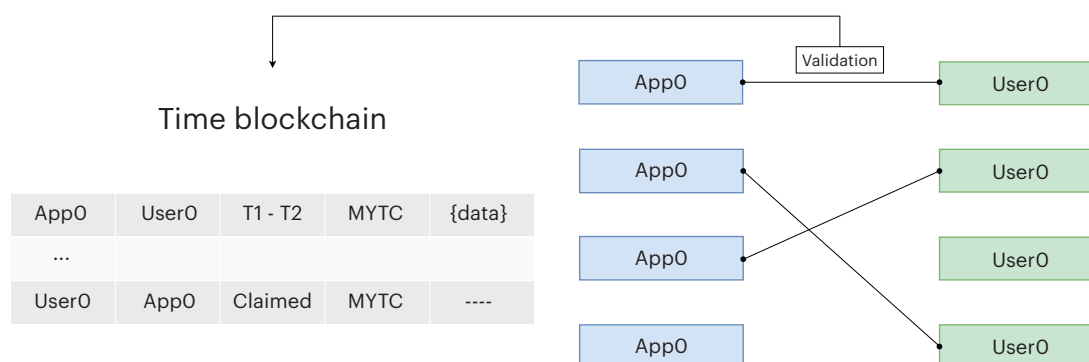


Схема валидации времени пользователя User0 в App0 в протоколе Chronos

В процессе взаимодействия приложения (сервиса) с пользователем, осуществляется валидация времени пользователя со стороны приложения, назовём его App0 (Рисунок выше). Являясь участником платформы **mytime**, App0 осуществляет депонирование криптовалюты MYTC в системе **mytime**, создавая в блокчейне Time запись вида:

ID сервиса	ID пользователя	t начала	t конца	Σ MYTC
------------	-----------------	----------	---------	---------------

Размер блока Time является ограниченным, поэтому туда попадают только записи приложений, депонирующих сумму в MYTC, превышающую минимальный порог, изменяющийся со временем в большую или меньшую сторону.

Гарантией отсутствия двойной траты при депонировании криптовалюты выступает эскроу-транзакция Money, транслируемая в сеть приложением App0 одновременно с записью в блокчейне Time. Нода проверяет сумму потраченного в сессии Time времени и вместе с приложением формирует транзакцию Money типа M из N мультиподписей. После того как пользователь запросит средства из клиентского приложения, нода проверяет закрытые сессии, и подписывает эскроу-транзакцию Money. Таким образом, криптовалюта MYTC расходуется с кошелька приложения на кошелек пользователя.

Нода **mytime** аккумулирует записи о потраченном времени и фиксирует момент, когда пользователь запрашивает перевод MYTC на свой кошелёк. Рассмотрим подробнее, как это происходит.

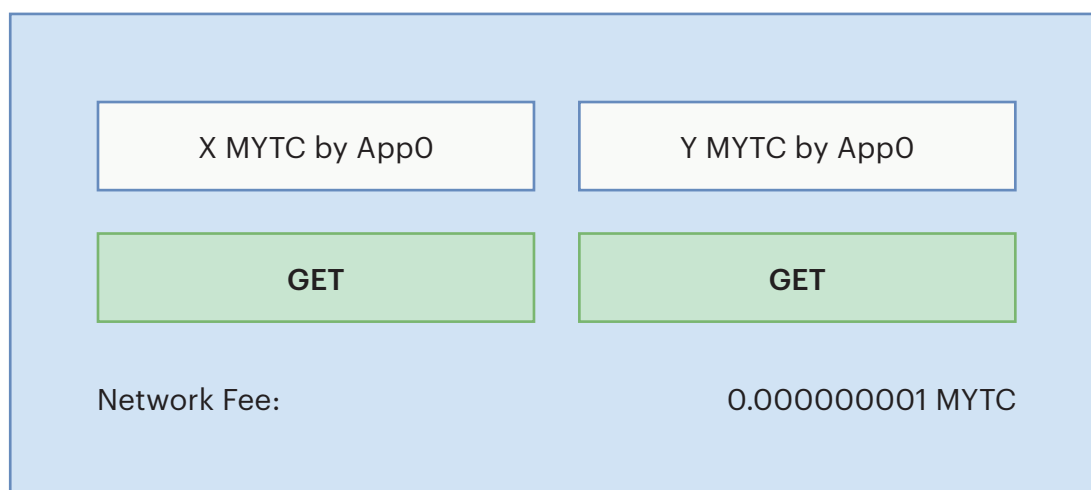


Схема валидации времени пользователя User0 в App0 в протоколе Chronos

В базовом приложении пользователя отображается количество начисленных MYTC и комиссия сети. Данная информация доступна через API **mytime** и следует из информации, хранимой в публичных блокчейнах **mytime** и текущей нагрузки сети. User0 может получить средства по нажатию кнопки «Get». Это событие запускает алгоритм подтверждения времени и зачисления средств MYTC пользователю.

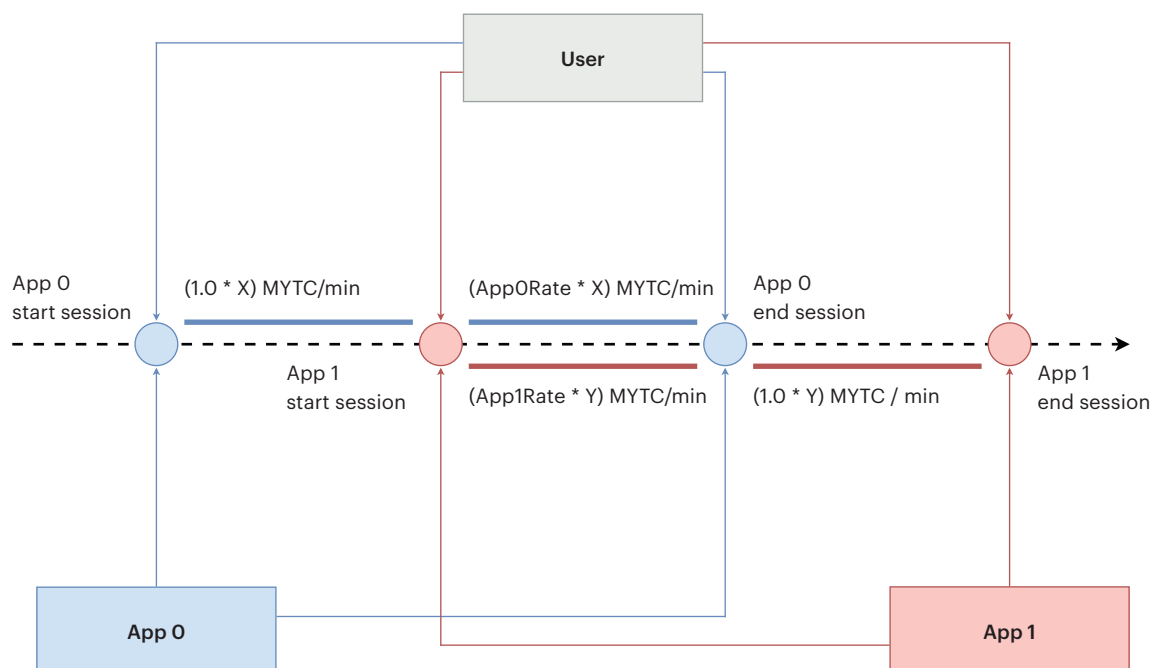
В процессе подтверждения задача ноды сводится к проверке соответствия конечной эскроу-транзакции сети, в которой «заморожены» средства приложения или сервиса **mytime**, и записей в блокчейнах Chronos. Если правила платформы **mytime** были соблюдены (пользователь получает вознаграждение только за время, потраченное в одном приложении), нода **mytime** подписывает транзакцию в Money, которая затем будет включена в блокчейн Money и пользователь получит в обмен на потраченное время запрашиваемую криптовалюту, минус комиссия сети.

3.2. Разрешение конфликтов при регистрации времени

Сервис может регистрировать время пользователей как на эксклюзивной основе, так и совокупно с другими приложениями. Если есть несколько параллельных сессий регистрации времени в области их пересечения, конфликт разрешается на основании предпочтений пользователя. Пользователь вправе указать, какая сессия регистрации времени (какое приложение) для него приоритетнее. В случае указанных приоритетов стоимость «минуты» времени в рамках сессии получит понижающий коэффициент.

Если пользователь явно не указывает приоритеты для сессии регистрации времени, система отдаст предпочтение более дорогой сессии. В этом случае более дешевые сессии будут проигнорированы.

Приложение может выставлять свои приоритеты и правила эксклюзивной регистрации. Например, приложение может игнорировать параллельные сессии и выплачивать полную стоимость времени пользователю или, наоборот, требовать от пользователя эксклюзивной траты времени в рамках только его сессии.



4. Алгоритм консенсуса Proof-of-Time

В **mytime** будет реализован алгоритм консенсуса Proof-of-Time, являющийся модификацией DPoS. Отличия главным образом касаются расчета весов голосов и вознаграждением при голосовании.

DPoS (Delegated Proof-of-Stake) — делегированное доказательство владения является измененной версией PoS (используется в Peercoin, Blackcoin, NXT). Главное отличие заключается в том, что в процессе создания блока участвуют не все участники сети, а только небольшая группа выбранных майнеров.

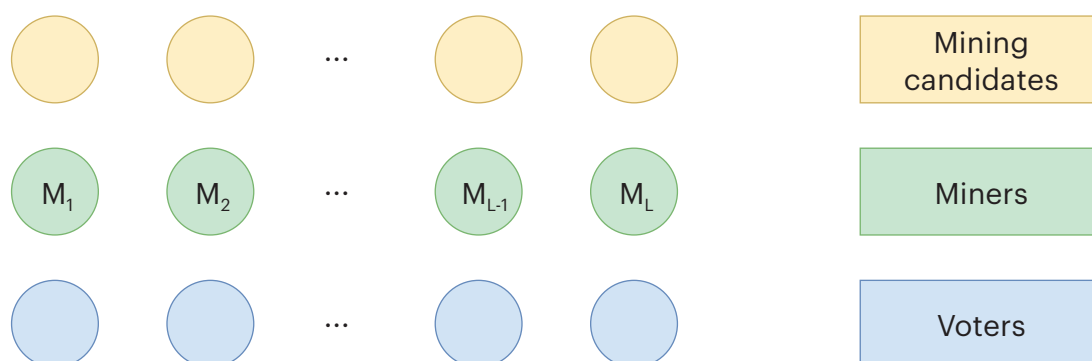
DPoS уже не раз доказал свою работоспособность — впервые примененный в BitShares в 2014 году, сегодня он используется в таких проектах, как EOS, Lisk, Steem и Tezos. Суммарная капитализация этих проектов к октябрю 2017 года составляет более 1 миллиарда долларов. Пока это ничтожно мало по сравнению с общей капитализацией криптовалют на базе PoW, но мы полагаем, что именно за PoS/DPoS лежит большое будущее.

Для того чтобы стать частью сети и делегатом (производителем) блоков, достаточно установить Full Node ПО для вычислительного узла, разработанное командой **mytime**, и иметь минимально необходимый баланс кошелька.

4.1. Сеть

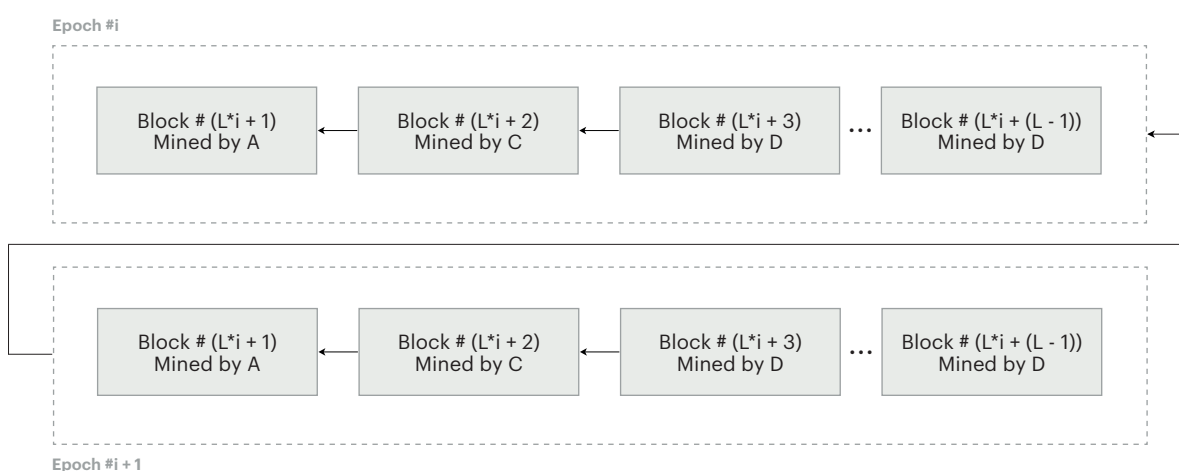
Выберем некоторый момент времени t_0 — все адреса, упомянутые в транзакциях внутри блокчейна к моменту t_0 можно разделить на три категории:

- Майнеры (адреса, ассоциируемые с получением комиссии за помещение транзакции в блок).
- Кандидаты в майнеры (адреса, изъявившие желание участвовать в процедуре майнинга, но не имеющие достаточно репутации).
- Голосующие (адреса, не желающие принимать участие в процедуре майнинга, но голосующие за одного или нескольких кандидатов).



4.2. Эпоха

Очевидно, что новые голосования должны проходить в сети постоянно, чтобы обеспечивать достаточный уровень конкуренции между кандидатами. Поэтому был введен термин «эпохи» — последовательности из L блоков, в которой каждый блок закреплен за определенным адресом. Если в течение времени блока B_{time} майнер не успел создать блок, то очередь переходит к следующему майнеру. После того, как последний блок будет создан, происходит процесс перевыбора майнеров, о котором рассказано ниже.



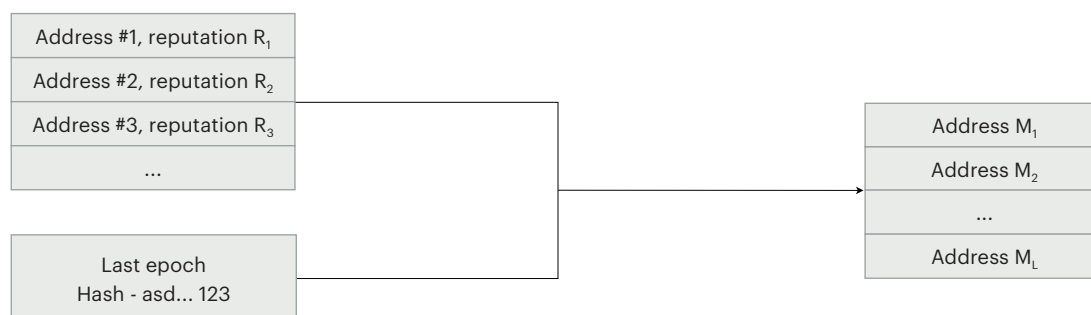
4.3. Процесс выбора майнеров

По окончании эпохи необходимо выбрать L новых майнеров для работы над следующей эпохой. Каждый адрес в сети имеет гарантированное право баллотироваться как майнер. Это желание документируется в форме специальной транзакции, как это сделано в Lisk. После этого адрес с ненулевой вероятностью попадет в список майнеров эпохи.

Для обеспечения безопасности сети необходимо решить несколько проблем:

- Майнеры выбираются псевдослучайным способом, минимизируя шанс регулярного попадания злоумышленника в список майнеров.
- Шансы адреса стать майнером будут пропорциональны его репутации. В противном случае можно будет создать доминирующий по размеру кластер адресов и управлять процессом майнинга.
- Так как пропуск майнером своей очереди увеличивает время подтверждения транзакции, такой майнер должен штрафоваться.

Для получения псевдослучайного фактора будет использоваться хэш последнего блока, гарантируя единый результат для всей сети.



4.4. Награда за майнинг

Помимо описанных выше проблем, есть еще один вектор атаки. Из-за холодного старта всей системы, довольно быстро сформируется список из L кандидатов, репутация которых будет существенно выше, чем у всех остальных кандидатов. Из-за этого они будут попадать в список майнеров эпохи намного чаще, чем «рядовые» конкуренты. А это в свою очередь может привести к централизации сети.

В BitShares эта проблема решается исключением адреса из списка кандидатов на некоторое время $t_{\text{down time}}$, если аккаунт принял участие в майнинге эпохи. Мы решили пойти другим путем: для избежания подобной ситуации награда за блок будет делиться между самим майнером и теми, кто за него проголосовал. Тем самым у голосующих появится мотивация поддерживать кандидатов с меньшей репутацией, что приводит к конкуренции нод за участие в эре.

4.5. Влияние депонированной криптовалюты на голос

Вес голоса за кандидата в майнеры зависит от нескольких параметров:

- R_{voter} — репутация голосующего адреса (это может быть как пользователь, так и сервис).
- D_{voter} — число депонированных MYTC с адреса голосующего.
- R_{miner} — репутация майнера.
- S_{miner} — успешность предыдущих участий пользователя в процессе майнинга.

Наибольший вес в итоговой формуле имеет именно число депонированной криптовалюты на адресе голосующего.

Под S_{miner} имеется в виду up-time пользователя, то есть соотношение числа созданных блоков к числу участий в голосовании в качестве кандидата.

4.6. Распределение голосующих адресов

Сервисы будут составлять подавляющее большинство среди всех голосующих. Это связано с тем, что механика работы сервисов подразумевает депонирование МҮТС, обеспечивая им максимальные веса голосов.

Мы считаем, что именно сервисы лучше всего подходят на роль голосующего органа, потому что в отличие от обычного пользователя, их действия будут создавать репутацию и дополнительную ценность, мотивируя сервис вести себя максимально честно по отношению к платформе и к пользователям.

5. Репутация и портрет пользователя

Протокол Chronos в базовом виде подвержен различным атакам злоумышленников, которые, например, могут создавать сети ботов и подтверждать их время. Полностью с ботами не могут справиться даже передовые технологии machine learning, поскольку на стороне ботов те же технологии. Всегда можно создать бота, неотличимого от человека по своим паттернам взаимодействия с сервисами.

Для эффективного отражения подобных атак введем в протокол понятие репутации.

Определение 1. Непосредственная связь пользователей транзакциями.

Пользователи U_i и U_j считаются непосредственно связанными транзакциями, если в блокчейне Time или блокчейне Money есть одна или более транзакций, в которых одновременно фигурируют оба пользователя.

Определение 2. Граф транзакций.

Граф транзакций — это взвешенный граф $G = (U, T)$, где:

$U = \{ U_0, U_1, \dots, U_n \}$ - множество вершин, представляющих всех пользователей (все кошельки) платформы **mytime**.

$T = \{ T_0, T_1, \dots, T_n \}$ - множество ребер, соединяющих вершины, и представляющих непосредственную связь транзакциями.

Каждому ребру графа присвоен вес W_{ij} , обозначающий численное выражение истории транзакций между двумя пользователями (кошельками) U_i и U_j . Математическое выражение веса W_{ij} — вопрос дальнейшего исследования. Оно будет выведено в процессе балансировки платформы.

Определение 3. Транзакционный портрет пользователя.

Транзакционный портрет пользователя U_p — это подграф $G^p = (U^p, T^p)$ графа транзакций, где:

$U^p = \{U_0, U_1, \dots, U_n\}$ - множество вершин, представляющих пользователя U^p и пользователей, непосредственно связанных с U^p транзакциями.

$T^p = \{T_0, T_1, \dots, T_n\}$ - множество ребер, соединяющих вершины и представляющих непосредственную связь транзакциями.

Определение 4. Транзакционное расстояние.

Транзакционное расстояние D_{ij} — мера связанности пользователей U_i и U_j платформы **mytime**. Транзакционное расстояние зависит от кратчайшего пути между U_i и U_j в графе транзакций, а также от максимального потока криптовалюты между пользователями. Точное математическое выражение для D_{ij} находится в процессе разработки.

Определение 5. Репутация пользователя.

Репутация пользователя U_p или степень доверия сети к пользователю — это мера разнообразия транзакционного портрета, определяемая как:

$$R_p = \frac{1}{n(n-1)} \sum_{i \in U^p} \sum_{j \in U^p, j \neq i} R_i D_{ij}, \text{ где:}$$

$U^p = \{U_0, \dots, U_n\}$ - множество вершин, представляющее пользователей, и непосредственно связанных транзакциями с пользователем U_p

n — количество пользователей, непосредственно связанных транзакциями с U_p

R_j — репутация пользователя U_j

D_{ij} — транзакционное расстояние между пользователями U_i и U_j

Чем меньше связаны между собой пользователи, непосредственно связанные с пользователем U_p и чем выше их собственная репутация, тем больше доверия к U_p как к живому человеку.

Математическая модель репутации находится в разработке и может быть изменена в дальнейшем.

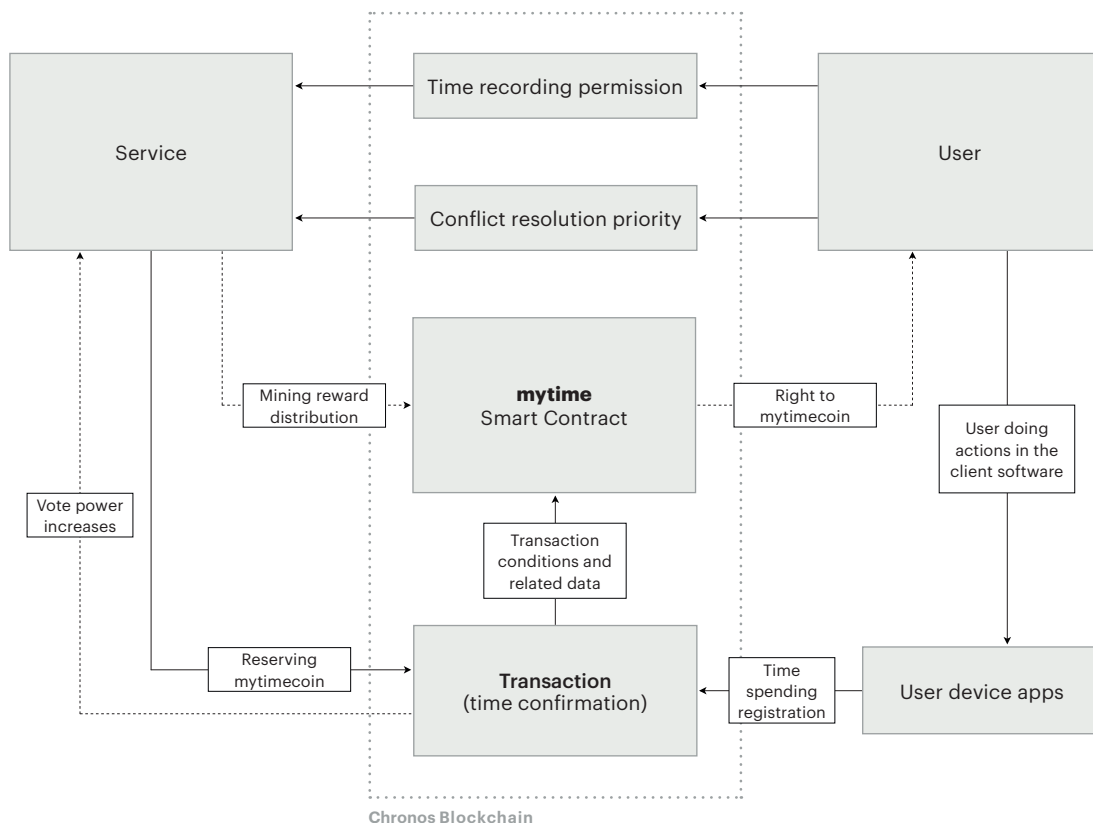
Помимо использования репутации для защиты сети от злоупотребления ботами, транзакционный портрет может быть использован для look-a-like поиска пользователей со схожим транзакционным портретом.

6. Смарт-контракты

На уровне протокола будет доступна поддержка смарт-контрактов. Такие контракты позволяют внедрять более сложные механики траты времени, а также прозрачные механики вознаграждения пользователей за совершения определенных действий в приложениях. Любое приложение может использовать связанный с ним контракт для обеспечения прозрачных сделок со временем.

Смарт-контракты позволяют реализовать различные варианты экономических отношений на базе протоколов **mytime**, среди которых:

- Фьючерсы на время пользователей.
- Прозрачный учет времени и оплаты труда.
- Распределение MYTC в сообществах и кланах.
- Начисление MYTC за выполнение некоторого набора условий.
- Обмен данными между сервисами без доступа к данным напрямую.
- Целевая благотворительность — оплата обучения спонсорами.



7. Криптовалюта MYTC

MYTC — классическая криптовалюта, где все транзакции имеют комиссию, которая формируется на основании текущей загруженности сети.

Конкуренция за размещение транзакции в блоке, определяет наличие минимальной стоимости интервала времени. Минимальная стоимость подстраивается под текущую нагрузку блокчейна Time. Транзакция не будет проведена, если объем депонированной криптовалюты меньше минимального порога.

Пользователь получает криптовалюту, депонированную в Chronos, с помощью вызова специальной функции в личном кошельке. Вызов данной функции формирует запрос на проведение транзакции, регистрируемой в блокчейне Time. Перед помещением данной транзакции в блок и после проверки закрытых оплаченных сессий нода обеспечивает подпись эскроу-транзакции в Money.

8. Эмиссия MYTC

Каждую минуту эмитируется N MYTCs, которые являются наградой за производство блока и распределяются среди всех голосовавших за ноду. Для участия в голосовании необходимо иметь минимальную долю в MYTC (принцип DPoS).

Депонированная криптовалюта образует депонированный Stake, который на порядок увеличивает голос сервиса за производителей блока. Этот Stake увеличивает голос в соответствии с количеством и частотностью записей депонированного времени, накопленного на счету сервиса, а также с учетом репутации пользователей сервиса.

Влияние депонированного Stake уменьшается со временем. Наибольшее значение имеют записи с минимальным прошедшим периодом. Такая механика делает выгодным регулярное подтверждение стоимости времени пользователей **mytime**.

Ноды (делегаты), которые занимаются упаковкой блоков, проверяют уникальность записей минута-пользователь и в случае одновременной записи за одну и ту же минуту корректируют стоимости времени пропорционально количеству сервисов, взаимодействующих с пользователями.

Это обеспечивает отсутствие коллизий, при которых пользователь пытается получить вознаграждение одновременно от нескольких сервисов в одно и то же время.

Конечные формулы эмиссии и влияния депонированного стейка на размер голоса будут получены по итогам имитационного моделирования.

9. Конституция платформы

9.1. Зачем нужна конституция

Анализируя историю развития таких популярных блокчейн-протоколов, как Ethereum, Bitcoin или Zcash, становится очевидно, что любая начальная спецификация не идеальна и всегда будет меняться в процессе пользования. Сегодня большинство спорных вопросов о развитии любой платформы решается форками, реализуемыми узкой группой людей, которые имеют наибольшее влияние на платформу.

Мы считаем, что такой подход по определению угрожает самой идеи распределенной одноранговой сети, поэтому блокчейн **mytime** будет разрабатываться с оглядкой на Tesoz и EOS в том, что касается саморегулирования.

Мы создаем платформу, которая сможет дать любому пользователю несколько базовых прав:

- Право высказать свое мнение на тему какого-то вопроса, о текущем или будущем состоянии сети, или сохранить нейтралитет.
- Право быть уверенным в том, что голос пользователя будет задокументирован вне зависимости от его действий.
- Право в любой момент предложить комьюнити свой вариант решения какого-то вопроса.

Формализация данных прав и реализация их в виде части протокола позволит нам говорить о **mytime** как о по-настоящему децентрализованной платформе, в которой любые предложения вносятся и реализуют именно пользователи платформы, а не узкий круг разработчиков и/или инвесторов.

9.2. Реализация конституции

Голосование за принятие новой поправки протокола будет длиться в течении заранее фиксированного числа блоков $N_{\text{voting length}}$. Первые два года функционирования **mytime**, Chronos Foundation оставляет за собой право вето на любое предложение по изменению.

Для вынесения решения более 80% «активных» пользователей должны участвовать в голосовании. Данная планка пока условна и будет выяснена в процессе моделирования.

Основной процесс голосования делится на 4 этапа, каждый из которых занимает четверть $N_{\text{voting length}}$

1. Любой желающий выкладывает свою версию протокола, где, по его мнению, решена обсуждаемая проблема.
2. Набравшее наибольшее количество голосов обновление протокола выставляется на общее голосование, в котором можно проголосовать «за», «против» или воздержаться (процент нейтральных голосов также будет учитываться в финальном решении).
3. Если кворум был достигнут и набрано достаточное количество голосов «за», то протокол реализуется в testnet. В противном случае он отвергается.
4. Если протокол успешно показывает себя в testnet и проходит еще одно голосование (по тем же правилам, что и предыдущее), то новый протокол имплементируется в главную сеть.

10. Интеграция с платформой

Любой независимый разработчик может создать собственное приложение, используя протоколы **mytime**, и провести интеграцию с другими приложениями платформы. Разработчик может запустить собственный сервис на базе своего приложения, либо интегрировать его в сервисы сторонних бизнесов.

Для разработчиков будут созданы ранние инструменты, облегчающие создание и запуск новых приложений:

- API для взаимодействия с блокчейнами **mytime**, голосования DPoS, работы с криптографией.
- Программное обеспечение для запуска full и light нод.
- Кошельки.
- Смарт-контракты.
- Доступ к распределенному хранилищу данных.
- API для доступа к биржам.
- Маркетплейс запросов от бизнеса на новые сервисы в **mytime**.
- Тестовая инфраструктура.
- Другие сервисы, спрос на которые появится во время развития **mytime**.

10.1. Приложения

Под приложением, интегрированным с платформой **mytime**, подразумевается любой программный продукт, использующий API для взаимодействия с протоколом Chronos.

Приложением может быть:

- Desktopное приложение для любой операционной системы.
- Мобильное приложение для любой операционной системы.

- Веб-приложение.
- Бот для мессенджера (Например, для Slack или Telegram).
- Плагин для произвольной системы (Например для JIRA).
- Серверное программное обеспечение.
- И так далее.

Приложения могут быть разработаны на любых языках программирования.

10.2. Базовые приложения

Помимо спецификации протокола, команда **mytime** разработает следующие базовые приложения:

- Эталонная реализация программного обеспечения для нод, обеспечивающих работу протокола.
- Базовое пользовательское приложение.
- Плагины для мессенджеров, интегрирующие социальные сообщества в **mytime**.

У базового пользовательского приложения две цели:

- Эталонная реализация протокола.
- Привлечение массового пользователя на платформу **mytime**.

Базовое пользовательское приложение будет состоять из следующих компонентов:

- Кошелька.
- Майнера минимального безусловного дохода.
- Маркета приложений на базе **mytime**.

На маркете приложений сразу будут представлены следующие приложения, разрабатываемые командой **mytime**:

- Приложение для общения социальных сообществ и плагина по управлению сообществами.
- Приложение для просмотра видео.

Базовое пользовательское приложение разрабатывается с учетом следующих требований:

- Приложение рассчитано на массового пользователя.
- Устанавливается в один клик и сразу приносит пользователю пользу.
- Взаимодействие с пользователем строится на игровых механиках.

Одновременно с базовым приложением для экспансивного захвата аудитории мы разрабатываем ботов для популярных мессенджеров: Telegram и Slack.

11. Chronos Foundation

Развитием сообщества и линейки сервисов **mytime** будет заниматься отдельная структура — Chronos Foundation.

Для массового распространения **mytime** и повсеместного проникновения МУТС мы будем развивать и поддерживать сообщество интеграторов и разработчиков вокруг платформы.

Развитие и поддержка — это:

- Разработка протокола Chronos и его базовой реализации в формате open source.
- Помощь в интеграции сервисов с **mytime**.
- Разработка типовых решений для фиксации времени пользователя.
- Инвестиции в сервисы, интегрирующиеся с **mytime**.
- Поощрение альтернативных реализаций базовых механизмов протокола.
- Организация конференций и хакатонов.
- Поддержка разработчиков open source-продуктов, используемых в платформе **mytime**.

12. Защита от атак

Вид атаки	Описание проблемы	Решение проблемы
Атака на DPoS	Генерация App и адресов для получения большинства при голосовании за майнинг-ноду для получения вознаграждения	Экономическое, институт репутации
Двойная трата	Двойная трата App для улучшения статистики\репутации из-за ошибок или с другими мотивами	Механизм эскроу
Атака секретной цепи (фальсификация истории транзакций)	Получение экономического эффекта от двойной траты за счёт подстановки ложной цепочки блоков (смарт-контракт или обычная сделка)	DPoS
Атака большинства на механизм репутации (аналог атаки 50 + 1% по хэшрейту)	Генерация нескольких App и множества адресов для атаки на механизм балансировки репутации	Свойства алгоритма репутации
Sybill attack	При небольшом количестве нод атакующий заменяет одну из нод и фальсифицирует информацию о блокчейне для получения выгоды	Trusted nodes, экономическое наказание для атакующих нод
DoS	1. Спам-транзакции. Чем дешевле транзакции, тем проще осуществить атаку данного типа. 2. Пиковые нагрузки на сеть. 3. Другие зависимые от архитектуры вычислительноёмкие операции, которые могут повлиять на работоспособность протокола и узлов сети.	Экономические свойства mytime.
Анализ пакетов	Просмотр трафика сети mytime в произвольном случае	Шифрование
Уязвимость кошельков к похищению		Разработка референсного кошелька с минимальной функциональностью: recovery seed, шифрование файла
Прочие ошибки в ПО и дыры в безопасности протокола, не обнаруженные на текущий момент	Проблема в выработке механизма оперативного вмешательства	Обновление протоколов

13. Экономика mytime

Долгосрочная работоспособность проектов, связанных с блокчейном, во многом определяется экономическими факторами — если у всех участников есть мотивация развивать платформу и увеличивать количество новых участников системы, создавать приложения, поддерживать работоспособность и т.д., то такая система может существовать долго и эволюционировать. Если такой мотивации нет, долгосрочное развитие проекта сомнительно. Именно по этой причине мы уделяем экономике **mytime** особое внимание.

13.1. Депонированная криптовалюта

Депонированная криптовалюта — это безусловное право А на получение средств от В. Отличие от эскроу-транзакций заключается в том, что депонирование криптовалюты выгодно самому А, поскольку это увеличивает его голос в DPoS и, соответственно, увеличивает объем эмиссионного вознаграждения. Технически депонирование представляет собой две транзакции: транзакцию в Time и эскроу-транзакцию в Money.

Свойства депонированной криптовалюты:

- Приносит вознаграждение А.
- Не принадлежит А.
- Не приносит вознаграждение В (если в смарт-контракте А и В не предусмотрено иное).
- Принадлежит В.
- Подтверждает стоимость времени В за взаимодействие с А.
- Операция бесплатна для А (если попадает в блок по отранжированной стоимости времени).
- Комиссия за смену состояния с депонирования на собственность ложится на В.
- А не может депонировать больше криптовалюты, чем у него есть.

- Безусловность депонирования, т.е. А не может вернуть криптовалюту обратно. Даже в случае разорения А, В сможет получить криптовалюту.
- При депонировании криптовалюты, А может записать в транзакцию набор произвольных данных.

Совокупность свойств депонированной криптовалюты создает экономическую основу для мотивации участников системы.

13.2. Мотивация участников системы

13.2.1. Мотивация пользователей

Мотивация подключения пользователей к сервисам платформы — получение максимального количества криптовалюты за каждую минуту своего времени.

Когда сервис распределяет вознаграждение от депонированной криптовалюты, пользователь имеет мотивацию держать деньги в депонированном виде, извлекая криптовалюту по мере необходимости в свой кошелек.

Пользователи зарабатывают криптовалюту в соответствии со своими циркадными ритмами, квалификацией, сферами деятельности и конкурирующими предложениями со стороны сервисов.

Вознаграждение от любого сервиса — одна и та же криптовалюта. Это избавляет пользователей от необходимости накапливать баллы и бонусы от сотен программ лояльности разных сервисов.

Пользователи мотивированы взаимодействовать с разнообразными сервисами и другими пользователями, поскольку это увеличивает репутацию в **mytime**.

13.2.2. Мотивация сервисов

Сервисами в системе могут быть как B2C-приложения для широкого рынка, так и внутрикорпоративные приложения, а также любые другие бизнесы, интегрирующие протокол в свои продукты.

На платформе **mytime** может быть реализовано множество моделей повышения эффективности существующих бизнесов. Также возможно создание принципиально новых моделей, невозможных вне платформы **mytime**.

Возможности предоставляемые сервисам платформой **mytime**:

- Микроплатежи для пользователей.
- Альтернатива банковскому протоколу для большинства бизнес-операций.
- Вознаграждение по алгоритму Proof-of-time — аналог банковских процентов на депозит.
- Автоматизация разных бизнес-операций через смарт-контракты.
- Безопасная работа с деперсонализированными данными.
- Автоматическое начисление премий за достижение KPI, связанных с временем.
- Конкурентное преимущество по сравнению с другими бизнесами, не использующими возможности **mytime**.
- Авансовое вознаграждение при привлечении нового пользователя в сервис в обмен на данные маркетинговых исследований, CPC, new customers profile ID и т.д.
- Возможность доставить контент туда, где пользователь гарантированно будет периодически проводить свое время.
- Снижение вознаграждения пользователей, использующих несколько сервисов одновременно (условный штраф за рассеивание внимания).

13.2.3. Мотивация валидаторов

Одной из проблем, с которой столкнутся B2C-сервисы, будут боты, эмулирующие действия реального пользователя. Другая проблема — валидация выполненной работы, действий, результата, по итогам которых происходит депонирование криптовалюты.

Для решения этих проблем мы вводим роль валидатора. Валидатор — это частный случай сервиса, отличающийся от остальных сервисов тем, что он заинтересован не во внимании пользователей, а в выполнении полезной работы для сервисов по подтверждению личности пользователей, их действий и результатов.

Мотивация валидатора — в получении вознаграждения за выполненную работу со стороны сервисов или пользователей.

Базовое программное обеспечение для валидаторов будет разрабатываться и выпускаться в рамках работы Chronos Foundation. Особое программное обеспечение для валидаторов может быть создано сторонними разработчиками, заинтересованными в получении коммерческой прибыли.

13.2.4. Мотивация нод

Как и в любом блокчейн-проекте, мотивация нод — получение вознаграждения за упаковку блока и комиссии за транзакции. В Proof-of-Time ноды получают только часть вознаграждения за упаковку блока, а остальное вознаграждение будут получать приложения/пользователи, поддерживающие ноду своими голосами.

Так как количество транзакций в **mytime** может составлять миллионы транзакций в минуту, ноды будут представлять собой вычислительные кластеры, в том числе развернутые в облачных сервисах Google/Amazon. Таким образом, будет происходить быстрая балансировка необходимого количества нод.

При негативных сценариях, вызванных резким падением курса или другими факторами, сеть **mytime** будет поддерживаться нодами, запускаемыми

Chronos Foundation. После стабилизации обстановки, ноды Chronos Foundation будут снова выведены из сети, освободив места для других участников.

13.2.5. Мотивация хранения данных

Метаинформация о взаимодействии пользователей с сервисами может достигать огромных размеров, поскольку сервисы почти не ограничены в формате записей. Мы предполагаем децентрализованное хранение данных по аналогии со Storj, FileCoin, Maidsafe, Siacoin, EOS. Решение о том, будем ли мы делать форк одного из разработанных решений и дорабатывать его под свои потребности или использовать один из готовых запущенных сервисов, будет принято во время разработки **mytime**.

Оплату за услуги по хранению метаданных будет проводить заинтересованный сервис.

14. Выводы

Экономические и социальные особенности блокчейн-платформы **mytime** могут задать новый уровень проникновения технологий блокчейна во многие сферы современной жизни за счет перестроения экономических отношений бизнесов и пользователей.

Программное обеспечение **mytime** поможет уменьшить издержки, возникающие при взаимодействии бизнесов и пользователей друг с другом.

В результате мы сможем построить новую экономику, в которой время каждого человека в любом его взаимодействии приносит ему доход, а каждое социальное формирование, частным случаем которого является бизнес, представляет собой совокупность взаимодействия людей, выраженную через стоимость времени каждого человека.

15. Отказ от ответственности

Информация, изложенная в этом Technical Paper, может быть неполной. Содержание документа не подразумевает каких-либо элементов договорных отношений, не является обязывающим для Компании и может быть изменено в будущем по мере проектирования и разработки экосистемы **mytime**.

Technical Paper не содержит инвестиционных, правовых, налоговых, регуляторных, финансовых, бухгалтерских или иных рекомендаций.

Technical Paper не должен рассматриваться как единственно верная, исчерпывающая база для оценки транзакций по приобретению mytimecoin.

Ничего в данном Technical Paper не может расцениваться как запрос на инвестиции, равно как и никоим образом не должно расцениваться в качестве предложения о покупке каких-либо ценных бумаг в какой-либо государственной юрисдикции.

Данный документ не попадает под действие какой-либо государственной юрисдикции, которая запрещает или любым иным образом ограничивает транзакции с криптовалютой.

Ряд заявлений, оценок и финансовых данных, содержащихся в данном Technical Paper, представляют собой прогнозы, а не фактическую информацию.

Ввиду совокупности неизвестных рисков и прочих неопределенностей, связанных с проектом, его фактические показатели могут существенно отличаться от прогнозов, приводимых в данном документе.

Компания не предлагает и не распределяет mytimecoin, не ведет бизнес в рамках регулируемой деятельности в Соединенных Штатах Америки, Китайской Народной Республике, Республике Корея, Государстве Израиль, Соединённом Королевстве Великобритании и Северной Ирландии, Республике Сингапур и иных странах и территориях, где транзакции или использование цифровых токенов и валют попадают под запретительные меры или требуют от Компании быть зарегистрированной, лицензированной в тех или иных государственных органах.

mytimescoin не предлагаются, не распространяются и не отчуждаются иным образом лицам, проживающим или зарегистрированным в Соединенных Штатах Америки (включая все штаты и округ Колумбия), Китайской Народной Республике, Республике Корея, Государстве Израиль, Соединённом Королевстве Великобритании и Северной Ирландии, Республике Сингапур, а также в странах или на территориях, где запрещены или каким-либо образом ограничиваются операции с криптовалютами.

Действия по приобретению такими лицами mytimescoin будут расценены как незаконные, несанкционированные и мошеннические. Такие действия могут повлечь за собой негативные последствия в соответствии с законами, применимыми в конкретной юрисдикции.

Компания обращает внимание каждого потенциального держателя mytimescoin на то, что Technical Paper предоставляется на том основании, что читатель является уполномоченным лицом на ознакомление с документом.

Каждому потенциальному держателю предоставляется право самостоятельно оценить легальность приобретения и осуществления других операций с mytimescoin на основании распространяющихся на него законов и иных актов, действующих в его юрисдикции, как в случае приобретения их у Компании, так и в случае перепродажи и осуществления других операций с ними.

Technical Paper на английском языке является основным официальным источником информации о проекте mytimescoin. В результате перевода данного документа на иные языки часть информации может быть утрачена, повреждена или искажена.

Точность перевода не гарантируется. В случае возникновения любых несоответствий и коллизий между переводами Technical Paper, его официальная версия на английском языке имеет преимущественную силу.

До участия в проекте настоятельно рекомендуем каждому потенциальному участнику/держателю проконсультироваться с личным юридическим, инвестиционным, налоговым, бухгалтерским, иным советником для анализа правовых и финансовых рисков, расчета потенциальных выгод и прочих последствий такого участия и/или любой транзакции, а также тщательно изучить нижеприведенную информацию.

16. Риски проекта

Приобретение mytimescoin связано с высокой степенью риска. Целый ряд факторов может оказать существенное негативное влияние как на стоимость mytimescoin, так и на всю платформу mytime.

Нижеприведенный перечень рисков и неопределенностей, с которыми могут столкнуться держатели mytimescoin не является исчерпывающим.

16.1 Риски, связанные со стоимостью mytimescoin

16.1.1. Отсутствие прав, областей применений, функциональных возможностей и иных атрибутов

mytimescoin не предоставляют никаких прав, не имеют областей применения, функциональных возможностей или особенностей, иных атрибутов, явных или подразумеваемых, включая любые направления использования, цели, функциональные возможности, атрибуты или особенности mytime.

mytimescoin не являются инструментом обладания любыми активами Компании и не могут рассматриваться как нематериальный актив.

Компания не дает обязательств, не гарантирует владельцам, что mytimescoin дают их держателям какие-либо права, имеют области применения, функциональные возможности, атрибуты или особенности.

16.1.2. Прекращение развития рынка mytimescoin

Поскольку ранее не существовало открытого рынка mytimescoin, запуск проекта может не привести к формированию активного или ликвидного рынка mytimescoin. Рыночная цена mytimescoin может быть неустойчивой.

Несмотря на предполагаемый спрос на mytimescoin, активный рынок может не сформироваться или прекратить развитие. В результате владелец не сможет своевременно продать или совершить иную операцию с mytimescoin.

В худшем сценарии развития событий рынок не сформируется или вскоре прекратит существование, а держатель mytimescoin потеряет возможность их реализации.

16.1.3. Спекулятивные риски

Оценка криптовалют на вторичном рынке зачастую непрозрачна. Стоимость mytimescoin может сильно колебаться в течение короткого периода времени.

16.1.4. Риск потери ценности

Существует значительный риск того, что держатель mytimescoin может потерять свои вложения целиком в результате их обесценивания.

Компания не гарантирует ценности mytimescoin и не прогнозирует их ликвидность. Компания не несет и не должна нести ответственность за рыночную стоимость mytimescoin, их ликвидность.

16.1.5. Невозможность возврата

Компания не обязана выкупать mytimescoin или каким либо иным способом возмещать средства их держателям по каким-либо причинам.

Никаких гарантий ценности mytimescoin не предоставляется и не будет предоставлено, в том числе не гарантируется их неотъемлемой ценности. Поэтому возврат вложенных средств может оказаться невозможен. Кроме того, он может быть ограничен законами и предписаниями, отличающимися от законов и предписаний, действующих в отношении держателя mytimescoin.

16.2. Риски блокчейна и программного обеспечения

16.2.1. Несвоевременная обработка смарт-контрактов

В блокчейнах Bitcoin и Ethereum производство блоков может происходить в произвольные моменты времени, поэтому существует риск несвоевременного исполнения смарт-контрактов. Владельцу следует осознавать и учитывать эту вероятность.

Bitcoin или Ethereum-блокчейн может не обработать транзакцию в момент ожидания покупателем, и покупатель может не получить mytimesoін в тот же день, когда совершает необходимое для этого действие.

16.2.2. Перегрузка сети

Сети Bitcoin и Ethereum подвержены перегрузкам, в течение которых транзакции могут быть отложены или потеряны. Отдельные лица и группы лиц могут намеренно загружать сети, пытаясь получить преимущество.

16.2.3. Риски разработки

Все свойства и изложенные в Technical Paper прогнозы экосистемы **mytime** и криптовалюты mytimesoін не проверены на практике. Их разработка может столкнуться с непреодолимыми сложностями технического характера.

Возможно, добиться функционирования платформы mytime не удастся, или она будет работать не так, как предполагалось. mytimesoін могут не получить заявленных функциональных возможностей.

Кроме того, платформа mytime ввиду высокой скорости появления инноваций может устареть и потерять актуальность в процессе разработки или незадолго после запуска.

16.3. Риски безопасности

16.3.1. Риск потери частных ключей

mytimesoін могут храниться в цифровом кошельке или хранилище, для доступа к которым требуется цифровой ключ или комбинация цифровых ключей.

Потеря ключей, связанных с цифровым кошельком или хранилищем, приведет к потере доступа к его балансу. Кроме того, третья сторона, получившая доступ к приватным ключам, которые использует держатель для доступа к кошельку или хранилищу, получит доступ к находящимся в них mytimesoін. Субъекты Компании не несут ответственности за потери, которые это может повлечь

16.3.2. Недостатки безопасности инфраструктуры mytime

Хакеры, иные группы и организации могут пытаться вмешаться в смарт-контракт или иные аспекты функционирования mytime различными способами, включая, помимо прочего, атаки вредоносного ПО, атаки типа «отказ в обслуживании» и другие распространенные методы нарушения нормального функционирования цифровых сервисов.

16.3.3. Сбой в подключении открытых криптографических ключей к аккаунту владельца.

В случае, если владелец mytimesoін не предоставит доступ для подключения открытых криптоключей к своему аккаунту, это может привести к тому, что третья сторона не сможет корректно распознать количество mytimesoін на балансе владельца в блокчейне Ethereum в момент формирования начальных балансов нового блокчейна, созданного на платформе **mytime**.

16.3.4. Несовместимость криптовалютного кошелька

Кошелек или поставщик услуг по хранению криптовалют, используемые владельцем, должны быть технически совместимы с mytimecoin. Несоблюдение этого условия может привести к тому, что владелец mytimecoin не получит доступа к своим mytimecoin.

16.4. Риски развития mytime

16.4.1. Риск зависимости от третьих лиц

Даже после запуска mytime будет полностью или частично полагаться на третьих лиц для принятия и реализации отдельных функций, а также для продолжения разработки, обслуживания и поддержки платформы. Нет гарантий того, что эти третьи стороны выполнят свою работу должным образом.

16.4.2. Зависимость платформы от команды разработки

Результаты деятельности проектной группы mytime, которая отвечает за поддержание конкурентоспособности всей экосистемы, в значительной степени зависят от состава команды. Потеря или ослабление членов управленческой команды или невозможность привлечь, сохранить и поддерживать дополнительный персонал могут оказать существенное неблагоприятное воздействие на mytime.

Конкуренция за персонал, обладающий опытом соответствующим задачам Компании, является высокой из-за небольшого числа квалифицированных специалистов. Дефицит кадров серьезно влияет на возможность привлекать дополнительный квалифицированный управленческий персонал, что может оказать значительное негативное влияние на платформу.

16.4.3. Отсутствие интереса к платформе

Даже если платформа будет завершена и запущена, успех платформы зависит от заинтересованности и участия третьих лиц. Их заинтересованность не может быть гарантирована.

16.4.4. Риск, связанный с другими проектами

Платформа может привести к созданию альтернативных проектов, продвигаемых неаффилированными третьими лицами.

16.4.5. Риск неблагоприятного колебания стоимости криптовалюты

Развитие платформы может быть прекращено из-за нехватки финансирования, ухода ключевого персонала, отсутствия коммерческих успехов и перспектив, а также иных факторов.

16.5. Риски, связанные с бизнесом компании

16.5.1. Конфликт интересов

Субъекты компании могут быть задействованы в операциях с аффилированными лицами. Конфликты интересов могут возникнуть как внутри Компании, так и между Компанией и аффилированными лицами. Заинтересованность может приводить к заключению сделок на условиях, не являющихся рыночными.

16.5.2. Риски, связанные с осуществлением деятельности на развивающихся рынках

Компания или некоторые из ее субъектов могут вести профессиональную деятельность на развивающихся рынках. Страны, относящиеся к данной группе, подвержены большим рискам, включая значительные юридические, экономические и политические риски.

16.6. Правительственные риски

16.6.1. Неразработанность нормативной базы

Юридический статус криптографических токенов, криптовалют, иных цифровых активов и технологии блокчейн остается неустановленным во многих странах. Предсказать, как скоро и каким образом государственные органы начнут регулировать распространение и использование перечисленных активов, а также технологии блокчейн, не представляется возможным.

Изменение законодательства может негативно влиять на Компанию в целом и на перспективы разрабатываемых ей технологий в частности.

Компания может прекратить распространение монет и разработку платформы или операции в определенной юрисдикции в случае, если такие действия будут признаны незаконными или законодательные изменения сделают их экономически нецелесообразными.

16.6.2. Неспособность получить, поддерживать или продлевать лицензии и разрешения.

Хотя на дату настоящего документа законом не установлено требований, обязывающих Компанию или владельца mytimesoин получать какие-либо лицензии и разрешения, необходимые для осуществления операций с цифровыми активами, существует риск того, что такие законодательные требования будут введены в будущем.

Регулирующие органы могут выдвинуть требования к участникам оборота криптовалюты, включая требования соблюдения различных стандартов, получения лицензий на операции с криптовалютой, идентификации, предоставления отчетности.

В таком случае биржевая торговля mytimesoин может быть приостановлена на неопределенный срок.

16.6.3. Риск со стороны государственного регулятора

Индустрия, в которой действует Компания, является новой и может подвергаться повышенному надзору и контролю.

Собственность Компании и проводимые ею операции регулируются предписаниями различных государственных органов и подвержены ежегодным проверкам.

Проверяющие органы могут заключить, что Компания нарушила законы, указы или правила и не может опровергнуть данные выводы или своевременно устранить нарушения.

Несоблюдение требований действующих законов, предписаний, полученных по результатам проверок со стороны государственных органов, могут привести к существенным санкциям от штрафов и до административного или уголовного преследования должностных лиц Компании.

Решения государственных органов, требования, санкции — любое увеличение государственного регулирования деятельности Компании может увеличить расходы Компании и отрицательно повлиять на ее деятельность.

16.6.4. Незаконные или произвольные действия государственных органов

Иногда органы государственной власти проявляют высокую степень свободы. Под влиянием коммерческих или политических соображений действуют выборочно, произвольно, без предварительного уведомления или в порядке, противоречащем закону.

Само по себе это создает риски для деятельности Компании. Кроме того, в таких условиях конкуренты Компании могут получать различные льготы и преференции от государственных органов, получая конкурентные преимущества.