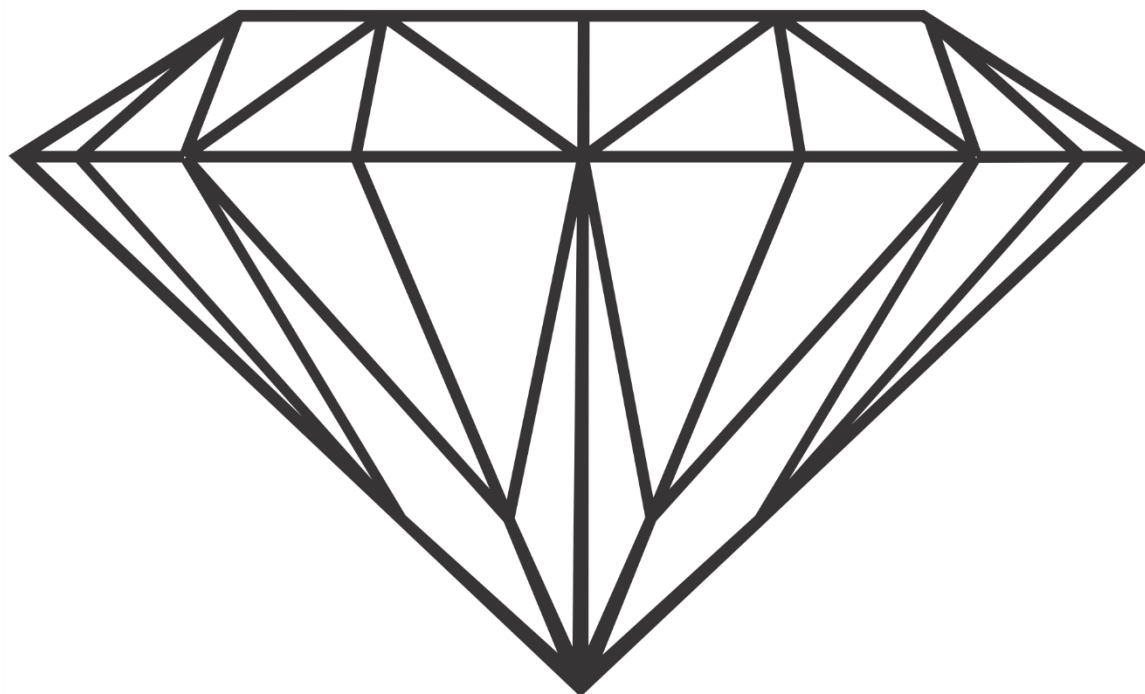


WISEPLAT

ТЕХНИЧЕСКАЯ БЕЛАЯ КНИГА

<https://oswiseplat.org/>



04 июля 2017 г.

Программное обеспечение WISEPLAT основано на блокчейн, а именно на использовании сохраненных криптографических записей, с открытым исходным кодом и пиринговыми сетями. На платформе WISEPLAT будут разработаны приложения нового типа – децентрализованные приложения. Децентрализованные приложения гибче, прозрачнее и надежнее, чем современное программное обеспечение, созданное с применением традиционных централизованных моделей.

Блокчейн WISEPLAT оперирует не с одним блокчейном, а с двумя основными блокчейнами и множеством блокчейн отдельных приложений. Первый блокчейн – операции с токенами WISE (быстрые транзакции, PoW), второй блокчейн – каталог приложений с блокировкой WISE в пользу пользователей приложений (масштабирование, DPoS/PoW). Такое разделение позволяет WISEPLAT проводить быстрые транзакции с токенами WISE и обеспечить эффективную масштабируемость для приложений

ОБРАТИТЕ ВНИМАНИЕ: КРИПТОГРАФИЧЕСКИЕ ТОКЕНЫ, УПОМЯНУТЫЕ В ДАННОМ ДОКУМЕНТЕ, ОТНОСЯТСЯ К КРИПТОГРАФИЧЕСКИМ ТОКЕНАМ WISE, ВЫПУЩЕННЫМ ДЛЯ РАЗРАБОТКИ НОВОЙ БЛОКЧЕЙН СИСТЕМЫ WISEPLAT. ОНИ НЕ ЯВЛЯЮТСЯ ТОКЕНАМИ СТАНДАРТА ERC-20, КОТОРЫЕ ВЫПУСКАЮТСЯ НА БЛОКЧЕЙН ETHEREUM В СВЯЗИ С ГЕНЕРАЦИЕЙ НА БЛОКЧЕЙН СИСТЕМЕ WISEPLAT.

Использование материалов этой белой книги разрешено только с личной, некоммерческой целью. Любое копирование, перепечатка, тиражирование и распространение материалов этой белой книги запрещено без предварительного письменного разрешения основателей WISEPLAT. Цитирование допускается при условии обязательного указания автора и активной гиперссылки на сайт WISEPLAT, размещенной непосредственно возле текстового блока. Коммерческое использование всех или любой части материалов сайта запрещено.

ПРАВОВАЯ ОГОВОРКА: WISEPLAT Техническая Белая книга написана только в информационных целях. WISEPLAT не гарантирует точности или выводов, сделанных в этом отчете, и этот отчет предоставлен “как есть”. WISEPLAT не даёт и отказывается от всех заявлений и гарантий, явных, подразумеваемых, установленных законом или иных, каких бы то ни было, включая, но не ограничиваясь:

1. по гарантии пригодности для продажи, пригодности для определенной цели, пригодности использования, титула или не нарушения прав третьих лиц;
2. что содержание данного документа не имеет ошибок;
3. что такой контент не будет нарушать прав третьих сторон.

WISEPLAT и её филиалы не несут никакой ответственности за ущерб или убытки любого рода, возникшие в результате использования ссылки, или использования этого документа или любой части этого документа, учитывая, что компания была предупреждена о возможности таких убытков. WISEPLAT и её филиалы ни в коем случае не несут ответственности перед любым лицом или организацией за любые убытки, потери, обязательства, затраты или расходы любого рода, будь то прямые или косвенные, косвенные, компенсационные, случайные, фактические, штрафные и любые другие, или связанные с использованием ссылки на этот документ, или связанные с использованием этого документа или любой части его содержания, включая без ограничений потерю бизнеса, дохода, прибыли, использование сведений, репутацию или другие нематериальные убытки.

ОГЛАВЛЕНИЕ

СОВРЕМЕННЫЕ ПРОБЛЕМЫ БЛОКЧЕЙН ПРИЛОЖЕНИЙ.....	5
СКОРОСТЬ ВЫПОЛНЕНИЯ	5
МАСШТАБИРУЕМОСТЬ	5
ОГРАНИЧЕННОСТЬ СМАРТ-КОНТРАКТОВ	5
АНОНИМНОСТЬ АККАУНТОВ	5
ДОВЕРИЕ	5
РЕШЕНИЕ, ПРЕДЛАГАЕМОЕ WISEPLAT	6
СКОРОСТЬ ВЫПОЛНЕНИЯ	6
Алгоритм согласования PoW/DPoS	6
Быстрые транзакции	7
Достижение скорости	8
Коммуникации между блокчейнами.....	9
МАСШТАБИРУЕМОСТЬ	9
Параллельное выполнение	9
Обратная совместимость с Ethereum Virtual Machine (EVM).....	9
Майнинг и вознаграждение	10
Инструменты.....	10
Вознаграждение за блок	10
Стоимость транзакции и Токен WISE	10
Обновление протокола	10
Плановые обновления.....	10
Срочные исправления.....	10
Архитектура WISEPLAT	11
ОГРАНИЧЕННОСТЬ СМАРТ-КОНТРАКТОВ	13
Смарт-контракты	13
Типы смарт-контрактов	13
АНОНИМНОСТЬ АККАУНТОВ	14
Создание адреса и ключей.....	14
Защита аккаунтов.....	14
Механизм мульти-подписей.....	14
Делегированные/Подчинённые адреса	14

Управление разрешениями.....	14
Идентифицируемые аккаунты.....	15
ДОВЕРИЕ	15
Открытый код.....	15
Коллегии независимых оценщиков	16
ДОХОД ИНВЕСТОРОВ WISEPLAT.....	16
ОКРАШЕННЫЕ ТОКЕНЫ	16
ICO / КРАУДФАНДИНГ	16
ВЫВОД НА БИРЖУ	16
АРЕНДА ПРИЛОЖЕНИЙ.....	17
КАПИТАЛИЗАЦИЯ ПЛАТФОРМЫ.....	17
СМАРТ-КОНТРАКТЫ	17
ЗАКЛЮЧЕНИЕ	17
БЛОК-СХЕМА 1	18
БЛОК-СХЕМА 2.....	19
БЛОК-СХЕМА 3.....	20

СОВРЕМЕННЫЕ ПРОБЛЕМЫ БЛОКЧЕЙН ПРИЛОЖЕНИЙ

Блокчейн (blockchain — цепочка блоков) — это неизменяемая структура данных, состоящая из списка блоков, где каждый следующий блок содержит хэш предыдущего блока. Нельзя изменить или удалить блок из середины цепи, не перестроив все блоки выше.

Подсчет хэша каждого блока вычислительно сложная операция, поэтому изменение данных в середине цепи становится практически невозможным или экономически не выгодным. Именно сложность подсчета хэша нового блока и ее легкость проверки на правильность хэша обеспечивает блокчейну устойчивость к неправомерным изменениям. На этом и держится безопасность блокчейна.

Блокчейн используется не только для криптовалют. Возможно хранить в блокчейне полноценные Тьюринг-полные программы, которые называются смарт-контрактами, что позволяет настроить блокчейн на выполнение прикладных задач.

Существующие на сегодня популярные реализации блокчейн системы сталкиваются с многими проблемами, т.к. на этапе планирования архитектур этих систем они и не планировали решать такие задачи.

СКОРОСТЬ ВЫПОЛНЕНИЯ

Текущая скорость транзакций, проводимых через систему Bitcoin, оставляет желать лучшего. Проект Ethereum планировал решить эту задачу сократив время генерации блока до 15 секунд, но параллельно нагрузил себя приложениями, которые очень активно генерируют свои транзакции, тем самым скорость в этом проекте тоже оставляет желать лучшего.

МАСШТАБИРУЕМОСТЬ

Ограниченность в скорости выполнения генерации блоков не дает системам адекватно масштабироваться при увеличении нагрузок.

ОГРАНИЧЕННОСТЬ СМАРТ-КОНТРАКТОВ

Ограниченность контрактов реализована с умыслом повышения безопасности системы. Но в таком случае большинство идей, приводящих к развитию и востребованности как блокчейн системы, так и приложений остаются за гранью реализации.

АНОНИМНОСТЬ АККАУНТОВ

Реализованная анонимность аккаунтов, это идейный плюс к системе. Но возникают задачи, в которых желательно определять роли и делегировать задачи определенным аккаунтам.

Нет возможности подтверждения своих собственных аккаунтов (по желанию владельца), что не позволяет пользователям получать статус идентифицируемых аккаунтов.

ДОВЕРИЕ

Доверие блокчейн системе — это одно, а доверие приложению — это другое. Из-за сложности кода, даже если он открыт, большинству людей не будет понятно, что же он в итоге делает. Возникает потребность в независимой оценке — на сколько можно доверять приложению.

РЕШЕНИЕ, ПРЕДЛАГАЕМОЕ WISEPLAT

Команда разработчиков WISEPLAT готова реализовать проект новой блокчейн системы, которая будет использовать лучшие подходы к решению проблем, с которыми столкнулись популярные блокчейн системы. Закладывая функционал и потенциал на этапе формирования архитектуры WISEPLAT, мы сможем оптимально решать задачу быстрых платежей, в то же самое время обеспечивая максимальную производительность для блокчейн приложений. Сохраняя обратную совместимость с громадным количеством инструментов для блокчейн Ethereum, мы сохраняем возможность большому количеству разработчиков эффективно использовать уже готовые наработки в новой блокчейн системе WISEPLAT.

Для успешного и перспективного развития децентрализованных приложений блокчейн система WISEPLAT должна удовлетворять следующим требованиям:

1. Открытый исходный код. Открытость кода позволяет получить доверие потенциальных пользователей.
2. Масштабируемость. Способность обработать большие объемы транзакций.
3. Бесплатное использование. Особенность децентрализованных приложений – наличие бесплатной платформы для пользователей приложений.
4. Децентрализованный консенсус.
5. Отсутствие центральной точки отказа. Все данные распределены между всеми узлами. Если один из узлов отказывает, то другие, независимо от него, продолжают работать. Т.е. нет центрального сервера, который может отказать.
6. Простота обновления и исправления ошибок.
7. Быстрые транзакции.
8. Поддержка приложений, которые могут использовать возможность параллельных и последовательных вычислений.

СКОРОСТЬ ВЫПОЛНЕНИЯ

Требования к современным системам заключается в эффективном сочетании их надежности, скорости и стоимости. Надежность системы WISEPLAT обеспечивается технологией блокчейн, когда ресурсоемкие процессы генерации новых блоков не позволяют злоумышленникам переписывать цепочки блоков в виду сильной экономической неэффективности.

Любой человек требует от систем скорости и не желает ждать. Понятно, что чем выше скорость, тем дороже будет система, но есть и исключения – это когда мы распараллеливаем процессы и используя примерно те же самые мощности достигаем лучших результатов. Этот же принцип мы закладываем в систему WISEPLAT, а именно разделяем систему платежей и систему приложений в разные блокчейн, причем каждое приложение в праве иметь свой собственный блокчейн. Это разделение позволяет иметь быструю скорость обработки платежей и быструю скорость обработки транзакций приложениями.

Блокчейн системы платежей будем называть первым блокчейном.

Блокчейн системы приложений будем называть вторым блокчейном.

Блокчейн отдельного приложения будем называть блокчейном приложения.

Теперь рассмотрим различие в алгоритмах консенсуса для этих блокчейн цепочек и способ осуществления быстрых транзакций для них.

Алгоритм согласования PoW/DPoS

Для подтверждения транзакций, в привычных нам централизованных системах, всегда использовался главный центр, учитывающий все движения средств. В разрабатываемом приложении транзакции подтверждаются узлами, которые напрямую взаимодействуют друг с

другом (P2P). Транзакции группируются в блоки. Блоки связываются между собой в цепочку. Каждый блок содержит ссылку на предыдущий блок. Все узлы хранят копию цепочки блоков и формируют новые блоки в соответствии с правилами. Важная функция этих правил защитить цепочку блоков от атак, а также достижение согласия в случае появления нескольких версий блокчейна.

Согласие в первом блокчейне достигается путем алгоритма Доказательства работы (англ. proof of work, PoW). Любой майнер с долей вычислительной мощности может открыть блок с вероятностью равной его доли в общей вычислительной мощности. Консенсус в виде доказательства работы является объективным, например, если новый узел сети имеет подключение хотя бы к одному "честному" пользователю, то он выберет действительный блокчейн, так как тот имеет большую суммарную вычислительную сложность.

Согласие во втором блокчейне достигается путем алгоритма Делегированного подтверждения доли (англ. delegated proof of stake, DPoS), где конечное слово остаётся за держателем средств. В DPoS, блоки порождаются predetermined числом пользователей системы (делегатами), которые получают за это вознаграждение и наказываются за злонамеренное поведение (например, за доказанное участие в двойном расходовании средств). В DPoS-алгоритмах, делегаты участвуют в двух процессах: построение блока транзакций и верификация действительности сгенерированного блока используя электронную подпись.

Блок создается отдельным пользователем и для того, чтобы считаться действительным, он обычно должен быть подписан более чем одним делегатом.

В DPoS доля учитывается одним из следующих способов:

- Делегаты выбираются в соответствии с их долей в системе.
- Делегаты получают голоса от всех пользователей, и сила голоса зависит от доли токенов у голосующего.
- Голоса делегатов выбираются пропорционально их гарантийному депозиту.

В системе WISEPLAT для второго блокчейна, доля делегатов в DPoS определяется пропорционально их гарантийному депозиту, что позволяет консенсусу в виде делегированного подтверждения доли быть объективным.

Тип согласия для блокчейн приложения в системе WISEPLAT определяется во втором блокчейне в записи самого приложения.

Быстрые транзакции

Если ограничить время генерации блока до минимально эффективных 12-15 секунд, то мы сталкиваемся с проблемой масштабируемости системы в целом. Количество транзакций увеличивается значительными темпами по мере роста популярности системы и 12-секундный блок может вместить около 180 транзакций. Для того, чтобы вмещать разумное количество транзакций необходимо увеличивать время, требуемое для генерации блока, тем самым увеличивая время ожидания подтверждения операции.

Все операции можно разделить на две категории:

- 1 – срочные, такие как платежи, и требующие чуть ли не мгновенного выполнения.
- 2 – средне срочные, такие как обмен данными с приложениями, не требующие мгновенного выполнения, но им нужна скорость для адекватной работы.

Таким образом предполагается использовать несколько цепочек блокчейна: первый блокчейн для финансовых операций с алгоритмом подтверждения PoW, второй блокчейн для публикаций

приложений с алгоритмом подтверждения DPoS и блокчейн приложений для работы с транзакциями приложений с алгоритмом подтверждения DPoS или PoW, определяемый на уровне второго блокчейна.

Блокчейн WISEPLAT, основан на Эфириуме. Новый подход к использованию нескольких блокчейнов позволит полностью раскрыть возможности при помощи умных контрактов, что даст гораздо большее пространство для создания приложений, и в то же время сохраняя ценность и стабильность работы.

Алгоритм сложности Wise Dagger Hashimoto - это одна из инноваций сети WISE – алгоритм сложности, который динамично подстраивается под хеш-рейт сети.

Расчетная сложность первого блокчейна приводит время генерации блока в среднем к 15 секундам.

Расчетная сложность второго блокчейна приводит время генерации блока в среднем к 45 секундам.

Расчетная сложность блокчейна приложения определяется на уровне второго блокчейна в записи самого приложения, и обычно составляет от 15-45 секунд.

Алгоритм смотрит на изменения хеш-рейта каждого блока и устанавливает сложность в зависимости от анализа временных меток блоков за последние 2 часа, меняя окно генерации блока.

WISE	Ethereum
<ul style="list-style-type: none">Алгоритм: Wise Dagger HashimotoВсего монет: ~1.500.000.000 <p>Время генерации блока</p> <ul style="list-style-type: none">первого блокчейна: 15 секундвторого блокчейна: 45 секундблокчейна приложения: 15-45 секунд <ul style="list-style-type: none">Награда за блок: 3 WISE не уменьшается ежегодно (применима к первому блокчейну)	<ul style="list-style-type: none">Алгоритм: Dagger HashimotoВсего монет: 1.800.000.000 <p>Время генерации блока</p> <ul style="list-style-type: none">15 секунд <ul style="list-style-type: none">Награда за блок: 5 ETH не уменьшается ежегодно

Достижение скорости

Разделяй и властвуй (лат. divide et impera) – позволяет использовать стратегию получения и поддержания власти, путём разделения большой концентрации власти на группы, которые индивидуально имеют меньше власти. Тем самым мы можем достичь максимальной скорости работы разделяя систему на несколько блокчейнов.

Первое, остающееся неизменным – это первый блокчейн, отражающий все операции с внутренними токенами WISE платформы WISEPLAT, построенный на устойчивой модели согласования PoW.

Второе, что нам необходимо – это цепочка, которая будет отражать текущие приложения в системе, а именно хранить параметры приложений, такие как: наименование приложения, тип приложения, ключевые слова, краткое описание приложения, корневой список делегатов приложения, построенная на устойчивой модели согласования DPoS.

Таким образом, пользователи платформы WISEPLAT будут иметь быстрые и надежные внутренние токены, базирующиеся на PoW, и в любой момент времени знать какие приложения

есть в системе и иметь возможность их установить из надежных дистрибьютеров благодаря DPoS. Приложения в своей архитектуре могут использовать PoW или DPoS и, например, выбирая архитектуру для приложения DPoS позволит проводить тысячи транзакций в секунду, что обеспечит отличную скорость на платформе WISEPLAT.

Коммуникации между блокчейнами

Основной блокчейн используется для отражения финансовых итераций, с возможностью небольших текстовых комментариев. В любое время можно получить актуальную информацию о счетах и движениях денежных средств и при необходимости инициировать свою транзакцию.

Со вторым блокчейном взаимодействие происходит при поиске приложений и их доверенных дистрибьютеров. Например, при нахождении приложения, которое интересно пользователю, он инициирует начальную синхронизацию блокчейн цепочки приложения с доверенными дистрибьютерами и с другими участниками сети по P2P.

Приложения получают возможность осуществлять любые коммуникации между собой через блокчейны приложений, т.к. в любой момент времени известны доверенные дистрибьютеры приложений, и есть возможность быстро синхронизировать блокчейн цепочки приложений.

МАСШТАБИРУЕМОСТЬ

Использование нескольких блокчейнов становится ответом проблемы масштабируемости для Bitcoin и других блокчейнов, например, Ethereum.

Идея, заключается в обеспечении стабильного канала платежей по первому блокчейну и запись промежуточных транзакций приложений – в свои отдельные блокчейн цепочки каждого отдельного приложения.

Например, пользователь, используя второй блокчейн может найти приложение, решающее его задачи, пусть это будет некий цифровой контент. Тогда провайдер цифрового контента и его потребитель, в первом блокчейне будут отражать свои движения денежных средств за контент, а в блокчейне приложения будут фиксировать транзакции, приводящие к платежам. При использовании такой архитектуры, платформа может адаптироваться к потоку в тысячи транзакций в секунду.

Параллельное выполнение

Архитектура платформы WISEPLAT позволяет приложениям параллельно выполняться на любом множестве компьютеров. Согласование результатов их работы обеспечивается архитектурой блокчейна приложения. Максимальная пропускная способность приложения обеспечивается использованием механизма консенсуса DPoS.

Обратная совместимость с Ethereum Virtual Machine (EVM)

Для максимальной эффективности повторного использования уже созданных приложений, в платформе WISEPLAT предусмотрена обратная совместимость с Ethereum. Тем самым разработчики блокчейн системы WISEPLAT предоставили уже существующим инструментам и приложениям Ethereum возможность работать и развиваться на новой перспективной платформе WISEPLAT.

Виртуальная машина Ethereum Virtual Machine (EVM) использовалась для большинства существующих смарт-контрактов и теперь все они могут быть легко адаптированы для работы в блокчейн WISEPLAT. Контракты будут выполняться внутри своей песочницы в первом блокчейн.

Майнинг и вознаграждение

Недавний старт со средней сложностью сети позволит владельцам видеокарт поколения R9 280x чувствовать себя в майнинге WISE на равных с новым поколением видеокарт, т.к. сейчас эти карточки выдают 27MH/s, что даже больше стоковых 24 MH/s RX480.

Инструменты

В связи с поддержкой обратной совместимости с Ethereum, можно использовать любое доступное ПО майнинга соответствующей платформы для майнинга WISE.

Вознаграждение за блок

За майнинг блока первого блокчейна установлена фиксированная награда 3 WISE. Вознаграждение за майнинг второго блокчейна и блокчейн приложений – не предусмотрено.

Стоимость транзакции и Токен WISE

Одним из основных преимуществ платформы WISEPLAT является то, что архитектурно продумана возможность обеспечения максимальной пропускной способности выполнения транзакций для приложений, которая не зависит от рыночной стоимости токенов WISE.

Если владелец приложения хочет увеличить свою пропускную способность, то он должен увеличить количество доверенных дистрибьютеров в первом блокчейне осуществив соответствующее депонирование токенов WISE.

Обновление протокола

Платформа WISEPLAT определяет процесс, посредством которого происходит обновление протокола, это определено на уровне исходного кода системы и принятого соглашения об обновлении.

Плановые обновления

Для обычных обновлений, используется следующая процедура:

1. Во втором блокчейне генерируется блок обновления ядра приложения WISEPLAT.
2. В течении 30 дней блок получает одобрение 10/15 голосов.
3. При достижении 10 голосов, все ноды системы WISEPLAT начинают применять предложенное обновление.
4. Все ноды не обновившиеся в течении 7 дней, исключаются из работы.
5. По истечению 7 дней все полные ноды активируют предложенное обновление.

Процесс обновления блокчейна для добавления новых функций будет занимать от 2 до 3 месяцев.

Процесс обновления блокчейна исправляющий не критичные ошибки будет занимать от 1 до 2 месяцев.

Срочные исправления

Для критичных исправлений используется следующая процедура:

1. Во втором блокчейне генерируется блок критичного обновления ядра – приложения WISEPLAT.
2. В течении 12 часов блок получает одобрение 10/15 голосов.
3. При достижении 10 голосов, все ноды системы WISEPLAT начинают применять предложенное обновление.
4. Все ноды не обновившиеся в течении 12 часов, исключаются из работы.
5. По истечению 12 часов все полные ноды активируют предложенное обновление.

Процесс обновления блокчейна исправляющий критичные ошибки будет занимать от 12 до 24 часов.

Архитектура WISEPLAT

Рассмотрим архитектуру WISEPLAT на Блок-схеме №1.

Верхний уровень системы представлен двумя цепочками блокчейн:

Первый блокчейн – блокчейн системы платежей, базирующуюся на согласовании PoW. Все операции между аккаунтами происходят в нем. Смарт-контракты в первом блокчейне ограничены только своим блокчейном.

Второй блокчейн – блокчейн системы приложений, базирующуюся на согласовании DPoS. Делегаты для голосования выбираются из первого блокчейн и там же происходит блокировка средств делегатов. Второй блокчейн предназначен для публикаций приложений платформы WISEPLAT, благодаря этому пользователи могут получить всегда актуальную информацию о приложении из блока блокчейн. Информация о приложении из блока блокчейн содержит в себе следующее: наименование приложения, краткое описание, список доверенных делегатов этого приложения (с блокировкой их средств в первом блокчейне) и способ согласования цепочки блокчейн для этого приложения.

Следующий уровень представлен разными блокчейн для отдельных приложений (свой отдельный блокчейн для конкретного приложения) – называется блокчейном приложения. Блокчейн приложения определяется доверенными делегатами приложения, и генерирует соответствующим образом свои блоки в зависимости от выбранного способа его согласования POW/DPoS.

Разберем по Блок-схеме №1 каким образом клиент получает свое приложение из системы WISEPLAT.

Сначала пользователю необходимо подключиться к платформе WISEPLAT. Сделать это можно через приложение кошелька WiseWallet или через консоль командной строки. Приложение кошелька WiseWallet – это не просто кошелек для осуществления любых платежей, а приложение, которое может управлять и создавать смарт-контракты, искать и добавлять приложения, информировать пользователя о изменениях в составе делегатов его приложений, отображая увеличение капитализации или плановое уменьшение капитализации используемых им приложений.

Потом пользователь осуществляет поиск приложения (в блок-схеме [1]) по заданным критериям с возможной сортировкой по рейтингу. Как только пользователь определился с приложением, так сразу он может запустить его установку. Платформа WISEPLAT для каждого опубликованного приложения сообщает пользователю (в блок-схеме [2]) список доверенных дистрибьютеров этого приложения и способ согласования цепочки блокчейн этого приложения. Например, в Блок-схеме №1 показано, что приложение «APP1» имеет 4 доверенных дистрибьютера приложения, которые заблокировали 4*100 WISE в качестве гарантий надежности этого приложения, а приложение «APP2» имеет 3 доверенных дистрибьютера приложения, которые заблокировали 3*100 WISE в качестве гарантий надежности этого приложения соответственно. На этом моменте пользователь примерно может оценить надежность приложения, которая гарантируется страховым депозитом.

Получив список доверенных дистрибьютеров приложения, пользователь инициирует первоначальную загрузку приложения с доверенных дистрибьютеров (в блок-схеме [3], [4]) и одновременным поиском, и загрузкой этого приложения по P2P (в блок-схеме [5]) с других клиентов приложения. Достоверность информации, полученную по P2P с других клиентов

пользователь проверяет через контрольные суммы блоков, которые он всегда может уточнить у доверенных дистрибьютеров приложения.

После получения приложения, пользователь может его запустить и начать пользоваться.

Разберем по Блок-схеме №2 каким может быть приложение по скачкам для платформы WISEPLAT.

В этой блок-схеме мы рассмотрим работу внутренних и внешних смарт-контрактов.

Способ получения приложения аналогичный описанному ранее по Блок-схеме №1.

Предположим, что пользователь А приложения делает ставку на лошадь в забеге на ее победу в скачках, и пользователь Б делает противоположную ставку на эту же лошадь, для упрощения примера так же предположим, что суммы ставок равны. Свои ставки через приложение они оформляют смарт-контрактом в первом блокчейн. В этом смарт-контракте блокируются токены пользователей А и Б, и смарт-контракт подписывается тремя подписями: пользователя А, Б и третьей стороной – доверенным дистрибьютером приложения, которому доверяют оба пользователя, т.к. они пользуются его приложением (в блок-схеме [1]). После оформления отношений, пользователи ожидают результаты скачек. Распределенное приложение скачек через внешнее API (в блок-схеме [2]) получает результат скачек (в блок-схеме [3]). Пользователи приложений отправляют полученную информацию в виде транзакции доверенному дистрибьютеру (он же делегат цепочки приложения) на включение этой транзакции в блок блокчейн приложения (в блок-схеме [4]). Делегат цепочки подтверждает транзакцию подписывая блок, и она распространяется по блокчейн приложения. Приложение пользователей ожидают появление в цепочке транзакции по скачкам заключенного смарт-контракта, как только такая транзакция появляется, так сразу приложения пользователей А и Б проводят разблокировку смарт-контракта своими подписями с соответствующим направлением перечисления токенов (в блок-схеме [5]). Если пользователи А и Б не пытаются обмануть систему, то контракт выполняется при наличии не конфликтующего условия перечисления средств и обеих подписей пользователей А и Б. Если же возникает конфликт из-за предоставления пользователями не достоверной информации, то в его разрешение подключается третья доверенная сторона (в блок-схеме [6]) - доверенный дистрибьютер приложения (он же делегат цепочки приложения).

Разберем по Блок-схеме №3 каким может быть приложение биржи для платформы WISEPLAT.

В этой блок-схеме мы рассмотрим работу биржи и взаимодействие пользователей А и Б.

Способ получения приложения аналогичный описанному ранее по Блок-схеме №1.

Предположим, что пользователь А владеет 100 ETH и хочет их поменять на 100 BTC, и есть еще один пользователь Б, который владеет 100 BTC и хочет их поменять на 100 ETH. Т.к. пользователи А и Б не доверяют друг другу, рыночная цена BTC и ETH различна и это разные криптовалюты, то обмен пользователи могут совершить только через биржу.

Для работы с разными криптовалютами биржа имеет свои платежные адреса в каждой из криптовалют, тем самым обеспечивая надежный промежуточный слой, для обмена разных пар криптовалют.

Пользователь А и Б начисляют свои ETH и BTC соответственно, на платежные адреса биржи. Пользователь А выставляет на продажу свои 100 ETH заявкой в стакане ETH/WISE, например, за 100 WISE (в блок-схеме [4]) и размещает ордер на покупку 100 BTC за 170 WISE в стакане BTC/WISE (в блок-схеме [5]). Пользователь Б выставляет на продажу свои 100 BTC заявкой в стакане BTC/WISE, например, за 200 WISE (в блок-схеме [6]) и размещает ордер на покупку 100 ETH за 80 WISE в стакане ETH/WISE (в блок-схеме [7]). Таким образом у нас получилось два

стакана заявок по 2 заявки в каждом. Спред в цене между заявками будет сокращаться по мере увеличения количества пользователей биржи. При достижении согласия в цене между пользователями А и Б, они смогут поменяться криптовалютами BTC ↔ ETH. Естественно, пользователи А и Б имеют свои счета в WISE, откуда берутся недостающие WISE для обмена и куда перечисляются оставшиеся WISE после обмена.

ОГРАНИЧЕННОСТЬ СМАРТ-КОНТРАКТОВ

Платформа WISEPLAT дает возможность использовать весь потенциал Смарт-контрактов, позволяя выполнять Смарт-контракты между частными блокчейнами.

Смарт-контракты

Умный контракт (англ. Smart contracts) – алгоритм, описывающий набор условий, выполнение которых влечет за собой выполнение других запланированных задач, тем самым исключается человеческий фактор.

Основной принцип умного контракта состоит в полной автоматизации и достоверности исполнения договорных отношений.

Стороны подписывают умный контракт, используя свои цифровые подписи. После этого умный контракт вступает в силу. Автоматизированное исполнение обязательств контракта осуществляется на уровне платформы WISEPLAT, внутри системы, имеющей беспрепятственный доступ исполняемого кода к объектам умного контракта. Все условия умного контракта должны иметь математическое описание и ясную логику исполнения. Имея доступ к объектам контракта, умный контракт отслеживает по указанным условиям достижение или нарушения пунктов, и выполняет действия, прописанные в его коде.

Например, умный контракт можно эффективно реализовать для:

- Периодических платежей
- Партнерских программ
- Перевода токенов
- Осуществления страхования
- Обмена
- Ставки на спорт, на цену нефти, на деривативы и др.

Типы смарт-контрактов

Платформа WISEPLAT по сложности имеет три типа смарт-контрактов.

- Предопределенные
- Шаблонные
- Сложные

Предопределенные – контракты, в которых все поля заданы жестко и не могут выбираться.

Шаблонные – контракты, в которых некоторые поля могут выбираться из списка.

Сложные – контракты, которые пишут программисты.

По источнику поступления информации смарт-контракты делятся на:

- Внутренние контракты. Они используют информацию, находящуюся внутри системы, и не могут обращаться к внешним API. Для первого и второго блокчейн используются только внутренние смарт-контракты.
- Внешние контракты. Используются для блокчейн-приложений. Возможно выполнение контрактов с обращениями к внешним API.

АНОНИМНОСТЬ АККАУНТОВ

Возможность подтверждения своих аккаунтов в платформе WISEPLAT достигается использованием системы подтверждения аккаунтов, что позволит пользователям по их желанию для своих аккаунтов получать статус идентифицируемых аккаунтов.

Платформа WISEPLAT позволяет создавать не только обычных пользователей системы, но имеет механизм создания иерархии пользователей, тем самым предоставляя возможность управления второстепенными аккаунтами и их правами на осуществление операций.

Создание адреса и ключей

Для хранения, осуществления движения денежных средств и инвестирования в WISEPLAT есть специальные кошельки. Это уникальный механизм, который включает в себя большое количество расчетов по транзакциям и уникальный алгоритм защиты. Все транзакции хранятся в общедоступном виде, но без информации о реальном владельце этих адресов. Каждый пользователь системы может генерировать неограниченное количество пар ключей. Основное использование ключей – создание адреса и подтверждение правомочности формирования транзакций. Но они могут использоваться и для цифровой подписи или шифрования при переписке. Созданные ключи обычно хранят в специальном зашифрованном файле wallet.dat («кошельке»). Пользователь придумывает пароль только для доступа к информации из файла «wallet.dat», то есть для доступа к своим парам ключей. Каждому возможному адресу соответствует баланс, выраженный в WISE токенах. Все адреса с ненулевым балансом записаны в цепочку блоков, защищенную от изменений. Как ранее уже отмечалось, цепочка хранит лишь транзакции, поэтому баланс счета не хранится, а рассчитывается с учетом всех входов и выходов.

Защита аккаунтов

Для защиты от потерь при утери секретного ключа используют простое соглашение о мульти-подписи. Используя мульти-подписи для сделки, другая компания является стороной по каждой сделке. Это значительно сокращает риски, но увеличивает расходы и вводит некоторые обязательства для всех участников.

Механизм мульти-подписей

Мульти-подпись – механизм используемый для повышения уровня безопасности криптовалютных кошельков. Мульти-подпись предусматривает генерацию WISE-адреса, для которого требуется несколько приватных ключей (паролей), которые используются для авторизации платежа.

Платеж может быть подтвержден как этими ключами, так и их комбинацией. Мульти-подпись не позволяет злоумышленнику вывести средства с WISE-кошелька, т.к. ему необходимо получить еще и чужие подписи, которые требуются для авторизации операций, а список этих пользователей формируется заранее самим же пользователем.

Делегированные/Подчинённые адреса

WISEPLAT позволяет через встроенный механизм мульти-подписей организовывать делегирование ролей. Таким образом можно организовать такой пример: участник А совместно с участником Б, создают подчиненный им кошелек для участника В, накладывая на кошелек ограничения по количеству трат и их ежедневному объему.

Управление разрешениями

Механизм управления разрешениями для подчиненных аккаунтов определен на уровне системы WISEPLAT. И позволяет делегировать управление аккаунтами пользователей, тем самым привнося в систему дополнительный уровень безопасности.

Например, когда пользователь создает «мастер» аккаунт и для него «второстепенный» аккаунт, но с ограничением на осуществление платежей только в сторону «мастер» аккаунта. Тем самым «второстепенный» аккаунт может принимать любые платежи, но платить может только «мастер» аккаунту.

Идентифицируемые аккаунты

Платформа WISEPLAT имеет архитектурно запланированную возможность использовать системы подтверждения аккаунтов (при желании владельца аккаунта) для 100% идентификации аккаунта пользователя.

Тем самым появляется возможность для организаторов ICO, краудфандинга, лотерей и любых других программ для платформы WISEPLAT ограничивать участников не только по статусу идентифицируемый/не идентифицируемый, а также ограничивать участие по странам проживания/местонахождения, или применять еще более точный критерий к аккаунтам участников.

ДОВЕРИЕ

Все современные платформы ОС (Windows, Linux, Android и др.) имеют рейтинговые оценки приложений, что позволяет пользователям быстро и в большинстве случаев безопасно выбрать приложения, отвечающие им возможностями по решаемым задачам.

На платформе WISEPLAT разработчики учли такую особенность и реализуется она благодаря второму блокчейну APP WISE STORE. В этом блокчейне хранится основная информация по приложениям для платформы WISEPLAT: название приложения, тип приложения, ключевые слова, краткое описание приложения, корневой список делегатов приложения, построенная на устойчивой модели согласования DPoS.

В качестве гарантий надежности именно самих приложений используется модель согласования DPoS с депонированием средств, тем самым по каждому приложению можно посмотреть корневой список делегатов приложения и сколько они заблокировали средств в качестве гарантий своей надежности и естественно надежности самого приложения. В случае выявления недобросовестных приложений эти денежные средства списываются. Выход из делегатов возможен, но с блокировкой средств на 30 дней, по истечению которых они разблокируются автоматически. Платформа WISEPLAT будет информировать пользователей о изменениях в составе делегатов, отображая увеличение капитализации или плановое уменьшение капитализации приложения, для предотвращения быстрого «сливания» капитализаций приложений и защиты интересов пользователей приложений.

Тем самым получается рыночная модель надежности приложений, чем приложение более популярно, тем больше оно имеет делегатов и тем выше она капитализирует средства на свое приложение.

Открытый код

Программное обеспечение платформы WISEPLAT построено на принципе открытого программного обеспечения (англ. open-source software) с открытым исходным кодом. Так как исходный код доступен для просмотра, изучения и изменения, то это позволяет любым пользователям принимать участие в доработке системы WISEPLAT.

Просмотр и изучение исходного кода позволяет понять, платформа WISEPLAT делает именно то, что декларирует.

Коллегии независимых оценщиков

Даже если разработчики приложения заблокировали средства в качестве гарантий своей надежности и естественно надежности самого приложения, этого бывает недостаточно для 100% уверенности пользователей в безопасности использования приложения.

Поэтому, пользователи приложений могут образовывать группы независимых оценщиков для подтверждения надежности приложений, публикуя свои отзывы о работе с этими приложениями.

ДОХОД ИНВЕСТОРОВ WISEPLAT

Капитализация платформы базируется на увеличении количества приложений, которые будут создаваться сторонними разработчиками.

Ценность продукта WISEPLAT создает спрос на токены среди пользователей. Платформа позволяет решить две основных проблемы Bitcoin: обеспечивает быстрое проведение операций и эффективную масштабируемость за счет нескольких режимов работы.

В приложения платформы WISEPLAT будут интегрированы дополнительные услуги и товары, которые можно получить исключительно за WISE. Приложения платформы WISEPLAT имеют большой рынок для использования. В финансовом секторе могут применяться для таких целей: проведение платежей, цифровая идентификация, комплаенс, кредитование по принципу P2P, страхование, торговое финансирование и заключение сделок по ценным бумагам. Дополнительно проект будет иметь спрос среди частных блокчейнов. На базе системы WISEPLAT можно провести ICO компанию. Также, можно использовать смарт-контракты платформы на торговых площадках, крипто биржах, для хранения данных и создания прогнозов.

С развитием сети количество пользователей будет постоянно увеличиваться. Соответственно будет расти спрос на токены. Общее количество токенов ограничено. Учитывая вознаграждения майнеров, количество может незначительно вырасти, но это существенно не повлияет на ситуацию по спросу. Как следствие, на бирже токенов будет постоянно спрос при ограниченном предложении, что обеспечит доходность инвесторов.

ОКРАШЕННЫЕ ТОКЕНЫ

На платформе WISEPLAT можно проводить монетизацию приложений, используя для этого «окрашенные» токены, которые могут торговаться на бирже и соответственно приобретаться пользователями. Например, в играх эти «окрашенные» токены можно использовать для оплаты покупок внутри самой игры. Все основные методы монетизации приложений, которые используются сейчас в обычных приложениях могут и будут использоваться в приложениях системы WISEPLAT.

ICO / КРАУДФАНДИНГ

Разработчики приложений для платформы WISEPLAT могут создавать свои внутренние «окрашенные» токены (окрашенные монеты), тем самым WISEPLAT позволяет проводить ICO для приложений, предлагая возможность обменять (купить) токены приложений за токены WISE.

Краудфандинг позволяет как работающему бизнесу, так и стартапам привлечь инвестирование в свои проекты. Для этих целей организатор разрабатывает документацию с описанием проекта, востребованности его товара/услуги, указанием сроков завершения проекта и доходности. Затем организатор выпускает свои токены на платформе WISEPLAT и проводит ICO.

ВЫВОД НА БИРЖУ

Токены WISE после проведения ICO будут торговаться на популярных крипто-биржах.

Согласно дорожной карте приложений платформы WISEPLAT, сторонними разработчиками будет создана своя биржа для токенов WISE. Тем самым разработчики планируют предоставить возможность появления токенов приложений на этой бирже, при подаче разработчиками приложений соответствующего запроса на биржу.

АРЕНДА ПРИЛОЖЕНИЙ

Архитектура платформы WISEPLAT позволяет разработчикам приложений реализовать доступность их приложений пользователям на арендной основе. Это увеличивает востребованность пользователей в токенах WISE.

КАПИТАЛИЗАЦИЯ ПЛАТФОРМЫ

Для эффективного развития платформы WISEPLAT необходимо стремиться увеличивать капитализацию платформы.

В самой блокчейн системе WISEPLAT заложен механизм постоянного увеличения капитализации за счет размещения на ней новых приложений. Каждое приложение блокирует часть токенов WISE, тем самым как-бы на время выводя их из системы. Т.е. в прямом обращении становится меньше токенов, и их цена возрастает.

Для увеличения капитализации будут проводиться рекламные компании, направленные на привлечение сторонних разработчиков на платформу.

СМАРТ-КОНТРАКТЫ

В системе уделяется центральное внимание смарт-контрактам. Одни из них рассчитаны на простоту использования и массовый рынок, другие, сложные, будут разрабатываться за токены WISE. Спрос на токены будет увеличиваться, а цена, как следствие, повышаться.

ЗАКЛЮЧЕНИЕ

Платформа WISEPLAT – это успешная и высокодоходная блокчейн система. Она сочетает в себе самые ценные характеристики – открытость и децентрализацию. Открытость исходного кода продукта WISEPLAT, позволит развивать его любым социальным группам, участвовать в дискуссиях, проводить конференции и встречи.

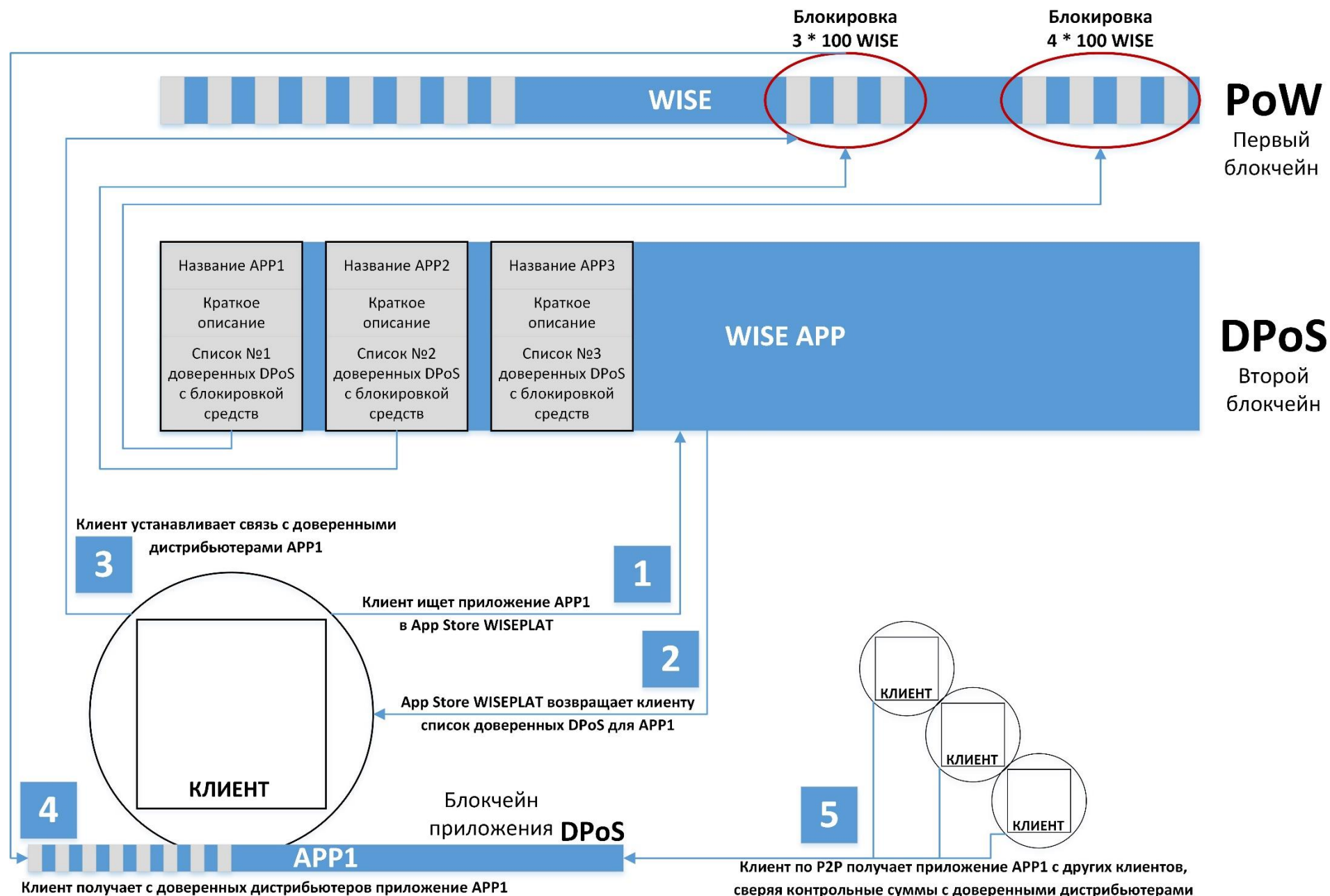
Платформа WISEPLAT эффективно решает проблему масштабируемости системы, обеспечивая максимальную скорость выполнения транзакций. Большим достоинством платформы WISEPLAT является ее пропускная способность. Этим не могут похвастаться Ethereum и многие другие блокчейн системы. Как следствие низкой пропускной способности, Ethereum не развивает никакие приложения и даже не предоставляет шаблоны смарт-контрактов. Потому, что система Ethereum не способна обработать большое число транзакций. Платформа WISEPLAT устроена так, что способна обработать большое количество транзакций и объединить приложения.

Платформа WISEPLAT может выполнять Смарт-контракты между частными блокчейнами и получать информацию от внешних API, тем самым убирая «ограниченность» смарт-контрактов.

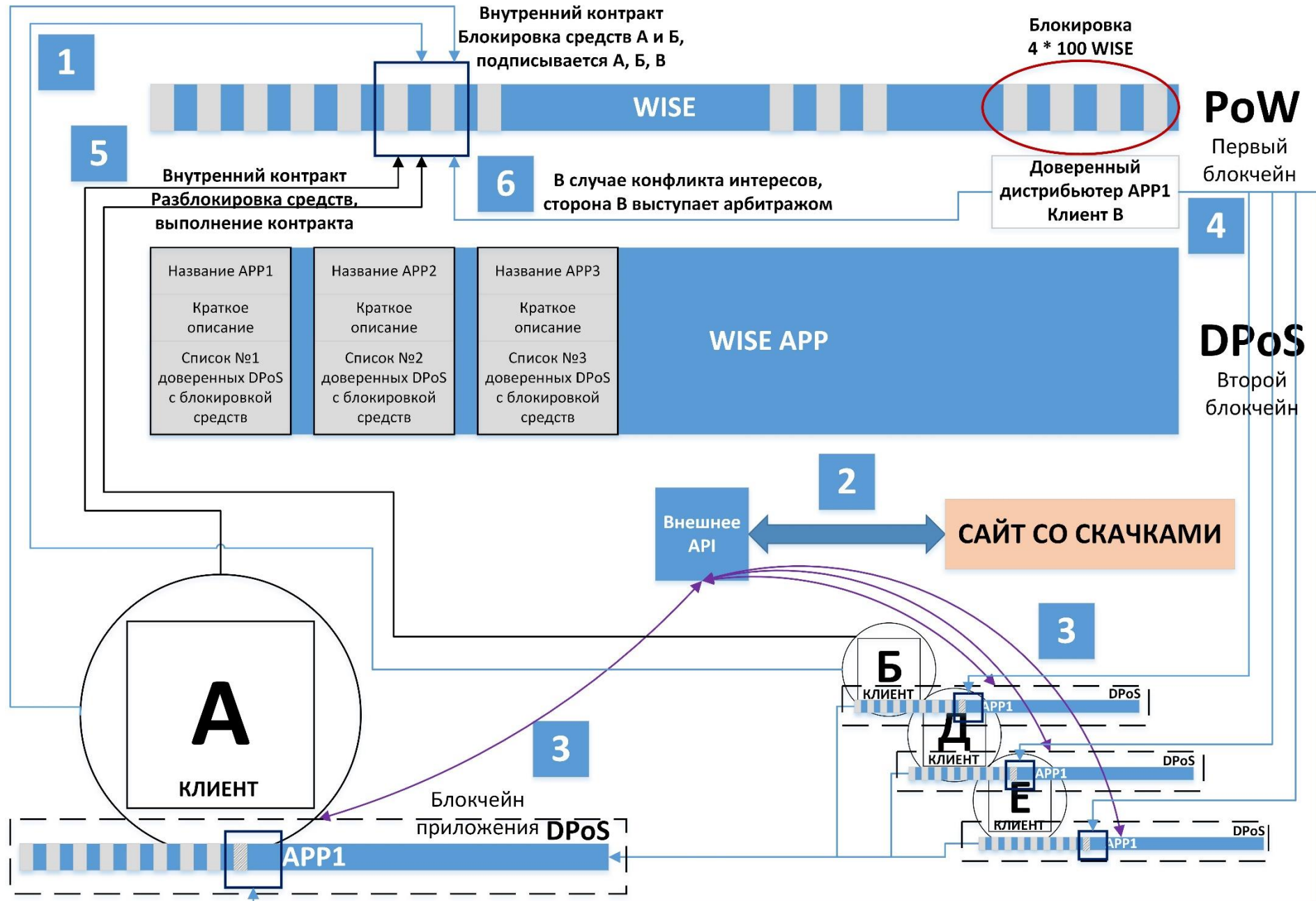
Платформа WISEPLAT позволяет установить доверие друг к другу между участниками благодаря возможности использования систем подтверждения аккаунтов.

Как в Apple/Google/Microsoft App Store, пользователи получают возможность оценить надежность приложений платформы WISEPLAT до момента начала их использования.

БЛОК-СХЕМА 1



БЛОК-СХЕМА 2



БЛОК-СХЕМА 3

