Конфиденциальность блокчейна и соответствие нормативным требованиям: На пути к практическому равновесию

Виталик Бутерин, Якоб Иллум, Маттиас Надлер, Фабиан Шаер и Амин Солеймани

Аннотация *B* данной статье мы рассматриваем Privacy Pools - новый протокол повышения конфиденциальности, основанный на смарт-контрактах. Мы обсуждаем плюсы и минусы этого протокола и показываем, как он может быть использован для создания разделительного равновесия между честными и нечестными пользователями. Суть предложения заключается в том, чтобы позволить пользователям публиковать доказательство нулевого знания, демонстрирующее, что их средства (не) происходят из известных (не)законных источников, без публичного раскрытия всего графа их транзакций. Это достигается путем доказательства принадлежности к пользовательским наборам ассоциаций, которые удовлетворяют определенным свойствам, требуемым нормативными актами или общественным консенсусом. Данное предложение может стать первым шагом на пути к будущему, когда люди смогут доказывать соответствие нормативным требованиям, не раскрывая всю историю своих транзакций.

***Индексные термины - блокчейн*, конфиденциальность, регулирование, смарт-контракты, доказательства нулевого знания.**

I. ВВЕДЕНИЕ

Публичные блокчейны прозрачны по своей сути. Основная идея заключается в том, что любой человек должен иметь возможность подтверждать транзакции, не полагаясь на централизованные третьи стороны. Это снижает зависимость и может стать нейтральной основой для различных приложений, включая, в частности, финансы и суверенные личности.

Однако существование публичного набора данных, содержащего каждую транзакцию каждого адреса блокчейна, проблематично с точки зрения конфиденциальности. Всякий раз, когда кто-то переводит актив на другой адрес и/или взаимодействует со смарт-контрактом, эта транзакция будет всегда видна в блокчейне.

Рассмотрим следующий пример: Алиса идет в ресторан и использует свой кошелек blockchain для оплаты ужина. Получатель теперь знает адрес Алисы и может проанализировать всю прошлую и будущую активность по этому адресу. Аналогично, Алиса теперь знает адрес кошелька ресторана и может использовать эту информацию для получения адресов кошельков других посетителей или для изучения доходов ресторана. Третьи лица, знающие адрес кошелька ресторана и располагающие информацией о том, что Алиса там обедает (например, из социальных сетей), могут легко вычислить адрес Алисы и также изучить ее прошлые и будущие транзакции.

Хотя пример с рестораном можно рассматривать как гипотетический сценарий, основополагающая концепция применима к любой транзакции, проводимой на публичной блокчейн-цепи. Каждое действие, совершенное на публичном блокчейне, публично записывается и доступно любому желающему, что позволяет третьим лицам анализировать финансовые операции и поведение пользователей.

Эти проблемы привели к появлению протоколов, повышающих конфиденциальность. Они позволяют пользователям вносить средства в протокол, используя один адрес, и выводить их из протокола в более поздний момент времени, используя другой адрес. Все операции по вводу и выводу средств по-прежнему видны в блокчейне, но связь между конкретным вкладом и его аналогом по выводу больше не является публичной.

Одним из наиболее известных протоколов, повышающих уровень конфиденциальности, является Tor- nado Cash. Он успешно решает вышеупомянутые проблемы, позволяя пользователям сохранять некоторую приватность. Однако помимо законных пользователей, пытающихся защитить свои данные, Tornado Cash использовался и различными злоумышленниками. Данные о депозитах свидетельствуют о том, что хакерские группировки переводили через этот протокол средства из незаконных источников. Данные о том, что протокол, повышающий конфиденциальность, использовался также северокорейской хакерской группировкой, в конечном итоге привели к включению адресов смарт-контрактов этого протокола в список *специально назначенных граждан и запрещенных лиц* (так называемый список SDN), который ведет *Управление по контролю за иностранными активами* (OFAC) США.

Основная проблема Tornado Cash заключалась в том, что у легальных пользователей было мало возможностей откреститься от преступной деятельности, к которой привлекал протокол. В Tornado Cash предусмотрена функция соответствия, которая позволяет пользователю создать доказательство того, с какого депозита был произведен тот или иной вывод средств. Хотя этот механизм и позволяет доказать свою невиновность, его использование сопряжено с необходимостью доверять централизованному посреднику и создает информационную асимметрию [1]. В связи с этим данный механизм не нашел широкого применения.

В данной статье рассматривается расширение этого подхода, позволяющее пользователям публично доказывать информативное, но все же широкое утверждение о том, с каких депозитов мог быть снят их депозит. При этом допускаются *доказательства принадлежности* ("Я доказываю, что мой вывод средств произошел с одного из этих вкладов") или *исключения* ("Я доказываю, что мой вывод средств *не произошел* с одного из этих вкладов"). Общая концепция была предложена в Privacy Pools [2]. В настоящей работе рассматривается это предложение и объясняется, как его составные части могут быть использованы для достижения разделительного равновесия между честными и нечестными пользователями протокола.

Отметим, что Privacy Pools предоставляет дополнительные возможности, расширяя набор действий пользователей. При необходимости они могут предоставлять более подробные доказательства конкретным контрагентам. Однако бывают случаи, когда достаточно доказательства принадлежности или исключения. Более того, возможность публикации этих доказательств

Публичное раскрытие информации имеет много преимуществ перед двусторонним.

Статья построена следующим образом. После этого краткого введения мы даем техническую информацию о доказательствах с нулевым знанием и пулах конфиденциальности. В разделе III мы обсуждаем, как используются и строятся ассоциативные наборы. В разделе IV мы подробно останавливаемся на технических деталях и особых случаях. В разделе V мы обсуждаем полученные результаты и переходим к практическим соображениям. Наконец, в разделе VI мы подводим итоги.

II. ТЕХНИЧЕСКАЯ БАЗА

В этом разделе мы даем краткий технический обзор, обсуждаем технические компоненты и общие принципы работы протоколов типа Privacy Pools.

A. Конфиденциальность блокчейна перед ЗК-СНАРКами

В прошлом сторонники блокчейна утверждали, что блокчейн позволяет сохранить конфиденциальность, несмотря на прозрачность всех транзакций, поскольку он обеспечивает *псевдонимность*: для использования блокчейна не нужно раскрывать информацию о своей личности вне сети. Вместо этого пользователи идентифицируются по числовым "адресам".

Сатоши в своем документе о биткойне утверждает именно это, заявляя, что "конфиденциальность можно сохранить, прервав поток информации в другом месте: сохранив анонимность открытых ключей. Общественность может видеть, что кто-то отправляет кому-то сумму, но без информации, связывающей транзакцию с кем-либо" [3]. К сожалению, такой уровень конфиденциальности оказался далеко недостаточным перед лицом современных средств кластеризации и анализа [4] [5]. В нефинансовых приложениях обеспечить конфиденциальность еще сложнее, поскольку они часто требуют от пользователей публикации в сети информации о себе другого рода. Например, регистрация имени на децентрализованных сервисах доменных имен, таких как ENS [6], предполагает проведение транзакции на блокчейне Ethereum, что создает публичную связь между вашими транзакциями и вашим именем на ENS.

По этой причине в публичных блокчейнах наблюдается движение в сторону повышения уровня конфиденциальности путем внедрения более мощных технологий. Самым первым нетривиальным решением для обеспечения конфиденциальности, получившим значительное распространение, была технология CoinJoin [7]. В рамках CoinJoin небольшие группы пользователей объединялись и смешивали свои монеты друг с другом в рамках одной транзакции. Если посмотреть на цепочку, то можно увидеть только общий набор входов и выходов данного раунда протокола CoinJoin, а не то, какой вход соответствует какому выходу. Теория заключалась в том, что пользователь мог участвовать во многих раундах протокола CoinJoin с разными группами людей, скрывая таким образом источник своих активов среди множества возможных входов. Компания Monero пошла еще дальше, использовав схему кольцевой подписи [8], позволяющую пользователям смешивать свои монеты с несколькими монетами других пользователей без необходимости какого-либо взаимодействия вне цепи. По мере совершенствования технологии [9] число участников каждого микса росло, увеличивая *набор анонимности* каждой транзакции: количество исторических транзакций, которые могли быть источником

этой трансакции. Однако такие методы многократного смешивания малых групп неизбежно несут в себе риски утечки данных [10].

Следующим логическим шагом на пути к повышению уровня криптографической конфиденциальности стало внедрение универсальных доказательств нулевого знания, которые используются в блокчейнах, таких как Zcash [11], и внутрицепочечных системах смарт-контрактов, таких как Tor- nado Cash. В таких системах набор анонимности каждой транзакции потенциально может быть равен всему набору всех предыдущих транзакций. Доказательства с нулевым знанием общего назначения, применяемые в данной работе, в отраслевом и научном сообществе чаще всего называют "ZK-SNARKs".

B. ZK-SNARKs

ZK-SNARK - это технология, позволяющая доказывать математические утверждения о некоторой комбинации открытых и закрытых данных, которыми владеет проверяющий, таким образом, чтобы они удовлетворяли двум ключевым свойствам:

- *Zero-Knowledge*: ничего о частных данных не раскрывается, кроме того факта, что частные данные удовлетворяют доказываемому утверждению.
- *Лаконичность*: доказательство короткое (в байтах) и может быть проверено очень быстро, *даже если в* основе доказываемого утверждения лежат тяжелые вычисления, требующие очень длительного времени для выполнения.

По обеим этим причинам ZK-SNARK привлекают большое внимание блокчейн-сообщества. Аспект лаконичности является ключевым в случаях использования ZK-SNARK для масштабируемости, таких как ZK-rollups [12]. Для описываемых нами случаев использования конфиденциальности краткость не столь важна, но аспект "нулевого знания" очень важен.[1]

Утверждение", которое доказывает ЗК-СНАРК, выражается в виде программы, которую часто называют "цир-кутом". Математически достаточно представить ее как функцию $f(x, w) \rightarrow \{\texttt{True}, \texttt{False}\}$, где x - открытый вход, w - закрытый вход, а $f(.)$ - вычисляемая функция. ZK-SNARK доказывает, что для данного x, известного как проверяющему, так и верификатору, проверяющий знает w такое, что $f(x, w)$ возвращает `True`.

C. Пример: ZK-SNARK в системах, подобных Zcash и Tornado Cash

Существуют незначительные различия между разными версиями Zcash и разными версиями систем, созданных по мотивам Zcash, таких как Tornado Cash. Однако базовая логика, от которой они зависят, очень похожа. В данном разделе описывается простая версия, которая примерно соответствует тому, как работают эти протоколы.

Монета" состоит из секрета s, который хранится у ее владельца. Из s можно получить два значения:

- Публичный "идентификатор монеты" $L = hash(s + 1)$

[1] Более полное введение в ЗК-СНАКРС см. в [13] и [14].

- Нуллификатор $U = hash(s + 2)$

Термин "*хэш*" относится к криптографической хэш-функции, например SHA256. Учитывая s, можно вычислить идентификатор монеты и нуллификатор. Однако при наличии набора нуллификаторов и публичных идентификаторов монет псевдослучайное поведение хэш-функции гарантирует, что вы не сможете определить, какой нуллификатор связан с каким идентификатором монеты, если не знаете секрет s, сгенерировавший их.

Блокчейн отслеживает все идентификаторы монет, которые уже были "созданы", и все "нуллификаторы", которые уже были "потрачены". Оба набора постоянно растут (если только протокол не хочет ввести ограничение по времени, до которого монеты должны быть потрачены).

Набор идентификаторов монет хранится в структуре данных, называемой *деревом Меркла*: если дерево содержит N элементов, то каждая смежная пара элементов хешируется (что приводит к $\lceil \frac{N}{2} \rceil$ хешам), каждая смежная пара этих хешей хешируется (что приводит к $\lceil \frac{N}{4} \rceil$ хешам), и так далее, пока все данные не будут зафиксированы в одном "корневом хеше".

Если задано определенное значение в дереве и хэш корня, то можно представить *ветвь Меркла*: "сестринские значения", которые хэшировались вместе на каждом шаге пути от этого значения к корню. Ветвь Меркла полезна тем, что представляет собой небольшой ($log_2(N)$ хэшей) фрагмент данных, который может быть использован для доказательства того, что любое конкретное значение действительно находится в дереве. На рис. 1 показан пример дерева Меркла с высотой 4.

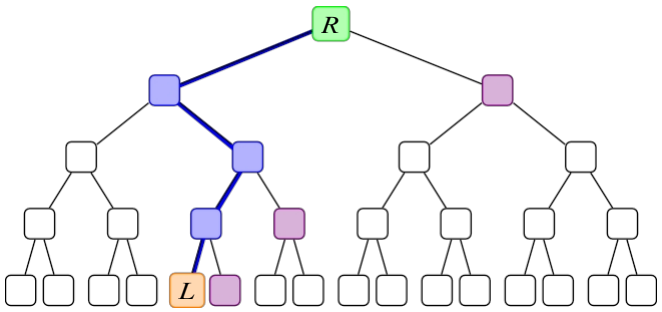


Рис. 1: Структура дерева Меркла, выделение ветви Меркла для данного значения в дереве. Оранжевый цвет - лист L, *по* которому проводится проверка; нижняя строка дерева представляет собой весь набор данных. Зеленый - корневой хэш R. Синий - путь от листа к корню. Фиолетовым - сестринские узлы на каждом уровне. Обратите внимание, что путь можно вычислить, начав с листа и хэшируя его вместе с сестринским узлом на каждом уровне, поэтому нет необходимости предоставлять сам путь.

Когда пользователь отправляет монету другому человеку, он предоставляет (i) нуллификатор U, который он хочет потратить, (ii) идентификатор L' новой монеты, которую он хочет создать (он попросит получателя дать ему его), и (iii) ZK-SNARK.

Он также содержит следующие открытые материалы:

- U , нуллификатор расходуемой монеты
- R - корневой хэш, по которому проверяется

доказательство Меркла. ZK-SNARK доказывает два

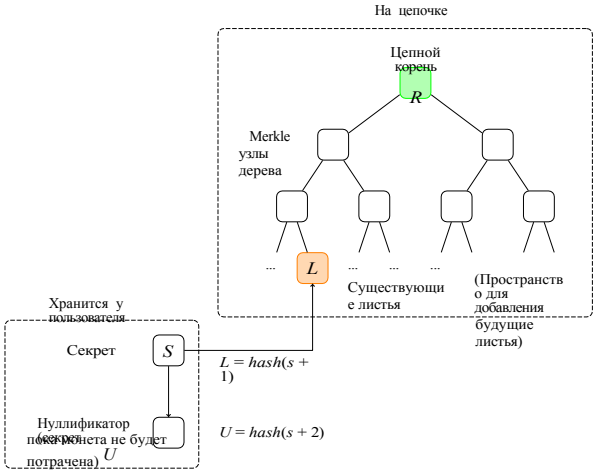
свойства:

- $U = hash(s + 2)$
- Ветвь Меркла действительна

За пределами ЗК-СНАРК протокол также проверяет это:

- R - текущий или исторический корневой хэш дерева идентификации монет
- U не входит во множество уже потраченных нуллификаторов

Если транзакция валидна, то она добавляет U в набор потраченных нуллификаторов, а L' - в список идентификаторов монет.



ZK-SNARK содержит следующие частные входы:

- Секрет пользователя s
- Ветвь Меркла в дереве идентификаторов монет, доказывающая, что монета с идентификатором $L = hash(s + 1)$ действительно была создана в какой-то момент в прошлом

Рис. 2: Некоторые структуры данных, задействованные в системе передачи монет с сохранением конфиденциальности. Дерево Меркла - это дерево идентификаторов монет; набор нуллификаторов не показан, но он также хранится на цепочке. Пока данная монета существует, но еще не потрачена, идентификатор монеты (L) находится на цепочке, но секрет (s) и нуллификатор (U) известны только владельцу монеты.

Раскрытие U не позволяет потратить одну монету дважды. Однако *никакая другая информация не раскрывается*. Все, что видит внешний мир, - это *момент* отправки транзакций; он не получает никаких знаний о том, кто отправляет или получает эти транзакции, или о том, какая монета является "той же монетой", что и предыдущая монета.

Из этой закономерности есть два исключения: *пополнение счета* и *снятие средств*. При пополнении счета идентификатор монеты создается без необходимости аннулирования предыдущей монеты. Депозиты не сохраняют приватность в том смысле, что связь между данным L и внешним событием, которое позволило добавить L (в Tornado Cash - внесение ETH в систему, в Zcash - добыча новых монет ZEC), является публичной. Другими словами, депозиты связаны с историей их прошлых транзакций. При выводе средств нуллификатор расходуется без добавления нового идентификатора монеты. Это может нарушить связь вывода с

соответствующего депозита и, следовательно, к истории прошлых операций. Однако снятие средств может быть связано с любыми будущими операциями, произошедшими после события снятия. [1]

Первая версия Tornado Cash не имела концепции внутренних переводов, она позволяла *только* пополнять и снимать средства. Более поздние версии, пока еще находящиеся в стадии эксперимента (альфа), также допускают внутренние переводы, и монеты произвольного номинала, включая поддержку операций "разделения" и "слияния", необходимых для работы с монетами произвольного номинала. О том, как расширить базовые системы передачи монет, сохраняющие конфиденциальность, и пулы конфиденциальности для работы с монетами произвольного номинала, мы расскажем в следующем разделе.

D. ZK-SNARKs в пулах конфиденциальности

Основная идея Privacy Pools заключается в следующем: вместо того чтобы просто доказать с нулевым знанием дела, что его вывод связан с некоторым ранее сделанным депозитом, пользователь доказывает принадлежность к более строгому *набору ассоциаций*. Ассоциативный набор может быть полным подмножеством ранее сделанных депозитов, набором, состоящим только из собственного депозита пользователя, или чем-то средним. Пользователь задает набор, предоставляя в качестве публичного ввода корень Меркла из этого набора.

Для простоты мы не доказываем напрямую, что ассоциативный набор действительно является подмножеством ранее сделанных вкладов; вместо этого мы просто требуем от пользователя доказать нулевые знания по *двум* ветвям Меркле, используя один и тот же идентификатор монеты в качестве листа в обоих случаях: (i) ветвь Меркле в R, корень общего набора идентификаторов монет, и (ii) ветвь Меркле в предоставленный корень ассоциативного набора R_A . Это показано на рис. 3.

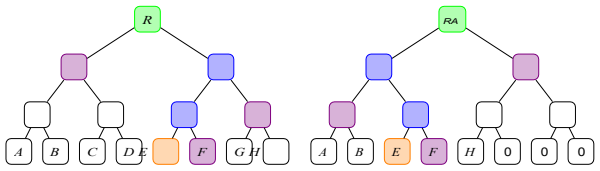


Рис. 3: Пользователь с нулевым знанием доказывает две ветви Меркла: одна доказывает, что его ID монеты находится где-то в дереве ID монет, а другая доказывает, что этот же ID монеты находится где-то в дереве, представляющем предоставленный пользователем набор ассоциаций (представленный его корнем R_A).

Предполагается, что полный набор ассоциаций будет доступен где-то в сети или в другом месте. В этом и заключается основная концепция: вместо того чтобы требовать от пользователя указывать, с какого именно депозита он снял средства, или, в крайнем случае, вообще не предоставлять никакой информации, кроме

III. ПРАКТИЧЕСКИЕ СООБРАЖЕНИЯ И ПРИМЕРЫ ИСПОЛЬЗОВАНИЯ

После этого технического введения мы переходим к прикладной стороне вопроса и анализируем, как протоколы, повышающие конфиденциальность, могут быть использованы на практике.

A. Примеры использования ассоциативных наборов

Чтобы проиллюстрировать ценность этой схемы в контексте правоохранительной деятельности, рассмотрим простой пример. Предположим, что у нас есть пять пользователей: Алиса, Боб, Карл, Дэвид и Ева. Первые четверо - честные, законопослушные пользователи, которые, тем не менее, хотят сохранить свою конфиденциальность, а вот Ева - воровка. Предположим также, что это общеизвестно. Общественность может не знать реальной личности Евы, но у нее достаточно доказательств, чтобы сделать вывод о том, что монеты, отправленные на адрес, который мы обозначим как "Ева", являются краденными. Так часто бывает на практике: большинство незаконных средств, которые, как было установлено, поступали в Tornado Cash, были получены в результате эксплуатации протокола DeFi - события, которое видно на публичном блокчейне.

При выводе средств каждый из пяти пользователей имеет возможность выбрать, какой набор ассоциаций он укажет. Их набор ассоциаций должен включать их собственный депозит, но они могут свободно выбирать, какие из других адресов включать. Сначала рассмотрим стимулы Алисы, Боба, Карла и Дэвида. С одной стороны, они хотят максимизировать свою конфиденциальность. Это толкает их к тому, чтобы сделать свои наборы ассоциаций более широкими. С другой стороны, они хотят снизить вероятность того, что их монеты покажутся подозрительными торговцам или биржам. У них есть простой способ добиться этого: Они не включают Еву в свой набор ассоциаций. Таким образом, для всех четверых выбор очевиден: сделать их ассоциативные наборы {Алиса, Боб, Карл, Дэвид}.

Ева, конечно, тоже хочет максимизировать свой набор ассоциаций. Но она не может исключить свой вклад, и поэтому вынуждена сделать так, чтобы ее ассоциативный набор был равен набору всех пяти вкладов. Выбор участниками набора ассоциаций показан на рис.
подтверждения отсутствия двойных трат, мы даем пользователю возможность указать набор возможных источников происхождения его средств, причем этот набор может быть как широким, так и узким по его желанию. Мы поощряем формирование экосистемы, которая облегчает пользователям определение наборов ассоциаций, соответствующих их предпочтениям. В остальной части данной статьи мы просто опишем инфраструктуру, созданную на основе этой простой базовой механики, и ее последствия.

4.

Несмотря на то, что сама Ева не дает никакой информации, путем простого исключения мы можем сделать однозначный вывод: вывод № 5 мог произойти только от Евы.

B. Построение ассоциативного ряда

Предыдущий раздел иллюстрирует один из возможных вариантов использования ассоциативных наборов в протоколах типа Privacy Pools, а также то, как честные участники могут отмежеваться от плохих участников. Заметим, что система не полагается на альтруизм Алисы, Боба, Карла и Дэвида; у них есть четкий стимул доказать свою непричастность.

Теперь рассмотрим более подробно построение ассоциативных множеств. В общем случае существует две основные стратегии построения ассоциативных множеств. Они описаны ниже и наглядно представлены на рис. 5.

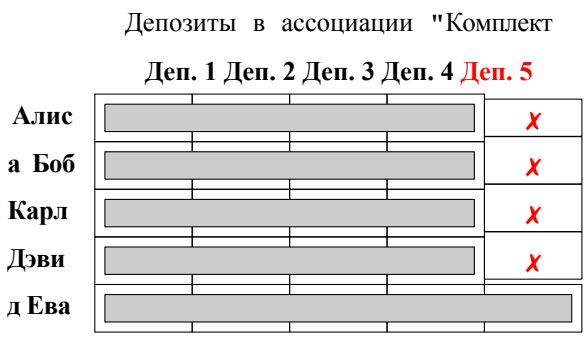


Рис. 4: Серая область в каждой строке представляет собой набор ассоциаций соответствующего пользователя. В нашем упрощенном примере мы предполагаем, что Алиса, Боб, Карл и Дэвид включают все остальные "хорошие" вклады в свои ассоциативные наборы и исключают вклад 5, который происходит из известного незаконного источника. Ева, с другой стороны, не может создать доказательство, которое не ассоциировало бы ее вывод средств с ее собственным вкладом.

- **Включение (или членство):** определение конкретного набора вкладов, для которых у нас есть конкретные основания считать их *низкорисковыми*, и построение ассоциативного набора, содержащего *только эти вклады*.
- **Исключение:** выделение определенного набора вкладов, по которым у нас есть конкретные основания полагать, что они относятся к *высокорисковым*, и построение ассоциативного набора, содержащего *все вклады*, *кроме этих.*

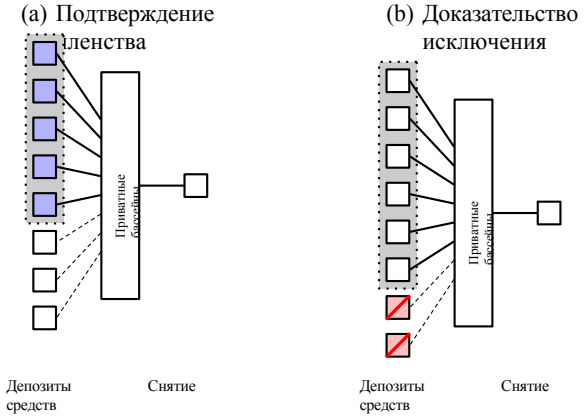


Рис. 5: Доказательство принадлежности включает в свое ассоциативное множество определенную коллекцию вкладов, в то время как ассоциативное множество доказательства исключения состоит из чего угодно, только не из определенной коллекции вкладов.

или в другом месте.

Мы настоятельно рекомендуем публиковать на цепочке как минимум корень Меркла набора ассоциаций; это лишает злоумышленников возможности осуществлять определенные виды атак на пользователей (например, предоставлять разным пользователям разные наборы ассоциаций в попытке их деанонимизации). Наборы в целом должны быть доступны либо через API, либо, в идеале, на недорогой децентрализованной системе хранения данных, например IPFS.

Возможность загрузки всего набора ассоциаций очень важна, так как это позволяет пользователям генерировать доказательства принадлежности к ассоциации.
в ассоциации, установленной локально, не раскрывая никакой дополнительной информации, даже АСП, о том, какой депозит соответствует осуществляемому им снятию.

Вот некоторые возможные конструкции практического функционирования АСП:

- **Добавлять с задержкой, исключать плохих игроков**: любой вклад автоматически добавляется в набор ассоциации через определенный период времени (например, 7 дней), но если система обнаруживает, что данный вклад связан с известным плохим поведением (например, крупными кражами или адресами в опубликованном правительством санкционном списке), то вклад никогда не добавляется. На практике это может быть реализовано как с помощью наборов, создаваемых сообществом, так и с помощью существующих провайдеров услуг по проверке транзакций, которые уже выполняют работу по выявлению и отслеживанию вкладов, связанных с неблаговидным поведением.
- **$N в месяц на человека**: для вступления в ассоциацию установить,
стоимость вклада должна быть меньше некоторого фиксированного максимума, а депонент должен с нулевым знанием дела доказать, что он является обладателем некоторого маркера, подтверждающего его личность (например, либо государственной системы идентификации личности, либо более легкого механизма, такого как верификация аккаунта в социальных сетях). Механизм нуллификатора с дополнительным параметром, представляющим текущий месяц, используется для того, чтобы каждая личность могла внести депозит в ассоциативный набор ровно один раз в месяц. Данная конструкция пытается реализовать дух многих распространенных сегодня правил AML, в которых платежи с низкой стоимостью ниже определенного порога допускают гораздо больший уровень конфиденциальности, чем платежи с высокой стоимостью.

С технической точки зрения они идентичны, так как оба доказывают против корня Меркле ассоциативного множества.

На практике пользователи не будут вручную выбирать

месторождения для включения в свой набор ассоциаций. Скорее, пользователи будут подписываться на услуги посредников, которых мы можем назвать *провайдерами ассоциативных наборов* (ASP), формирующими ассоциативные наборы с определенными свойствами. В некоторых случаях ASP могут быть полностью созданы на цепочке, без вмешательства человека (или искусственного интеллекта). В других случаях ASP будут генерировать наборы ассоциаций самостоятельно и публиковать их либо на цепочке

платежей. Отметим, что это может быть реализовано полностью в виде смарт-контракта, не требующего ручного контроля для поддержания текущей работы.

- **$N в месяц за одного доверенного члена сообщества**: то же самое, что $N в месяц за одного человека, но с более строгими условиями: пользователь должен подтвердить свое членство в сообществе с высоким уровнем доверия. Сообщество с высоким уровнем доверия соглашается с тем, что его члены обеспечивают конфиденциальность друг для друга.
- **Скоринг на основе ИИ в режиме реального времени**: Системы ASP, основанные на искусственном интеллекте, могут в режиме реального времени определять степень риска для каждого вклада, и система выводит ассоциативный набор, содержащий те вклады, степень риска которых ниже определенного порога. Потенциально АСП может выдавать несколько наборов, соответствующих нескольким пороговым уровням оценки риска.

IV. ДОПОЛНИТЕЛЬНЫЕ ТЕХНИЧЕСКИЕ ДАННЫЕ

В этом разделе мы анализируем, как предложение может поддерживать произвольные номиналы, и обсуждаем частные случаи, такие как повторное доказательство, двустороннее прямое доказательство и последовательное доказательство.

A. Поддержка произвольных деноминаций

Упрощенные монетные системы с сохранением конфиденциальности, описанные выше, поддерживают передачу монет только одного номинала. Zcash поддерживает произвольные номиналы благодаря использованию модели UTXO. Каждая транзакция может иметь несколько входов (что требует публикации нуллификатора для каждого входа) и несколько выходов (что требует публикации идентификатора монеты для каждого выхода). Каждый созданный идентификатор монеты должен содержать зашифрованное значение номинала. Помимо подтверждения достоверности нуллификаторов, каждая транзакция должна сопровождаться дополнительным доказательством того, что сумма номиналов создаваемых монет не превышает сумму номиналов расходуемых монет. Рисунок 6 иллюстрирует это дополнительное доказательство.

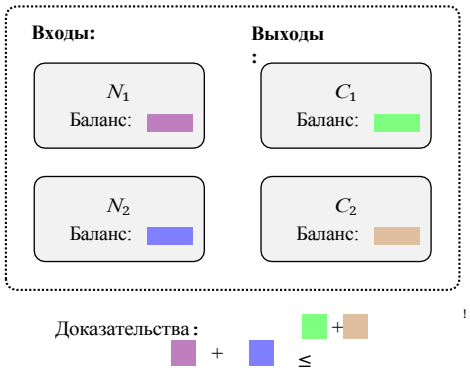


Рис. 6: ZK-SNARK доказывает дополнительное утверждение, что зашифрованные номиналы представляют собой такие числа, что сумма чисел на выходе не превышает сумму чисел на входе. В зависимости от конструкции может потребоваться также явное доказательство того, что все вновь созданные номиналы монет неотрицательны.

Эта конструкция может быть расширена для поддержки депозитов и снятий, просто рассматривая депозит как вход (незашифрованный), а снятие - как выход (незашифрованный). Для упрощения анализа конструкция может быть ограничена. Например, можно разрешить *только* частичное снятие средств, при этом транзакции будут иметь один зашифрованный вход и два выхода: один незашифрованный выход, представляющий снятие средств, и зашифрованный выход "*change*", представляющий оставшиеся средства, которые могут быть использованы для последующих снятий.

Возникает естественный вопрос о том, как можно расширить эту конструкцию для поддержки Privacy Pools. Простое подключение ее к Privacy Pools "как есть" не является идеальным, поскольку граф транзакций не соответствует нашим интуитивным ожиданиям: если пользователь делает депозит в 10 монет, а затем тратит их в четырех последовательных снятиях 1 + 2 + 3 + 4 монет, то мы *хотим,* чтобы все четыре снятия рассматривались как имеющие первоначальный депозит в 10 монет в качестве источника.

Но в результате мы *получаем то,* что показано на рис. 7: первое снятие имеет в качестве источника депозит в 10 монет, но затем второе снятие имеет в качестве источника вывод сдачи в 9 монет, созданный первым снятием, и так далее. На практике это вызывает проблемы, поскольку требует от ASP проверки промежуточных депозитов и добавления их в свой набор ассоциаций.

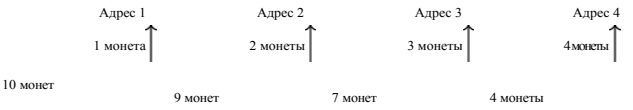


Рис. 7: На графике UTXO кажется, что источником каждого изъятия является изменение выхода предыдущего частичного изъятия. Но в экономическом смысле "реальным" источником в каждом случае является первоначальный депозит.

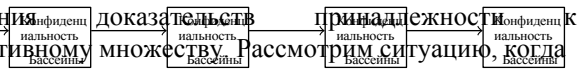
Если мы хотим, чтобы все четыре вывода средств в данном примере могли заявить о первоначальном депозите в 10 монет как о своем источнике, нам необходимо решить две проблемы одновременно: (i) убедиться, что каждый частичный вывод средств не связан публично с другими, и (ii) позволить каждому частичному выводу средств заявить о депозите как о члене своего набора ассоциаций.

Если мы поддерживаем только частичное снятие средств (а не более сложные транзакции с несколькими входами и несколькими выходами), гарантируя, что каждое снятие средств имеет один определенный соответствующий "первоначальный депозит", то существует множество способов, с помощью которых мы могли бы сделать это напрямую. Одним из естественных и очень расширяемых подходов является распространение некоторых обязательств в отношении информации через транзакции. Например, мы можем потребовать, чтобы транзакция содержала обязательство *hash*(*coinID*+*hash*(*r*)), добавив некоторое случайное значение *r* для слепоты, и потребовать от ZK-SNARK доказать, что обязательство в транзакции фиксирует то же значение, что и его родитель, если родитель сам является снятием, или просто фиксирует идентификатор монеты исходного депозита, если родитель является депозитом. В результате каждая транзакция в цепочке должна содержать обязательство по идентификатору монеты первоначального депозита, и это значение должно быть доказано в предоставленном наборе ассоциаций транзакции.

Для повышения конфиденциальности от атак, связанных с суммированием баланса (например, если я вношу 10 монет, а затем снимаю 7,2859, а потом 2,7141, то эти два снятия могут быть соотнесены только на основании сумм), мы, возможно, захотим также поддерживать *объединение монет*: если у меня осталось несколько монет, я могу объединить их со своим следующим вкладом. Чтобы адаптироваться к такому сценарию, мы можем потребовать, чтобы транзакция фиксировала *набор* идентификаторов монет, а транзакция с несколькими входами фиксировала *объединение* своих родителей. Вывод средств будет содержать доказательство того, что *все* зафиксированные идентификаторы монет находятся в его ассоциативном наборе.

B. Особые случаи

1) Повторное подтверждение: Для снятия депозита по протоколу, аналогичному Privacy Pools, пользователю необходима секретная информация о депозите. Эта же секретная информация затем используется для построения доказательств принадлежности к ассоциативному множеству. Рассмотрим ситуацию, когда



Алиса вывела свои средства, создала и опубликовала доказательство принадлежности к ассоциативному набору. Позже она захочет потратить свои средства у продавца, который потребует доказательства принадлежности к другому набору. Пока Алиса хранит свою секретную информацию, она сможет сгенерировать новое доказательство против ассоциативного набора продавца. Аналогичным образом Алиса может сгенерировать новое доказательство против обновленной версии исходного набора ассоциаций. Сохранение секретной информации дает Алисе большую гибкость, но может внести дополнительные риски.

Другой сценарий возникает в контексте расследования конкретного события. Предположим, что произошло некое нехорошее действие с монетами на цепочке, и первоначальное расследование выявило набор возможных входов, с которых могли поступить эти монеты. Это может быть связано с тем, что рассматриваемые монеты поступили от участника, чей набор ассоциаций представляет собой небольшое сообщество, или с сочетанием доказательств по цепочке и других доказательств, которые позволили получить частичную информацию о том, кто стоит за этим событием. В этом случае другие участники могут захотеть доказать свою непричастность к этому событию, чтобы доказать свою невиновность, и личность преступника будет раскрыта. В качестве альтернативы, если событие вызывает споры, но многие люди поддерживают его, даже если они сами не были виновны, они могут отказаться от такого доказательства.

2) Двусторонние прямые доказательства: В некоторых сценариях пользователю может потребоваться сообщить другой стороне точное происхождение снятых им средств. Например, если Алиса хочет положить снятые средства на депозит в банк, то банк может запросить полную информацию о происхождении средств. В ответ Алиса может создать ассоциативный набор, содержащий только ее депозит, и построить доказательство против этого набора. Мы ожидаем, что такие доказательства будут исключением, и они будут способствовать частичной конфиденциальности только при двустороннем обмене информацией. Более того, передача такого доказательства предполагает сильное доверие к получателю, который не будет распространять его дальше.

Другой, более продвинутый вариант: Алиса с нулевым знанием доказывает, что одно из следующих утверждений истинно:
(i) "это снятие находится в этом ассоциативном наборе", или (ii) "я - банк", или (iii) "по данным этого конкретного сервиса временной метки (это может быть сервер или блокчейн), с момента создания этого доказательства прошло более 10 секунд". Только банк, получивший доказательство в реальном времени (iii) и знающий, что он не создавал его самостоятельно (ii), сможет доверять доказательству: если доказательство попадет в чужие руки, то убедить получателя в том, что доказательство не подделано, будет сложно. Таким образом, устраняется большая часть риска, связанного с утечкой конфиденциальной информации.

3) Последовательные доказательства: Давайте представим себе более долгосрочный сценарий будущего, в котором системы, подобные Privacy Pools, будут использоваться не просто время от времени, а *в подавляющем большинстве транзакций*. Именно к такому миру стремятся первые системы обеспечения конфиденциальности, такие как Zcash. При этом возникают некоторые новые сложности, которые не проявляются в мире, где Privacy Pools используется эпизодически.

Для адаптации к такому миру потребуется следующая модификация протокола: Наряду с транзакциями ввода и вывода средств, протокол должен поддерживать *внутреннюю* операцию *отправки,* которая потребляет существующий идентификатор монеты и генерирует новый идентификатор монеты, принадлежащий другому лицу. С точки зрения анализа протокола это эквивалентно тому, что отправитель выводит средства на адрес получателя, а затем получатель немедленно переводит их обратно, но при этом повышается эффективность за счет сокращения количества шагов и доказательств на цепи с двух до одного.

Предположим, что Алиса отправляет монету Бобу; то есть она выполняет внутреннюю отправку, которая (возможно, частично) расходует идентификатор монеты, принадлежащий Алисе, и создает новый идентификатор монеты с параметрами, предоставленными Бобом. Затем Боб хочет немедленно потратить монету, отправив ее Карлу, и он предпочел бы, чтобы его транзакция по расходованию средств также была приватной. Здесь возникает наша проблема: *задержки включения*. Во многих конфигурациях, предложенных нами выше, ASP не захотят сразу же добавлять новую монету Боба в свой набор ассоциаций, поскольку им необходимо следить за возможностью того, что источником средств является не Алиса, а кто-то, кто только что украл средства из кошелька Алисы. Задержка с включением нужна для того, чтобы дать Алисе время сообщить об инциденте, а третьим лицам - обнаружить его.

Другим аналогичным примером может быть следующий: "Алиса" - это протокол DeFi, а Боб хочет вывести средства из протокола DeFi и немедленно использовать их для частного платежа Карлу. В этом сценарии на одного человека меньше, но в остальном он очень похож.

В условиях быстро меняющейся экономики одни и те же средства могут перемещаться несколько раз в неделю или даже чаще, и задержки при включении будут представлять серьезную проблему. Одно из возможных решений этой проблемы может заключаться в том, что в случае, если в кошельке пользователя нет монет, достаточно "зрелых" для включения в набор ассоциаций, пользователь может просто отправить их через транзакцию, не сохраняющую конфиденциальность. Однако мы предлагаем другой вариант, при котором утечка информации будет меньше.

Когда Боб платит Карлу, Боб также напрямую передает Карлу ветвь Меркла и секрет, которые были использованы для генерации платежа. Это позволяет Карлу видеть то, что видит Боб: что платеж от Алисы был в истории монеты. Если впоследствии выяснится, что большое количество монет, связанных с каким-либо недобросовестным участником, было размещено и быстро рециркулировало, Карл сможет доказать, что его монеты поступили из конечного источника, не связанного с недобросовестным участником.

Если Карл затем отправит монеты Дэвиду, то он передаст ветвь Меркла и секрет от Боба, а также добавит свой собственный. Теперь предположим, что Дэвид отправляет свои монеты Эмме, но к тому моменту, когда он это делает, в ассоциативный набор уже добавлен вклад, сделанный Алисой. Тогда Дэвиду уже не нужно предоставлять ветвь Меркла и секрет от Алисы; вместо этого он может просто сгенерировать доказательство принадлежности к набору ассоциаций от имени Алисы. После того как платеж Боба будет добавлен в набор ассоциаций, ветвь и секрет Меркла Боба аналогичным образом

устаревают. Концепция заключается в том, чтобы каждый пользователь получал только основную и минимальную информацию, необходимую для того, чтобы быть уверенным в получаемых им средствах. Рисунок 8 иллюстрирует этот пример.

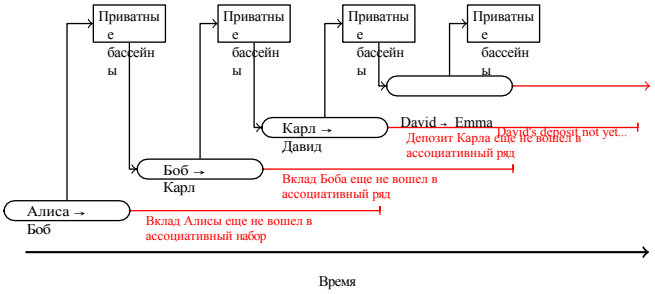


Рис. 8: Когда Дэвид отправляет свою транзакцию Эмме, ему необходимо предоставить ветвь Меркла и секрет от себя, Карла и Боба, но не от Алисы, поскольку платеж Алисы Бобу теперь находится в ассоциативном множестве.

На практике у одной монеты может быть несколько "источников". Возможно, Боб - продавец кофе, он получил 5 монет от Алисы, 4 монеты от Эшли и 7 монет от Анны, и в конце дня ему нужно отправить 15 монет Карлу, чтобы заплатить за ужин. Дэвид, в свою очередь, возможно, получил 15 монет от Карла, еще 25 монет от Криса и хочет отдать 30 монет Эмме, которая является обменщицей. В этих более сложных случаях мы следуем тому же принципу: историю, которая достаточно стара, чтобы ее добавили в наборы ассоциаций, можно игнорировать, а историю, которая была более свежей, необходимо передать дальше.

V. ДИСКУССИЯ

Системы, подобные Privacy Pools, позволяют пользователям добиться большей конфиденциальности данных о своих финансовых операциях, сохраняя при этом возможность доказать свою непричастность к известной противозаконной деятельности. Мы ожидаем, что добросовестные пользователи будут мотивированы к участию в такой схеме сочетанием двух факторов:
(i) стремление к конфиденциальности и (ii) желание избежать подозрений.

A. Общественный консенсус и наборы ассоциаций

Если существует идеальный консенсус относительно того, какие средства являются "хорошими", а какие "плохими", то система приведет к простому сепаратному равновесию. Все пользователи с "хорошими" активами имеют сильные стимулы и возможность доказать свою принадлежность к набору ассоциаций, состоящему только из "хороших". Плохие участники, напротив, не смогут предоставить такое доказательство. Они все равно смогут внести "плохие" средства в пул, но это не даст им никаких преимуществ. Каждый сможет легко определить, что средства были выведены из протокола, повышающего конфиденциальность, и увидеть, что при выводе средств используется набор ассоциаций, включающий вклады из сомнительных источников. Более того, "плохие" средства не запятнали бы "хорошие". При выводе средств с законных вкладов их владелец может просто исключить все известные "плохие" вклады из своего набора ассоциаций.

В тех случаях, когда глобального консенсуса не существует, а вывод о том, воспринимаются ли фонды как "хорошие" или "плохие", зависит от точки зрения общества или юрисдикции, наборы ассоциаций могут существенно различаться. Предположим, что существуют две юрисдикции с различными наборами правил. Субъекты юрисдикций *A* и *B* могли бы использовать один и тот же протокол, повышающий конфиденциальность, и выбрать для выдачи доказательство, удовлетворяющее требованиям их соответствующей юрисдикции. Оба субъекта могут легко достичь конфиденциальности в рамках своего набора ассоциаций и исключить снятие средств, не соответствующее требованиям соответствующей юрисдикции. При необходимости можно выдать доказательство членства на пересечении обоих наборов ассоциаций и тем самым убедительно продемонстрировать, что депозит, соответствующий его снятию, соответствует требованиям обеих юрисдикций.

Таким образом, предложение является очень гибким и должно рассматриваться как нейтральная инфраструктура. С одной стороны, оно устойчиво к цензуре. Она позволяет любому человеку присоединиться к выбранному им набору ассоциаций и оставаться частным лицом в своем собственном сообществе. С другой стороны, посторонние лица могут запросить подтверждение соответствия конкретных наборов ассоциаций нормативным требованиям. Таким образом, даже если бы внутри протокола, повышающего приватность, существовало сообщество недобросовестных участников, они не смогли бы завуалировать сомнительный источник вклада, если бы эта информация была точно отражена при построении ассоциативного набора.

B. Свойства набора ассоциаций

Для того чтобы ассоциативные наборы были эффективными, они должны обладать определенными свойствами. Наборы должны быть *точными,* чтобы пользователи могли быть уверены в том, что они могут безопасно расходовать свои средства после их снятия. Кроме того, свойства каждого набора должны быть *стабильными*, т.е. маловероятно, что они изменятся со временем. Это ограничивает необходимость повторного подтверждения снятия средств с помощью новых наборов. Наконец, для достижения значимой конфиденциальности важно, чтобы ассоциативный набор был достаточно *большим* и включал в себя широкий спектр вкладов. Однако эти характеристики противоречат друг другу. В общем случае большие и разнообразные наборы могут обладать лучшими свойствами конфиденциальности, но, скорее всего, будут менее точными и стабильными, в то время как меньшие наборы легче поддерживать, но они обеспечивают меньшую конфиденциальность.

C. Практические соображения и конкуренция

Регулируемые организации, принимающие криптоактивы, должны убедиться, что законы и нормативные акты, которым они подчиняются, разрешают прием таких средств. Сегодня многие из таких организаций используют так называемые *инструменты скрининга транзакций*: программное обеспечение или сервис, анализирующий блокчейн для выявления потенциально подозрительной активности, связей с незаконными адресами или других несоответствующих требованиям транзакций. Как правило, инструменты скрининга выражают риск, связанный с каждой транзакцией, в виде оценки риска. Этот показатель основан на назначении передаваемых средств и истории их транзакций. Протоколы, повышающие конфиденциальность, могут представлять определенную сложность в этом отношении. Они устраняют видимую связь между вкладами и изъятиями. Таким образом, при наличии

протокола, повышающего конфиденциальность, оценка риска должна учитывать доказательства и присваивать балл на основе набора ассоциаций.

Инструменты и услуги для проверки транзакций в основном предоставляются специализированными компаниями, обладающими опытом как в анализе блокчейна, так и в соответствующих юридических областях. В идеале эти компании (как и все остальные) должны иметь доступ ко всем доказательствам членства и соответствующим наборам ассоциаций, чтобы обеспечить ак-куратную оценку рисков по всем транзакциям. Поэтому мы предлагаем хранить все доказательства на блокчейне или в другом общедоступном хранилище доказательств. Исключение составляют доказательства членства размером 1, которые передаются конкретному контрагенту. По понятным причинам эти доказательства не должны находиться в открытом доступе.

Наличие доказательств в свободном доступе на цепочке влечет за собой дополнительные транзакционные издержки, но снижает усилия по координации, выравнивает условия игры и уменьшает риск того, что поставщики инструментов проверки могут иметь квазимонополию благодаря знанию непубличных доказательств.

Общая настройка Privacy Pools очень гибкая. Создавая специальные наборы ассоциаций, можно адаптировать протокол к самым разным условиям использования. Приведем два примера таких специализированных наборов ассоциаций: (i) Консорциум коммерческих банков может создать набор ассоциаций, включающий только депозиты своих клиентов. Это гарантирует, что любой вывод средств, создающий доказательство против этого набора, прошел процедуру "Знай своего клиента" (KYC) и "Отмывание денег" (AML) в одном из банков-участников, но не раскрывает, какой вывод принадлежит тому или иному клиенту. (ii) В случаях, когда финансовому посреднику необходимо документально подтвердить точный источник средств, он может запросить у пользователя доказательство против ассоциативного набора, включающего только депозит пользователя. Эти доказательства затем обмениваются с посредником на двусторонней основе, что позволяет ему отслеживать средства так, как будто пользователь никогда не использовал Privacy Pools. Хотя это требует от пользователя уверенности в том, что посредник не раскроет доказательства, в идеале это позволяет пользователю соблюдать требования законодательства, не раскрывая информацию широкой общественности.

D. Варианты и альтернативы проектирования

Система, основанная на ассоциативных наборах, zk-доказательствах и добровольном раскрытии информации, является очень гибкой. И хотя это замечательно, поскольку предложение может быть адаптировано к различным юрисдикциям, следует быть очень осторожным в выборе конкретной конструкции. В частности, есть две потенциальные корректировки, против которых мы выступаем. Мы считаем, что они проблематичны с точки зрения требований к доверию и могут породить квазимонополистические рыночные структуры.

Далее мы кратко опишем и обсудим эти альтернативные подходы:

1) *Централизованный доступ*: доступ могут получить правоохранительные органы, провайдеры скоринга криптописков или другие подобные субъекты

видеть связи между транзакциями пользователя, оставаясь при этом конфиденциальными для всех остальных.

2) *Общесистемный разрешительный список*: система конфиденциальности может накладывать ограничения на то, какие пользователи могут вносить монеты в ее пул, либо требуя от них предоставления дополнительного доказательства, либо требуя от них выждать некоторый период времени, в течение которого централизованная система оценки рисков может отклонить вклад.

Оба подхода весьма схожи в том смысле, что предоставляют особые привилегии конкретным организациям. Это приводит к возникновению сложных вопросов управления: Кто получает доступ к этой информации? Кто имеет право управлять разрешениями?

Частные фирмы не представляются хорошим вариантом, поскольку любые специальные привилегии, скорее всего, приведут к возникновению олигополистических рыночных структур, когда несколько фирм будут иметь доступ к данным, позволяющим им предоставлять эти услуги, а все остальные не смогут конкурировать.

Аналогичным образом, в случае предоставления таких полномочий государственным учреждениям, особенно в международном контексте, возникнет множество вопросов, связанных с управлением и политикой. Даже если "ключ с черного хода" будет предоставлен организации, которая сегодня на 100% заслуживает доверия, не злоупотребляет этими полномочиями в политических целях и не зависит от других организаций, которые могли бы оказать на нее давление с целью злоупотребления ее полномочиями, было бы наивно полагать, что это статичная игра. Организации, их члены, национальные государства и политические структуры внутри организации меняются с течением времени. Возможно давление извне, и существование особых привилегий может создавать дополнительные стимулы для недобросовестных субъектов к подрыву и получению влияния на систему управления организацией.

Более того, атака изнутри или извне организации, или ошибка представителя централизованной структуры могут иметь далеко идущие последствия. Мы считаем, что создание такой центральной точки отказа должно быть предотвращено.

При этом мы признаем, что различные размеры транзакций и ситуации могут потребовать различных комбинаций доказательств. Например, для крупных транзакций многие пользователи, скорее всего, будут предоставлять базовое доказательство исключения на цепочке и дополнительно предоставлять контрагенту более подробную информацию об источнике.

E. Потенциал дальнейших исследований

Хотя данное исследование дает представление о том, как протоколы повышения конфиденциальности на основе zkSNARK могут быть использованы в регулируемой среде, есть несколько областей, которые требуют дальнейшего изучения.

Во-первых, важно понимать, что конфиденциальность, достигаемая с помощью этих протоколов, зависит от множества различных факторов. Недостаточно большие наборы ассоциаций, неправильный выбор корня, ошибки пользователей могут позволить злоумышленнику связать снятие средств с конкретным вкладом. Кроме того, выбор других пользователей может негативно повлиять на вашу конфиденциальность. В крайнем случае

В этом случае все остальные участники пула опубликовали бы доказательство своего членства размером 1, раскрыв прямую связь между своими депозитами и снятиями. Очевидно, что это неявно раскрывает связь между единственными оставшимися транзакциями ввода и вывода средств. В более тонком примере ограничения из различных доказательств членства могут быть использованы для извлечения информации и потенциальной связи между депозитами и изъятиями с высокой вероятностью. Как только информация из этих доказательств будет объединена с метаданными транзакций, свойства конфиденциальности протокола могут быть нарушены. И, наконец, злоумышленник может составить предложенные наборы ассоциаций таким образом, чтобы максимизировать извлекаемую информацию или повысить кажущуюся анонимность, добавив депозиты, для которых известны соответствующие снятия. Все эти вопросы требуют дальнейших исследований для оценки обеспечиваемых свойств конфиденциальности. Аналогичным образом было бы интересно продолжить изучение свойств разделяющего равновесия, смоделировать поведение хороших и плохих игроков при определенных предположениях и то, как *публичные* доказательства первых повлияют на конфиденциальность вторых. Наконец, ученые-юристы могли бы продолжить изучение конкретных требований к раскрытию информации. Предложение, описанное в данной статье, является весьма адаптируемым, и мнение специалистов в области права может помочь в адаптации протокола и экосистемы вокруг него для обеспечения соответствия требованиям различных правовых юрисдикций.

VI. ЗАКЛЮЧЕНИЕ

Во многих случаях конфиденциальность и соответствие нормативным требованиям воспринимаются как несовместимые понятия. В данной работе предполагается, что это не обязательно так, если протокол, повышающий конфиденциальность, позволяет своим пользователям доказать определенные свойства происхождения их средств. Например, предположим, что пользователи могут доказать, что их средства не связаны с вкладами из известных незаконных источников, или доказать, что средства являются частью определенного набора вкладов, не раскрывая при этом никакой дополнительной информации.

Такая ситуация может привести к возникновению разделительного равновесия, когда честные пользователи будут сильно заинтересованы в том, чтобы доказать принадлежность к заданному, соответствующему требованиям набору ассоциаций, сохраняя при этом конфиденциальность внутри этого набора. И наоборот, для недобросовестных пользователей такое доказательство невозможно. Это позволяет честным пользователям отмежеваться от вкладов третьих лиц, с которыми они не согласны или которые могут помешать им использовать свои средства в регулируемой среде. Мы утверждаем, что данное предложение является достаточно гибким и может быть адаптировано для потенциального удовлетворения большого количества нормативных требований.

Этот документ следует рассматривать как скромный вклад в возможное будущее, в котором финансовая конфиденциальность и регулирование могут сосуществовать. Мы хотим стимулировать дискуссию и направить ее в более позитивное и конструктивное русло. Для расширения и модификации данного предложения потребуется сотрудничество между практиками, учеными из различных областей, политиками и регулирующими органами, а конечной целью является создание

инфраструктура, повышающая уровень конфиденциальности, которая может быть использована в регулируемой среде.

Благодарность

Особая благодарность Митчеллу Голдбергу, Катрин Шулер и Дарио Туэркауфу за ценный вклад, Эмме Литтлджон за корректуру и Дарио Туэркауфу за помощь в создании графического дизайна.

ССЫЛКИ

[1] М. Надлер и Ф. Шаер, "Tornado cash и конфиденциальность блокчейна: A primer for economists and policymakers," *Federal Reserve Bank of St. Louis Review*, vol. 105, no. 2, pp. 122-136, 2023.

[2] A. Soleimani, "Privacy pools", 2023, репозиторий gitHub. [Онлайн]. Доступно: https://github.com/ameensol/privacy-pools

[3] S. Накамото, "Биткойн: одноранговая система электронных денег", 2008 г. [Online]. Доступно: https://bitcoin.org/bitcoin.pdf.

[4] S. Meiklejohn *и др.*, "Куча биткоинов: Характеристика платежей среди людей без имен", 2013 г. [Online]. Доступно: https: //cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf

[5] C. Канг *и др.*, "Деанонимизация сети биткойн с помощью кластеризации адресов", 2020 г. [Online]. Доступно: http://dpnm.postech.ac.kr/papers/ Blocksys/changhoon blocksys2020.pdf

[6] "Сервис имен Ethereum, децентрализованный нейминг для кошельков, сайтов и , 2023". [Online]. Доступно: https://ens.domains/.

[7] Г. Максвелл, "Coinjoin: Конфиденциальность биткойна для реального мира", 2013 г., дата обращения: август: 22 августа. [Online]. Доступно: https://bitcointalk.org/?topic= 279249.

[8] J. Liu *et al.*, "Linkable spontaneous anonymous group signature for ad hoc groups", 2004 г. [Online]. Доступно: https://eprint.iacr.org/2004/027. pdf

[9] B. Гуделл *и др.*, "Concise linkable ring signatures and forgery against adversarial keys", 2019 г. [Online]. Доступно: https://eprint.iacr.org/2019/ 654

[10] M. Мозер *и др.*, "Эмпирический анализ прослеживаемости в блокчейне monero ", 2018 г. [Online]. Available: https://arxiv.org/pdf/1704.04299/

[11] "Zcash", 2023 г. [Online]. Доступно: https://z.cash/

[12] V. Бутерин, "Неполное руководство по роллапам", 2021 г. [Online]. Доступно: https://vitalik.ca/general/2021/01/05/rollup.html

[13] M. Petkus, "Why and how zk-snark works", *CoRR*, vol. abs/1906.07221, 2019. [Online]. Available: http://arxiv.org/abs/1906.07221

[14] A. Беренцен, Дж. Ленци и Р. Ниффенеггер, "Введение в доказательства нулевого знания в блокчейн и экономику", *Обзор Федерального резервного банка Сент-Луиса*, № готовится к публикации, 2023 г. [Online]. Доступно: https://research.stlouisfed.org/publications/review/2023/05/12/. an-introduction-to-zero-knowledge-proofs-in-blockchains-and-economics