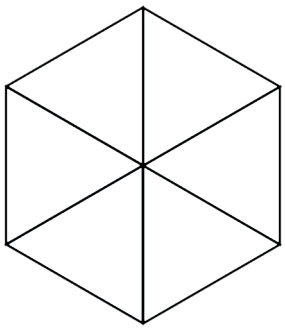

ASURE: ПЕРВАЯ МАСШТАБИРУЕМАЯ БЛОКЧЕЙН СЕТЬ ДЛЯ ДЕЦЕНТРАЛИЗОВАННЫХ СИСТЕМ СОЦИАЛЬНОГО ОБЕСПЕЧЕНИЯ

Paul Mizel, Fabian Raetz и Gamal Schmuck
Asure Foundation

1 Октября, 2019

https://asure.network

Аннотация

Социальное обеспечение является важным элементом экономического и политического развития общества. Однако в мире более 4.1 миллиарда человек не имеют доступа к системам социального обеспечения. [1] И с другой стороны, существующие социальные системы имеют другие проблемы, которые необходимо преодолеть по демографическим причинам (например, коэффициент рождаемости 1.5 по сравнению со средним мировым показателем 2.5) или по причинам затрат (административные расходы более 50% или даже больше, чем 100%). В настоящее время блокчейн Ethereum может выполнять максимум 1.3 миллиона транзакций в день. [2] Системы социального обеспечения частично основаны на нескольких сотнях миллионов транзакций в месяц и следовательно, они не могут быть устойчиво реализованы с использованием технологии блокчейна на сегодняшний день.

Системы социального обеспечения, основанные на блокчейне, имеют ряд преимуществ в сравнении с обычными системами социального обеспечения. Они обеспечивают постоянное и намного более высокое качество данных, используемых и хранящихся благодаря целостности процесса, неизменности и устойчивости системы, что позволяет проводить точный анализ в реальном времени. Прозрачность и неизменность транзакций обеспечивают защиту системы от манипуляций и коррупции. Используя блокчейн для устранения громоздкого и подверженного ошибкам ручного труда, можно достичь высокой степени автоматизации, экономичности, а также простоты отслеживания бизнес-процессов.

Прошлые разработки технологии блокчейн и их результаты показывают, что финансовые транзакции выполняемые через них, могут быть выполнены безопасно, автоматически и без каких либо посредников. Это говорит о том, что системы социального обеспечения, как системы обслуживающие население и использующие финансовые транзакции на основе правил, являются разумным вариантом использования публичного блокчейна.

Блокчейн Ethereum соответствует таким решениям, как Casper и Sharding в конвейере, что в конечном итоге решит проблему масштабируемости на уровне 1. Даже в отношении людей, которые не имеют доступа к каким-либо системам социального обеспечения, количество транзакций необходимых для платежей и выплат, составляет по крайней мере количество вовлеченных людей, то есть миллиарды транзакций в месяц только лишь для пенсионной системы.

Целью данного документа является изучение решения уровня 2 для оптимальной масштабируемости при сохранении всех пре-

имуществ технологии блокчейн в отношении децентрализованных систем социального обеспечения.

Примечание: asure.network находится на стадии разработки. В настоящее время ведутся активные исследования и новые версии этого документа появятся на сайте http://asure.network Для комментариев и предложений, свяжитесь с нами по адресу research@asure.network.

Словарь терминов

EVM Виртуальная машина Ethereum предназначена для использования в качестве среды выполнения для смарт контрактов на основе Ethereum.

Blockchain Система, в которой ведется учет транзакций на нескольких компьютерах, которые связаны между собой в одноранговой сети.

Ethereum Децентрализованная программная платформа, которая включает в себя смарт контакрты и распределенные приложения (ĐApps).

ETH Родной токен блокчейна Ethereum.

BTC Родной токен блокчейна Bitcoin.

ERC20 Технический стандарт, используемый для смарт контрактов в блокчейне Ethereum для реализации токенов.

SmartContract Смарт контракт это компьютерный протокол, предназначенный для упрощения, проверки или обеспечения выполнения согласования или исполнения контракта в цифровом виде. Смарт контракты позволяют совершать заслуживающие доверия транзакции без участия третьих лиц. Эти транзакции отслеживаются и необратимы.

Account Хеш открытого ключа, который может содержать значения. Доступ возможен только при наличии соответствующего закрытого ключа.

GDPR Общее положение о защите данных (ЕС) 2016/679 ("GDPR") это положение в законодательстве ЕС о защите данных и конфиденциальности для всех лиц в Европейском союзе (ЕС).

PAYG метод финансирования социального страхования, в особенности пенсионного обеспечения, а также медицинского страхования и страхования по безработице. Уплаченные взносы используются непосредственно для финансирования бенефициаров, то есть они выплачиваются обратно им.

Содержание

1 Вступление

Экосистема Asure состоит из сети Asure, блокчейна Asure, платформы Asure и других сторонних приложений.

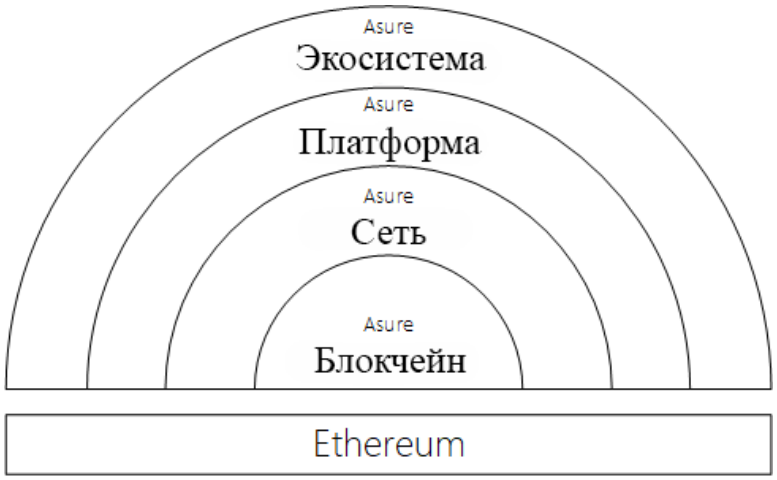

Рис. 1: Экосистема Asure

Сеть Asure это масштабируемая блокчейн сеть для децентрализованных систем социального обеспечения. Asure закладывает основу для доступа 10 миллиардов людей к системам социального обеспечения и обеспечивает огромное социальное воздействие там, где это больше всего необходимо. [3]

Являясь технологической базой, которая обеспечивает оптимальную производительность в отношении пропускной способности транзакций при сохранении децентрализованного характера сети, она гарантирует требуемый уровень прозрачности и экономической эффективности в системе. Сеть реализована в виде множества боковых цепей Plasma, которые связаны с блокчейном Asure, а также с блокчейном Ethereum или любым другим EVM-совместимым блокчейном. Каждый сайдчейн управляется несколькими независимыми провайдерами узлов, которым необходимо иметь долю токенов ASR для достижения консенсуса между ними и следовательно, внутри сети. Имея долю токенов ASR, провайдеры узлов могут зарабатывать дополнительные токены, предоставляя свою вычислительную мощность. Для каждой системы социального обеспечения в сети Asure будет сайдчейн.

Блокчейн Asure содержит рутчейн Asure и связанные сайдчейны. Рутчейн предлагает преимущества как в области безопасности, так и в

области межцепной связи. Все работающие узлы блокчейна Asure представляют Asure Network. Платформа Asure соединяет бэкэнд-инфраструктуру с приложениями, которые могут использоваться конечными пользователями или программными интерфейсами для разработчиков, чтобы создавать приложения поверх платформы Asure.

1.1 Системы социального обеспечения

Социальное обеспечение это система страхования, в которой застрахованные риски (такие как болезнь, материнство, потребность в длительном уходе, несчастные случаи на работе, связанные с работой заболевания, безработица, снижение трудоспособности, старость и смерть) покрываются совместно всеми застрахованными лицами. Системы социального обеспечения абсорбируют многие жизненные риски, предотвращают чрезвычайные трудности и таким образом это создет социальный баланс.

Люди, которые не имеют доступа к системам социального обеспечения, рискуют стать нищими, если их постигнет судьба, такая как болезнь, неурожайность или инвалидность. Тогда им, возможно придется обналичить сбережения, продать скот и другие средства производства и отправить своих детей на работу вместо школы, чтобы найти финансы на ежедневные расходы. [20]

Люди, которые пользуются базовым социальным обеспечением, более склонны вкладывать средства в образование и физический капитал, что сопряжено с дополнительными рисками, но и перспективой улучшения доходов. Эмпирические исследования показывают, что существование систем социального обеспечения, особенно в неформальном секторе, усиливает склонность к инвестициям и таким образом способствует экономическому росту именно там, где это наилучшим образом способствует сокращению бедности. [21]

Существует широкий спектр систем социального обеспечения и все они различаются по своему конкретному применению. Для целей данного документа мы определяем функциональность наиболее распространенных систем социального обеспечения следующим образом:

Пенсия

Пенсионная система состоит из ряда вкладчиков и пенсионеров. Участники системы платят ежемесячные страховые взносы, которые перераспределяются на нынешних пенсионеров. Взамен вкладчики имеют право на получение своей пенсии по истечении определенного периода времени,

исходя из времени и суммы уплаченных взносов. В некоторых системах страховые взносы выплачиваются компанией от имени участника, что означает значительное сокращение необходимых транзакций. Выплаты пенсий обычно происходят в установленный день, и все пенсионеры получают выплаты одновременно. Это делает его идеальным вариантом использования для транзакций массовых выплат.

Здравоохранение

Стороны в сфере здравоохранения разнообразны, есть застрахованные люди которые платят премию, есть врачи, больницы, аптеки и другие поставщики услуг, которые выставляют счета. Они могут быть компенсированы системой или через застрахованного, который отправляет счета в систему и получает возмещенные расходы. Здесь существуют различные возможности реализации обработки партиями, застрахованный может представить накопленные счета в конце года, или врачи, больницы, аптеки и другие поставщики услуг также могут представлять свои коллективные счета партиями.

Безработица

Страхование по безработице это защита от потери работы. Участники имеющие работу, оплачивают премию, в случае потери работы у участников есть время, чтобы найти работу снова.

Страхование социального обеспечения

Страхование социального обеспечения, это страхование по долгосрочному уходу или страхование по уходу являющееся обязательным страхованием для покрытия риска зависимого от долгосрочного ухода. Пособия по социальному страхованию предоставляются на основе "уровней потребности в долгосрочном уходе". В случае профессиональной, амбулаторной или (частично) стационарной помощи, расходы покрываются до определенной максимальной суммы (включая средства по уходу, меры по улучшению жизненной среды, а также пособия по добровольному уходу). Поэтому обязательное социальное страхование не является полной страховкой. Чтобы получить полное покрытие, необходимо оформить частную дополнительную страховку по уходу. В случае необходимости застрахованное лицо имеет право на помощь по уходу в качестве дополнительного социального пособия, ориентированного на потребности.

Поддержка детей и молодежи

В Германии, поддержка детей и молодежи охватывает все услуги и задачи государственных и независимых учреждений, работающих на благо молодежи и их семей. Благополучие детей и молодежи не является главной опорой социального страхования, но в основном обеспечивается независимыми учреждениями, которые тесно сотрудничают с властями. Он в основном финансируется за счет денег налогоплательщиков.

Страхование от инвалидности / Страхование от несчастных случаев

Целью обязательного страхования от несчастных случаев является предотвращение несчастных случаев на производстве, профессиональных заболеваний и связанных с работой рисков для здоровья, а также восстановление здоровья и профессиональной деятельности застрахованных лиц "всеми соответствующими средствами"в случае наступления этих страховых случаев.

1.2 Блокчейн

Блокчейн - это децентрализованная база данных, которая содержит постоянно растущий список записей транзакций. База данных расширена хронологически линейно, подобно цепочке, в которую постоянно добавляются новые элементы внизу (отсюда и термин "блокчейн"). Если блок завершен, создается следующий. Каждый блок содержит контрольную сумму предыдущего блока. Сатоши Накамото разработал Биткойн в 2009 году являясь одной из первых реализаций блокчейна, которая демонстрирует потенциал технологии для финансовых транзакций. [4]

Прорывной потенциал блокчейна становится все более очевидным. После изобретения блокчейна Ethereum и виртуальной машины Ethereum (EVM) миру были предоставлены инструменты, необходимые для создания работающих децентрализованных автономных организаций (DAO). В такой системе несколько органов управления контролируют разные компоненты, и ни один из них не является полностью доверенным для всех остальных. [5] Технология блокчейн идеально подходит для автономного и децентрализованного социального обеспечения.

2 Сеть Asure

Сеть Asure состоит из клиентов узлов, в которых блокчейн Asure работает и синхронизируется между отдельными узлами с помощью консенсуса. Для достижения количества требуемых транзакций нагрузка должна быть распределена по нескольким цепочкам блоков. Одна или несколько цепочек блоков могут быть специфичны для одной системы социального обеспечения. Чтобы извлечь выгоду из экосистемы, большая добавленная стоимость для масштабируемости возникает только тогда, когда активы могут быть переданы между несколькими блокчейнами. Кроме того, специализированные сайдчейны могут извлечь выгоду из безопасности рутчейна и таким образом, активы будут лучше защищены. [6]

2.1 Требования

Основные требования к социальному обеспечению и блокчейну в масштабируемом сценарии:

Пропускная способность транзакций

Сеть Asure должна быть способна масштабировать пропускную способность транзакций через сайдчейны до такой степени, чтобы страны и резиденты могли совершать свои финансовые транзакции в пределах внешней цепи.

Конфиденциальность

Чтобы защитить конфиденциальность пользователей, никакие личные данные не могут храниться в блокчейне. По возможности, транзакции не должны назначаться пользователю. Персональные данные зашифрованы и хранятся вне блокчейна. Используя метод Zero-Knowledge-Proof (Доказательство с нулевым разглашением), можно полностью избежать хранения личных данных.

Для того чтобы социальное обеспечение на основе блокчейна было установлено, оно должно соответствовать руководящим принципам защиты данных и конфиденциальности национальных и международных норм, таких как Общее положение о защите данных (GDPR) в Европейском союзе. [7]

Прозрачность

Прозрачность в сети Asure является важным фактором защиты систем социального обеспечения от коррупции и манипуляций. Уважая конфиденциальность пользователей, важно обеспечить прозрачность системы, в целом, чтобы включить например статистику общего денежного потока в реальном времени.

Бизнес-правила для системы

Социальное обеспечение имеет много влияющих факторов и правил, которые должны выполняться, адаптироваться и осуществляться, поэтому мы обязаны иметь возможность выполнять собственные бизнес-правила в сайдчейне с EVM или EWASM.

Безопасность

Система, которая организует и хранит финансовые транзакции систем социального обеспечения, должна удовлетворять множественным требованиям безопасности. Необходимо убедиться, что данные не могут быть обработаны или украдены, а система устойчива к атакам, сбоям и другим ошибкам.

2.2 Другие технологии

Пун и Бутерин представили платформу Plasma в 2017 году для решения проблемы масштабирования путем организации нескольких независимых блокчейнов в древовидную иерархию. Последовательные предложения Plasma описали места вне цепи для простых передач взаимозаменяемых и не взаимозаменяемых токенов. Эти предложения включают Plasma MVP, Plasma Cash и Plasma Debit. Платформа Plasma находится в стадии активного исследования и в зависимости от применения и требований, реализация Plasma варьируется.[8] Loom и OmiseGO являются одними из первых, кто внедряет платформу Plasma и продолжает свои исследования в этой области.

Платформа Plasma была представлена совсем недавно и является одним из наиболее многообещающих предлагаемых решений для масштабируемых вычислений на блокчейн. Plasma имеет очень обширную белую книгу, но не содержит всей технической информации, необходимой для немедленной реализации. Plasma может обеспечить масштабируемость для приложений на Ethereum. Это специфический для приложения протокол сайдчейна.

С другой стороны, Polkadot был представлен Gavin Wood (Гэвином Вудом) в 2017 году. Целью концепции является создание гетерогенного многоцепного решения, которое позволяет соединять индивидуально адаптированные сайдчейны с общедоступными блокчейнами. Polkadot позволяет различным блокчейнам обмениваться сообщениями безопасным и надежным способом.

Raiden Network это решение для автономного масштабирования с технологией платежей и каналов связи, позволяющее осуществлять почти мгновенные и с низкой комиссией, масштабируемые платежи. Он дополняет блокчейн Ethereum и работает с любым токеном, совместимым с ERC20.

2.3 Plasma

Сеть Asure будет использовать платформу Plasma для создания масштабируемой сети блокчейнов для реализации потребностей систем социального обеспечения.

Чтобы еще больше повысить ограничения уровня 1 для эффективного функционирования системы социального обеспечения, масштабирование уровня 2 считается наиболее эффективным решением. Это облегчает реализацию безопасности в системе, поскольку она опирается на уровень 1. Решение будет спроектировано как комбинация рутчейна Asure и соответствующего сайдчейна для соответствия всем потребностям систем социального обеспечения.

Сайдчейны Asure могу быть связаны со смарт контрактами Ethereum или любыми другими технологиями блокчейна, которые работают с шаблонами проектирования Plasma.

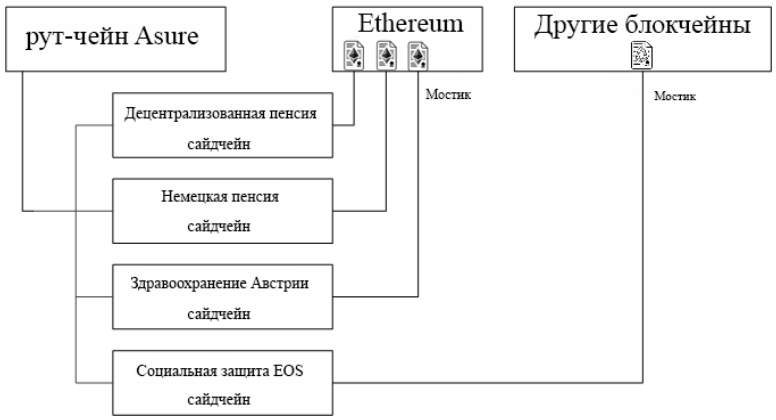

Рис. 2: Сайдчейны Asure

3 Блокчейн Asure

С технической точки зрения системы социального обеспечения можно охарактеризовать как ряд основанных на правилах (финансовых) операций, которые осуществляются между (обычно) незначительно изменяющейся совокупностью различных сторон при условии поддержания равновесия между депонированной и выведенной стоимостью в течение определенного периода времени. Такая система может быть реализована в цифровом виде путем создания блокчейн-системы, которая поддерживает смарт контракты и криптовалюты.

Обычные системы социального обеспечения в настоящее время генерируют до сотен миллионов транзакций в месяц, это зависит от количества участвующих сторон и конкретного варианта использования социального обеспечения.

Ежемесячные пенсионные взносы	= 54.445 Mio
Ежемесячные пенсии	= 25.646 Mio
Ежемесячные пенсионные операции	= 80.091 Mio

Таблица 1: Например, немецкая система пенсионного обеспечения: [12]

Чтобы разработать систему блокчейн, которая сможет обрабатывать все эти транзакции, необходимо увеличить достижимую пропускную способность транзакций системы и автоматическую пакетную обработку внутри транзакции, чтобы уменьшить общее количество транзакций до минимума.

Оба требования могут быть решены путем использования сайдчейна, как указано в Plasma Framework. Блокчейн Asure функционирует как масштабируемый сайдчейн реализации Asure Plasma. Это рутчейн сети Asure и закладывает основу для оптимальной масштабируемости в отношении систем социального обеспечения на основе блокчейна.

Активы, переданные из блокчейна Ethereum в один из сайдчейнов Asure, блокируются в контракте Asure Plasma на блокчейне Ethereum до тех пор, пока не будет выполнена транзакция выхода из блокчейна Ethereum. В соответствии со спецификациями Plasma MVP, эквивалент этого значения создается с помощью шаблона проектирования оператора (Proof-Of-Authority) в блокчейне Asure и присваивается пользователю.

Затем доступные активы в блокчейне Asure можно использовать для транзакций в системе. Консенсус между всеми провайдерами узлов в блокчейне Asure достигается с помощью алгоритма proof-of-stake с использованием адаптированной версии механизма консенсуса Tendermint.

[14] Tendermint может обрабатывать объем транзакций до 10000 транзакций в секунду. С помощью зон и концепций шардинга этот размер можно увеличить в 1000 раз. Это обеспечит устойчивую работу системы социального обеспечения на блокчейне. [15]

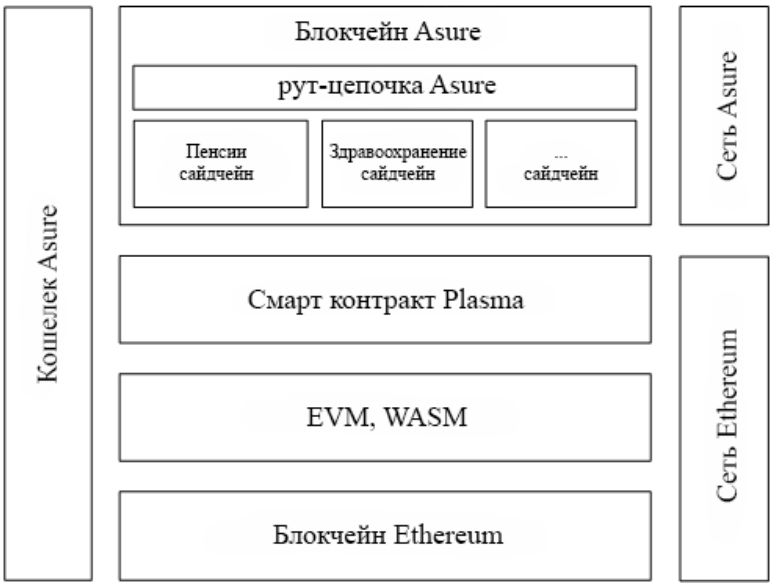

Рис. 3: Архитектура Asure

У блокчейна Asure есть несколько основных принципов.

3.1 Безопасность

Блокчейн Asure включает в себя несколько функций, которые защищают его от таких атак, как несанкционированные расходы, двойные расходы, подделка активов и вмешательство в блокчейн.

Каждый блок, добавленный в блокчейн, начиная с блока, содержащего конкретную транзакцию, является подтверждением этой транзакции. В идеале получатели и отправители, получающие платежи, должны дождаться, пока хотя бы одно подтверждение не будет распространено по сети, прежде чем предполагать, что платеж был сделан. Чем больше подтверждений ожидает получатель, тем сложнее злоумышленнику успешно отменить транзакцию в блокчейне, если только злоумышленник не контролирует более половины всей производительности сети, то в этом случае это называется атакой на 51 процент. Эта платформа не предназначена для предотвращения таких атак, а скорее для поощрения распространения блоков.

3.2 Алгоритм Консенсуса

Существуют разные версии алгоритмов доказательства. Proof-of-work подвергается резкой критике из-за огромного энергопотребления.[13] Долгосрочное принятие и движение сообщества движутся к алгоритму proof-of-stake, где валидаторы создают блоки и получают вознаграждение за правильную работу. Блокчейн Asure будет использовать согласованный алгоритм Proof-of-Stake (PoS). В первой реализации MVP будет использоваться механизм консенсуса Tendermint.[14]

3.3 Конфиденциальность с (ZK-SNARKS и ZK-STARK)

Среди прочего, блокчейн Asure учитывает аспекты конфиденциальности, которые имеют огромное значение для социального обеспечения.

ZK-SNARKS (Zero-Knowledge Succinct Non-interactive Argument of Knowledge) дает возможность проводить анонимные транзакции. ZK-SNARKS не устойчивы к квантовым вычислениям. ZK-STARK (Zero-Knowledge Scalable Transparent Argument of Knowledge) это последнее новшество которое устойчиво к квантовым вычислениям и нацелено на достижение конфиденциальности в блокчейне с использованием быстрых масштабируемых вычислений. [16]

Поскольку Ethereum также проводит исследования на уровне 1 в этой области, транзакции социального обеспечения могут оставаться анонимными для застрахованных пользователей. [17]

Использование технологии с нулевым разглашением еще не вполне осуществимо, но это изменится в будущем.

3.4 EVM, WASM, eWASM, *WASM

EVM обеспечивает тьюринг-полноту, так что Ethereum может запустить обычную программу, также известную как смарт контракт. Plasma EVM это новая версия Plasma, которая может выполнять EVM в ее цепочке и ее клиенты могут основываться на текущих клиентах Ethereum (go-ethereum, py-evm, parity). Мы предлагаем реализацию Plasma с принудительной проверкой состояния, чтобы гарантировать только правильное состояние, отправленное в рутчейн, предоставляя способ входа и выхода из хранилища учетных записей между двумя цепочками, поскольку каждая цепочка имеет идентичную архитектуру. Еще одним преимуществом является то, что инструменты разработки Ethereum также могут быть использованы в цепи Plasma.

eWASM это просто «приправленное» подмножество Ethereum WebAssembly, представляющее собой двоичный формат инструкций. eWASM опирается на инструкции, которые очень близки к реальному процессору. Улучшения производительности значительны и кажутся более безопасными. WebAssembly поддерживается Mozilla, Google, Apple и Microsoft, сообщество также активно, это будет широко используемый веб-стандарт.

Блокчейн Ethereum обрабатывает около 15 транзакций в секунду (TPS), что недостаточно для внедрения системы социального обеспечения. Улучшения Ethereum (также называемые Layer 1), которые в настоящее время находятся в стадии разработки, должны значительно увеличить количество TPS. Улучшения включают в себя алгоритм консенсуса на основе Proof-of-Stake (PoS), шардинг, а также введение eWASM - виртуальной машины на основе WebAssembly.

3.5 Другие технологии

Parity Substrate это высокоуровневая структура для создания криптовалют и других децентрализованных систем с использованием новейших исследований в технологии блокчейн.

Cosmos-SDK - это блокчейн платформа, позволяющая разработчикам легко создавать настраиваемые взаимодействующие блокчейн приложения в сети Cosmos Network без необходимости воссоздания общей функциональности блокчейна, что устраняет сложность создания приложения Tendermint ABCI. Мы рассматриваем SDK как npm-подобную инфраструктуру для создания защищенных блокчейн приложений поверх Tendermint.

LotionJS стремится сделать написание новых блокчейнов более быстрыми. Он построен поверх Tendermint с использованием протокола ABCI. Lotion позволяет создавать безопасные, масштабируемые приложения, которые могут легко взаимодействовать с другими блокчейнами в Cosmos Network.

4 Платформа Asure

Платформа Asure состоит из компонентов, которые предоставляют сеть и протокол для использования и построения систем социального обеспечения, в том числе клиента, SDK, инструментов и приложений веб-интерфейса. Цель платформы - создать экосистему, в которой системы социального обеспечения могут разрабатываться, тестироваться, моделироваться, управляться и начать использоваться как можно быстрее.

4.1 Клиент

Основным клиентом является точка входа в сеть Asure, способная запустить узел. Узлы соединены друг с другом в одноранговой сети и передают новую информацию по протоколу gossip. Каждый узел хранит полную копию полностью упорядоченной последовательности событий в блокчейне Asure. Узлы используются для формирования и управления сетью Asure и обеспечения включения транзакций в блокчейн Asure.

4.2 Комплекты разработки программного обеспечения (SDK)

SDK предоставляет стандартизированные функции, на которых могут быть построены приложения. Наша основная цель - упростить разработку новых экосистемных решений, чтобы они практически не требовали поддержки разработчиков.

4.3 Инструменты

Инструменты поддерживают создание, тестирование и моделирование созданных решений в сети и блокчейне Asure и ускоряют процесс разработки.

4.4 Фронтенд приложения

Чтобы добиться одобрения пользователя, предоставляются стандартные приложения блокчейна, такие как блокчейн проводник, пул, мобильные приложения (Android, iOS), чтобы сделать возможным использование мобильных платежей в глобальном масштабе с кошельком, а также раскрыть весь потенциал мобильной коммерции.

5 Опыт работы

Основным направлением деятельности Asure в сфере социального обеспечения является пенсионное страхование. В рамках продолжающегося исследования мы перенесли специфические аспекты немецкой пенсионной системы в блокчейн Ethereum. Основываясь как на нашем практическом опыте, так и на опыте, накопленном за годы работы в области страхования, мы разработали теоретическую основу функционирования децентрализованной пенсионной системы, а также практическую реализацию такой системы.

5.1 Исследования технологии блокчейн и автоматизации

Технический директор Asure, Фабиан Рец (Fabian Raetz), в 2013 году провел исследовательский проект в Университете прикладной науки и искусства в Дортмунде, где проанализировал новые технологии блокчейна и их возможное приминение. [18]

В 2014 году небольшая команда во главе с Полом Мизелем (Paul Mizel) и Фабианом Райцем (Fabian Raetz) разработала собственную валюту, основанную на блокчейне в качестве доказательства концепции и проверила различные виды проблем блокчейна и экономические системы (монета NRJ). [19]

В конце 2015 года Paul Mizel создал команду в Киеве для инновационных проектов на основе ИИ «Insure Chat», «Insure Assistant» и «Insure Advisor». В результате были созданы полностью автоматизированные чат-боты для поддержки, управления заявками и других задач с уникальным механизмом обучения и подключением к социальным платформам, таким как Facebook, Telegram, Skype и другие.
Технический стек: IBM Watson, Microsoft Bot Framework, MS Luis, .NET.
Используемые алгоритмы: интеллектуальный анализ текста, регрессионный анализ, SVM, нейронные сети.

5.2 Немецкая пенсионная система

Чтобы продемонстрировать потенциал социального обеспечения, основанного на блокчейне, Asure создал прототип, основанный на модели немецкой государственной пенсионной системы с выплатой пенсии по факту.

Asure dApp станет эталонной реализацией для dApps, использующих блокчейн и платформу Asure.

Это предоставит

- техническое технико-экономическое обоснование пенсионной системы Германии, внедренной на блокчейне Ethereum и протоколе / платформе Asure.
- полная реализация кошелька.

- обзор и управление вашими страховыми полисами.
- страховой магазин, чтобы найти и купить страховые полисы.

Пожалуйста, попробуйте Asure dApp, который в настоящее время работает на тестовой сети Ethereum Rinkiby: https://dapp.asure.io

5.3 Децентрализованная пенсионная система

Чтобы продемонстрировать, что блокчейн может решать проблемы в глобальном масштабе, Asure также разработала прототип глобальной пенсионной системы, которая полностью децентрализована и следовательно, не принадлежит ни правительству, ни какой-либо страховой компании.

Это эксперимент в альфа-фазе, призванный показать, как можно улучшить системы социального обеспечения в будущем с помощью технологии блокчейн.

Идея состоит в том, чтобы внедрить пенсионную систему с оплатой по факту на блокчейне Ethereum. Участники платят свои взносы в ETH и получают токены ERC20 взамен. Никакие вклады не вкладываются в рынок капитала и, следовательно, проценты не начисляются. Вместо этого, оплаченные ETH используются непосредственно для выплаты невыплаченных пенсионных требований. Сколько пенсии будет выплачиваться, зависит от того, сколько пенсионных токенов имеет пенсионер, то есть сколько взносов он внес в систему.

Как правило, системы pay-as-you-go работают только потому, что штаты вводят обязательные системы социального обеспечения и таким образом, могут гарантировать стабильное количество участников и выплаты взносов. В децентрализованной пенсионной системе никто не может быть принужден к членству. Членство в Asure создает несколько стимулов, которые должны привести к массовому принятию.

В децентрализованной пенсионной системе, как и в классической, любой кто вносит больший вклад, получает более высокую пенсию. Долгосрочные выплаты также играют роль. Чем дольше осуществляются регулярные выплаты, тем дольше будет выплачиваться пенсия.

Рис. 4: Модель PAYG

В настоящее время децентрализованное пенсионное приложение Asure работает на тестовой сети Ethereum Rinkeby. Он был разработан во время ETHBerlin Hackathon и доступен по ссылке: `https://ethberlin.asure.io`

Пенсия это ставка, по которой сумма, которую я плачу, по меньшей мере так же велика, если не больше, чем выплата. Децентрализованная пенсия основана на немецкой пенсионной системе и имеет "генерационный контракт". Молодое поколение платит старшему поколению в соответствии со своими возможностями, а взамен пенсии распределяются по токенам в виде токенов пенсионных прав (PET).

Модели стимулирования были разработаны в рамках проекта

Система исключает управление возрастом, что позволяет избежать мошенничества. Время делится на периоды, где период - месяц. В течение каждого периода могут быть сделаны депозиты. Для каждого периода фиксированная целевая цена может измениться, если медиана депозитов предыдущего периода будет сильно отличаться от целевой цены.

Если максимальное количество периодов было оплачено, также возможно максимальное количество пенсионных выплат. Предположим, что максимальное количество периодов равно 480 и равно 40 годам. Для ежемесячных выплат 40 лет, есть требование 40-летней пенсии. Если кто-то использовал систему только в течение 2 лет, заявка подана только на 1 месяц. Стимул к максимальному использованию системы вознаграждает участников с большим сроком пенсионного обеспечения.

$$entitlementMonths = \frac{payedMonths^2}{12 \cdot 40 years} \tag{1}$$

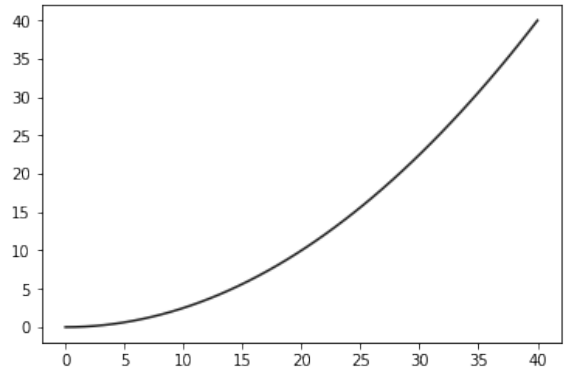

Рис. 5: Децентрализованные пенсионные выплаты относительно получаемых лет

Поскольку каждый может платить в системе разные суммы, максимальный плательщик получает максимальное двойное пенсионное право. Все те, кто платит больше, чем целевая цена периода, получат больше PET, но не более чем 2 за период. Максимально достижимые 960 PET, это позволит вам впоследствии претендовать на вдвое большее перераспределение, чем тот, кто активирует 480 PET.

$$DPT = \begin{cases} 1 + \frac{amount - amount_{max}}{targetPrice - amount_{max}} * DTP_{bonus} & amount \geq targetPrice \\ \frac{amount - amount_{min}}{targetPrice - amount_{min}} * DTP_{bonus} & otherwise \end{cases} \quad (2)$$

$$targetPrice - amount_{max} \neq 0 \quad and \quad targetPrice - amount_{min} \neq 0 \quad (3)$$

В качестве дополнительного стимула для ранних пользователей в системе был предоставлен бонус, который имеет множитель 1.5, а время логарифмического приближения к 1.0 планируется приближать ежегодно.

$$DTP_{bonus} = f(year) = 1.5 - 0.12 * log(year) \quad (4)$$

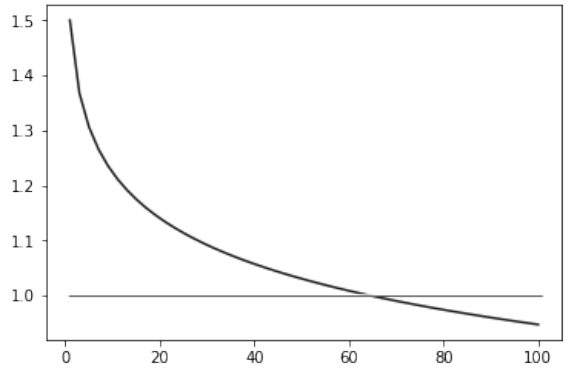

Рис. 6: Децентрализованный пенсионный бонус по годам

Если все выходят из системы, последние участники получают больше вознаграждений, поэтому мы гарантируем, что система останется прибыльной, поскольку нулевые участники системы снова будут установлены в исходное состояние.

Из-за ограничения в максимум 2 PET или с коэффициентом 1.5 первоначально 3 ПЭТ в течение периода в первые годы появляется возможность использования в системе нескольких счетов для оплаты, в которой система предотвращает передачу этих PET.

С помощью этих стимулов и прозрачного дизайна и подхода DAO это начнется как социальный эксперимент после необходимых симуляций и корректировок параметров в сети Ethereum.

Преимущества

Независимая крипто пенсия имеет много преимуществ, межпоколенческий контракт обеспечивает инфляционную безопасность. Он автономен и децентрализован в соответствии с идеей DAO. Там нет посредников. Конфиденциальность защищена, потому что никакие личные данные не нужны для участия в системе. Он полностью прозрачен, так как все транзакции находятся в блокчейне, а также с открытым исходным кодом.

Узнать больше

Мы суммировали наши идеи о том, как основанная на перераспределении система взаимного пенсионного обеспечения могла бы выглядеть и поделились нашими результатами с более широким сообществом.
Depot Paper: `https://www.asure.network/asure.depot.en.pdf`

6 Дальнейшея работа

Эта работа представляет собой единый путь к созданию сети Asure; Однако мы также считаем, что эта работа станет отправной точкой для будущих исследований децентрализованных систем социального обеспечения. В этом разделе мы определяем и заполняем две категории будущей работы. Это включает в себя работу, которая была завершена и просто ожидает описания и публикации и открытых вопросов для улучшения существующих протоколов.

6.1 Текущая работа

Следующие темы представляют текущую работу.

- Реализация Plasma MVP.
- Мобильное приложение (Android, iOS)
- Исследование децентрализованной системы социального обеспечения.
- Контракты и протоколы интерфейса Asure-in-Ethereum.
- Полная реализуемая спецификация протокола Asure.

6.2 Открытые вопросы

Есть еще области для улучшений, которые могут положительно повлиять на производительность сети. К ним можно вернуться позже после сбора достаточного количества статистических данных, по которым можно определить важность и необходимость внесения изменений:

- Лучшее решение для массовых стратегий входа и выхода.
- Безопасное решение проблемы недоступности данных.
- Более практическое применение SNARK/STARK.
- Лучшая стратегия для более быстрого внедрения систем социального обеспечения и новых экономических моделей.
- Лучший примитив для функции доказательства Proof-of-Stake, которая является публично-переменной и прозрачной.

Поскольку социальное обеспечение является лишь специализированной формой страхования, очевидно, что поддержка децентрализованного страхования на платформе также очевидна, и это хорошая пара для расширения этой платформы для рынка. Экосистема Asure состоит из сети Asure, протокола Asure, платформы Asure, на которой работают потенциальные сторонние приложения в области социального обеспечения и страховой среды. Признание экосистемы будет неуклонно расти из-за возникающих сетевых эффектов и синергии.

7 Организация

Asure является некоммерческой организацией, основанной на трех основных принципах: инновации, сотрудничество и исследования с сообществом участников, занимающихся исследованиями и разработками для новых разработанных решений, созданных в сети Asure, блокчейном и платформой для разработки решений блокчейна с системами социального обеспечения и страхования в стиле DAO.

Организация включает в себя исследователей технологий, а также экспертов по страхованию. Asure является неотъемлемым компонентом нашей работы, который позволяет нам координировать взаимодействие в различных частях экосистемы.

8 Благодарность

Эта работа является совокупным усилием нескольких сотрудников команды Asure Foundation и не была бы возможна без помощи, комментариев и обзора соавторов и консультантов Asure Foundation. Мы также благодарим всех наших сотрудников и консультантов за полезные беседы; в частности, Andrey Kuchaev, Alexander Böhner, Dirk Mattern, Dennis Rittinghof, Michael Lurz, Emanuel Kuceradis и профессор доктор Hirsch.

Заключение

Хотя поиск функциональных масштабирующих решений, касающихся блокчейн-систем, является широкой темой и требует много дополнительных исследований в целом, в оценках этого документа утверждается, что эффективные решения для улучшения или даже замены существующих систем могут быть построены с использованием блокчейна при со-

хранении финансовых и социальных факторов и социально-культурной выгоды. Plasma имеет большой потенциал для работы в качестве технологической базы масштабирования специально для систем социального обеспечения на основе блокчейна. Принимая во внимание некоторые трудности, такие как недоступность данных, другие проблемы и большое сообщество, работающее над этими проблемами, это каменистый путь, но все же возможный.

Мы в Asure считаем, что будущее социального обеспечения и страхования будет определяться технологиями блокчейна децентрализованным образом, что создает совершенно новый опыт, ориентированный на цифровой мир. Это может быть достигнуто только при использовании децентрализованной платформы блокчейна в качестве основы для создания сети, блокчейна, платформы и протокола для любых видов риска в мире.

Концепция реализации социального обеспечения через блокчейн уникальна и предлагает огромный потенциал для улучшения жизни людей во всем мире. Продвижение социального обеспечения на блокчейне принесет больше доверия, удовлетворения, свободы и мира во всем мире. Asure концептуально открыт и мы считаем, что он очень хорошо подходит в качестве фундаментальной платформы для очень большого числа решений в области социального обеспечения в ближайшие годы.

С нашей продажей токенов мы хотим, чтобы широкий круг людей участвовал в этом долгосрочном путешествии и создал историю успеха, изменив принципы социальной защиты в нашу новую цифровую эпоху. Примите участие в этом путешествии и присоединяйтесь к нашему событию по созданию токенов - мы с нетерпением ждем возможности приветствовать вас на борту!

Вебсайт	`https://asure.network`
Медиум:	`https://medium.com/AsureNetwork`
Твиттер:	`https://twitter.com/AsureNetwork`
Телеграм канал:	`https://t.me/AsureNetwork`
Фейсбук:	`https://fb.me/AsureNetwork`

Список таблиц

Список иллюстраций

Список литературы

[1] World social protection report 2017-2019, *Universal social protection to achieve the sustainable development goals*, International Labour Office, Geneva, 2nd edition, 2017.

[2] Etherscan, *Ethereum Transaction Chart*, `https://etherscan.io/chart/tx`, 2017.

[3] Worldometers, *World Population Forecast (2020-2050)*, `http://www.worldometers.info/world-population/`, 2017.

[4] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, `https://bitcoin.org/bitcoin.pdf`, 2009.

[5] Carmela Troncoso, Marios Isaakidis,George Danezis, Harry Halpin, *Systematizing Decentralization and Privacy: Lessons from 15 Years of Research and Deployments, In Proceedings on Privacy Enhancing Technologies*, De Gruyter Open, volume 2017, 2017.

[6] David Knott, *Construction of a Plasma Chain 0x1*, `https://blog.omisego.network/construction-of-a-plasma-chain-0x1-614f6ebd1612`, 2017.

[7] GDPR Info, *General Data Protection Regulation*, `https://gdpr-info.eu/`, 2018.

[8] Joseph Poon and Vitalik Buterin, *Plasma: Scalable Autonomous Smart Contracts*, `https://plasma.io/`, 2017.

[9] Minimal Viable Plasma, `https://ethresear.ch/t/minimal-viable-plasma/426`, 2017.

[10] Plasma Cash, `https://ethresear.ch/t/plasma-cash-plasma-with-much-less-per-user-data-checking/1298`, 2017.

[11] Ethereum, `https://ethereum.org`, 2014.

[12] Deutsche Rentenversicherung, *Wichtige Eckzahlen*, `https://www.deutsche-rentenversicherung.de/Allgemein/de/Navigation/6_Wir_ueber_uns/02_Fakten_und_Zahlen/03_statistiken/wichtige_eckzahlen_node.html`, 2016.

[13] Andrew Tayo, *Proof of work, or proof of waste?*, https://hackernoon.com/proof-of-work-or-proof-of-waste-9c1710b7f025, 2017.

[14] Jae Kwon, *Tendermint: Consensus without Mining*, https://tendermint.com/static/docs/tendermint.pdf, 2014.

[15] Zach, *Tendermint: Benchmarks*, https://github.com/tendermint/tendermint/wiki/Benchmarks, 2018.

[16] Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, Michael Riabzev, *Scalable, transparent, and post-quantum secure computational integrity*, https://eprint.iacr.org/2018/046.pdf, 2018.

[17] Christian Reitwiessner, *zkSNARKs in a nutshell*, http://chriseth.github.io/notes/articles/zksnarks/zksnarks.pdf, 2016.

[18] Fabian Raetz, *Aufbau und Funktionsweise des Bitcoin-Protokolls*, 2014.

[19] NRJ Coin Project, *NRJ Coin Project*, https://github.com/nrjcoin-project, 2014.

[20] European Report on Development (ERD): Deutsches Institut für Entwicklungspolitik, https://www.die-gdi.de/erd/, 2018.

[21] Health as Human Capital: Theory and Implications A New Management Paradigm, HCMS Group, http://www.hcmsgroup.com/wp-content/uploads/2012/05/WP01-HHC-Theory-and-Implications-2012-01-161.pdf, 2012.

[22] etherscan.io: gaslimit chart, https://etherscan.io/chart/gaslimit, 2012.

Сделано в Германии с ♡