Y2 (этил-ксилол)
Арабская лига Y2 Лаборатория нового энергетического топлива Smart
Smart
Преобразование невозобновляемых ресурсов в возобновляемые ресурсы

Э м б л е м а Лиги Арабской лиги, монета Y2 LOGO, Y2 Лаборатория нового энергетического топлива LOGO

Г е н е р а л ь н ы й секретарь Лиги арабских государств

П о д т в е р ж д е н и е подписи Ahmed Aboul Gheit Y2

К р а т к о е описание:

К о г д а Сатоши запустил блоккун в биткойне в январе 2009 года, он также представил миру два новых непроверенных революционных концепта. Первый - биткойн, децентрализованная одноранговая онлайн-валюта, которая поддерживает стоимость без какой-либо гарантии акт и в о в , внутренней стоимости или центрального эмитента. До сих пор Биткойн привлекал большое внимание общественности. Что касается политики, это валюта, которая не имеет центрального банка, и она имеет резкие колебания цен.

Т е м не менее, большой эксперимент Сатоши Накамото также имеет не менее важную роль в биткойне: концепция блочной цепи, основанная на доказательстве рабочей нагрузки, позволяет людям достичь консенсуса в отношении порядка транзакций. Биткойн как приложение м о ж н о охарактеризовать как систему от первого к файлу: если у человека есть 50 БТД и одновременно отправляет эти 50 БТД в A и B, только первая подтвержденная транзакция вступит в силу. Не существует неотъемлемого метода определения того, какая из двух транз а к ц и й прибывает первой. Эта проблема на протяжении многих лет препятствовала развитию децентрализованной цифровой валюты. Блоккайн Накамото - первое надежное децентрализованное решение. Теперь внимание разработчиков начинает быстро переходить на вторую час т ь технологии биткойнов и как блокировки используются в других областях, кроме денег.

П р и л о ж е н и я , которые часто упоминаются, включают использование цифровых активов в цепочке для представления нестандартных валют и финансовых инструментов (цветные монеты), владение некоторыми основными физическими устройствами (интеллектуальными активами) и несменными активами, такими как доменные имена (валюта домена) И более продвинутые приложения, такие как децентрализованные обмены, финансовые производные, двухточечные системы азартных игр и цепочек и системы репутации.

Еще одна важная область, которую часто задают, - это «умные контракты» - системы, которые автоматически переносят цифровые активы на основе заранее установленных правил. Например, у человека может быть контракт на хранение в форме «A может снимать до X монет в день, B может иметь до Y в день, A и B могут быть свободно извлечены вместе, а A может остановить право вывода B». Логическим продолжением такого рода контрактов являются децентрализованные автономные организации (DAO) - долгосрочные интеллектуальные контракты, которые содержат активы организации и кодируют правила организации. Целью монеты Y2 является создание блочной цепи со встроенным зрелым полным языком Turing. Этот язык может использоваться для создания контрактов для кодирования произвольных переходов состояний. Пользователи могут просто реализовать логику с использованием нескольких строк кода. Создайте все системы, упомянутые выше, и многие другие системы, которые мы не могли себе представить.

каталог

○ Тарифы

○ Вычисление и Тьюринг завершены

○ Валюта и выпуск

○ Расширяемость

● Обзор: децентрализованные приложения

● Заключение

● Комментарии и расширенное чтение

— — — —

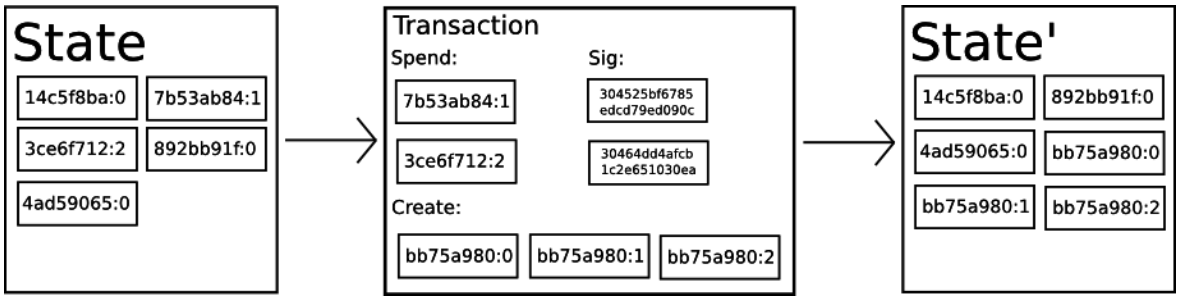
история

Концепция децентрализованной цифровой валюты, как и альтернативное применение регистрации собственности, была создана несколько десятилетий назад. Большинство анонимных электронных денежных соглашений в 1980-х и 1990-х годах были основаны на методе ослепления Шаумяна. Эти электронные соглашения о наличных средствах обеспечивают высокую частную валюту, но эти протоколы не пользуются популярностью, поскольку все они полагаются на централизованный посредник. В 1998 году б-деньги Вэй Дай впервые представили идею создания валюты путем решения вычислительных проблем и децентрализованного консенсуса, но это предложение не дало конкретного метода достижения децентрализованного консенсуса. В 2005 году Хэл Финни представил концепцию «многоразовых доказательств работы», в которой используется мышление b-money и вычислительная сложность хеш-акций Адама Ада (Hashcash).) Трудности создания валюты криптовалюты. Тем не менее, эта концепция снова теряется в идеализации, потому что она полагается на доверенные вычисления в качестве задней части.

Поскольку валюта является заявкой перед приложением, порядок транзакций имеет решающее значение, поэтому децентрализованные валюты должны найти способы достижения децентрализованного консенсуса. Основным препятствием для всех предыдущих биткойнских электронных валютных соглашений является то, что хотя исследование о том, как создать безопасную систему виртуозной отказоустойчивости с несколькими консенсусами, длилось уже много лет, вышеупомянутый протокол разрешил половину проблем. , Эти протоколы предполагают, что все участники системы известны и создают форму границы безопасности, такую как «Если N-участник участвует в системе, система может терпеть злонамеренных участников N / 4». Однако проблема с этим предположением заключается в том, что в случае анонимности граница безопасности, установленная системой, уязвима для атак на ведьм, поскольку злоумышленник может создавать тысячи узлов на сервере или ботнете, тем самым в одностороннем порядке обеспечивая большинство доля.

Инновация Накамото - это введение концепции, которая сочетает в себе очень простой децентрализованный консенсусный протокол на основе узлов с механизмом проверки рабочей нагрузки. Узел получает право участвовать в системе через механизм проверки рабочей нагрузки, а транзакция упаковывается в «блоки» каждые десять минут, тем самым создавая постоянно растущую цепочку. Узел с большим количеством мощности имеет большее влияние, но гораздо сложнее получить больше энергии, чем вся сеть, чем создать один миллион узлов. Несмотря на то, что модель биткойн-блокчейков очень проста, она оказалась достаточно хорошей для использования. В ближайшие пять лет она станет краеугольным камнем более 200 валют и соглашений по всему миру.

Биткойн как государственная система перехода



стехнической точки зрения, книги Биткойна можно рассматривать как систему государственного перехода, которая включает в себя все существующее состояние собственности биткойнов и «функции передачи состояния». Функция перехода состояния принимает текущее сос т о я н и е и транзакцию как входные данные и выводит новое состояние. Например, в стандартной банковской системе статус является балансом. Запрос на перевод X USD из учетной записи A на учетную запись B является транзакцией. Функция передачи состояния вычитает X USD из учетной записи A и увеличивает счет B. X долларов. Если баланс учетной записи A меньше X долларов, функция перехода состояния вернет сообщение об ошибке. Таким образом, мы можем определить функцию перехода состояния следующим образом:：

```
APPLY(S,TX) > S’ or ERROR
```

В упомянутой выше банковской системе функция перехода состояния следующая：

```
APPLY({ Alice: $50, Bob: $50 },”send $20 from Alice to Bob”) = { Alice: $30,Bob: $70 }
```

но：

```
APPLY({ Alice: $50, Bob: $50 },”send $70 from Alice to Bob”) = ERROR
```

«Состояние» системы биткойнов представляет собой коллекцию всех биткойнов (технически известных как «неизрасходованные транзакционные выходы или UTXO»), которые были выкопаны и не были потрачены. Каждый UTXO имеет номинал и владелец (определяется адресом 20-байтового криптографического открытого ключа). Транзакция включает в себя один или несколько входов и один или несколько выходов. Каждый вход содержит ссылку на существующий UTXO и криптографическую подпись, созданные закрытым ключом, соответствующим адресу владельца. Каждый вывод содержит новое UTXO, добавленное к состоянию.

В системе биткойнов функция перехода состояния APPLY (S, TX) - & gt; S 'может быть в общем случае определена следующим образом：

1. Каждый ввод транзакции:

● Если упомянутый UTXO не существует в текущем состоянии (S), возвращается сообщение об ошибке

● Если подпись не соответствует сигнатуре владельца UTXO, возвращается сообщение об ошибке

2. Если все граничные значения фаз UTXO меньше всех фасетов выхода UTXO, возвращается сообщение об ошибке

3. Возвращаясь к новому состоянию S ', все входные UTXO удаляются в новом состоянии S', и все выходные UTXO добавляются.

Первая часть первого шага не позволяет отправителю транзакции тратить несуществующий биткойн, а вторая часть запрещает отправителю транзакции тратить другие биткойны других людей. Второй шаг обеспечивает сохранение значений. Соглашение о платеже Bitcoin заключается в следующем. Предположим, Алиса хочет отправить Боба 11.7 BTC. Фактически, у Алисы не может быть ровно 11,7 БТД. Предположим, что минимальная сумма биткойны, которую она может получить, равна: 6 + 4 + 2 = 12. Таким образом, она может создать транзакцию с тремя входами и двумя выходами. Первый результат имеет номинал 11,7 БТД, владельцем является Боб (адрес Бобкойна Боба), второй выпуск имеет номинал 0,3 БТК, а владельцем является сам Алиса, что является изменением.

Если у нас есть надежная централизованная сервисная организация, система перехода состояния может быть легко реализована, и вышеуказанные функции могут быть просто закодированы точно. Однако мы хотим построить систему биткойнов как децентрализованную валютную систему. Чтобы все соглашались с порядком транзакций, нам необходимо интегрировать государственную систему перехода с системой консенсуса. Децентрализованный консенсусный процесс Bitcoin требует, чтобы узлы в сети постоянно пытались упаковать транзакции в «блоки». Сеть предназначена для генерации блока примерно каждые десять минут. Каждый блок содержит временную метку, случайное число, ссылку на предыдущий блок (т. Е. Хэш) и все транзакции, которые произошли с момента создания предыдущего блока. список. Таким образом, с течением времени создается непрерывно растущая блок-цепочка. Она постоянно обновляется, чтобы представить последнее состояние книги биткойнов.

Согласно этой парадигме алгоритм проверки того, действителен ли блок, выглядит следующим образом:

1. Проверьте, существует ли предыдущий блок, на который ссылается блок, и действителен.

2. Проверьте, является ли метка времени блока более поздней, чем отметка времени предыдущего блока и раньше, чем в ближайшие 2 часа.

3. Проверьте правильность рабочей нагрузки блока.

4. Назначьте конечное состояние предыдущего блока S [0].

5. Предположим, что TX является списком транзакций транзакций, содержащим n транзакций. Для всех i, принадлежащих 0 ... n-1, выполняется переход состояния S [i + 1] = APPLY (S [i], TX [i]). Если какая-либо транзакция i совершает ошибку при переходе состояни я , выйдите из программы и верните ошибку.

6. Возврат верен. Состояние S [n] является конечным состоянием этого блока.

П о сути, каждая транзакция в блоке должна обеспечивать правильный переход состояния. Обратите внимание, что «состояние» не закодировано в блоки. Это абсолютно абстракция, которая запоминается контрольным узлом. Для любого блока вы можете начать с состояния создания и добавлять каждую транзакцию в каждом блоке, чтобы (действительно) вычислить текущее состояние. Кроме того, вам нужно обратить внимание на порядок транзакций в блок. Если в блоке есть две транзакции A и B, B проводит UTXO, созданный A. Если A до B, этот блок действителен, в противном случае этот блок недействителен.

И н т е р е с н о й частью алгоритма проверки блока является концепция «проверки рабочей нагрузки»: SHA256 хэширует каждый блок и обрабатывает полученный хэш как 256-битное значение, которое должно быть меньше заданного динамически скорректированного значения. Во вр е м я написания этой книги целевое число составляет приблизительно 2 ^ 190. Цель доказательства рабочей нагрузки состоит в том, чтобы затруднить создание блока, тем самым предотвращая

злонамеренное восстановление блокады. Поскольку SHA256 является полностью непредсказуемой псевдослучайной функцией, единственный способ создать правильный блок - просто постоянно пытаться и делать ошибки и постоянно увеличивать количество случайных чисел, чтобы увидеть, меньше ли новое значение хэш-функции, чем целевое значение. Если текущее целевое значение равно 2 ^ 192, это означает, что требуется 2 ^ 64 попытки генерировать действительный блок в среднем. В общем, сеть Bitcoin сбрасывает целевое значение каждые 2018 блоков, гарантируя, что средний блок генерируется каждые деся т ь минут.

Д а в а й т е проанализируем, что происходит, когда в сети Bitcoin есть злоумышленник. Поскольку криптографический фундамент Bitcoin очень безопасен, злоумышленники захотят атаковать части, которые не защищены непосредственно криптографией: порядок транзакций. Ст р а т е г и я злоумышленника очень проста:

1. Отправить 100BTC продавцу для покупки товаров (особенно электронных товаров, которые не нужно отправлять по почте).

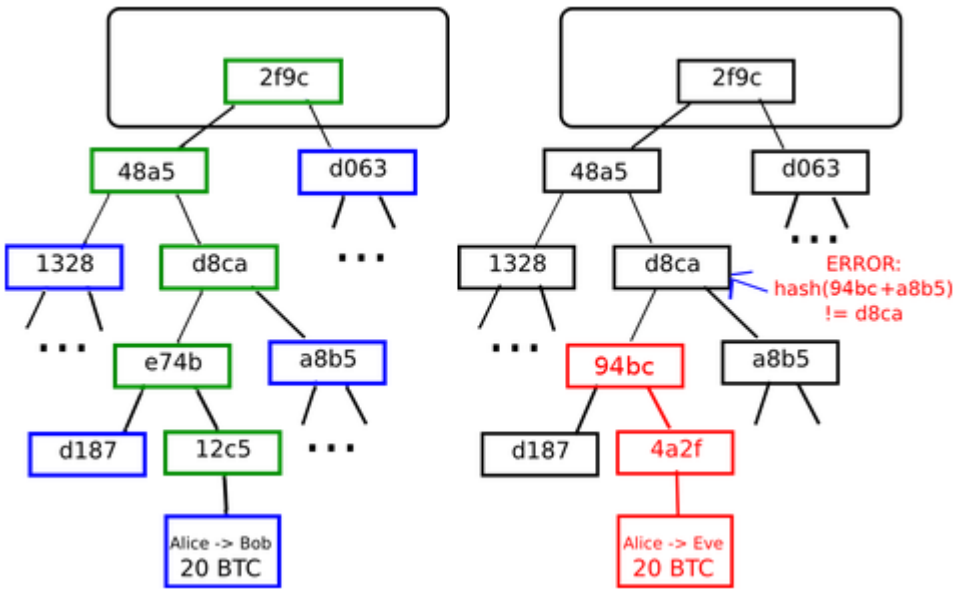
2. Подождите, пока продукт не будет выпущен.

3. Создайте еще одну транзакцию и отправьте тот же 100BTC в свою учетную запись.

4. Сделайте так, чтобы сеть Bitcoin считала, что транзакция, отправленная в вашу учетную запись, является первой, которая будет отправлена.

К а к только шаг (1) произойдет, транзакция будет упакована в блоки в течение нескольких минут, предполагая 270000-й блок. Примерно через час на этом блоке будет пять блоков, каждый из которых косвенно указывает на транзакцию для подтверждения транзакции. В э т о время продавец получил платеж и отправил его покупателю. Поскольку мы предполагаем, что это цифровой продукт, злоумышленник может немедленно получить товар. Теперь злоумышленник создает другую транзакцию и отправляет тот же 100BTC в свою учетную запись. Если злоумышленник передает это сообщение только всей сети, эта транзакция не будет обрабатываться. Будет запущена функция перехода состояния APPLY (S, TX), и будет обнаружено, что эта транзакция будет принимать UTXO, который больше не находится в состоян и и . Таким образом, злоумышленник расходится с блочной цепью и восстанавливает 270000-й блок из 269999-го блока в качестве родительского блока, где новая транзакция заменяет старую транзакцию. Поскольку данные блоков разные, для этого требуется подтверждени е рабочей нагрузки. Кроме того, поскольку новый 270000-й блок, созданный злоумышленником, имеет другой хеш, исходные блоки 270001 до 270005 не указывают на него, поэтому исходный блок-цепочка и новый блок злоумышленника полностью изолированы. В случае с бл о ч н о й цепью длинная ветвь блокады считается честной блокчейной. Легитимные будут находиться вдоль исходного блока 270005. Только атакующий будет в новом 270000-м блоке. , Для того, чтобы атакующий максимизировал свою блокировку, он должен обладать большей маневренностью, чем вся сеть, кроме него (т.е. 51% атаки).

Д е р е в о Меркель



С л е в а : только предоставление небольшого количества узлов на дереве Merkle достаточно, чтобы дать юридическое доказательство ветви.

П р а в и л ь н о : любая попытка изменить любую часть дерева Меркель в конечном итоге приведет к несогласованности где-то в цепочке.

Одной из важных возможностей масштабирования системы Bitcoin является то, что ее блоки хранятся в многоуровневых структурах данных. Хэш блока - это просто хэш заголовка блока. Заголовок блока - это длина корневого хеша дерева Merkel, содержащего временную метку, случайное число, последний хэш блока и все транзакции блоков. Около 200 байт данных.

Дерево Меркель - это двоичное дерево, состоящее из набора листовых узлов, набора промежуточных узлов и корневого узла. Наименьшее количество листовых узлов содержит базовые данные. Каждый промежуточный узел представляет собой хэш двух его дочерних узлов. Корневой узел также является хешем из двух его дочерних узлов и представляет вершину дерева Меркель. Цель дерева Merkel - разрешить разброс фрагментов данных: узлы могут загружать заголовки блоков из одного источника, загружать другие части связанного с ними дерева из другого источника и все еще иметь возможность подтвердить, что все данные верны , Это происходит из-за хэш-диффузии: если злоумышленник пытается добавить поддельную транзакцию в нижнюю часть дерева, результирующие изменения приведут к изменениям в верхних узлах дерева и изменениям на узлах более высокого уровня, что в конечном итоге приведет к корневому узлу. Изменения и изменения в хеш-блоке, поэтому соглашение будет записывать его как совершенно другой блок (почти наверняка с неправильным подтверждением рабочей нагрузки).

Соглашение Меркель имеет решающее значение для долгосрочной устойчивости Биткойна. В апреле 2014 года полный узел в сети Bitcoin - узел, который хранит и обрабатывает все данные для всех блоков - потребовал 15 ГБ памяти и вырос со скоростью более 1 ГБ в месяц . В настоящее время это место для хранения приемлемо для настольных компьютеров, но мобильные телефоны не смогли загрузить такие огромные данные. Только коммерческие организации и энтузиасты будут выступать в качестве полноценных узлов в будущем. Протокол упрощенного платежа (SPV) позволяет создать другой тип узла. Такой узел называется «легким узлом». Он загружает заголовок блока, использует заголовок блока, чтобы подтвердить подтверждение рабочей нагрузки, а затем загружает только ветвь Merkel tree, связанную с ее транзакцией. ". Это позволяет лёгкому узлу безопасно определять статус любой транзакции биткойнов и текущий баланс учетной записи, просто загружая небольшую часть всей цепочки.

Другие блокирующие приложения

Идея применения идеи blockchain к другим областям давно появилась. В 2005 году Ник Сабо выдвинул концепцию «права собственности на собственность». В этой статье описывается, как развитие технологии репликации баз данных может создавать системы на основе блокнозов, которые могут применяться для регистрации права собственности на землю. Создание включает, например, права собственности и незаконное вторжение. Подробные рамки для таких концепций, как Грузия и земельный налог. Однако, к сожалению, в то время не существовало практической системы баз данных копирования, поэтому этот протокол не был реализован на практике. Однако после успешного децентрализованного консенсусного развития системы биткойнов в 2009 году многие другие применения блокады стали появляться быстро.

● namecoin - Создана в 2010 году, известная как децентрализованная база данных регистрации имен. Децентрализованные протоколы, такие как Tor, Bitcoin и BitMessage, требуют определенного подтверждения, чтобы другие пользователи могли взаимодействовать с пользователями. Однако единственным доступным идентификатором во всех существующих решениях является псевдослучайный хеш, такой как 1LW79wp5ZBqaHW1jL5TciBCrhQYtHagUWy. В идеале люди хотят иметь учетную запись с именем «george». Однако проблема заключается в том, что если кто-то может создать учетную запись «george», другие люди также могут создать учетную запись «george», чтобы притворяться. Единственное решение - это первый файл. Только первый регистратор может успешно зарегистрироваться, а второй не может зарегистрировать одну и ту же учетную запись. Эта проблема может использовать согласованный протокол Биткойна. Валюта доменного имени является самой ранней и наиболее успешной системой для внедрения системы регистрации имен с использованием блок-цепи.

● Цветные монеты. Цель цветных монет - предоставить людям возможность создавать свою цифровую валюту в блочной цепочке биткойнов или, что более важно, валютном цифровом токене. В соответствии с соглашением о цветовой валюте люди могут выпускать новые валюты, назначая цвета конкретному биткойнному UTXO. Этот протокол рекурсивно определяет другие UTXO как тот же цвет, что и вход транзакции UTXO. Это позволяет пользователю сохранять UTXO, которые содержат только определенный цвет. Отправка этих UTXO - это отправка обычных биткойнов и оценка полученных цветов UTXO путем отслеживания всей цепочки блоков.

● Metacoins. Идея Metacoins заключается в создании нового протокола в блочной цепочке биткойнов с использованием транзакций биткойна для сохранения валютных транзакций, но с использованием другой функции передачи состояния APPLY. Поскольку протокол обмена валюты не может блокировать недействительные валютные транзакции в блочной цепочке биткойнов, добавив правило, что если APPLY '(S, TX) вернет ошибку, этот протокол по умолчанию будет использовать APPLY' (S, TX) = S. Это обеспечивает простое решение для создания произвольных расширенных криптографических валютных протоколов, которые не могут быть реализованы в системе биткойнов, а стоимость разработки очень низкая, поскольку проблемы в сети уже обрабатываются протоколами биткойнов.

Поэтому в целом существует два способа установления консенсусного протокола: создание отдельной сети и установление соглашения о сети Bitcoin. Хотя такие приложения, как монеты с доменными именами, преуспели с использованием первого метода, реализация этого метода очень сложна, поскольку каждому приложению необходимо создать отдельный блок-цепочку и установить и протестировать все переходы состояний и сетевые коды. Кроме того, мы прогнозируем, что применение децентрализованных консенсусных технологий будет подчиняться распределению полномочий по закону. Большинство приложений слишком малы, чтобы гарантировать безопасность свободных блок-цепочек. Мы также заметили большое количество децентрализованных приложений, особенно децентрализации. Автономным организациям необходимо взаимодействовать с приложениями.

С другой стороны, есть недостатки подхода на основе биткойнов, который не наследует характеристики биткойна, которые могут быть использованы для упрощения подтверждения платежа (SPV). Биткойн может упростить подтверждение оплаты, поскольку биткойн может использовать глубину блок-цепи в качестве агента проверки. В какой-то момент, когда предки транзакции сейчас достаточно далеко, их можно считать частью правового государства. Напротив, протокол обмена валюты, основанный на блочной цепочке биткойнов, не может заставить блок-цепь исключать транзакции, которые не соответствуют протоколу обмена валюты. Поэтому упрощенное подтверждение платежа в безопасном валютном протоколе требует обратного сканирования всех блоков до тех пор, пока исходная точка блоксхемы не подтвердит, действительна ли определенная транзакция. В настоящее время все «легкие» реализации соглашений на основе долларовой валюты на основе биткойнов полагаются на доверенные серверы для предоставления данных. Это лишь довольно субоптимальный результат для криптографических валют, которые устраняют необходимость доверия.

скрипт

Даже если биткойн-протокол не расширен, он может в некоторой степени достичь «умных контрактов». Биткойновский UTXO может принадлежать более чем одному публичному ключу или может принадлежать более сложным сценариям, написанным на языке программирования на основе стека. В этом режиме расходы на такой UTXO должны предоставлять данные, которые удовлетворяют сценарию. Фактически, основной механизм владения открытым ключом также реализуется сценарием: сценарий берет подпись эллиптической кривой как входную, проверяет транзакцию и владеет адресом этого UTXO и возвращает 1, если проверка прошла успешно, иначе она возвращает 0. Более сложные сценарии используются для других сценариев приложений. Например, можно создать скрипт (multi-signature), для которого требуется сбор двух из трех закрытых ключей для подтверждения транзакций. Этот сценарий полезен для корпоративных счетов, сберегательных счетов и некоторых коммерческих агентов. Сценарии также могут использоваться для отправки вознаграждений пользователям, которые решают вычислительные проблемы. Люди могут даже создать такой скрипт: «Если вы можете предоставить доказательство того, что вы отправили мне определенную сумму денег для упрощенного подтверждения платежа, этот биткойн UTXO принадлежит вам», в сущности, система Bitcoin позволяет использовать разные пароли Изучайте децентрализованный обмен валюты.

Тем не менее, язык сценариев биткойн имеет некоторые серьезные ограничения:

• Отсутствие полноты Turing - это означает, что, хотя язык сценариев биткойнов может поддерживать несколько вычислений, он не может поддерживать все вычисления. Основным недостатком является утверждение цикла. Цель не поддерживать инструкции цикла заключается в том, чтобы избежать бесконечных циклов в подтверждении транзакции. Теоретически это препятствие, которое можно преодолеть для программистов сценариев, поскольку любой цикл можно моделировать с помощью нескольких итераций оператора if, но это может привести к неэффективности использования пространства сценариев, например, реализации Альтернативный алгоритм подписи эллиптической кривой, вероятно, потребует 256 повторений умножения, каждый раз, когда требуется отдельное кодирование.

● Ценностно-слепота. Сценарий UTXO не обеспечивает мелкомасштабный контроль за объемом вывода учетной записи. Например, мощное приложение контракта оракула является контрактом хеджирования. Каждый из битконов A и B отправляет биткойны стоимостью 1000 долларов на контракт хеджирования. Через 30 дней скрипт отправляет биткойну стоимостью 1000 долларов США на A до Б. Отправляйте оставшиеся биткойны. Хотя для достижения контракта хеджирования требуется оракул, чтобы определить, какое значение биткойна для доллара, этот механизм достиг значительного прогресса в сокращении доверия и инфраструктуры по сравнению с сегодняшним полностью централизованным решением. Однако, поскольку UTXO является неделимым, единственный способ достичь этого контракта - использовать очень много UTXO с разными наименованиями (например, для каждого k с максимумом 30, существует UTXO 2k) и очень неэффективно. Сделайте оракул предсказывать правильный UTXO для отправки в A и B.

• Отсутствие состояния - UTXO может быть потрачен или не потрачен, что не оставляет места для многофазных контрактов или сценариев, требующих любого другого внутреннего состояния. Это затрудняет реализацию многоступенчатых опционных контрактов, децентрализованных предложений обмена или двухэтапных соглашений о криптографических обязательствах, которые необходимы для обеспечения того, чтобы вознаграждения были рассчитаны. Это также означает, что UTXO может использоваться только для установления простых одноразовых контрактов, а не для таких контрактов с более сложными состояниями, таких как децентрализованные организации, что затрудняет достижение метапротоколов. Двоичный статус в сочетании со значением слепых означает, что другого важного приложения - лимита снятия невозможно достичь.

Blockchain-blindness - UTXO не видит данные блок-цепи, такие как случайные числа и хэш предыдущего блока. Этот дефект лишает язык сценариев потенциального значения на основе случайности, что серьезно ограничивает применение в других областях, таких как игры.

Мы рассмотрели три метода построения расширенных приложений для криптовалюты: построение нового блочного ключа, использование скриптов в блочной цепочке биткойнов и установление протокола мета-монеты в блочной цепочке биткойнов. Метод создания новой блокчейки может свободно реализовывать произвольные функции, затраты времени на разработку и стимулировать усилия. Метод использования скриптов очень прост в реализации и стандартизации, но его возможности ограничены. Хотя протокол обмена валюты очень прост в реализации, он имеет недостаток в слабой масштабируемости. В системе монет Y2 наша цель - создать общую структуру, которая может иметь все преимущества этих трех режимов одновременно.

В а л ю т а Y2

В а л ю т а Y2 основана на цифровой валюте Ближневосточной Арабской Лиги, которая изменяет распределение возобновляемых ресурсов нефти. Y2 - цифровая валюта, выпущенная Лабораторией Новой Энергии Y2. Y2 выпускается для ускорения разработки новой топливной добавк и Y2. Ожидается, что новая топливная присадка Y2 будет доступна впервые в 2020 году и увеличит существующий Y2 примерно на 20 раз к 2035 году. Достичь более 170 раз: 1 монета равна 1 бутылке Y2, сохранить мир, защитить глобальные возобновляемые ресурсы (ОО Н назвала план спасения ресурсов, Y2 и Соединенные Штаты стали инициатором плана спасения). Технические аспекты имеют завершенность Тьюринга, осознание ценности (Значимость, осведомленность о блочных цепочках и добавленная многопользовательская мощь намно г о сильнее, чем умные контракты, которые могут предоставить биткойн-скрипты.

У ч е т н а я запись Y2

В системе монет Y2 состояние состоит из объектов, называемых «учетными записями» (каждая учетная запись - 20-байтовый адрес) и состояния передачи значения и информации между двумя учетными записями. Счет монеты Y2 содержит четыре части:

• Случайный номер, используемый для определения счетчика, который может обрабатываться только один раз за транзакцию

• Текущий баланс Y2 на счете

• Код договора учетной записи, если таковой имеется

• Хранение учетных записей (по умолчанию пуст)

В а л ю т а Y2 является основным зашифрованным топливом внутри Новой Энергии Y2 и используется для покрытия транзакционных издержек. В общем, монеты Y2 имеют два типа учетных записей: все внешние счета (контролируемые частными ключами) и договорные счета (контро л и р у е м ы е кодами договоров). У всех внешних учетных записей нет кода, и люди могут отправлять сообщения из внешней учетной записи, создавая и подписывая транзакцию. Каждый раз, когда учетная запись контракта получает сообщение, активируется код внутри догов о р а , позволяя ему читать и записывать внутренние хранилища, а также отправлять другие сообщения или создавать контракты.

Н о в о с т и и транзакции

Y2 новости монеты несколько похожи на биткойн торговли, но есть три важных различия между ними.

В о -первых, сообщения монеты Y2 могут создаваться внешними объектами или контрактами, тогда как биткойн-транзакции могут создаваться только извне.

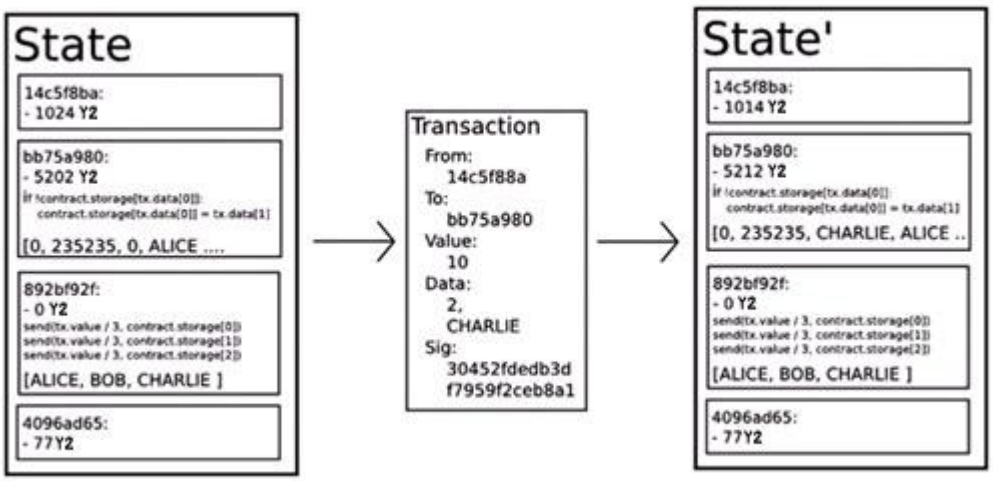
В о -вторых, сообщения монеты Y2 могут необязательно содержать данные.

В -третьих, если получатель сообщения монеты Y2 является учетной записью контракта, вы можете выбрать ответ, а это значит, что сообщение монеты Y2 также содержит концепцию функции.

«Т р а н з а к ц и я » в валюте Y2 относится к сигнатурному пакету данных, в котором хранится сообщение, отправленное из внешней учетной записи. В транзакции есть получатель сообщения, подпись, используемая для подтверждения отправителя, баланс кредитного счета Y2, д а н н ы е для отправки и два значения, известные как STARTGAS и GASPRICE. Чтобы предотвратить экспоненциальные взрывы и бесконечные циклы кода, каждая транзакция требует ограничений на вычислительные этапы, которые возникают в результате выполнения кода, включ а я начальное сообщение и все сообщения, которые являются результатом выполнения. STARTGAS - это предел, GASPRICE - это стоимость каждого шага расчета. Если во время исполнения транзакции «топливо израсходовано», все изменения статуса восстанавливаются до и х первоначального состояния, но уже оплаченные сборы за транзакции не подлежат возмещению. Если топливо по-прежнему остается, когда исполнение транзакции приостановлено, топливо будет возвращено отправителю. Контракт создания имеет отдельный тип транзакци и и соответствующий тип сообщения, адрес контракта рассчитывается на основе случайного числа учетной записи и хэша данных транзакции.

В а ж н ы м следствием механизма обмена сообщениями является то, что свойство «первичного гражданина» валюты Y2 - договор имеет те же права, что и внешний счет, включая право отправлять сообщения и создавать другие контракты. Это позволяет контракту одновременно обслуживать несколько разных ролей. Например, пользователь может сделать член децентрализованной организации (контракт) стать посреднической учетной записью (другим договором), индивидуальной квантовой сертификацией для параноидального использования синего Лицо с подписью Портера (третий контракт) и самоподписанным лицом, использующим учетную запись, обеспеченную пятью секретными ключами (четвертый контракт), предоставляет посреднические услуги. Сила платформы монеты Y2 заключается в том, что децентрализованные организационные и агентские контракты не должны заботиться о том, какой тип счета приходится на каждого участника контракта.

Функция передачи состояния валюты Y2



Функция передачи состояния валюты Y2：`APPLY(S,TX) -> S'`，Можно определить как：

1. Убедитесь, что формат транзакции правильный (то есть, имеет правильное значение), что подпись действительна и что случайное число соответствует случайному числу учетной записи отправителя. Если нет, возвращается ошибка.

2. Рассчитайте комиссию за транзакцию: fee = STARTGAS * GASPRICE и определите адрес отправителя из подписи. Вычтите плату за транзакцию со счета отправителя и увеличьте случайное число отправителя. Если баланс аккаунта недостаточен, возвращается ошибка.

3. Установите начальное значение GAS = STARTGAS и вычтите определенное количество топлива из числа байтов в транзакции.

4. Перенести значение из учетной записи отправителя на счет получателя. Если учетная запись получателя еще не создана, создайте эту учетную запись. Если принимающая учетная запись является договором, введите код контракта до тех пор, пока код не закончится или топливо не закончится.

5. Если на счету отправителя недостаточно денег или на исполнение кода заканчивается топливо, передача стоимости не выполняется, а исходный статус восстанавливается, но комиссия за транзакцию также должна быть уплачена, а комиссия за транзакцию добавляется к счету.

6. В противном случае вернуть все оставшееся топливо отправителю, а отработанное топливо отправляется в распределительный центр в качестве комиссии за транзакцию.

Исполнение кода

Код контракта на монету Y2 написан на низкоуровневом языке байт-кода на основе стека. Код состоит из серии байтов, каждый байт представляет операцию. В общем случае выполнение кода представляет собой бесконечный цикл. Счетчик программ увеличивается на единицу (начальное значение равно нулю) и выполняется один раз, пока выполнение кода не будет завершено, или не будет обнаружена ошибка, команда STOP или RETURN. Операция может получить доступ к трем типам пространства для хранения данных:

Стек, последний в первом хранилище данных, 32-байтовые значения могут быть перенесены в стек.

● Память, бесконечно расширяемая очередь байтов.

● Долгосрочное хранение контракта, хранение секретного ключа / значения, когда секретный ключ и значение имеют размер 32 байта. В отличие от стека и памяти, которые сброшены в конце вычисления, содержимое хранилища будет поддерживаться в течение длительного периода времени.

Код может получить доступ к значению, отправителю и данным в полученном сообщении так же, как и к данным заголовка блока. Код также может возвращать очередь байтов данных в качестве вывода.

Формальное исполнение модели PCM-кода удивительно просто. Когда виртуальная машина монеты Y2 запущена, ее полное состояние вычисления может быть определено кортежем (block_state, transaction, message, code, memory, stack, pc, gas), где block_state является глобальным состоянием, содержащим все остатки на счете и хранение. , Каждый раунд выполнения, вызывая первый байт кода (программный счетчик) кода, найдена текущая инструкция, и каждая команда определяет, как она влияет на сам кортеж. Например, ADD выталкивает два элемента и подталкивает их сумму в стек, уменьшает расход газа (топливо) и добавляет один к ПК, SSTORE выталкивает верхние два элемента и вставляет второй элемент в первый Каждый элемент определяет место хранения контракта, что также уменьшает значение газа до 200 и увеличивает pc на единицу. Хотя существует много способов оптимизации монет Y2 с помощью компиляции «точно в момент времени», базовая реализация монет Y2 может быть реализована в сотнях строк кода.

приложение

В общем, есть два приложения выше Y2. Первая категория - это применение новой энергии Y2, которая обеспечивает поддержку возобновляемых источников энергии для всех стран, учреждений и частных лиц, которым нужна сырая нефть, которая может использоваться для продаж, инвестиций и других связанных приложений. Второй тип - это финансовые приложения, а Y2 можно преобразовать из ресурсов в финансы. Будущее, несомненно, станет финансово-энергетическим комплексом, который будут приветствоваться мировыми финансовыми профессионалами.

Система токенов

Система токенов в цепочке имеет множество приложений: от субвалютных средств, представляющих активы, такие как доллары или золото, к акциям компании, индивидуальные жетоны, представляющие интеллектуальные активы, защищенные непогашенные купоны и даже отсутствие связи с традиционными ценностями. Система токенов для очков вознаграждения. Внедрение системы токенов в монетах Y2 удивительно просто. Ключевым моментом является понимание того, что все системы валют или токенов в основном представляют собой базу данных со следующими операциями: вычесть X единиц из A и добавить X единиц в B, при условии, что (1) A Перед транзакцией имеется не менее X единиц, и (2) сделка одобрена A. Реализация символической системы заключается в реализации такой логики в контракте.

Основной код для реализации системы токенов с языком Змея выглядит следующим образом：

```
from = msg.sender

to = msg.data[0]

value = msg.data[1]

if contract.storage[from] >= value:

contract.storage[from] = contract.storage[from] value
```

```
contract.storage[to] = contract.storage[to] + value
```

Это, по сути, минимальная реализация функции перехода состояния банковской системы, которая будет описана далее в этой статье. Необходимо добавить дополнительный код, чтобы обеспечить возможность распределения валюты в начальной и другой предельных ситуациях, в идеале добавляя функцию, позволяющую другим контрактам искать баланс адреса. Этого достаточно. Теоретически, система токенов, которая действует как дочерняя валюта, основанная на монете Y2, может включать важную функцию, которая отсутствует в цепочной валюте на основе биткойна: возможность напрямую использовать эту валюту для оплаты транзакционных сборов.

Финансовые деривативы и валюта со стабильной стоимостью

Финансовые производные являются наиболее распространенным применением «умных контрактов» и одним из самых простых в реализации с кодом. Основная проблема при достижении финансовых контрактов заключается в том, что большинство из них должны обращаться к внешнему эмитенту цен, например, очень требовательная заявка - это умный контракт на хеджирование Y2 (или другой криптовалюты) по отношению к долларовым ценам. Однако контракт должен знать цену Y2 против доллара США. Самый простой способ - заключить договор о предоставлении данных, который поддерживается конкретной организацией (например, Nasdaq), которая призвана дать агентству возможность обновить контракт по мере необходимости и предоставить интерфейс, который позволяет другим контрактам отправлять контракт через Сообщение о контракте, чтобы получить ответ, содержащий информацию о ценах.

Когда эти ключевые элементы все на месте, контракт на хеджирование выглядит следующим образом:

П о д о ж д и т е , пока A войдет в 1000 Y2 валюты. ,

П о д о ж д и т е B, чтобы ввести 1000 Y2 валюты.

П р и запросе контракта на предоставление данных в память записывается значение доллара 1000 монет Y2, например x долларов.

Ч е р е з 30 дней A или B разрешено «реактивировать» контракт на отправку монет Y2 стоимостью $ x (запрашивать данные для предоставления контракта по новой цене и рассчитать) до A и отправить оставшиеся монеты Y2 в B.

Т а к и е контракты имеют исключительный потенциал в криптографическом бизнесе. Одной из проблем с криптовалютой, которую часто критикуют, является ее волатильность цен, хотя большому числу пользователей и предприятий может потребоваться безопасность и удобство криптографических активов, они менее склонны к 23% -ному снижению активов за один день. Ситуация с ценностью. До сих пор наиболее распространенным рекомендуемым решением было одобрение издателем активов.

Н а практике, однако, эмитент не всегда заслуживает доверия, и в некоторых случаях банковская система слишком хрупка или недостаточно честна, чтобы сделать такие услуги невозможными. Альтернативные решения представляют собой производные финансовые инструмент ы . Больше не будет отдельного эмитента, который предоставляет резервы для поддержки актива. Вместо этого это децентрализованный рынок, состоящий из спекулянтов, которые готовы повысить цену криптографического актива. В отличие от эмитентов, спекулянты не и м е ю т права торговаться, потому что контракты хеджирования замораживают свои резервы в контрактах. Обратите внимание, что этот подход не полностью децентрализован, потому что по-прежнему существует потребность в надежном источнике данных, который предоставл я е т информацию о ценах, хотя по-прежнему вызывает сомнения, что он все еще снижает требования к

инфраструктуре (в отличие от издателей, издателю цены не требуется Лицензирование и, по-видимому, классифицируется как свободная речь) и огромный шаг вперед в с н и ж е н и и потенциальных рисков мошенничества.

С и с т е м а идентификации и репутации

С а м а я ранняя альтернативная валюта, монета доменных имен, пыталась использовать биткойн-подобную блок-цепочку для предоставления системы регистрации имен, где пользователи могли бы регистрировать свои имена с другими данными в публичной базе данных. Наиболе е распространенным вариантом использования является система доменных имен, которая имеет доменное имя типа bitcoin.org (или «bitcoin.bit» в валюте имени домена) и IP-адрес. Другие примеры приложений включают системы проверки электронной почты и потенциальн о более совершенные системы репутации. Вот основной контракт на предоставление системы регистрации имен, аналогичной валюте домена, в валюте Y2：

```
if !contract.storage[tx.data[0]]:

contract.storage[tx.data[0]] = tx.data[1]
```

К о н т р а к т очень прост, он представляет собой базу данных в сети монет Y2, которая может быть добавлена, но не может быть изменена или удалена. Любой может зарегистрировать имя в качестве значения и никогда не изменяться. Более сложный контракт на регистрацию имен будет содержать «функциональное предложение», которое позволяет запрашивать другие контракты, а также механизм для того, чтобы иметь имя «владелец» (т. Е. Первый владелец регистрации) изменить данные или передать право собственности. Вы даже можете д о б а в и т ь репутацию и доверять сетевым функциям.

Д е ц е н т р а л и з о в а н н о е хранилище

В последние несколько лет были запущены некоторые популярные онлайн-хранилища файлов, в частности Dropbox, которые позволяли пользователям загружать свои резервные копии на жестком диске, предоставлять службы резервного копирования и разрешать пользователям получать ежемесячные абонентские сборы. Однако на данный момент рынок хранения файлов иногда относительно неэффективен, а поверхностное наблюдение за существующими службами показывает, что, в частности, на уровне Мистической долины 20-200 ГБ, которая не и м е е т ни свободного места, ни скидок на уровне предприятия. Ежемесячная стоимость хранения файлов означает стоимость оплаты всего жесткого диска за один месяц. Законопроект Y2 позволяет создать децентрализованную экосистему хранения, чтобы пользователи могл и арендовать свои собственные жесткие диски или неиспользуемое сетевое пространство, чтобы получить небольшой доход, тем самым уменьшив стоимость хранения файлов.

О с н о в н ы м компонентом такого объекта является то, что мы называем «децентрализованным контрактом Dropbox». Контракт работает следующим образом. Во-первых, кто-то делит данные, которые необходимо загрузить в куски, шифрует каждую часть данных для защиты конфи д е н ц и а л ь н о с т и и создает дерево Merkel. Затем создайте контракт со следующими правилами. Для каждого N блоков контракт будет извлекать случайный индекс из дерева Merkel (используя хэш предыдущего блока, к которому можно получить код контракта, чтобы обеспеч и т ь случайность), а затем дать первый Сущности X Y2 монеты для подтверждения доказательства права собственности на блок с аналогичной упрощенной верификацией (SPV) с определенным индексом в дереве. Когда пользователь хочет снова загрузить свой файл, он мо ж е т использовать протокол канала микроплатежей (например, заплатить 1 Saab за 32 кбайт), чтобы восстановить файл, наиболее рентабельным методом является оплата лица, который не публикует последнюю транзакцию, но Заменить исходную транзакцию после каждых 32k байт с помощью немного более рентабельной транзакции с тем же случайным числом.

В а ж н о й особенностью этого соглашения является то, что, хотя кажется, что один человек доверяет многим случайным узлам, которые не готовы потерять файлы, он может тайно делить файлы на множество небольших блоков, а затем через контракт на мониторинг, что каж д ы й маленький блок все еще возвращается. Сохраняется узлом. Если контракт все еще выплачивается, он дает доказательства того, что кто-то все еще сохраняет документ.

Д е ц е н т р а л и з о в а н н а я автономная организация (DAO)

В обычном смысле концепция децентрализованной автономной организации (DAO) относится к виртуальному объекту с определенным количеством членов или акционеров, полагаясь, например, на 67% голосов, чтобы решить потратить деньги и изменить код. Члены будут вместе решать, как организация выделяет средства. Метод распределения средств может быть вознаграждением, заработной платой или более привлекательными механизмами, такими как вознаграждение за работу с внутренней валютой. Это просто использует криптографическую технологическую цепочку для фундаментальной репликации юридической значимости традиционных компаний или некоммерческих организаций для обеспечения соблюдения. До сих пор во многих дискуссиях вокруг DAO была сосредоточена «капиталистическая» модель «децентрализованной автономной корпорации» с акционерами, разделяющими дивиденды, и торгуемыми акциями, а в качестве альтернативы описывается Организация «децентрализованное автономное сообщество» позволит всем членам иметь равные права при принятии решений и требует согласия 67% голосов при добавлении или вычитании членов. У каждого может быть только одно членство. Это правило должно выполняться группой.

Вот краткое описание того, как реализовать DO с использованием кода. Самый простой дизайн - это код, который может самостоятельно модифицировать, если две трети участников согласуются. Хотя код теоретически неизменен, код можно легко изменить, разместив скелет кода в отдельном контракте и указывая адрес вызова контракта на сменное хранилище. Существует три типа транзакций в простой реализации такого контракта DAO, отличающийся данными, предоставленными транзакцией:

● [0, i, K, V] Индекс регистрации - это рекомендация iизменить содержимое индекса адреса хранилища K на v.

● [0, i] регистрирует голосование за предложение i.

● [2, i] Подтвердите рекомендацию i, если голосов достаточно.

Тогда у контракта есть определенные условия для каждого элемента. Он будет вести учет всех открытых изменений в хранилище и таблицу проголосовавших. Существует также таблица всех участников. Когда согласие большинства в две трети получается для любого изменения хранимого контента, окончательная транзакция будет выполнять это изменение. Более сложная структура добавит встроенные функции голосования для отправки транзакций, увеличения или уменьшения членов или даже предоставления таких представителей для голосования, как назначенная демократия (то есть любой может поручить другому лицу голосовать от своего имени, а такая делегация Отношения могут быть переданы, поэтому, если A-делегаты B, то B делегаты C, тогда C решит голосование A). Этот проект позволит DAO органично развиваться как децентрализованное сообщество, чтобы люди могли в конечном итоге передать задачу выбора подходящих кандидатов для экспертов, в отличие от нынешней системы. Поскольку члены сообщества постоянно меняют свое командное время, эксперты легко появятся. И исчезнуть.

Альтернативной моделью является децентрализация компании, когда у любой учетной записи может быть от 0 до более акций, и для принятия решения требуется согласие большинства в две трети акций. Полная структура будет включать функцию управления активами - возможность подавать заказы на покупку и продажу акций и возможность принимать такие заказы (при наличии в контракте механизма соответствия заказов). Делегаты по-прежнему существуют в форме назначения демократии, что приводит к концепции «совета».

В будущем могут быть реализованы более продвинутые механизмы организационного управления, и теперь децентрализованная организация (DO) может начать работу с децентрализованных автономных организаций (DAO). Разница между DO и DAO неоднозначна. Общая разделит е л ь н а я линия заключается в том, может ли управление быть достигнуто посредством политически-подобного процесса или «автоматизированного» процесса. Хорошим интуитивным тестом является стандарт «без универсального языка»: если два члена не являются Работает ли одна и та же языковая организация? Очевидно, что простая традиционная фондовая холдинговая компания потерпит неудачу, и соглашение о биткойне, подобное этому, скорее всего, будет успешным. «Футархия» Робин Хансена, «механизм организации управления путем прогнозирования рынка, является реальной. Хороший пример того, как может выглядеть «автономное» управление. Обратите внимание, что не нужно предполагать, что все DAO превосходят все ДО, автономия - это всего лишь парадигма, которая имеет большие преимуще с т в а в некоторых конкретных сценариях, но может оказаться невозможной в других местах. Возможно, существует много полулегалов.

Д а л ь н е й ш е е применение

1. Сохранение кошелька. Предположим, Алиса хочет убедиться, что ее деньги в безопасности, но она боится потерять или взломать, чтобы украсть ее секретный ключ. Она ставит монеты Y2 в контракте с Бобом. Как показано ниже, контракт является банком:

А л и с а может снимать до 1% средств каждый день.

Б о б может снимать до 1% средств каждый день, но Алиса может использовать свой секретный ключ для создания транзакции, которая отменяет права выхода Боба.

А л и с а и Боб могут снимать деньги произвольно.

В общем, для Алисы достаточно 1% в день. Если Алиса хочет снять больше, она может обратиться за помощью к Бобу. Если секретный ключ Алисы украден, она может немедленно найти Боба для перевода своих средств на новый контракт. Если она потеряет свой секретный ключ,

Боб может медленно поднять деньги. Если Боб проявляет злобу, она может отключить свои права на выход.

2. Страхование сельскохозяйственных культур. Человек может легко создать финансовый производный контракт, используя погодные условия, а не любой индекс цен в качестве ввода данных. Если фермер Айовы покупает финансовый производный инструмент, который отменя е т платежи, основанные на осадках в Айове, то, если произойдет засуха, фермер автоматически получит платеж, и если будет достаточное количество осадков, он будет Очень рад, потому что его урожай будет очень хорошим.

Д е ц е н т р а л и з о в а н н ы й издатель данных. Для финансовых контрактов, основанных на различиях, фактически можно децентрализовать издателя данных, передав «Cherindian» соглашение. Принцип работы Xie Lindian следующий: N-party предоставляет входные значения для сист е м ы для заданных данных (например, цена Y2 / USD), все значения сортируются, и каждый узел, который обеспечивает значение от 25% до 75%, будет иметь Чтобы получить вознаграждение, у каждого есть стимул для предоставления ответов, которые другие предоставят . Ответ, который большое количество игроков может на самом деле договориться, по-видимому, является правильным ответом по умолчанию. Это создает теоретически доступное количество значений, включая цену Y2 / USD, температуру в Берлине. Даже децентрализован н ы й протокол с результатами особо сложного расчета.

4. Многозадачные интеллектуальные контракты. Биткойн позволяет заключать торговые контракты на основе множества подписей. Например, для сбора средств можно использовать 5 частных ключей. Например, 5 частных ключей могут быть использованы для сбора 4 общих ф о н д о в . Если только 3 счета тратят 10% средств каждый день, только 2 могут тратить только 0,5% средств каждый день. , Кроме того, многозначная подпись в монете Y2 является асинхронной, что означает, что обе стороны могут регистрировать подпись на блок-цепоч к е в разное

время, а последняя подпись автоматически отправляется после того, как подпись на месте.

5. Облачные вычисления. Технология PCM также может использоваться для создания проверяемой вычислительной среды, которая позволяет пользователям предлагать другим выполнять вычисления, а затем выборочно запрашивать доказательства, которые правильно вычисляю т с я на случайно выбранном контрольном пункте. Это позволяет создавать рынок облачных вычислений, где любой пользователь может участвовать со своими рабочими столами, ноутбуками или выделенными серверами. Проверки на месте и депозиты безопасности могут быть использованы для обеспечения надежности системы (т. Е. Ни один узел не может быть обманут Lee). Хотя такая система может не подходить для всех задач, например, задачи, требующие расширенной межпроцессной связи, нелегко выполнять в облаке большого узла. Те м не менее, некоторые другие задачи облегчают реализацию параллелизма: на таких платформах очень легко реализовать SETI @ home, folding @ home и алгоритмы генов.

6. Игра «точка-точка». Любое количество соглашений о равноправных азартных играх может быть перенесено на блоки Y2-монеты, такие как Frank Stajano и Cyberdice Ричарда Клейтона. Простейшим азартным соглашением является на самом деле такой простой контракт, к о т о р ы й используется для ставки на разницу между значением хэша и значением угадывания следующего блока, в соответствии с которым могут быть созданы более сложные протоколы азартных игр для достижения практически нулевой стоимости и Нет мошеннических азарт н ы х игр.

7. Прогноз рынка. Будь то бог или монета Шилина, предсказать рынок будет легко. Прогноз рынка с валютой Schering может оказаться первым основным приложением «футархии» в качестве децентрализованного соглашения об управлении организацией.

8. Цепь идет на централизованный рынок, основанный на системах идентификации и репутации.

Разное и внимание

Улучшенная реализация протокола призраков

Протокол «Greedy Heviest Observed Subtree» (GHOST) был нововведением, представленным Йонатаном Сомполинским и Авивом Зоаром в декабре 2013 года. Мотивация по протоколу Ghost заключается в том, что текущая быстродействующая блок-цепочка страдает от низкой безопасности из-за высокой блокировки блоков, потому что блоки должны тратить определенное количество времени (установленное на t) на всю сеть, если скорость отклонения высокая, она будет простой. Из-за большей доли вычислительной мощности он более эффективен.

Как описывает Сомполинский и Зоар, протокол-призрак решает первую проблему снижения сетевой безопасности путем включения блока отходов при расчете, какая цепочка «самая длинная», то есть не только блок Родительский блок и предыдущий блок предков, блок аннулированных потомков блока предков (известный в терминологии монеты Y2 как «tert block») также добавляются для вычисления того, какой блок имеет максимальный объем работы для его поддержки. доказательство. Мы превзошли соглашение, описанное Sompolinsky и Zohar, чтобы решить вторую проблему - тенденцию централизации, Y2 монеты выплачивают 87,5% вознаграждений за блок отходов, что способствует подтверждению нового блока со статусом «неясного блока» и включает их. Вычисленный «блок корзины» получит 12,5% вознаграждения, но комиссия за транзакцию не будет присуждена блоку дяди.

Монета Y2 реализует упрощенную версию протокола-призрака, которая идет только на пятый этаж. Его характеристика заключается в том, что блок отходов может быть только вторым блоком второго поколения родителя для блока потомков пятого поколения как статус бл

о к а дяди, а не блока более позднего поколения (например, шестого поколения родительского блока). Блок или блок потомков третьего поколения блока деда включены в расчет. Для этого есть несколько причин. Во-первых, безусловный призрачный протокол даст избыточ н у ю сложность вычислению того, какой третичный блок данного блока является законным.

п л а т а

П о с к о л ь к у каждая транзакция, выпущенная в блок-цепочку, берет на себя расходы на загрузку и проверку, необходим механизм регулирования, включающий сборы за транзакции, для защиты от спам-транзакций.

О д н а к о , когда ему дается специальное, менее точное предположение об упрощении, лазейки в этом рыночном механизме чудом устраняют его влияние. Аргумент таков. Предположения:

1. Торговля предоставляет k шагов для предоставления вознаграждений kR всем, кто включает торговлю, где R задается трейдером, и оба k и R видны (грубо) заранее.

2. Стоимость каждого узла для обработки каждого шага - C (т. Е. Эффективность всех узлов согласована).

3. Есть N узлов, каждая с одинаковой вычислительной мощностью (т. Е. 1 / N от общей мощности сети).

О д н а к о есть несколько важных отклонений от этих предположений и реальной ситуации:

1, поскольку дополнительное время проверки задерживает трансляцию блока и, таким образом, увеличивает вероятность того, что блок станет блоком отходов, обработка транзакций будет стоить больше, чем другие контрольные узлы.

2. Распределение силы на практике может оказаться крайне неравномерным.

3, спекулянты, которые разрушают сеть как своих, политических оппонентов и сумасшедших, существуют, и они могут разумно создавать контракты, чтобы их затраты были намного ниже, чем другие контрольные узлы.

Первый пункт выше привел к включению меньшего количества транзакций, а второй - к НК, поэтому влияние этих двух точек по крайней мере частично компенсировало друг друга. Пункты 3 и 4 являются основными проблемами, а в качестве решения мы просто построили Плавающий верхний предел: ни один блок не может содержать больше BLK_LIMIT_FACTOR, чем долгосрочная экспоненциальная скользящая средняя. В частности,：

```
blk.oplimit = floor((blk.parent.oplimit * (EMAFACTOR – 1) + floor(pare
nt.opcount * BLK_LIMIT_FACTOR)) /EMA_FACTOR)

BLK_LIMIT_FACTOR и EMA_FACTOR Временно установлено значение
65536 и 1.5Константы, но могут быть скорректированы после более
глубокого анализа。
```

Вычисление и завершение Тьюринга

Команда JUMP позволяет программе отскакивать где-то в коде, а инструкции JUMPI, которые допускают условные выражения, например, при x <27: x = x * 2, выполняют условные переходы. Во-вторых, контракты могут вызывать другие контракты и иметь потенциал для достижения рекурсии посредством рекурсии. Это, естественно, приводит к проблеме: может ли злоумышленник принудительно отключиться, заставляя весь узел вводить бесконечный цикл? Эта проблема возникает из-за проблемы в компьютерной науке, которая называется проблемой отключения питания: нет никакого способа узнать в общем смысле, может ли данная программа завершить работу в течение ограниченного периода времени.

К а к описано в разделе о переходах состояний, наше решение решает проблему, устанавливая максимальное количество вычислений для каждой транзакции. Если оно превышено, вычисление возвращается в исходное состояние, но плата по-прежнему остается. Новость работа е т так же.

З л о у м ы ш л е н н и к видит контракт, содержащий контракт, такой как send (A, contract.storage [A]); contract.storage [A] = 0 и затем отправляет его достаточно для выполнения первого шага, но недостаточно для выполнения второго шага. Сделка (т. Е. Изъятие, но не ум е н ь ш а е т остаток на счете). Автору контракта не нужно беспокоиться о защите аналогичной атаки, потому что все изменения возвращаются, если выполнение останавливается на полпути.

Ф и н а н с о в ы й контракт работает за счет извлечения медианной информации из девяти частных издателей данных для минимизации риска. Злоумышленник берет на себя одного из поставщиков данных, а затем проектирует механизм вызова адреса переменной, как описано в раз д е л е DAO, для изменения. Поставщик данных повернулся, чтобы запустить бесконечный цикл, пытаясь убедить любую попытку запросить средства из этого финансового контракта, будет приостановлен из-за истощения топлива. Тем не менее, финансовый контракт может ус т а н о в и т ь ограничения на топливо в сообщении для предотвращения таких проблем.

П о л н а я замена Turing - Turing неполная, где инструкции JUMP и JUMPI не существуют, и только одна копия каждого контракта разрешена для существования в стеке вызовов в данный момент времени. В такой системе вышеупомянутая система вознаграждения и неопределен н о с т ь эффективности решения, окружающего нас, могут не понадобиться, поскольку стоимость исполнения контракта будет определяться его размером. Кроме того, Тьюринг является неполным или даже не является большим ограничением. Во всех примерах контрактов, кот о р ы е мы предполагали до сих пор, нужно только циклически циклически, и даже этот цикл можно заменить повторением

26 однострочных сегментов кода. Принимая во внимание серьезные проблемы и ограниченные преимущества, принесенные полнотой Тьюринга, почему бы п р о с т о не использовать неполный язык Тьюринга? Тот факт, что Тьюринг является неполным, далек от кратких решений. Почему? Пожалуйста, рассмотрите следующий контракт：

```
C0: call(C1); call(C1);

C1: call(C2); call(C2);

C2: call(C3); call(C3);

…

C49: call(C50); call(C50);

C50: (run one step of a program and record the change in storage)
```

Т е п е р ь отправьте такую транзакцию на A. Таким образом, в 51 транзакции у нас есть контракт, который требует 250 вычислений. Он может попытаться поддерживать максимальное количество исполняемых шагов для каждого контракта и вызывать другие контракты для ре к у р с и и . Расчеты по контракту могут выполнять шаги для обнаружения таких логических бомб заранее, но это будет препятствовать созданию контрактов для других контрактов (поскольку создание и исполнение вышеуказанных 26 контрактов можно легко включить в один контракт). Другая проблема заключается в том, что поле адреса сообщения является переменной, поэтому, как правило, даже не возможно заранее знать, какой из других контрактов будет вызывать контракт. Таким образом, у нас наконец есть удивительный вывод: пол н о е управление Тьюрингом удивительно легко, и при отсутствии такого же контроля, неполное управление Тьюринга на удивление сложно - почему бы не сделать соглашение Тьюрингом полным?

В а л ю т а и выпуск

К о д о в а я сеть Y2 содержит свою внутреннюю валюту Y2. Монета Y2 играет двойную роль, обеспечивая значительную ликвидность для различных операций с энергетическими активами, и, что более важно, она обеспечивает механизм для оплаты транзакционных издержек. Чтоб ы облегчить и избежать будущих споров (см. Текущую дискуссию mBTC / uBTC / Satoshi), разные имена номинальной стоимости будут установлены заранее:

Э т о следует рассматривать как расширенную версию концепций «meta» и «minutes» или «bitcoin» и «cong». В ближайшем будущем мы ожидаем, что «Y2 монеты» будут использоваться в качестве обычных транзакций и «Finney». Используемые для микро-транзакций «Saab» и «Wei» используются для обсуждения реализации сборов и соглашений.

С п р а в о ч н о е введение:

Л и г а арабских государств является региональной международной организацией, созданной для укрепления сотрудничества и сотрудничества между арабскими странами. Аббревиатура Арабская лига или Лига арабских государств. В марте 1945 года представители Египта, Ир а к а , Иордании, Ливана, Саудовской Аравии, Сирии и семи арабских стран в Йемене провели встречу в Каире, приняли «Договор о Лиге арабских государств» и объявили о создании альянса. К 1993 году насчитывалось 22 государства-члена. Цель заключается в укреплени и тесного сотрудничества между государствами-членами, обеспечении независимости и суверенитета арабских стран и координации их деятельности. В середине ноября 2011 года Лига арабских государств приостановила членство в Сирии, 27 ноября того же года Лига ар а б с к и х государств решила наложить экономические санкции против Сирии сразу после встречи министров иностранных дел в столице Египта Каире. 5 июня 2017 года Лига арабских государств, возглавляемая Саудовской Аравией, опубликовала заявление об исключении Кат а р а из этой организации. Задачи: Тесное сотрудничество между государствами-членами, координация политической деятельности друг с другом, защита независимости и суверенитета арабских стран,

продвижение общих интересов арабских стран и содействие экономичес к о м у , финансовому, транспортному, культурному, здравоохранению, социальному обеспечению, Гражданство, паспорта, визы и правосудие тесно сотрудничают. Государства-члены уважают политическую систему друг друга, и споры между ними не следует применять силой. Д о г о в о р ы и соглашения, заключенные между государствами-членами и другими странами, не являются обязательными для других стран.

В настоящее время насчитывается 22 члена Лиги арабских государств: Алжир, ОАЭ, Оман, Египет, Палестина, Бахрейн, Джибути, Кувейт, Ливан, Ливия, Мавритания, Марокко, Саудовская Аравия, Судан, Сомали, Тунис, Сирия, Йемен, Ирак, Иордания, Ко Cat. 16 ноября 2011 года Лига арабских государств официально прекратила свое членство в Сирии. 26 марта 2013 года Лига арабских государств решила предоставить Сирии «Национальную лигу» для сирийской оппозиции на месте Лиги арабских государств, но она еще не реализована.

М о д е л ь распределения выглядит следующим образом:

● Y2 м о н е т ы б у д у т п р е д л а г а т ь с я п о ц е н е 2,220 и е н з а м о н е т у Y2 в р а м к а х м е р о п р и я т и я п о з а п у с к у . М е х а н и з м , п р е д н а з н а ч е н н ы й д л я ф и н а н с и р о в а н и я м о н е т ы Y2 д л я р а з р а б о т к и н о в ы х т о п л и в н ы х д о б а в о к Y2 и о п л а т ы д л я р а з р а б о т ч и к о в , у ж е и с п о л ь з у е т с я в д р у г о й к р и п т о г р а ф и и . Успешное использование на валютной платформе. Ранние покупатели получат большие скидки. BTC и ETH (изменения в чистых ценах) от продажи будут в полной мере использованы для оплаты зарплаты и вознаграждений разработчиков и исследователей, проектов, котор ы е инвестируют в криптографические валютные экосистемы, и добавок Y2 нового энергетического топлива. Глобальное развитие, распространение и занятость.

В общей сложности 270 миллионов штук были распространены впервые в мире, и на Биржу было распространено 34,5 миллиона штук.

Исходная страна, количество и доля：

страна	Количество (единица: десять тысяч)	бухгалтерский учет
Соединенные Штаты Америки	1356.6	19.38%
Корея	910	13%
Китай	900	12.85%
Россия	800	11.42%
Соединенное Королевство	520	7.42%
EU	320	4.57%
Япония	300	4.28%
Франция	250	3.57%
Саудовская Аравия	250	3.57%
Австралия	250	3.57%
Индия	250	3.57%
Италия	200	2.85%
Индонезия	200	2.85%
Канада	200	2.85%

Германия	150	2.14%
Южная Африка	100	1.42%
Мексика	100	1.42%
индейка	100	1.42%
Бразилия	100	1.42%
Аргентина	50	0.71%

Генеральный секретарь Лиги арабских государств Ахмед Абул Гейт призвал всех присоединиться к этой организации, которая спасет мир;

Лаборатория нового энергетического топлива Y2 (ранее Специальная лаборатория Лиги арабских государств) была создана в 2003 году и переименована в Лабораторию Y2 в 2017 году. За 15 лет она предоставила более 1000 технической поддержки (научных патентов) для Лиги арабских государств и стран Ближнего Востока. Y2 стремится исследовать использование нового энергетического развития и стремится обслуживать страны-члены Лиги арабских государств и разделять озабоченность Союза. Y2 принадлежит подразделению заместителя Генерального секретаря Агентства, находящегося под стражей в Лиге арабских государств.

Запуск Y2 увеличит энергию в мире более чем в 20 раз. К 2020 году он будет экономить потребление энергии в 10-25 раз. В 2030 году использование энергии будет сохранено в 170 раз и более.

1 апреля 2018 года - 6 июня - начало глобального события.

Моды Y2 были выпущены во всем мире 7 апреля и торгуются 30 июня: 7 бирж, включая OKEX, BitMEX, Binance, GDAX, K-net, B-net, HitBTC, YOKI, бит-Z и P-сеть. Цена 295 дирхамов.

Единица выпуска: Y2 Лаборатория нового энергетического топлива (Y2 برتقة مخ ة الطاقة جديدة الوقود)

Основные сотрудники：

Y2 Lab Главный научный сотрудник, генеральный директор Y2 Currency, 2011 Нобелевская премия по химии, сопредседатель Арабского цифрового валютного фонда： Shechtman（شختمان）

Наследник наследного принца Саудовской Аравии, сын короля Салмана, главного стратегического сотрудника валюты Y2: Мохаммад бин Салман Аль Сауд（سعود ألسلمان بن محمد）

Технический консультант Y2 Lab, PayTabsCEO, Главный технический директор, Y2 Валюта：Abdulaziz Al Jouf（الجوف عبدالعزيز）

Y2 Lab Scientist, Нобелевская премия по химии 2016, Главный операционный директор Y2 Currency：PIERRE Sovar（مالسوير）

Т о л ь к о поддержка: BTC, ETH (изменение цены)

П р и м е р : 1 BTC = 46 000 юаней, то есть 1 BTC = 133.33333333 Y2

П р и м е р : 1ETH = 2500 юаней, то есть 1 ETH = 7.24763681 Y2

● 0.099x (x - о б щ а я п р о д а н н а я с у м м а) б у д е т п е р е д а в а т ь с я BTC, ETH (д в и ж е н и е р е а л ь н о й ц е н ы), а т а к ж е в к л а д ч и к о в д е н е ж н ы х с р е д с т в и л и д р у г о е д е т е р м и н и р о в а н н о е ф и н а н с и р о в а н и е д л я у ч а с т и я в р а н н и х в к л а д ч и к а х д о у с п е ш н о г о р а з в и т и я , е щ е о д и н 0.099x б у д е т в ы д е л е н д л я долгосрочных исследовательских проектов ,

Р а з л о ж е н и е разложения

Б е с к о н е ч н а я линейная модель роста снижает риск чрезмерной концентрации богатства в Биткойне и дает людям, живущим в настоящем и будущем, справедливый шанс получить деньги, сохраняя при этом стимулы к приобретению и хранению монет Y2 в качестве долгосрочных Взгляд на «темпы роста денежной массы» стремится к нулю. Мы также делаем вывод о том, что с течением времени монеты всегда будут потеряны из-за небрежности и смерти. Если потеря монеты является фиксированной долей годовой денежной массы, то денежная масса в конечном общем обращении будет стабильной. При значении, равном годовому денежному обороту, деленному на коэффициент потерь (например, когда коэффициент потерь составляет 1%, когда поставка достигает 30x, каждый год выкопается 0,3x и каждый раз теряется 0,3x, достигая равновесия).

В дополнение к методу линейной выдачи, рост поставок монеты типа биткойн Y2, как правило, является нулевым в долгосрочной перспективе.

р а с т я ж и м о с т ь

П р о б л е м ы с масштабируемостью представляют собой общую проблему для монет Y2. Как и биткойн, монеты Y2 также страдают от того факта, что каждая транзакция требует, чтобы каждый узел сети справлялся с этой дилеммой. Текущий размер блока биткойнов составляет о к о л о 20 ГБ, который растет со скоростью 1 МБ в час. Если сеть Bitcoin обрабатывает транзакции Visa-class 2000tps, она будет расти с 1 МБ каждые три секунды (1 ГБ в час, 8 ТБ в год). Y2 монеты могут также испытывать аналогичные или даже худшие шаблоны роста , потому что на блочной цепочке монет Y2 много приложений, а не биткойн как простая валюта, но для монет Y2 нужно сохранить состояние вместо Факт полной истории блокчейнов улучшил ситуацию.

П р о б л е м а с большими блочными цепями - это риск централизации. Если размер блока цепочки увеличивается, скажем, до 100 ТБ, вероятным сценарием будет то, что только очень небольшое количество крупных торговцев будет запускать полные узлы, в то время как обыч н ы е пользователи используют легкие узлы SPV. Это вызывает опасения по поводу риска мошенничества при полном партнерстве с узлами (например, смена вознаграждения за блок, предоставление BTC). Легкие узлы не смогут сразу обнаружить это мошенничество. Конечно, может быть хотя бы один честный полный узел, и через несколько часов через такие каналы, как Reddit, просочилась мошенническая информация, но слишком поздно, чтобы средний пользователь сделал все возможное, чтобы отменить блоки, которые уже были сгенерир о в а н ы . Все они столкнутся с огромными неосуществимыми проблемами координации в том же масштабе, что и успешная атака на 51%. В биткойне это проблема сейчас, но изменение, предложенное Питером Тоддом, может облегчить эту проблему.

В последнее время монеты Y2 будут использовать две дополнительные стратегии для решения этой проблемы. Определенное количество полных узлов гарантировано. Во-вторых, и что еще более важно, после обработки каждой транзакции мы будем включать корень промежуто ч н о г о дерева состояний в цепочке. Даже если проверка блока централизована, до тех пор, пока существует честный контрольный узел, централизованная проблема может быть устранена протоколом проверки. Если выдается неправильный блок, блок либо находится в непр а в и л ь н о м формате, либо состояние S [n] неверно. Поскольку S [0] верна, должно быть первое состояние ошибки S [i], но S [i-1] верна, узел проверки будет предоставлять индекс i вместе с обработкой APPLY (S [i-1], TX [i]) -> S [i] Требуется подмножество узло в дерева Патрисии. Этим узлам будет поручено выполнить эту часть вычисления, чтобы увидеть, соответствует ли полученное S [i] ранее предоставленным значениям.

К р о м е того, более сложно злонамеренно освободить незавершенный блок для атаки, в результате чего недостаточно информации, чтобы определить, является ли блок правильным. Решение является протоколом «запрос-ответ»: узел проверки вызывает целевой индекс транза к ц и и , а легкий узел, получающий информацию о вызове, не доверяет соответствующему блоку до тех пор, пока другой или верификатор не предоставит подмножество узлов Patricia как правильное. доказательства.

О б з о р : децентрализованные приложения

В ы ш е у п о м я н у т ы й контрактный механизм позволяет любому человеку установить приложение командной строки (в основном говоря) через глобальный консенсус по сети на виртуальной машине, который может изменить состояние, доступное для всей сети, как «жесткий диск». Однако для большинства людей отсутствие адекватного удобства для интерфейса командной строки, используемого в качестве механизма доставки транзакций, делает децентрализацию привлекательной альтернативой. Наконец, полное «децентрализованное приложение» до л ж н о включать базовые компоненты бизнес-логики (независимо от того, полностью ли реализованы монеты Y2, с использованием монет Y2 и других системных комбинаций (таких как слой сообщений P2P, в одном из которых планируется разместить клиентов монеты Y2 Оконч а н и е срока службы или другой режим только для системы] и компоненты верхнего графического интерфейса пользователя. Клиент монеты Y2 разработан как веб-браузер, но включает поддержку объектов API Javascript для ПК, которые могут использоваться конкретными в е б -страницами, которые клиент видит для взаимодействия с блочной цепочкой Y2. С точки зрения «традиционных» веб-страниц эти веб-страницы являются полностью статическим контентом, поскольку блокчин и другие децентрализованные протоколы полностью заменяют с е р в е р для обработки инициированных пользователем запросов. Наконец, децентрализованный протокол обещает использовать какую-то форму монеты Y2 для хранения веб-страниц.

в ы в о д

С о г л а ш е н и е о векселе Y2 изначально было задумано как усовершенствованная версия криптовалютности, которая обеспечивает высокоразвитые функции, такие как цепные контракты, ограничения на снятие средств и финансовые контракты, рынки азартных игр и т. Д., Пос р е д с т в о м очень распространенного языка. Протокол монеты Y2 не будет напрямую «поддерживать» любое приложение, но наличие полного языка программирования Turing означает, что теоретически произвольные контракты могут быть созданы для любого типа транзакции и приложения. Тем не менее, что более интересно в монетах Y2, так это то, что протокол монеты Y2 идет дальше чистой валюты, сосредоточившись вокруг децентрализованного хранилища, децентрализованных вычислений и децентрализованных рынков прогнозирования и де с я т к о в аналогичных концепций для установления соглашений и децентрализации Приложения могут существенно повысить эффективность вычислительной индустрии и обеспечить сильную поддержку других протоколов P2P, добавив экономические уровни в первый раз. Наконец, также будет большое количество приложений, которые не имеют никакого отношения к деньгам.

К о н ц е п ц и я произвольных переходов состояний, реализуемых протоколом монеты Y2, обеспечивает платформу с уникальным потенциалом: в отличие от закрытых соглашений, предназначенных для отдельных целей, таких как хранение данных, азартные игры или финансы, монет ы Y2 являются открытыми в дизайне и Мы считаем, что он чрезвычайно подходит в качестве базового слоя для обслуживания чрезвычайно большого количества финансовых и нефинансовых соглашений, которые появятся в ближайшие годы.

К о м м е н т а р и и и расширенное чтение

к о м м е н т а р и й

1. Опытный читатель заметит, что адрес биткойна на самом деле является хешем открытого ключа эллиптической кривой, а не самим открытым ключом, но на самом деле вполне разумно ссылаться на хэш общего ключа как открытый ключ с криптографической точки зрения. Это связано с тем, что криптографию в биткойне можно рассматривать как алгоритм пользовательской цифровой подписи. Открытый ключ состоит из хэша открытого ключа эллиптической кривой. Подпись состоит из открытого ключа эллиптической кривой, связанного с сиг н а т у р о й

эллиптической кривой. Алгоритм проверки включает использование Ключ обеспечивает хэш-ключ открытого ключа эллиптической кривой для проверки открытого ключа эллиптической кривой, а затем использует открытый ключ эллиптической кривой для проверки под п и с и эллиптической кривой.

2. С технической точки зрения, медиана первых 11 блоков.

3. Внутренне, 2 и «CHARLIE» - это числа, последний имеет огромный формат кодирования base256, число может быть от 0 до 2 ^ 256-1.