Insights Network

- Обмен данными блокчейн
29 сентября 2017 (v0.5)

Брайан Галлахер
Insights Network
bg@insights.network

Дарвин Ло
Insights Network
darwin@insights.network

Питер Фрэндс Франдсен
Partisia
pff@partisia.com

Джаспер Бьюс Нильсен
Partisia
jbn@partisia.com

Курт Нильсен
Partisia
kn@partisia.com

Аннотация

В настоящее время брокеры данных собирают информацию о людях по всему миру из самых разных источников, как онлайн, так и оффлайн. Данные упаковываются в профили, а затем продаются организациям, которые могут использовать их для принятия решений, влияющих на жизнь простых людей без их ведома. Недавние технологические достижения, такие как блокчейн и безопасное многопартийное вычисление, позволяют создать превосходную платформу для проведения маркетинговых исследований, одновременно контролируя и помещая монетизацию данных в руки людей, которые их и генерируют.

info@insights.network

Содержание

info@insights.network

1 Основная информация

Ничто в настоящем документе не представляет собой предложение о продаже или настаивание на предложении о покупке, не содержит никаких предложений, приглашений или продажи INSTAR токенов Insights Network в любой юрисдикции, в которой такое предложение, ходатайство или продажа были бы незаконными. Вы должны внимательно прочитать и полностью понять этот технический документ и любые обновления. Каждый потенциальный покупатель токенов должен будет пройти процесс «посадки», который включает проверку личности и другую определенную документацию, которую вы должны внимательно прочитать и понять полностью, потому что вы будете юридически связаны. Обязательно проконсультируйтесь с соответствующими экспертами и другими лицами.

В этом техническом документе описывается наше видение платформы Insights Network на данный момент. Хотя мы намерены попытаться реализовать это видение, примите к сведению, что оно зависит от целого ряда факторов и подвержено большому количеству рисков. Вполне возможно, что платформа Insights Network никогда не будет реализована или принята, или что будет реализована только часть нашего видения. Мы не гарантируем каких-либо заявлений в этом техническом документе, поскольку они основаны на наших нынешних убеждениях, ожиданиях и предположениях, о которых не может быть никакой уверенности в связи с различными предвиденными и непредвиденными событиями, которые могут произойти.

Пожалуйста, знайте, что мы планируем много работать над тем, чтобы достичь видения, изложенного в этом техническом документе, но вы не можете полагаться на что-либо из этого. Блокчейн, криптовалюты и другие аспекты нашей технологии и эти рынки находятся в зачаточном состоянии и будут подвержены множеству проблем, конкуренции и изменяющейся среде. Мы попытаемся обновлять наше сообщество по мере того, как все будет расти и изменяться, но не берем на себя никаких обязательств.

2 Предыстория

2.1 Проблема

Существуют организации, называемые брокерами данных, которые собирают информацию о людях из разных источников, как онлайн, так и оффлайн. В первую очередь, они покупают данные из интернет-сервисов и мобильных приложений, которые собирают информацию о своих пользователях и отслеживают их поведение в приложении.

Данные используются для создания профилей на отдельных потребителей. Acxiom, ведущий брокер данных, имеет в среднем 1500 экземпляров информации о более чем 200 миллионах американцев. Acxiom и другие брокеры данных могут объединять всю информацию, имеющуюся у каждого из них, для создания подробных отчетов о поведении потребителей в широком спектре отраслей.

Брокеры данных зарабатывают много денег. В 2012 году Acxiom, как сообщается, сделал 1,13 миллиарда долларов на продажах, получив прибыль в размере 77,26 миллиона долларов. Форбс сообщает, что индустрия большой аналитики данных получает 200 миллиардов долларов в год, и к 2019 году почти все компании будут клиентами брокеров данных, таких как Acxiom. Но потребители, которые фактически управляют промышленностью, не получают прибыли.

В результате потребители только испытывают на себе множество негативных последствий. Централизованно-управляемые базы данных дают возможность хакерам украсть большое количество персонально идентифицирующей информации всего за одну атаку, что позволяет широко использовать кражи личных данных и мошенничество. Недавно хакеры нарушили системы Equifax и похитили личные данные более чем 140 миллионов американцев. Это не отдельный случай. В прошлом было несколько атак, в том числе на Acxiom, и если их не остановить, в будущем таких атак будет больше.

Потребители должны требовать новый стандарт хранения личной и конфиденциальной информации, которая используется в исследованиях рынка. В настоящее время это осуществляется в GDPR по всей Европе, и вскоре США последуют этому примеру.

2.2 Решение

Недавние достижения в области децентрализованного хранения, цифровых валют и умных контрактов позволяют нам создать децентрализованную, стимулируемую платформу для проведения маркетинговых исследований и безопасного хранения потребительских данных. Организации смогут использовать нашу платформу для запроса данных от точно определенных групп населения среди членов Insights Network.

Пользователи Insights Network, а не брокеры, будут продавать свои данные. Используя умные контракты, которые выполняют транзакции между анонимными сторонами, пользователи смогут продавать свои данные, не раскрывая свою личность, а только общую демографическую информацию. Уникальная комбинация блокчейна и безопасного многопартийного вычисления (SMC) позволяет обеспечить обмен данными

и оплатой между поставщиком и запросчиком без участия третьей стороны. В то время как блокчейн делает обмен прозрачным, SMC сохраняет данные по-настоящему безопасными до тех пор, пока соглашение не будет достигнуто и оплачено. Мы считаем, что, позволяя участникам получать прибыль от своего участия, организации получат данные, которые в результате станут более актуальными и более эффективными. В то же время прибыль, получаемая в настоящее время брокерами, вместо этого перейдет к законным владельцам данных - потребителям.

3 Наш продукт

3.1 Обзор

В первую очередь, мы обслуживаем двух типов пользователей: тех, кто запрашивает данные, кого мы называем ззапросчиками, и тех, кто их предоставляет, кого мы называем поставщиками. Запросчиками обычно являются организации, но каждый может покупать токены INSTAR и использовать их для отправки запроса на данные в Insights Network. Поставщики - это пользователи, которые выполняют запрос, предоставляя данные; те, кто соответствует запросу демографических данных, получают компенсацию за свои данные в токенах INSTAR.

Запросчики хотят иметь возможность собирать данные, которые:
• **Релевантные.** Они хотят иметь возможность собирать данные от конкретных групп населения, например, только тех, чей возраст от 20 до 35 лет.
• **Надежные.** Собранные данные не содержат обмана. То есть данные собираются от определенных поставщиков, которые честно предоставили свою информацию. К примеру, запросчики, ожидают честных ответов в опросах от их целевой аудитории, а не ботов.
• **Своевременные и удобные.** Запросчики должны иметь возможность быстро получить ответы на свои вопросы, не беспокоясь о деталях того, как достичь своей целевой аудитории.

Поставщики хотят убедиться в следующем:
• **Согласие.** Их данные не собираются без явного разрешения.
• **Конфиденциальность.** Слишком личная информация, например, их личность, не предоставляется, а только общие демографические детали.
• **Оплата.** Поставщики получают оплату за предоставленные данные.
• **Безопасность.** Их данные обрабатываются безопасно.

Традиционные маркетинговые исследовательские фирмы собирают данные за определенный период времени и предоставляют единый отчет своим клиентам. На нашей платформе запросчикам никогда не придется закрывать запрос на данные. Их отчеты, которые они смогут просмотреть в любой момент во время сбора данных, обновляются, поскольку данные от поставщиков принимаются и пересылаются по умному контракту.

По мере того, как в нашей сети доступно больше информации, данные, доступные для запросчиков через платформу, становятся более всеобъемлющими, что, в свою очередь, дает возможность разрабатывать более полные отчеты, в том числе те, которые объединяют данные из нескольких запросов. Вот несколько примеров того, как можно использовать Insights Network:
• Исследовательская фирма может захотеть провести опрос чтобы узнать, кто победит, если президентские выборы будут повторно запущены в этот момент времени.

• Макдональдс может захотеть запустить опрос, чтобы получить обратную связь по новому пункту меню.
• Университеты могут проводить опросы в течении квартала или семестра, чтобы получать обратную связь о качестве обучения на постоянной основе.
• Высокоуровневый аукцион может принимать анонимные заявки от проверенных лиц без необходимости в KYC.

Родственная группа вариантов использования адресует так называемую асимметричную информацию путем профилирования индивидуумов и компаний. Финансовым примером может быть кредитор, который меньше знает о способности заемщика погасить кредит, чем заемщик. Это может привести к повышению процентных ставок к заемщику взамен компенсации ожидаемого риска. Решением этой проблемы является информация, которая позволяет профилировать как можно больше отдельных лиц и компаний для разделения, например, заемщиков с низким уровнем риска и заемщиков с высоким. Аналогичные проблемы возникают в страховом бизнесе, где страховая компания знает мало о профиле застрахованных сторон. Другим примером является дифференциация продукта, когда поставщику не хватает информации о предпочтениях клиентов, чтобы определить наиболее подходящее меню продуктов или контрактов. Одним из примеров последнего вида может быть проблема разработки правильного меню мобильных подписок в отношении цены, данных и т. д.

Insights Network предоставляет платформу, которая позволяет отдельному человеку или компании сотрудничать с, например, банками и страховыми компаниями для решения этой проблемы на равных условиях. Insights Network может стать уникальным источником информации для профилирования физических лиц и компаний.

3.2 Функциональность

Insights Network - это безопасная инфраструктура для децентрализованного обмена данными, которая имеет множество различных приложений. Вначале мы сосредоточимся на опросах, но она также станет основой для других приложений, таких как схемы роялти, рекламные объявления и схемы лояльности.

Insights Network состоит из следующих компонентов:
• Аутентификация
• Профили пользователей
• Децентрализованное посредничество данных
• Опросы
• Двустороннее оценивание

Запросчик - это пользователь, который помещает запрос в Insights Network для получения информации от определенной группы пользователей. Поставщики - это пользователи, которые выполняют такой запрос.

3.2.1 Аутентификация

Обычная практика среди приложений сегодня - возможность для пользователей войти в систему, используя свою учетную запись Facebook. Мы создаем аналогичную услугу для приложений, чтобы дать возможность своим пользователям входить в систему, используя свою учетную запись Insights Network. Эта функция понравится пользователям, которые не хотят раскрывать свою личность в приложениях. В качестве дополнительного преимущества приложения могут использовать сеть Insights Network для предоставления токенов своим пользователям в рамках программы

вознаграждения и позволят им начислять токены в качестве таких выгод как мили авиакомпаний.

Аутентификация выполняется конфиденциально с помощью SMC.

3.2.2 Профили пользователей

Пользователи поддерживают свой профиль в сети Insights Network. Они могут просматривать свой профиль, который содержит демографическую информацию и другую общую, не идентифицирующую информацию. Они могут вносить исправления, заполнять отсутствующие данные и удалять информацию. Кроме удаления информации, для выполнения других действий используются токены INSTAR.

Например, 25-летняя женщина, проживающая в Лос-Анджелесе, может захотеть получать рекламу, связанную с ее политическими интересами, поэтому она может предпочесть сохранить линию, которая указывает, что она республиканка. Но она, возможно, не захочет получать опросы в отношении матери-одиночки, поэтому она удалит эту линию. Она также может видеть, что ее профессия неизвестна, и она может захотеть заполнить эту линию в обмен на токены INSTAR.

Профили пользователей сохраняются конфиденциальными либо на стороне клиента, либо с помощью SMC.

3.2.3 Децентрализованное посредничество данных

Основная цель Insights Network - обеспечить децентрализованный обмен данными между поставщиками и запросчиками, который состоит из:
- Сопоставления профилей поставщиков с запросом
- Безопасной передачи данных
- Безопасной оплаты

Подлежащие обмену данные первоначально представляют собой опрос, состоящий из соответствующей исходной информации и ответов, предоставленных пользователем на вопросник. Уникальная комбинация блокчейна и SMC обеспечивает обмен конфиденциальной информацией и платежами без участия третьих сторон.

3.2.4 Опросы

Любой, кто находится в сети Insights Network, независимо от того, является он физическим лицом или организацией, может опубликовать опрос на платформе. Платформа дает возможность указать целевую аудиторию, а также то, сколько токенов пользователи в целевой аудитории получат, когда они отправят правдивый и действительный ответ. Процесс выглядит следующим образом:
1. Запросчик публикует опрос с указанием целевой аудитории.
2. Пользователи нашего приложения, которые соответствуют интересующей запросчика целевой аудитории, получают уведомление.
3. Пользователи заполняют опрос, предоставляют его в Insights Network, и средства перечисляются на их счет.

3.2.5 Двустороннее оценивание

Во избежание нежелательного поведения Insights Network реализует систему двустороннего оценивания, в соответствии с которой запросчик может оценивать поставщиков и наоборот.

В качестве поставщика возможно злоупотребление системой и отправка неправдивых данных. Проявления нежелательного поведения могут быть обнаружены запрочиком при анализе данных. Предоставление запросчикам возможности оценивать провайдеров будет противодействовать такому поведению.

Запросчики могут использовать данные вне согласованной цели. Такое нежелательное поведение может быть обнаружено поставщиком, поскольку публикуются окончательные отчеты. Предоставление поставщику возможности оценивать запросчиков, будет противодействовать такому поведению.

Такое децентрализованное регулирование нежелательного поведения посредством двухстороннего оценивания известно благодаря таким сервисами, как Uber и Airbnb.

3.2.6 Пример: Gambeal

Gambeal - приложение для iOS, которое отправляет опросы посетителям ресторанов быстрого питания, выплачивая небольшую денежную награду за каждый опрос, который они заполняют. Чтобы доказать посещение ресторана, каждый пользователь должен приложить фотографию своего чека вместе с каждой заявкой, которая проверяется до выдачи вознаграждений. Gambeal значительно вырос без каких-либо преднамеренных маркетинговых усилий и обрабатывает тысячи транзакций каждую неделю. Это будет первое партнерское приложение Insights Network, и его успех пока служит хорошим предзнаменованием для других партнерских приложений.

В рамках интеграции с Insights Network Gambeal поменяет систему аутентификации на систему на основе SMC, которая позволит пользователям входить в систему, не раскрывая своей личности как, например, при входе с Facebook. В приложение входят только общие демографические данные, и благодаря тому что оно является частью сети Insights Network, пользователь может монетизировать свои данные по своему усмотрению.

Кроме того, Gambeal переключится с денежных вознаграждений на токен INSTAR, используя API универсального протокола Mobius для интеграции. В настоящее время Gambeal использует PayPal для осуществления платежей пользователям, что заставляет их ждать дни, пока деньги поступят в учетную запись PayPal, а также пользователи вынуждены платить до 3% комиссии в транзакционных сборах. Помимо обеспечения лучшей конфиденциальности, использование Insights Network позволит Gambeal быстро и недорого обрабатывать транзакции своих пользователей. Интеграция с сетью Insights Network для аутентификации и выплаты вознаграждений представляет собой явное улучшение для пользователей.

3.3 Технические проблемы

Существует немало проблем, которые необходимо решить. Следующие функции Insights Network позволяют создавать и выполнять запросы:
• **Проверка подлинности.** Поставщики доказывают, что они настоящие люди путем аутентификации с помощью нескольких партнеров по проверке, таких как компании,

проверяющие документацию на удостоверение личности, службы, выполняющие проверку анкетных данных, или даже работодатель поставщика, и получают цифровую проверку подлинности от Insights Network, которую они могут использовать для подтверждения подлинности в транзакциях с запросчиками. Используя методы из распределенной криптографии, партнеры по проверке никогда не передают своею информацию никакой другой стороне, сохраняя конфиденциальность поставщиков, а поставщики получают компенсацию в токенах для прохождения этого процесса.
• **Интенсифицированное исследование рынка**. Запросчики могут публиковать опросы и получать ответы на них, используя умный контракт Insights Network. Умный контракт отправляет токены поставщикам из целевой аудитории, которые предоставили действительный элемент данных.
• **Проверяемые с помощью блокчейна результаты**. По усмотрению запросчика элементы данных из запроса могут быть записаны в регистр для общего обозрения. Поскольку регистр выполняется с использованием блокчейна, любой, кто смотрит на эти записи, будет иметь уверенность в том, что элементы данных не были подделаны. Эта функция важна для определенных видов запросов, таких как опросы и голосования. При необходимости данные могут быть зашифрованы с использованием информационно-теоретически безопасного шифрования на блокчейн.
• **Семантическая проверка частных данных.** Без привлечения третьей стороны поставщик сможет удержать данные до тех пор, пока не получит платеж от запросчика, а запросчик сможет удержать платеж до тех пор, пока действительность данных поставщика не будет подтверждена.

4 Технические решения

Двумя основными техническими компонентами нашего решения являются блокчейн и протоколы для выполнения безопасного многопартийного вычисления (SMC). Обе эти технологии используют распределенную криптографию для устранения необходимости поручать третьей стороне важную роль в выполнении транзакции; то есть они обе «ненадежны». В то же время две технологии обеспечивают дополнительные свойства: блокчейн - прозрачность транзакции, а SMC - конфиденциальность.

SMC инкубировалась в академических кругах более трех десятилетий. Ее использование в промышленности было ограничено из-за вычислительных затрат. Но в 2008 году компания в Дании, Partisia, впервые запустила коммерческое внедрение SMC, заменив традиционный аукцион на двойной. С тех пор производительность на порядок улучшилась и сейчас система начинает получать признание в промышленности.

Блокчейны начались с биткойна. Затем Ethereum ввел блокчейн, который поддерживал умные контракты. Мы делаем ставку на то, что EOS, который использует новый алгоритм блочного производства для достижения гораздо более высокой пропускной способности транзакции, чем у биткойна и Ethereum, станет следующим крупным блокчейном, и именно это мы и будем развивать.

Мы видим совместный выдающийся рост блокчейн и SMC. Более того, мы думаем, что их будут объединять через дополнительные черты, как делаем это мы в нашей системе. Вместе с нашими партнерами Partisia, которые помогают в разработке и внедрении нашей системы, мы считаем, что мы начинаем новую тенденцию в области «ненадежных» вычислений. В этом разделе мы расскажем о том, как мы планируем использовать SMC и блокчейн для решения проблем, изложенных в разделе 3.3.

4.1 Блокчейн

Блокчейн подразумевает внедрение защищенного от несанкционированного доступа публичного регистра. Состояние регистров определяется консенсусом между независимыми серверами, которые образуют сеть, называемую сетью блокчейн. Невозможно, чтобы один сервер или даже небольшая группа серверов, действующих в договоре, вмешивались в записи регистров, не будучи обнаруженными при этом другими серверами. До тех пор, пока в сети достаточно независимых серверов, совместимых с протоколами, регистр защищен от несанкционированного доступа.

В дополнение к ведению учета движения средств между счетами, блокчейны также способны вести учет изменений в состоянии программы. Программы, размещенные в сети блокчейн, называются умными контрактами или децентрализованными приложениями. В Insights Network используется блокчейн и умные контракты на базе блокчейн для протоколирования, сборки результатов безопасного многопартийного вычисления и перевода средств между учетными записями.

4.1.1 Блокчейн платформа EOS

Мы работаем на EOS, предстоящей операционной системе блокчейн. Хотя она еще и не выпущена, система быстро развивается, и даже во время написания этого документа, в настоящее время, мы строим локальный тестовый узел, а также страхуем наше развитие, одновременно создавая Ethereum. В этом разделе говорится, почему мы выбрали EOS.

До EOS Дэн Лаример, архитектор EOS, создал два успешных блокчейн проекта - Steemit и BitShares. Steemit - единственное блокчейн-приложение, которое обрабатывает действительную рабочую нагрузку в 17 000 активных пользователей ежедневно. Graphene, блокчейн, используемый в BitShares, показал, что он может обрабатывать по 20 000 транзакций в секунду в сети. Когда EOS будет выпущена, она будет иметь большую пропускную способность, чем любая из существующих сейчас действующих блокчейн сетей, что потребуется для того, чтобы справиться с уровнем активности, который мы ожидаем в сети Insights Network.

Кроме того, EOS будет иметь несколько функций, которые делают ее пригодной для работы с приложениями, такими как Insights Network.
1. EOS выделяет ресурсы, такие как пропускная способность транзакции, для каждой учетной записи в соответствии с количеством токенов EOS, хранящихся в этой учетной записи. Она также позволяет приложениям оплачивать свое использование, а это значит, что пользователям не нужно платить каждый раз, когда они используют приложение, в отличие от других сетей блокчейн, таких как Ethereum.
2. Умные контракты и децентрализованные приложения (dApps) могут быть модернизированы, чтобы внедрять новые функции и исправлять ошибки, что позволит нам быстро улучшить Insights Network в соответствии с использованием в реальном мире.
3. Многие из наших пользователей - обычные люди, и нет гарантии, что их устройства безопасны; неизбежно, что некоторые из их счетов будут взломаны. В отличие от других сетей блокчейн, EOS позволяет восстанавливать взломанные учетные записи с помощью назначенного партнера, если пользователи предоставят документацию по идентификации и пройдут многофакторную аутентификацию.

Часть выручки от нашей продажи токенов будет использоваться для приобретения и хранения токенов EOS. Владельцам токенов EOS предоставляется гарантированная

полоса пропускания транзакций по сети без сбоев, вызванных другой деятельностью, происходящей в блокчейне EOS. Например, в случае атаки или отказа в обслуживании системы пользователи по-прежнему имеют право на свою долю в пропускной способности транзакции. EOS называет это «ограничением скорости».

Еще одним важным фактором для Insights Network является безопасность. Вывод запроса данных может включать в себя выплату большого количества токенов. Если кто-то попытается выполнить несанкционированный запрос данных, может произойти нежелательная транзакция. EOS предоставляет несколько функций, которые помогут в этой и других критически важных для безопасности ситуациях.
1. EOS позволяет нашим пользователям требовать, чтобы некоторые операции были одобрены несколькими сторонами. В случае запроса данных наши пользователи могут предусмотреть, чтобы для подачи запроса требовалось одобрение нескольких людей в их организации. Согласно техническому документу EOS эта функция, которая называется «многопользовательский контроль», является самым крупным вкладом в безопасность, и при правильном использовании она может значительно уменьшить риск кражи из-за взлома.
2. EOS позволяет приложениям добавлять задержку до того, как операции записываются в блокчейне и становятся необратимыми. В течении периода ожидания пользователи уведомляются по электронной почте или смс-сообщению, что происходит в этой операции, и им предоставляется возможность остановить ее, если они не разрешили эту операцию. В случае запроса данных наши пользователи будут предупреждены о несанкционированных запросах данных и им будет предоставлена возможность их отменить.

Мы считаем, что EOS имеет светлое будущее. Она хорошо финансируется - EOS собрала 185 миллионов долларов только за первые пять дней ежегодного распределения токенов; также мы получаем постоянную поддержку от команды EOS. Учитывая эти и другие факторы мы определили, что EOS будет наиболее подходящей для наших нужд.

4.2. Безопасное многопартийное вычисление (SMC)

Безопасное многопартийное вычисление относится к классу современных криптографических решений, которые позволяют вычислять неизвестные данные. Сначала это может показаться невозможным, но с использованием правильной криптографии это не так, и в дополнение к SMC этот класс решений включает такие методы, как zkSNARKs и гомоморфное шифрование. SMC достигает этой цели, преобразовывая вычисления в распределенное вычисления, в которых ни один участник не видит полный ввод, а лишь его часть, которая сама по себе не дает информации о полном вводе.

Основные аспекты этой концепции можно отнести к Шамиру (1979), вместе с теорией, основанной в 1980-х годах (Chaum 1988). Хотя то что SMC целом применима было теоретически доказано в середине 1980-х годов, вычислительная сложность SMC препятствовала ее практическому использованию в течение двух десятилетий. Первое крупномасштабное и коммерческое использование SMC было сделано компанией Partisia, расположенной в Дании, в 2008 году, когда они использовали SMC для замены традиционного аукциона на двойной (Bogetoft et al., 2009).

С 2008 года технология созрела как с точки зрения вычислительной скорости, так и с характеристиками протоколов SMC. Накладные расходы вычислений сократились примерно на 1/1 000 000. Развитие SMC можно проследить, прочитав следующие

документы: Пинкас и другие (2009); Шелат и Шен (2011); Нильсен и другие (2012); Фредериксен и Нильсен (2013); Фредериксен и Нильсен (2014); Линделл и Рива (2015); Нильсен и другие (2017).

Для помощи в разработке и внедрении наших пользовательских протоколов SMC мы сотрудничаем с Partisia, которая в 2008 году разработала и развернула первую производственную реализацию SMC. С тех пор они выделили сервис для шифрования данных, использующих SMC, чтобы избежать необходимость хранить полную копию любого ключа на сервере, а также настраиваемый «черный пул» SMC для Tora, который обрабатывает транзакции на сумму 3 миллиарда долларов ежедневно. Наконец, они также помогают поддерживать платформу SMC с открытым исходным кодом под названием FRESCO. Очевидно, что ни одна другая организация не имеет более глубоких знаний и опыта в производственной реализации SMC.

---

www.sepior.com
www.tora.com

4.2.1 Пользовательские системы SMC

SMC применима к разнообразному набору приложений. Это не один протокол, а растущий класс решений, каждый из которых имеет разные характеристики. Ряд систем SMC был разработан для удовлетворения конкретных потребностей различных приложений, таких как управление ключами и соответствие финансового порядка.

Общие для всех решений SMC следующие роли, каждую или несколько из которых имеет каждый человек или организация:
1. **Вычислительные** стороны несут ответственность за проведение распределительных вычислений.
2. **Вводные стороны** имеют материалы для расчетов, которые они хотели бы сохранить конфиденциальными. С этой целью они используют метод, называемый секретным совместным использованием, для разложения каждой вводной на части, которые доставляются различным вычислительным сторонам. У каждой вычислительной стороны нет более одной части для ввода, и ни одна из частей не дает достаточно информации для получения всех данных исходного ввода.
3. **Результативные стороны** - те стороны, к которым высылают свои результаты остальные. Результативные стороны собирают данные, полученные из вычислительных сторон в результате общего расчета.

Существенно, что ни одна из сторон никогда не увидит исходные данные, кроме вводных.

Пользовательские системы SMC могут отличаться по следующим параметрам:
- **Основные операции**. Это операции, которые используются для определения вычислений. Система SMC будет иметь либо арифметические, либо булевы операции.
  - **Арифметические операции** более удобны для выражения статистических анализов
  - **Булевы операции** более эффективны при сопоставлении шаблонов.

• **Криптографические примитивы.** Система SMC будет использовать одну или несколько из следующих криптографических операций.
  ○ **Секретное разделение**: метод разделения данных на части, которые сами по себе не дают информации об исходных данных. Секретный обмен очень распространен в системах SMC.
  ○ **Забываемый перевод**: класс протоколов для передачи данных, в котором отправитель посылает одну из нескольких частей данных, но не знает, какую именно из них.
  ○ **Гомоморфное шифрование**: класс схем для создания зашифрованных текстов, которые могут быть вычислены.
• **Модель доверия**
  ○ **Доверие к себе:** сторона предполагает, что она может доверять только себе.
  ○ **Честное большинство**: сторона должна полагаться на то, что большинство сторон честны.

Различные комбинации этих параметров приводят к различным свойствам:
• **Отказоустойчивость:** при доверии к себе каждая сторона необходима для продолжения вычислений, и система потерпит неудачу, если даже одна из сторон не сможет или не желает участвовать. Если система полагается на честное большинство, операция может быть завершена, даже если некоторые из сторон не смогут выполнить свои обязанности.
• **Безопасность**
  ○ **Пассивная безопасность**: до тех пор, пока все вычислительные стороны следуют протоколу, ни одна из сторон не видит ничего, кроме вывода вычислений. Также известна как «полу-честная» безопасность.
  ○ **Активная безопасность**: ни одна из сторон не узнает ничего, кроме вывода вычислений, даже при наличии злонамеренных сторон, которые умышленно пытаются отклониться от протокола.
  ○ **Скрытая безопасность**: Система способна идентифицировать, если какая-либо сторона имеет пятидесятипроцентную вероятность быть злонамеренной, что является подозрительным, и принимать карательные меры.
• **Производительность**. Активная безопасность часто намного менее эффективна, чем пассивная. Скрытая безопасность обеспечивает аналогичные гарантии активной безопасности, но гораздо более эффективна.

Из-за характера технологии пользовательские системы обязаны достигать приемлемого уровня производительности. Partisia разрабатывает специализированные SMC-системы с 2008 года и будет помогать Insights Network при разработке и внедрении собственной системы SMC с требуемыми гарантиями безопасности и производительности. Примечательно, что это будет одна из первых систем SMC для взаимодействия с блокчейн.

4.2.2 Решение SMC Insights Network

SMC будет использоваться для решения следующих технологических проблем в Insights Network:
Аутентификация на базе SMC, SMC-сопоставление профилей и проверка данных. Для достижения хорошей производительности мы разработали специальные протоколы к каждому из этих вариантов использования.

В нашей аутентификации на основе SMC вычисление производится с цифровым доказательством подлинности, которое можно рассматривать как сертификат, и выполняется поставщиком, Insights Network и партнерами по проверке, выбранными

поставщиком. Доказательство содержит имя учетной записи поставщика в EOS, основные демографические данные и подписывается Insights Network. Чем больше уверенности существует в подлинности поставщика - то есть, чем более качественные партнеры по проверке за него ручаются, чем больше основных демографических данных предоставляется, тем больше оплата.

SMC получает следующие вводные, которые остаются неизвестными для всех участников вычислений, кроме первоначального владельца:
• Insights предоставляет закрытый ключ, используемый для подписи цифрового доказательства подлинности.
• Поставщик предоставляет имя своей учетной записи в EOS, которое будет включено в цифровое доказательство подлинности, а также демографические данные, которые он хочет включить в сертификат.
• Каждый партнер по проверке, которому дано имя учетной записи EOS поставщика, предоставляет основные демографические данные.

Во время вычислений подтверждается личность поставщика, а основные демографические данные перекрестно проверяются. В случае успеха запросчик получает сертификат, который он сможет использовать для подтверждения своей подлинности в следующих транзакциях.

Для сопоставления профилей на базе SMC и проверки элементов данных мы используем двухсторонний протокол SMC со скрытой безопасностью между запросчиком и поставщиком. Скрытая безопасность - это ослабленная версия активной безопасности, в которой может быть проверена пятидесятипроцентная вероятность обмана одной из сторон. Обман может быть наказан и предотвращен публикацией доказательств в блокчейне. Благодаря скрытой безопасности, а не полностью активной безопасности, мы можем обеспечить защиту от вредоносного поведения и в то же время предоставить гораздо более эффективное решение, что важно для достижения хорошего пользовательского опыта.

Мы должны принять во внимание, что клиент-поставщик Insights может работать на ноутбуке или телефоне с ограниченным сетевым подключением и вычислительной мощностью. Протокол SMC, который мы разработали, устраняет эти ограничения со следующими свойствами:
• Минимальные «путешествия»: между запросчиком и поставщиком существует только два раунда обмена сообщениями, что минимизирует эффект латентности сети и плохой связи.
• Ассимметричное вычисление: запросчик выполняет основную часть работы, чтобы компьютер или мобильное устройство поставщика не перегружалось.

Наконец, при использовании стандартных схем шифрования, кто-то в будущем может воспользоваться преимуществами улучшенной вычислительной мощности для взлома зашифрованных данных, хранящихся в блокчейне. С другой стороны, наша система использует информационно-теоретически защищенное шифрование данных, которое невозможно взломать, даже если злоумышленник имеет неограниченное время и вычислительные ресурсы. Следовательно, в нашей системе только запросчик может расшифровать данные, которые он приобрел, как сейчас, так и в любой момент в будущем.

4.3 Решение технических задач

4.3.1 Подтверждение подлинности

Поставщики сохраняют свою анонимность, участвуя в Insights Network. Но запросчики должны знать, что, хотя они анонимны, поставщики, которые выполняют запросы данных, являются реальными людьми, правдивыми насчет своих характеристик. Есть отдельный процесс, посредством которого поставщик обеспечивает подтверждение личности.

Наша система использует информацию от нескольких сторон, чтобы проверить личность поставщика. Например, одна из сторон может быть работодателем поставщика. Другая сторона может подтвердить документ, удостоверяющий личность поставщика.

Мы называем эти стороны партнерами по проверке. Если поставщик проходит проверку, система выдает цифровое доказательство подлинности, подписанное Insights Network, и публикует его в блокчейне, где оно доступно для запросчиков. Цифровое доказательство подлинности - это цифровой документ, содержащий имя учетной записи поставщика в блокчейн, которое используется в качестве идентификатора конечной точки в одноранговом протоколе, по которому общаются поставщики и запросчики; оно аналогично функции с сертификатом TLS. Наша система с использованием SMC предназначена для того, чтобы каждая сторона могла предоставить информацию, которую она хранит, в качестве вводных данных для процесса проверки, не раскрывая ее другим сторонам.

Что касается проверки подлинности, вводные данные являются конфиденциальной информацией, которую проводят партнеры по проверке, а вычисления проверяет эту информацию и создают цифровое доказательство подлинности. Когда вычислительные стороны SMC заканчиваются свои подсчеты, они отправляют промежуточные результаты поставщику, который собирает их в цифровое доказательство подлинности, подписанное Insights Network.

Insights Network не использует суб-вычисление, но вносит свой закрытый ключ в качестве вводной, которая используется в вычислении для генерации подписи цифрового доказательства подлинности.

4.3.2 Отправка запроса данных

За небольшую плату запросчик может отправить запрос данных на умный контракт Insights. Запрос будет включать опрос для заполнения поставщиками, образец, описывающий целевую аудиторию, и сколько нужно заплатить за действительный элемент данных. Запрос также будет включать токены, которые должны храниться в условном депонировании для умного контракта, чтобы произвести оплату квалифицированным поставщикам, предоставившим действительные данные. Поскольку может быть задействовано большое количество токенов, для обеспечения дополнительной безопасности запросчик может убедиться в том, что каждый запрос был одобрен несколькими сторонами из их организаций, используя систему разрешений блокчейн. После того как запросчик будет удовлетворен полученными элементами данных, он может закрыть запрос, а все токены, оставшиеся в условном депонировании, возвращаются на его учетную запись.

4.3.3 Выполнение запроса данных

Периодически клиент Insights Network, используемый поставщиком, с помощью умного контракта Insights Network будет проверять, есть ли открытые запросы данных. Он загружает их локально и использует профиль поставщика чтобы выбрать, какие из них отображать. В этом разделе описывается процесс, с помощью которого поставщик отправляет элемент данных для запроса.

Поставщик выбирает запрос данных и заполняет соответствующий опрос, который создает элемент данных. Затем он отправляет свой сертификат запросчику вместе с ID запроса данных, чтобы показать свой интерес к отправке элемента данных. Запросчик использует открытый ключ Insights Network, чтобы убедиться, что сертификат действителен и гарантирует, что имя поставщика соответствует имени учетной записи в сертификате. Если при проверке все подтверждается, запросчик генерирует секретный ключ, который впоследствии может использоваться для шифрования (а также дешифрования) элемента данных и инициирования протокола безопасного многопартийного вычисления с поставщиком.

Обе стороны предоставляют исходные данные для расчета, которые протокол запрещает разглашать другой стороне. Поставщик предоставляет свой профиль и элемент данных, которые он создал. Запросчик предоставляет шаблон профиля, формат данных и секретный ключ, который он сгенерировал для этого конкретного случая и который хранится для последующего использования.

Вычисление, которое обе стороны осуществляют совместно, заключается в проверке, соответствует ли элемент данных формату и шифрует элемент данных с помощью секретного ключа. Полученные суб-вычисления предназначаются двум сторонам, которые выполняют их, и отправляют результаты в умный контракт для сборки в конечный результат. Если конечным результатом является зашифрованный элемент данных, а не пустое значение, тогда умный контракт отправляет поставщику токены, на которые он имеет право в соответствии с условиями запроса данных. Если нет, то элемент данных недействителен, и его рейтинг снижается.

Примечательно, что схема шифрования, используемая в нашей системе, является информационно-теоретически защищенной. То есть, даже если злоумышленник имеет неограниченные вычислительные мощности и время, он не сможет взломать элемент данных. Это означает, что мы можем хранить зашифрованные элементы данных в блокчейне, не беспокоясь о том, что через 10 лет кто-то сможет взломать его, когда улучшится вычислительная мощность, к которой схема нашего шифрования будет уязвима.

4.3.4 Соответствие профилей

Поставщик имеет право предоставить элемент данных, только если его профиль соответствует необходимому запросчику шаблону. Один из способов, которым это может быть реализовано - предоставить поставщику возможность отправить свой профиль запросчику для проверки. Но это может быть нарушением конфиденциальности, поскольку профили могут содержать информацию, которую поставщики могут предпочесть не раскрывать. В любом случае степень, в которой запросчики должны знать, что находится в профиле, заключается в том, соответствует ли он шаблону, который они ищут; им действительно не нужно знать точное содержание профиля. Например, запросчику может потребоваться только знать, что возраст поставщика составляет от 21 до 30, а не то, что ему 25 лет.

Как описано в Разделе 4.3.3, сопоставление профилей в нашей системе выполняется внутри безопасного многопартийного вычисления. Поставщик предоставляет свой профиль в качестве вводной в SMC, который в силу протокола никогда не показывается запросчику.

4.3.5 Безопасный обмен проверенными данными

Учитывание запросчика и поставщика. Запросчик захочет купить данные у поставщика, если они соответствуют определенным требованиям. Но поставщик не желает, чтобы запросчик видел данные до получения платежа, потому что если у запросчика уже есть данные, он может взять их без оплаты. В то же время запросчик не желает платить за данные поставщика, если он не знает, что данные хороши соответствуют шаблону.

В нашей системе элемент данных проверяется и шифруется внутри безопасного многопартийного вычисления. Поставщик и запросчик выполняют суб-вычисления, но есть умный контракт, который объединяет результаты в конечный результат. Эффективное сохранение подтвержденного и зашифрованного элемента данных на блокчейне, который доставляет данные запросчику, и отправка платежа поставщику происходит в одной транзакции, которая является либо полностью неудачной, либо полностью успешной; действительный элемент данных доставляется запросчику, а токены отправляются поставщику.

4.3.6 Хранение

Основными категориями данных, которые проходят через Insights Network, являются профили, элементы данных и информация, используемая в процессе проверки личности поставщиков. Профили будут легко сохраняться на локальных устройствах поставщиков. Элементы данных будут храниться в зашифрованном виде в состоянии умных контрактов Insights Network, которые записываются в регистр. Профили используются для определения целевой аудитории, но SMC гарантирует, что они останутся приватными.

4.3.7 Демографические данные поставщика

Поставщики сохраняют профиль, который включает демографическую информацию, в клиенте Insights Network. Некоторые поля в профиле фиксированы, например, пол и год рождения. Другие можно изменять, такие как доход и статус в отношениях.

Поставщики могут изменять некоторые поля, но каждое изменение записывается в блокчейн. Запросчики могут использовать эту информацию, чтобы избежать мошенничества; например, запросчик может захотеть избежать те профили, в которых данные о доходе изменялись больше чем 3 раза за 3 года. Кроме того, если запросчик обнаруживает подозрительную активность, за плату он может указать на этого поставщика в нашей двусторонней системе оценивания.

5 Экономика токен

5.1 Двусторонний рынок

Insights Network - это платформа, которая облегчает транзакции между двумя отдельными группами: запросчиками и поставщиками. Запросчики нуждаются в

информации от поставщиков и готовы заплатить, чтобы получить ее. Такая динамика известна как двусторонний рынок.

Двусторонние рынки, как правило, трудно запускать. Основная причина размещения запросов в Insights Network заключается в наличии поставщиков, которые будут их выполнять. В то же время основная причина, по которой поставщики присоединяются к Insights Network состоит в том, что существует достаточно запросов для получения денег. Вначале на платформе недостаточно одной группы, чтобы привлечь другую.

Чтобы помочь в запуске рынка, мы выпускаем новый токен ERC-20, который мы называем INSTAR. Пользователи, которые размещают свои данные в Insights Network и участвуют в маркетинговых исследованиях, будут вознаграждены токенами INSTAR. Владельцы токенов INSTAR смогут отправлять запросы данных или продавать токены тем, кто хочет их приобрести.

Поставщики смогут продавать токены, выплачиваемые им запросчиками, вкладывать их в такие вещи, как мили авиакомпаний или фирменные подарочные карты и отправлять их другим пользователям через кошелек Insights Network. По мере того, как поставщики будут присоединятся к Insights Network, больше запросчиков будет привлечено к размещению запроса данных, что, в свою очередь, привлечет еще больше поставщиков. Это явление известно как сетевой эффект, который приводит к росту сети.

5.2. Распределение токенов

Токены будут распределяться следующим образом:
Общий объем поставки токенов INSTAR: 300MM
- 5% токенов будут проданы в предпродаже со скидкой
- 35% токенов будут проданы при продаже токена
- 30% токенов будут посвящены экосистеме
- 30% токенов будут зарезервированы компанией для команды, консультантов, операций, будущих разработок, найма, R&D

90 миллионов токенов будут выданы экосистеме для использования в качестве оплаты для ранних пользователей, чтобы заполнить их профили, а также участвовать в исследованиях рынка, проводимых Insights Network и ранними партнерами. Предоставляя токены экосистемы ранними пользователям, мы создаем сотни миллионов элементов данных, которые создают жизнеспособную сеть. Например, если каждый ранний пользователь получает токен для импорта десяти простых экземпляров проверенных данных в свой клиент, эти 90 миллионов токенов генерируют 900 миллионов элементов данных для Insights Network.

90 миллионов токенов INSTAR будут зарезервированы для использования компанией в качестве компенсации для команды Insights Network, включая учредителей, сотрудников и консультантов, что побудит их увеличить спрос на услуги, предлагаемые Insights Network, а таким образом и спрос на токены INSTAR, сделав сеть привлекательным местом для проведения маркетинговых исследований.

Следует отметить, что во время бета-тестирования Desktop Client Insights Network токен Insights ERC-20 будет использоваться до тех пор, пока платформа EOS не будет полностью функционировать и станет общедоступной, после чего произойдет одноразовая миграция для владельцев токенов, чтобы они могли обменять свои токены ERC-20 INSTAR на эквивалентную валюту INSTAR EOS.

Предел продажи токена - 25 000 ETH

5.3 Использование средств

Развитие - 50%
Операции - 25%
Маркетинг - 15%
Юридические расходы - 10%

6 Команда

Брайан Галлахер - Школа бизнеса Carey, Y-Combinator
Дарвин Ло - Стэнфорд, Компьютерная наука, Y-Combinator
Брэндан Зауча - Школа бизнеса Carey,, Y-Combinator
Дилан Герман - Университет Иллинойс, Инженерия
Дино Амарал - Доктор философии, Криптография

Если у вас есть страсть к «большим данным», вы специалист в области компьютерной науки и любите стартапы, свяжитесь с нами:
team@insights.network

6.1 Консультанты

Курт Нильсен
Джаспер Бьюс Нильсен
Питер Фрэндс Франдсен
Эндрю Розенер
Джейсон Хэмлин
Дэвид Гобуд

6.2 Партнеры

Partisia является пионером в коммерческих реализациях SMC. Первое крупномасштабное и коммерческое использование SMC было сделано Partisia в 2008 году, когда они заменили традиционный аукцион на двойной по контрактам на производство. Другие ключевые достижения включают в себя выделение Sepior, которое использует SMC для предоставления чистого клауд-решения для управления «небезопасными» ключами и выделение Secata, которое обеспечивает внебиржевое сопоставление на финансовых рынках для ценных бумаг, а также конфиденциальность - контроль статистических анализов, таких как совместный кредитный рейтинг.

7 План осуществления

Insights: Q1-Q3 2017
- Доказательство концепции
- Запуск веб-сайта Insights Network
- Разработка тестирования сети EOS

Insights: Q4 2017
- Обновленный технический документ для включения SMC
- Предварительная продажа токена
- Интеграция приложения Gambeal

Insights: Q1 2018
- Массовая продажа токенов INSTAR

Insights: Q2 2018
- Безопасное многопартийное вычисление
- INSTAR App Client Бета-версии ERC-20 выкупаем на клиенте

Insights: Q3 2018
- Открытие бета-версии платформы EOS

Insights: Q4 2018
- Потребительский клиент INSTAR EOS блокчейн полностью функционален

8 Заключение

Брокеры данных собирают личную информацию о людях без их разрешения и продают ее всем, кто готов заплатить, в том числе и таким организациям, которые оказывают значительное влияние на жизни людей, включая университеты, больницы и страховые компании. Это не просто вторжение в личную жизнь; это слежка. И потребители мало что могут сделать, чтобы остановить этот процесс, даже если они знают, что это происходит.

К счастью, правительства во всем мире борются с брокерами данных. Европейский союз принял Положение об общей защите данных, которое регулирует, как организации должны обрабатывать персональные данные. Бразилия запрещает передачу данных, которые содержат личную информацию, третьей стороне (PII). В Соединенных Штатах сенатор Эдвард Марке (D-MA) спонсирует законопроект «Закон о подотчетности и прозрачности брокеров данных» от 2017 года.

Мы будем работать над продвижением правил, требующих более высокого стандарта для обработки конфиденциальной личной информации. Но даже при отсутствии правил мы полагаем, что наше решение будет превосходить существующих брокеров данных и победит при свободной рыночной конкуренции, предоставив превосходную информацию и возможность потребителям контролировать свои собственные данные.

Мы прогнозируем, что через 10-20 лет из-за роста децентрализованных технологий больше не будет посредников. Организации будут использовать нашу платформу для непосредственного взаимодействия с потребителями по их данным. Организации в настоящее время платят 200 миллиардов долларов в год за эти данные - Forbes прогнозирует, что эта сумма только увеличится. Мы считаем, что Insights Network будет расти, чтобы удовлетворить эту потребность, и перенести контроль над данными от организаций, таких как Acxiom, к их законным владельцам - потребителям.

9 Источники

1. EOS.IO Technical White Paper
2. Multi Party Computation: From Theory to Practice
3. The secretive world of selling data about you (Newsweek)
4. 6 predictions for the $125 billion Big Data Analytics market in 2015 (Forbes)
5. Acxiom database hacked (Computerworld)
6. Equifax announces cybersecurity incident involving consumer information (Equifax)
7. Bogetoft P, Christensen DL, Damgaard IB, Geisler M, Jakobsen T, Kroejgaard M, Nielsen JD,
   Nielsen, JB, Nielsen K, Pagter J, Schwartzbach MI and Toft T (2009) Secure multiparty computation goes live, Lecture Notes in Computer Science, vol 5628, pp. 325–343.
8. Chaum D, Crepeau C, and Damgaard IB. (1988) Multiparty unconditionally secure protocols
   (extended abstract). In 20th ACM STOC, Chicago, Illinois, USA,May 24, 1988, ACM Press, pp.
   11–19.
9. Shamir A (1979) How to share a secret, in Communications of the ACM 22, 11, pp. 612–613.
10. Pinkas B, Schneider T, Smart NP and Williams SC (2009) Secure Two-Party Computation Is
    Practical. Asiacrypt 2009.
11. Shelat A and Shen C (2011) Two-output Secure Computation With Malicious Adversaries.
    EUROCRYPT 2011.
12. Nielsen JB, Nordholt PS, Orlandi C and Burra SS (2012): A New Approach to Practical Active-Secure Two-Party Computation. CRYPTO 2012.
13. Frederiksen TK and Nielsen JB (2013) Fast and Maliciously Secure Two-Party Computation
    Using the GPU. ACNS 2013.
14. Frederiksen TK and Nielsen JB (2014) Faster Maliciously Secure Two-Party Computation Using
    the GPU. SCN 2014.
15. Lindell Y and Riva B (2015) Blazing Fast 2PC in the Offline/Online Setting with Security for
    Malicious Adversaries. CCS 2015.
16. Nielsen BN, Schneider T and Trifiletti R (2017) Constant Round Maliciously Secure 2PC with
    Function-independent Preprocessing using LEGO. NDSS 2017.

info@insights.network