ИИ и блокчейн — будущее или хайп? —А.Нам, А.Нечесов, А.Колонин, А.Галиева, Д. Пальчунов— Семинар AGI

А.КОЛОНИН [00:00:03] : Коллеги, всем добрый вечер. Мы начинаем очередное заседание русскоязычного сообщества разработчиков сильного искусственного интеллекта, которое сегодня проводится вместе с семинаром конференции «Знания, онтология и теории». вот и повестка нашего сегодняшнего семинара это обсуждение следующих вопросов есть ли будущего технологии распределенного реестра и блокчейна в частности вообще есть ли будущее у этих технологий как инструменты демократизации финансовой сферы в частности или вообще инструменты демократизации есть ли будущее этих технологий, как инструменты демократизации искусственного интеллекта и повышения уровня его безопасности? И, наконец, как технологии искусственного интеллекта могут помочь перечисленным высшей технологиям? Мы начнем с… докладов. Вот, соответственно, доклады, наверное, не обязательно должны быть напрямую связаны с озвученными вопросами. Они просто позволят спикерам рассказать о их собственной перспективе взаимодействия искусственного интеллекта и блокчейна и их будущего. Но, если будет возможность, я бы попросил спикеров как-то отнестись к вопросам, обозначенным для дискуссии. А после докладов к нам присоединяться в качестве спикеров Александр Балдачев и Виктор Носко, и мы попытаемся обсудить уже сфокусированно перечисленные здесь вопросы. И я с удовольствием предоставляю слово для первого доклада Александру нам, бизнес-кейсы применения ИИ-блокчейн. Александр представляет лабораторию блокчейн Сбера. Александр, пожалуйста.

А.НАМ [00:01:54] : Да, коллеги. Добрый день. Я сейчас свою презентацию покажу. Так, видно мою презентацию? Да. Да, ну, во-первых, спасибо большое за приглашение на эту конференцию. Для нас большая честь. Я возглавляю лабораторию блокчейн в Сбербанке. И наша лаборатория занимается исследованием технологии блокчейн, но у нас такой очень прикладной фокус. Все-таки мы работаем в коммерческой организации, и наша основная задача – это разработка продуктов и, соответственно, получение дохода. Вот поэтому в моем докладе… Я попытался сделать фокус на использовании технологии блокчейн в бизнесе, ну и показать вообще, какой фокус внимания сегодня у Сбербанка к этой технологии. Так как Сбербанк занимался раньше в основном финансовыми сервисами, сегодня Сбер – это не только банкно-технологическая компания, но все же финансовые продукты остаются, наверное, основными в нашей экосистеме. влияние на банковские и финансовые продукты. Так что ж, давайте посмотрим, как вообще меняется эра денег. Мы недавно буквально исследовали с коллегами отчет глобальной консалтинговой компании McKinsey, в сентябре вышел их очередной отчет по влиянию технологии. на платежный рынок и здесь очень все структурировано так написано смотрите по мнению коллег из макинзи мы сейчас с вами находимся в четвертой эре развития денег мы знаем да мы прошли с вами бумажную эру где использовались наличные деньги, банковские книжки, люди приходили в отделение, стояли в очереди, ну, чтобы снять деньги или положить их. Потом у нас была эра пластиковая, появилась пластиковая карта, это была большая инновация. По сути, карточка стала ключом к нашим счетам и... появились банкоматы, теперь не обязательно нужно приходить в отделение, можно

какие-то операции провести в банкомате. И банкомат, и карточка, это были такими инновационными технологиями на нашем рынке. Дальше мы с вами все плавно перешли в эру технологическую. McKinsey это называет эра счетов. Почему счетов? потому что теперь чтобы получить доступ к книгам карточка больше не нужна теперь мы с вами все пользуемся интернетом смартфоном появились у нас там разные методы платежа apple pay google pay и прочие и теперь панки по сути стали предлагать такие back office на и функции и вот теперь с 20 года вообще в новую эру, нырнули, чем же эта эра отличается? Во-первых, у меня очень интересное название, decoupled эра, что значит decoupled, это значит, что мы с вами переходим в эру атомарную, у нас теперь нету одного какого-то решения, у нас теперь появилось очень много разных решений, то цифровые валюты центральных банков это вообще новый инструмент вы слышали у нас на российском рынке сейчас центральный банк выпустил цифровой рубль теперь у нас люди могут пользоваться еще третьей формой денег и что здесь важно понимать что в этой эре новой эре технологии начинают играть ключевую роль. Какие технологии выделяют коллеги из McKinsey? В первую очередь, искусственный интеллект. Дальше, блокчейн. Они тут называют это как децентрализация, токенизация, но мы с вами как эксперты понимаем, что речь идет про технологию блокчейн. И в-третьих, они говорят про открытые API, про платформы. параллельно посмотрим на эволюцию технологии блокчейн, то окажется, что мы уже большой путь технология прошла, то есть 2008-2009 года с момента появления биткоин уже прошло порядка 15 лет, и в мире блокчейн мы с вами сейчас живем в так называемой area defy децентрализованных решал проблему переводов peer-to-peer транзакций, то в мире DeFi у нас появляются новые финансовые сервисы. За счет смарт-контрактов мы можем с вами оказывать такие услуги, как депозиты, кредиты, торговля, страхование. То есть, по сути, сегодня что происходит? Сегодня появляется совершенно новый рынок, если раньше у нас были банки, централизованные институты, которые оказывали финансовые продукты, то сейчас параллельно у нас есть новая цифровая инфраструктура на базе блокчейна. корпоративным блокчейном. Почему банки обратили внимание сейчас именно на децентрализованные финансы? По нескольким показателям. Обычно корпорации, финансовые институты смотрят на так называемый mass adoption, то есть это на спрос со стороны пользователей. И вот сегодня по многим оценкам насчитывается более 400 миллионов пользователей блокчейна. По оценкам в нашей лаборатории, это достаточно. Большая цифра, мы скорее более консервативные, нам кажется, что таких вот пользователей, их там около 100 миллионов. Но тем не менее 400 миллионов – это все пользователи мира, которые когда-либо проводили транзакция с криптовалютой. Так вот, что интересно? Интересно, что блокчейн сейчас по темпу роста пользователей очень похож на интернет. вот у нас интернет развивался именно так, то есть в 97-98 годах насчитывалось 400 миллионов пользователей и это значит, что блокчейн пользователей будет у нас миллиард где-то к 2030 году это показывает, что рынок достаточно перспективный Если раньше криптовалютой пользовались в основном скриптоны, люди продвинутые, то сейчас это вышло в масс адаптшн. Следующий показатель, куда смотрят корпорации и банки, это венчурные инвестиции. Вот у нас в блокчейн индустрии с вами в 2021 году было инвестировано 30 миллиардов долларов и из них 30% в проекты децентрализованных финансов. потому что венчурные фонды, когда заливают инвестиции в проекты, они по сути создают предложение, то есть за счет этих инвестиций стартапы начинают разрабатывать новые продукты, появляется предложение, чем больше инвестиций, тем больше проектов, соответственно, тем

больше будет пользователей. Как я говорил, корпорации, в том числе Сбербанк, раньше занимались корпоративным блокчейном. Вот здесь вот на слайде написано, что 77 корпораций из 100 крупнейших, они развивали блокчейн. Но если мы с вами посмотрим, какой именно блокчейн, то мы увидим, что это все корпоративные... платформы Hyperledger, Quorum, Corda, это все корпоративные так называемые Permissioned платформы, то есть там у нас есть какой-то один институт, который контролирует этот блокчейн и отвечает за подключение пользователей, а публичный блокчейн он был вне поля зрения корпораций, корпорации не занимались но какая сейчас тенденция с 2022 года крупнейшие банки мировые стали обращать внимание на DeFi, децентрализованные финансы, этот тренд, он сейчас происходит на публичных сетях, эфириум, полигон и поэтому банки стали внимательно смотреть, что же там такое происходит Вот в качестве примера могу рассказать, крупнейший американский банк JP Morgan в ноябре 2022 года выпустил стейбл коин на публичной сети Polygon, Societe Generalis, французская финансовая группа, они в этом году на эфириуме выпустили стейбл коин, привязанный к евро, австралийский вот этот вот NAP, они тоже в этом году на эфириуме стали проводить трансграничные переводы, ну и многие-многие другие банки сейчас активно занимаются децентрализованными финансами том числе кстати говоря Сбербанк мы тоже сейчас экспериментируем с публичными сетями и пока только в тестовой в тестовой тестовой среде потому что у нас законодательства еще нету но мы этим занимаемся вот ну и наконец чтобы Картинка была объективная, нужно сказать, что DeFi, децентрализованные финансы, ну и вообще блокчейн для банков, это не всегда. скажем так, возможности, есть еще и открытые вопросы. Вот сегодня мы выделяем следующие риски, присущие блокчейну и дезентрализованным финансам. В первую очередь это регулирование и законодательство. Большинство регуляторов мира, как вы знаете, отрицательно-негативно относятся к децентрализованным финансам, и вот регулирование, оно сдерживает развитие этой индустрии. Второй момент – это вопросы безопасности. Мы смотрели отчет американской компании Chainalysis, 8 миллиардов в 22 году и в 23 году это потери инвесторов, пользователей криптовалют от мошенников, 8 миллиардов долларов, если совокупно рынок сейчас порядка 60 миллиардов, то 8 миллиардов это большая цифра, третий момент низкая ликвидность, так как у нас много разных блокчейн платформ ни в одном проекте нету достаточной ликвидности. Дальше стоимость транзакции высокая, так называемый GAS-FI, и пока вопрос с транзакциями не решится, мы с вами не увидим массового использования этой истории. Ну и наконец, это клиентский опыт UX-UI, то есть пользовательский опыт крайне плохой. То есть для того, чтобы воспользоваться каким-то сервисом, нужно иметь понимание техническое, разбираться в криптографии и делать достаточно много приседаний, чтобы купить криптовалюту и получить какую-то доходность. Теперь, возвращаясь к теме нашего сегодняшнего доклада. Конечно же, мы тоже в лаборатории исследуем вопросы, а где же искусственные интеллекты блокчейн пересекаются и какая между ними есть синергия. Мы пока не все можем инициативы и проекты озвучить в силу коммерческой тайны, но мы можем выделить несколько моментов. которые есть в блокчейне, то искусственный интеллект может частично какие-то из этих проблем решить. Вот допустим, все, что касается регулирования. Сейчас очень большая проблема – это понимать вообще, в какой стране какое регулирование, потому что каждая страна идет по своему пути. Кто-то жестко запрещает, кто-то наоборот разрешает, создаются какие-то хабы и так далее. Искусственный интеллект мог бы, инструменты на базе искусственного интеллекта

могли бы как раз-таки эту проблему частично решить. То есть многие инвесторы, многие корпорации, они работают на разных рынках, то есть глобальной корпорации. И вот вместо того, чтобы вручную постоянно проверять... а какая здесь регуляция, а здесь криптовалюты запрещены или не запрещены, а как они здесь учитываются, как ценные бумаги или как что? Вот это можно все автоматизировать за счет искусственного интеллекта и частично проблему решить. Дальше, смотрите, мы выделяли безопасность как большой риск. Здесь тоже мы видим, что решение на базе искусственного интеллекта для автоматического определения мошенников сейчас в большом спросе. И здесь роль искусственного интеллекта очень большая. То есть здесь можно определять… строить какие-то инструменты, чтобы заранее превентивно находить скам-проекты, находить мошенников, находить уязвимости в смарт-контрактах. это очень интересная история. когда мы говорим про ликвидность, вот третий пункт был, низкая ликвидность. здесь тоже искусственный интеллект инвесторов, а почему мало инвесторов, потому что в децентрализованных финансах, там нет посредника, там нет банка, значит некому обратиться, если у тебя проблема какая-то, ну вот ты не можешь допустим что-то сделать или ты забыл пароль от кошелька, тебе некому обратиться. ты полностью отвечаешь за сохранность своих криптоактивов отсутствует даже телефон техподдержки, просто некому позвонить использование чат-ботов помогло бы решить проблемы с техподдержкой и, соответственно, это бы увеличило количество инвесторов и помогло бы с ликвидностью вот это вот третий кейс, который мы изучаем Ну а дальше вот три пункта, это уже, ну скажем так, наши размышления, я с коллегами вот вчера мы собрались, подискутировали, сейчас рынок генеративного искусственного интеллекта, он очень централизован, да, ну наверняка сегодня будут обсуждения, то есть крупные технологические компании, они разрабатывают свои модели, для большинства людей эти модели это какой-то black box, черный ящик мы не понимаем как они работают, и блокчейн мог бы демократизировать доступ то есть если бы мы использовали блокчейн, возможно бы Каждая компания, каждый пользователь смог бы получить доступ, и это было бы более эффективно. Это очень большое направление, мне кажется, здесь будет много высказываний экспертов. Оставим это на дискуссию. Следующее. Очень тоже такая интересная история. Это подтверждение. что какой-то контент был сгенерирован с помощью искусственного интеллекта или с помощью человека. Вот сейчас вот этот момент такой, он очень-очень актуален. И здесь, опять-таки, мы могли бы использовать блокчейн для того, чтобы подтверждать, Ну и, наконец, самая, как мне кажется, важная история, в блокчейне можно сохранять приватность. И это очень актуально будет для как раз-таки больших моделей искусственного интеллекта, когда данные, которые идут на вход, их нужно оставить приватными. Здесь мы можем использовать разные примитивные протоколы, то же самое ZK, сейчас новая история ZKML, когда используется ZKProof в искусственном интеллекте. И вот здесь это тоже большое направление, здесь тоже можно подискутировать. Ну вот я вот специально, наверное, здесь сейчас остановлюсь, чтобы оставить какие-то вопросы для обсуждения и дать вам потом возможность позадавать вопросы, коллеги. Спасибо.

А.КОЛОНИН [00:21:37] : Александр, спасибо. Коллеги, есть какие-то короткие вопросы на понимание, чтобы получить короткий ответ и двинуться дальше? Или перейдем к следующему спикеру? Коротких вопросов нет. Тогда оставим дискуссию на

после всех докладов. И следующее слово предоставляется Андрею Нечесову, Институт математики Сибирского

А.НЕЧЕСОВ [00:22:08] : Здравствуйте. Сейчас, секундочку. Так, надо поделиться экраном.

А.КОЛОНИН [00:22:25] : Ну, давай презентацию.

А.НЕЧЕСОВ [00:22:27] : Да-да. Здравствуйте еще раз. Спасибо за приглашение, чтобы выступить в качестве докладчика на этой конференции. Статья наболевшая, давно мы ее пытались реализовать, аксиоматизировать теорию блокчейна. Ну, во-первых, давайте я расскажу о себе, наверное, немножко о том опыте, который я имею. Во-первых, сейчас я являюсь сотрудником Института математики, работаю в команде Гончарова Сергея Семастьяновича, академика. Он специалист в области логики, теории вычислимости и других направлений в логике. И я в свое время очень активно занимался именно блокчейном, где-то это был 2017 год, когда я активно начал заниматься, погрузился в блокчейн непосредственно, начал разрабатывать смарт-контракты на Solidity для Эфириума. Мы провели несколько ICO для наших заказчиков из США. Они были успешны. ICO, контракты стандарта ERC-20, там, ну, были хорошо все написано. Деньги собрали, но были там проблемы у них, у американцев, и это ICO закончилось у них плачевно, но я тогда получил первый опыт и понял, что это огромные возможности. На самом деле, возможности в том, что по сути вас никто не регулирует, никаких запретов нет на сбор средств Возможности, конечно, большие, но правительству это не нравится. Это вопрос к тому, вообще есть ли у будущего блокчейна. Я скажу так, вот первое. затравлю тему немножко то что людям конечно обычным это очень-очень выгодно что у них есть свобода и контроль над финансами свобода оплат можно за границу за рубеж никакие банки не контролируют ничего и в то же время у правительства конечно проблема они не отслеживают ваши счета и хотят держать всех под контролем своих граждан, поэтому идет борьба двух вот этих вот как бы сообществ. Какое победит, посмотрим, но пока что, я думаю, примерно идет такой баланс на самом деле. Вроде где-то запрещают какие-то криптовалютные биржи и так далее, но находится другая более децентрализованная криптовалютная биржа или еще какие-то решения. Поэтому посмотрим, что будет в Ну а давайте я все-таки вернусь к аксиматизации теории блокчейна. Так вот, впервые, когда мы задумались о аксиматизации, это был 2017 год, когда Сергей Севастьянович предложил прореферировать статью своей ученицы на семинаре теории вычислимости, это была статья итальянских математиков, они привели самый простейший блокчейн, Аксиомы из интуиционистской логики, и поэтому, в общем, классическая, во-первых, логика как бы не работала, во-вторых, они сами пишут, что это просто тестовый блокчейн, он никак не относится, не связан ни с биткоином, ни с эфириум блокчейном, ну и так далее. Сразу отмечу, я в свое время работал только с proof-of-work консенсусами, то есть и тогда еще эфириум был proof-of-work, и биткоин. Proof-of-stake, конечно, мы изучали и другие виды децентрализованных решений, как Tangle graph, то есть для IOT. Это все есть, но, скажем так, по ощущениям было следующее, что нужно, во-первых, попытаться аксиматизировать то, что ты хорошо знаешь. Знаешь proof-of-work консенсус. Поэтому мы засучили рукава и начали разбираться в видах блокчейнов, которые работают на Proof-of-Work консенсусе. На самом деле их достаточно много, но все они примерно очень похожи. Сейчас я покажу.

Во-первых, как мы привыкли, в биткоине есть цепочка блоков, и нет никаких анкл-блоков или омер-блоков и других вещей. Допустим, в эфириуме и в других блокчейн-решениях были такие понятия, как анкл-блок – это тот блок, который был сгенерирован параллельно. Но чтобы его не отбрасывать, как форк некий, чтобы выбирать наиболее длинную цепочку по активности, мы его добавляли в следующий блок. Как видно здесь, в новый блок добавляется родительский блок и указываются анкл-блоки. Для чего это нужно? Во-первых, мы не отбрасываем уже найденные блоки, которые на самом деле находятся не так просто, потому что, чтобы найти блок, который бы удовлетворял нужным параметрам, нужно решить достаточно трудную вычислительную задачу. По сути, мы... Генерируем очень много различных вещей, смотрим, совпадает ли хэш, например, в биткоине, чтобы было n нулей впереди после всех сжатий. Это достаточно сложно, перебираются миллиарды и миллиарды вариантов. Поэтому, чтобы не отбрасывать такие блоки, которые на самом деле хорошие, на которых точно была произведена работа, просто так их сюда не вставить в Proof for Consensus, здесь было такое найдено решение, что добавляем их в виде анкл-блоков к новому блоку. Как минимум, у нас уже есть 2 разновидности. Во-первых, в биткоине анкл-блоков нет, в эфириуме есть. То есть вот здесь тоже жадные алгоритмы, ГОСТ используют, выбирается самая длинная ветка в наиболее в индуктивно задаваемом, наиболее ветвящемся по дереве. Вот, например, если использовать алгоритм ГОСТ, то фактическим блокчейном, которым нужно учитывать транзакции, это вот блоки A0, A1, A2, A3, A4. Но если использовать просто Longest Rule, то это блоки с A0, B1 и B6, то есть по биткоину, если блокчейн биткоины. Как видим, у нас как минимум есть два варианта. То есть первый вариант, мы должны, если мы используем ГОСТ-алгоритм, то мы в принципе можем блоки B1, B6 просто выбросить на самом деле. Они не участвуют в формировании ветвистости вот этого поддерева, который начинается с корня A1. Ситуация такая, что блок D2 и D3, если мы выбросим, то дерево оспудеет на самом деле, оно будет слабое, то есть и тогда уже, если мы еще и F3 выбросим, то у нас вот эта ветка B1, B6 будет по блокам более… содержать больше блоков, и она просто победит, то есть выбрасывать лишние блоки, которые участвуют в алгоритме консенсуса, в договоренности, в которой мы должны выбирать реальный блокчейн, даже если их транзакции даже не участвуют в реальном блокчейне, нельзя. Поэтому, как минимум, у нас должны быть следующие операции. То есть у нас должна быть функция, которая выбирает общий блокчейн, так сказать, с теми вспомогательными блоками, как анкл-блоки или для ветвящего дерева просто блоки. Она выбирает под дерево a0, a1, a2, a3, вот все под дерево за исключением b1 и b6 блоков. не участвует в алгоритме консенсуса. Дальше есть функция блокчейна – выбрать из самого ветвящегося под дерево, ну, грубо говоря, индуктивно вот этого Задоноваевого, конкретную, правильную ветку. Далее у нас, смотрите, то есть когда мы говорим о блокчейнах, на самом деле мы работаем не с цепочками блоков, как мы хотели бы, а мы работаем постоянно с деревьями, потому что из деревьев мы должны выбирать под деревья или ветви дерева, то есть на самом деле у нас объектами выступают деревья, но ветка дерева это тоже цепочка блоков на самом деле в блокчейне, это тоже дерево, но просто без ветвлений. Поэтому два типа в нашей теории будет объектов, которые мы хотим максимализировать. Это деревья и это блоки. Больше ничего в этой теории нет. То есть хотелось бы сделать так, чтобы эта теория была именно, чтобы моделью этой теории были такие всем известные модели, как биткоин и эфириум. То есть. Это означает, что мы не все операции биткоина должны как бы здесь закодировать, а вот то, что мы закодировали, вот в этой теории,

оно будет, если взять вот эти, по сути, функции на моделях биткоина и эфириума, они будут выполняться, теория, получается, выполняется в модели биткоина и эфириума. Далее мы ввели понятие родительского отношения. Ввели понятие функции добавления к дереву T, в котором есть блок X некоторого блока У. Также была такая достаточно тонкая тоже вещь – это точная нижняя грань для двух блоков в дереве T. На самом деле, тоже важно, чтобы она находилась. Константный символ 0 – это Genesys блок на самом деле для того, чтобы мы как бы сразу ограничили теорию, что у каждого блокчейна есть свой Genesys блок. И далее мы ввели обязательно условие – это линейный предпорядок на деревьях. То есть мы можем сравнить два любых дерева и выбрать то, которое… которая поэтому предпорядку больше, на самом деле, это очень важно, по сути, вот этот линейный предпорядок, он и задает консенсус, к которому мы все так привыкли proof-of-work, на самом деле, здесь не только proof-of-work пройдет, но proof-of-stake тоже пройдет, но не все варианты. не эксперт как раз в Proof of Stake или Proof of Activity, Authority и так далее консенсусов, но вполне возможно, что взять эти все результаты и перенести на другие виды консенсуса проблем не будет. Есть отношение эквивалентности на блоках, это когда хэши блоков совпадают, а вот внутреннее содержимое этих блоков разное, то есть они могут быть эквивалентны, но не равны. Далее мы ввели обозначение, то есть, что значит блок лежит ниже другого блока в дереве t, это от меньше либо равно b, равно b, это вот, по сути, совпадает, вот эти условия выполняются. И t эквивалентны, то есть одно дерево t равно другому, это когда оно меньше либо равно t. То есть у нас на самом деле возникают, допустим, две ветки одинаковой длины, это два дерева. То есть, по сути, вот они T равны, получается. Дальше мы ввели аксиоматику. Как я уже сказал, функция B у нас выделяет общий блокчейн из дерева. То есть, если мы выделили один раз общий блокчейн из дерева, отбросили вот те вот, если вспомните рисунок B1, B2, B3, B6 блоки, то второй раз, если мы эту же функцию применим к тому, что осталось, на самом деле ничего не изменится, больше мы ничего выбросить не можем. Это вот первое аксиома, второе аксиома, это что, если x принадлежит тому, что мы выбрали из дерева, то это и будет самому дереву принадлежать, ну и так далее. 3, 0, b, t, это означает, что у нас, по сути… 3.0 – это предикат, выделяющий, что B от T должно содержать, быть под деревом. Во-первых, это будет дерево, элемент дерева, и будет содержать как раз Genesis-блок этот предикат определяет. x принадлежит bc bt, следовательно, x принадлежит bt, это означает, что если x принадлежит блокчейну от того, что мы от функции bt, да, от того поддерева, которое получилось, то x будет принадлежать bt, ну и… Что здесь еще? Вот дерево. Что это дерево будет? Что 3, 0, b, c, a, b, t. То есть, это логические правила, это абстрактные аксиомы, которые, в принципе, подходят для большинства Proof-of-Work блокчейнов, которые, по крайней мере, были 5 лет назад. Может быть, сейчас какие-то новые появились, я не знаю. Это вот первый блок – это блокчейн аксиомы, второй блок – это аксиомы эквивалентности. Ну, здесь тоже эквивалентности блоков, если два блока эквивалентны, то если один эквивалентен второму, а второй третьему, то третий будет первым эквивалентен третьему, ну и так далее. Аксиомы порядка, аксиомы нуля, что genesis-блок принадлежит любому дереву, и что здесь еще для любого, так, я уже, так, для любого x. Ну да, что последнее Zero Axiom Tool говорит о том, что 0 всегда по порядку ниже, чем x в дереве t. Здесь Axiom ограниченности мы ввели. На самом деле, Axiom ограниченности, они… задают структуру дерева. Вот эта точная нижняя грань очень полезна для того, чтобы эта структура была деревом, чтобы это не была решеткой или еще каким-то другим объектом, который мы не приемлем. Вот эти аксиомы, по сути,

вырезают все лишнее и оставляют... То есть синтаксически мы задали как раз структуру дерева за счет вот этих вот точных нижних граней. Это, кстати, идея пришла, когда в 22 году мы разбирали статью Рида, где он аксиоматизировал бесконечные деревья. Но на самом деле здесь в общем случае как бы, то есть мы рассматриваем пока что конечные варианты, но скорее всего и на бесконечных здесь все пройдет. две аксиомы генерации, то есть мы можем сгенерить по дереву T1 большее дерево, T2, и в другую сторону по большому дереву мы можем отщипнуть листочек и получим дерево меньшее, то есть то что останется это будет меньшее просто дерево. Вот это две больших аксиомы, они достаточно сложные, но как бы почитав их ничего сложного в них нет. Родительская аксиома, в каких случаях Два блока являются материнским и дочерним относительно дерева T, ну и аксиомы identity, то есть когда B равны, тогда и только тогда, когда равны, и деревья равны, когда эквивалентны, то есть два эквивалентных блока в дереве быть не может, если они не равны, потому что нарушается структура дерева, то есть вообще в блокчейне это нонсенс получится. Основные теоремы, мы доказали, что биткоин, модель биткоина, блокчейна биткоина является моделью теории T, и то, что модель эфириума тоже является моделью теории T, то есть все аксиомы теории T выполнимы в этих моделях. Оставшиеся аксиомы, вот эти вот, которые сложны, на самом деле они жестко между собой завязаны и независимость относительно их показать не получается, но если их все выкинуть, а вот оставить только баундеры аксиомы эквивалентности Zero и блокчейн, то тоже они будут, каждая из них относительно тех тоже независима, то есть это говорит о том, что они каждая в отдельности будет независимо относительно первой группы Axiom. Вот такая вот статья получилась, я считаю это на самом деле наша первая попытка аксиоматизировать то, что до этого не было аксиоматизировано, построить тот мост между программированием и теми блокчейн решениями, которые есть на сегодняшний день. Ну и мы сейчас разрабатываем свою платформу, в которой участвует Сергей Севазьянович Гончаров, Дмитрий Иванович Свериденко, я участвую, студенты участвуют, ну и разрабатываем. интеллектуальную дельта-платформу на базе блокчейн-решений. Притом не просто в основе лежит один блокчейн, а мы работаем с мультиблокчейнами сейчас. Я, к сожалению, картинку не стал вставлять, но кому будет интересно. Мультиблокчейны – это вообще фишка последних лет. Это когда Николай и Павел Дуров написали свой whitepaper для Telegram Open Network или The Open Network сейчас, как их называют. Там как раз впервые было указано, говорилось про мульти блокчейны. Мне что понравилось, на каждом из этих уровней они решают, по сути, есть такая общеизвестная трилемма блокчейна, что нельзя там одновременно достичь высоких показателей по трем параметрам. безопасность, децентрализация и масштабируемость, а вот на уровне мультиблокчейнов вот по каждым двум параметрам на каждом из уровней мы достигаем либо мы достигаем безопасности и децентрализации на верхнем допустим уровне, а на нижних уровнях мы достигаем масштабируемости, то есть большой скорости записи, а просто вот эти вот блокчейны нижнего уровня там раз в сутки отсылает в более высокого уровня блокчейна свой снимок, то есть если вдруг кто-то подменит эти более слабые блокчейны, то просто снимок не совпадет с помощью хэш-функции сжатия, не совпадет с тем, что было, то есть я считаю это отличное решение, и у нас как раз в Дельта платформе это решение сейчас реализуется. Очень интересно это применение для Узбекистана, к нам приезжал как раз стажер, и была задача для Узбекистана разработать модели умных городов, где много различных умных устройств, откуда им информацию писать. писать могут локально, но как писать? Как привычнее работать,

чтобы был единообразный формат, а привычнее всего на самом деле работать с блокчейном, то есть его можно писать локально, как вот предыдущий докладчик говорил, что многие приватные блокчейны делали. А потом этот приватный можно сделать децентрализованным на самом деле, проблем вообще нет, все зависит от того, от наших хотелов. Поэтому устройства могут писать на локальные компьютеры с любой скоростью, там децентрализации не будет, но в виде блокчейн структур. А дальше по иерархии это поднимается все выше и выше, и в конечном счете, если нам нужна безопасность, пишем. более высокие уровни блокчейна. Скорость пишем в нижнем. Плюс, огромный плюс блокчейна в том, что на них можно исполнять умные контракты, то есть программы в децентрализованных средах, это вообще круто. Когда эфирио вышел, как раз это было основное преимущество его перед теми же решениями на биткоин, потому что... На биткоине вы не можете в общем случае как бы исполнять умные контракты. Есть скриптовый небольшой язык, ну и все. Вот, смарт-контракты по сути это, если говорить с точки зрения искусственного интеллекта, то мы можем закладывать какие-то умные алгоритмы, вешать, завертывать, обертывать в смарт-контракты. и хранить их в блокчейн структурах, то есть, во-первых, есть неподдельность данных, мы видим, на каких, да если это будет нейронная сеть, то мы будем видеть, на каких данных она обучалась, а действительно ли там никто не подменил эти данные в какой-то период времени, если подменил, то мы будем видеть, что выше стоящих уровней блокчейна слепок вот этот уже не бьется, то есть хэш-функция не совпадает, то есть перспективы на самом деле блокчейна для Искусственного интеллекта огромный. Как я уже сказал, есть четыре проблемы, ну или три проблемы искусственного интеллекта. Это проблема централизации, когда искусственный интеллект находится в руках одной корпорации. Ну, тот же Чаджи-Пити, да, в руках OpenAI. Мы не знаем, как он настроен, как его разработчики настраивают. Есть проблема аудита многих вещей. Есть просто объяснительная проблема, как объяснить, как она работает, то есть даже если мы вскроем эту нейронную сеть с миллиардом параметров, нам непонятно, почему она принимает такое решение. Blackbox проблема, ну и еще ряд проблем, которые реально нам непонятны с блокчейном и с другими решениями на базе смарт-контрактов. Смарт-контракты и блокчейн нам помогают, по крайней мере, частично решить все эти проблемы. Ну вот вкратце так, спасибо за внимание, если у кого-то есть вопросы, комментарии, задавайте, наши контакты, если кому-то будет интересно посотрудничать, пишите, все, спасибо.

А.КОЛОНИН [00:44:25] : Андрей, спасибо, коллеги, есть у кого-то короткие вопросы для коротких ответов на понимание? Хорошо. Тогда двигаемся дальше. Следующий доклад, собственно, мой. Давайте я сейчас тоже расшарю свой экран. Так. Мне нужно расшарить свой экран. Так. И... Да, поскольку я сегодня буду выступать немножечко в роли блокчейн-пессимиста, я в двух словах скажу, что я с блокчейном серьезно и, точнее, с распределенным реестром, потому что на самом деле блокчейн является частым случаем технологии распределенного реестра. С этой технологией я сталкивался серьезно трижды. 95-96 и даже немножко 97 годах я занимался разработкой системы безналичных расчетов по пластиковым карточкам за Байкали. И в связи с тем, что объективно была невозможность обеспечить надежную связь между различными точками продажи и зачисления денег в системе безналичных расчетов. Нам просто… мы оказались перед необходимостью разработки технологии распределенного реестра между различными точками расходования и пополнения

финансовых ресурсов на этих карточках. Это было мое первое столкновение с этой технологией. Потом, начиная с 97-го года… По 2002 год я занимался разработкой системы семантического моделирования, описания и редактирования антологии на основе распределенного репликации и реализации своего собственного протокола. как языка межпротокола обмена между различными дизентрализованными узлами, так и достижения того, что сейчас принято называть консенсусом. Ну и, наконец, в 2017 году я был одним из людей, которые стояли у истоков модного и известного проекта Singularity Net, посвященного соединению. искусственного интеллекта и блокчейна. При этом я на сегодняшний день имею высказать некоторый скепсис именно в части того, что существуют фундаментальные проблемы, которые не позволяют совместить с одинаковой успешностью достижения четырех целей. Я выделяю не три, а четыре цели, то есть первое – это дешевизна выполнения транзакций или то что называется GASFI. Третье это безопасность выполнения транзакций, где под безопасностью можно подразумевать как возможность взлома, как обеспечение защиты от взлома кошелька, так и исключение той ситуации, когда вы вроде как заплатили деньги или вам вроде как заплатили деньги а потом спустя какое-то время выясняется что транзакция не прошла ну и ведь вы оказываетесь ситуации когда вы бы не получили за оказанную услугу вот либо вам не получили оказанный сервис. Ну и наконец децентрализация и демократизация, которая вроде как призвана обеспечить отсутствие централизованного контроля и злоупотребления. возможность злоупотребления некоторым институтам, возможности управления и манипуляции всей экосистемой. Так вот, эти четыре, грубо говоря, все эти четыре составляющие равняются константе. Если, к примеру, мы хотим увеличить скорость выполнения транзакций за счет так называемого оптимистика лапа, когда мы заранее проводим сначала транзакцию, а потом в течение какого-то время финализируем ее за счет валидаторов. И в какой-то момент выясняется, что валидаторы не верифицировали транзакцию, транзакция отменяется, но мы по сути тем самым нарушаем безопасность. Или в конечном итоге увеличение скорости оказывается... иллюзорным, потому что на самом деле то, что транзакция прошла, ничего не означает до тех пор, пока не прошло так называемое финалитета, время финализации транзакции, когда мы можем считать, что транзакция прошла и таким образом, казалось бы, расплатившись заказчику кофе за 30 секунд, мы должны ждать еще полчаса, пока не убедимся, что наша кофе действительно оплачена или что нам за это кофе заплатили. Ну или другой пример, если мы увеличиваем скорость за счет и безопасность за счет усиленной криптозащиты транзакций, мы тем самым теряем стоимость, то есть применение дорогостоящих криптографических алгоритмов увеличивает скорость транзакции. Ну или наоборот, если мы выносим обработку транзакции с сайдчейны, мы, казалось бы, увеличиваем скорость одновременно и дешевизну, но при этом мы жертвуем децентрализации, потому что на самом деле мы сегментируем сеть, вот у нас получаются просто маленькие сети отдельно, каждую сеть отдельно взломать проще, чем всю сеть в целом, Потому что там меньше участников, которые участвуют в консенсусе, и, соответственно, мы теряем и в децентрализации, и в демократизации, и в безопасности. И с тем, чтобы решить перечисленные проблемы, в свое время мы пришли к пониманию так называемого репутационного консенсуса. Вот на самом деле понятие репутационный консенсус сейчас в различных работах используется немножко по-разному. То есть, есть то, что мы называем честный репутационный консенсус. Вот и мы были первые, кто его предложил. Но существуют работы, где под репутационным консенсусом подразумевается, на самом деле, некоторая вариация Proof of Authority,

где предполагается, что репутация просто прошивается в сетку институтам, которые, по сути, управляют тем или иным блокчейном или той или иной системой распределенного реестра. Вот здесь я буду говорить именно о том, что мы подразумеваем proof of reputation или доказательство репутации, которое основывается на том, что мы называем текучая репутация. Сразу обращу внимание, что терминология немножечко Плавает в этих вопросах, как мы знаем, на самом деле, под блокчейном часто подразумевают систему распределенного реестра, в то время как в чистом виде блокчейн это достаточно частый и не всегда самый эффективный пример реализации технологии распределенного реестра. Точно так же под консенсусом... часто поднимают сегодня не только сам алгоритм достижения консенсуса между его участниками. То есть, это чисто в виде математический алгоритм того, как участники и контракт, описывающий то, как участники договариваются о принятии или не принятии того или иного блока или той или иной цепочки блоков. А в расширительном смысле под консенсусом обычно подразумевают также некоторые критерии отбора участников, которые принимают участие в консенсусе, и в том числе возможно веса этих участников, которые отобраны для участия в консенсусе, когда эти участники голосуют за принятие того или не принятие того или иного решения, того Значит, основные методы на сегодняшний день репутационного консенсуса основаны на… То есть, я буду сегодня говорить о консенсусе в расширительном смысле, говоря в первую очередь именно о взвешивании узлов, принимающих решения в консенсусе или допускаемых или недопускаемых. консенсусу на основании соответствующего веса. Итак, первый способ взвешивания участников основан на доказательстве силы, что называется, то есть у кого больше вычислительных мощностей, имеют больше возможности контролировать контролировать формирование цепочек-блоков и таким образом с одной стороны имеют возможность с большей вероятностью эксплуатировать блокчейн, значит известные атаки, когда майнер владеет, получает возможность управления формирование блоком он в процессе формирования блока он анализирует последовательность транзакций вот и осуществляет так называемый front running если он видит что значит в результате осуществления каких-то транзакций как которые оказываются в данном блоке происходят те или иные изменения цены, он соответствующим образом размещает свои собственные транзакции до или после тех транзакций, которые обнаруживает в том блоке, который ему доверено формировать, и тем самым люди, которые совершают которые заявили эти транзакции после сформирования блока, они обнаруживают, что у них покупка или продажа прошла совсем не по той цене, по которой они рассчитывали. Ну, а, соответственно, человек или узел, который формировал этот блок, он получает свою маржу. Не говоря уже о том, что Proof of Work – это разрушительный для экологии консенсус, который требует электричества, загрязняет окружающую среду и все тому подобное. Следующий консенсус это так называемый proof-of-stake, причем proof-of-stake имеет неприятное с точки зрения теории демократизации общества с помощью консенсуса свойство, что те, кто обладают большими деньгами, получают большую возможность по формированию блоков, транзакций. И, соответственно, получают большую возможность получения компенсации за поддержку блокчейна. Соответственно, Proof-of-Stake в полной мере реализует принцип «богатое становится богаче», что тоже, в общем, недостаточно демократично. Хотя, с точки зрения скорости выполнения транзакции и дешевизны транзакции, этот способ является гораздо более зеленым и экологически чистым, чем proof-of-work. Ну и самая распространенная на сегодняшний день версия консенсуса proof-of-stake, это delegated proof-of-stake, она по сути вообще

как-то элиминирует... дискредитирует основные идеи блокчейна потому что и демократизацию общества с помощью блокчейна потому что на самом деле отбор тех кто принимают участие в консенсусе осуществляется на основе отдельного голосования которое как бы выходит за рамки самого алгоритма консенсуса Поэтому мы предложили так называемый алгоритм Proof of Reputation, который позволяет взвешивать участников как с точки для отбора их для участия в консенсусе, так и при необходимости учета голосов при голосовании за принятие либо неприятие тех блоков в зависимости уже, собственно, от самого алгоритма вычислительного консенсуса. То есть, мы предлагаем только алгоритм взвешивания, который является определенным расширением принципа PageRank, который был в свое время изобретен изобретателями Google. для рейтингования страниц. С той разницей, что наш алгоритм рейтингования участников, он, во-первых, имеет комплексную природу, то есть наш алгоритм может основываться как на транзакциях в сети, так и на нетранзакционных взаимодействиях, если Допустим, блокчейн охватывает не только финансовую экосистему, но и социальную сферу, включая в себя, допустим, комментарии, посты, лайки, комменты, реплай и упоминания. Соответственно, тот, кто получает более лайков, он тоже имеет возможность получать большую репутацию. Ну и сама репутация считается следующим образом, если у нас в момент времени t1 есть некоторые участники с какой-то репутацией, то когда мы хотим рассчитать репутацию в момент времени t2, мы берем все транзакции, которые совершили за момент времени t1, t2 минус t1, и по каждой транзакции явную или неявную репутационную оценку, которая была совершена. в интервале между временами T2 и T1, мы присваиваем тому участнику, которому эта оценка выставлена, но эта оценка взвешивается репутацией того, кто проставляет эту оценку. Таким образом, не явно у нас все сообщество. Абсолютно всё сообщество участвует в формировании как репутации одного отдельного участника, так и неявно принимает участие в голосовании за формирование блоков имени того участника, который входит в группу консенсуса по результатам отбора на основе рейтингов, полученных с помощью текущей репутации. И что важно, эта репутация меняется со временем, потому что мы имеем возможность... Если, допустим, какой-то человек становится более активным или становится менее активным, его репутация может убывать или увеличиваться. Ну вот здесь показан алгоритм, у меня нет времени распространяться по поводу его деталей. Есть соответствующие публикации, есть две реализации кода алгоритма текущей репутации на Python и на Java. В качестве источников репутации, как я уже сказал, могут репутационные оценки, вроде лайков или вроде, значит, чаевых, если чаевые оформляются как отдельные транзакции в финансовой экосистеме, вот, либо неявные репутационные оценки на основе транзакций, да, то есть, если просто какой-то агент А переводит агенту В какие-то суммы денег, то чем больше эти суммы, то тем больше мы считаем, что агент А вкладывает в репутацию агента Б. Вот это могут быть другие неявные репутационные оценки, например, упоминание участников в социальной сети или комментарии на их посты. В принципе, это может быть даже комментария с учетом сентимента, отрицательного или положительного. Система, которую мы разрабатываем с 2014 года по сегодняшний день на основе платформы E-Agents, она позволяет рассчитывать текущую репутацию на основе данных из таких сетей, как Reddit, Twitter, ВКонтакте, из любых форумов Discourse. групп телеграмм, групп коммуникационных в слаке и из таких блокчейнов как голос.ид, стимат и эфириум, при том что в эфириуме учитываются только финансовые транзакции, а в стимате и в голосе мы также учитываем не транзакционное взаимодействие в виде упоминаний,

комментариев и лайков. На примере маркетплейсов мы осуществляли математическое моделирование таких маркетплейсов, как Амазон, и обнаружили, что наш алгоритм позволяет выявлять ботнеты, предназначенные для репутационных накруток, над недобросовестным участником с достаточно высокой точностью. Вот здесь вот показан пример, красные это все представители которые у которых репутация оказывается ниже 50 процентов а синие это представители, так сказать, примеры честных продавцов на Амазоне, репутация которых оказывается выше 80%. Естественно, есть некоторые фальспозитивы и фальснегативы, но в целом точность разделения мошенников и честных продавцов существенно превышает, чем любые скоринговые модели, начиная от модели пятизвездочной системы, которую использует Amazon, укончая различные варианты, не включающие собственно взвешенную текучую репутацию. Также пример из работы одного из моих студентов. Была разработана экспериментальная платформа для моделирования. как репутационного консенсуса, как алгоритма консенсуса для блокчейна. И были показаны хорошие результаты как по пропускной способности, так и по времени достижения консенсуса и скорости формирования блоков. Вот. И также была показана эффективность этой системы текущей репутации для рекомендательных систем, это работа другого моего студента, где было показано, что учёт репутации участников социальной сети при взвешивании, при расчёте рекомендации от этих участников, при построении рекомендательной системы на основе данных социальной сети существенно повышают точность от 48 до 96%. Какие есть варианты реализации вот этого репутационного консенсуса? Ну, во-первых, есть различные варианты его расчета. Первый вариант — это мы можем обновлять то, что мы называем reputation snapshot или срез репутации участников на уровне каждого блока. То есть мы можем реализовать схему алгоритм блокчейна, где элемент в логику формирования каждого блока репутации всех участников всего блокчейна или обновление участников только тех, которые транзакции входят в данный блок. Это один алгоритм. Второй алгоритм это периодическое обновление блокчейна, которое предполагает, что обновление репутации происходит раз в день, раз в час, раз в месяц, раз в неделю. На основе транзакций, которые происходят либо в блоках между двумя снапшотами, либо это если не блокчейн, а DAG или какая-то другая система распределенного реестра. Все равно включаются только транзакции, проходящие за определенный интервал для обновления вот этого снапшота. Ну и здесь как раз показано пример того, какие транзакционные и нетранзакционные. Взаимодействие мы можем учитывать между двумя снапшотами. Вверху показано то, что мы называем эндорсинг рейтингс или подписывающие рейтинги, то есть статические взаимодействия между участниками. То есть если кто-то кому-то поставил какое-то количество звездочек постоянно или кто-то поставил на кого-то или кто-то, кому просто записался кому-то в последователь, включив опцию follow в социальной сети, это то, что мы называем endorsing ratings, они являются статическими до тех пор, пока они имеют место быть зафиксированными в системе. И следующее – транзакционные рейтинги. Транзакционные рейтинги бывают эксплиситные, то есть это либо типсы, как я сказал, либо звездочки, поставленные за конкретную транзакцию или за доказание конкретной услуги. Либо это лайки или воты, которые ставятся в социальной сети обычной, либо на блокчейне. И есть неявные рейтинги. Это транзакции финансовые, кто-то кому-то денег перевел, это упоминания и это комментарии. В том и в другом случае, наша репутационная система в состоянии строить репутационные снапшоты с использованием как транзакционных, так и нетранзакционных рейтингов. Если мы говорим о реализации алгоритма

репутационного консенсуса основанного на репутации, то существует несколько вариантов его реализации. Как раз сейчас мы в рамках проекта SingularityNET обсуждаем как раз архитектуру нового репутационного консенсуса в рамках этого проекта. Первый вариант это то, что называется reputation централизованное, когда мы предполагаем, что у нас где-то отдельно от блокчейна существует какая-то система расчета репутации и просто при информировании каждого блока или периодически алгоритм блокчейна, он берет из off-chain репутационного агентства, получает расчет текущей репутации. расчёты репутационных снапшотов, при этом на самом деле эти снапшоты могут быть получены из различных источников. И тогда возникает вопрос, какому источнику больше доверять, если эти источники расходятся. И в этом смысле более интересным вариантом в правом случае является… децентрализованный консенсус на основе сайдчейна, когда на самом деле расчёт консенсуса происходит тоже в некотором распределённом реестре, своим собственным консенсусом по поводу, посвящённым формированию репутационного снапшота. То есть, идея заключается в том, что у нас есть часть участников, которые аллоцируют свои ресурсы на поддержание репутационной системы, на периодический расчёт И с одной стороны они получают некоторую компенсацию от экосистемы за осуществление функций реализации этих репутационных снапшотов, а с другой стороны они имеют возможность получать эту компенсацию только в том случае, если их репутационные расчеты достигают консенсуса с другими участниками и они между собой достигают консенсуса в сайд-чене, который... собственно и обслуживает весь блокчейн в плане репутационного построения репутационных снапшотов. Ну и наконец, с левой стороны внизу показан алгоритм, когда у нас формирование репутационного снапшота децентрализованным методом на основе репутационного консенсуса происходит в рамках своего собственного консенсуса по расчету репутации происходит в рамках самого алгоритма блокчейна, который запускается либо периодически, либо опять-таки при формировании каждого блока. И тогда имеет место говорить о так называемом reputation mining, потому что в рамках основного блокчейна майнеры репутации, они получают, по сути дела, компенсацию за репутационные расчеты. Вот соответствующая работа, тоже ссылка приведена, можно ознакомиться с подробностями. Ну и последняя работа, которая сейчас у нас называется work in progress. Это как раз к вопросу об использовании искусственного интеллекта, о котором я сегодня мало говорил. Это использование методов искусственного интеллекта или анализографов для более надежного выявления так называемых voting rings, или кольцевых голосований или круговой поруки. формируются замкнутые цепочки, как для формирования фейковых транзакций, так и для формирования накруток репутационных. Вот. И существуют идеи по поводу того, как мы можем... осуществить анализ графовый для выявления таких замкнутых циклов и минимизации этих репутационных накруток для получения очищенных репутаций, где вот эти вот кольцевые составляющие в репутации, они вычитаются из. репутационных снапшотов и позволяют получить репутацию очищенную от кольцевого шума. Спасибо. Есть ли какие-то вопросы ко мне, как к предыдущему спикеру?

А.НЕЧЕСОВ [01:10:36] : Антон, у меня вопрос. Еще раз, это Андрей Мечезов. Да. Подскажите, все-таки, с репутационным консенсусом, насколько там вообще безопасность соблюдается, потому что в Proof-of-Work консенсусе все понятно, мы не можем там строить блоки быстрее, чем мировая вычислительная мощность, потому что мы просто не сможем решать Те трудоемкие задачи, которые ставятся перед нами

за счет того, что чем быстрее мы генерим блоки, тем быстрее возрастает сложность. Здесь как решается этот вопрос? Может я прослушал, говорили или нет? Вот именно с репутационным консенсусом. Вот атака 51%, почему не взять и за счет репутации как-то построить другую ветку и так далее? вообще генезис-блок первый, там наделить репутацией высоким репутационным значением, как кого-то другого, например.

А.КОЛОНИН [01:11:40] : Нет, смотрите, здесь как раз идея в том, что в тех репутационных консенсусах, которые в половине случаев, если поискать в интернете, называются репутационными консенсусами, там как раз Это опасность есть, потому что там действительно на репутации просто можно взять и наделить. А тут репутации вы наделить не можете, потому что репутация рассчитывается на основе предыдущего репутационного снапшота. А предыдущий репутационный снапшот рассчитан на основе предыдущего репутационного снапшота. А рассчитываются они на основе предыдущего репутационного снапшота, на основе тех транзакций, которые записаны в блокчейне. То есть мы просто делали имитационное моделирование. где просто мы поняли, что там есть результаты, которые показывают, что накрутить гораздо труднее.

А.НЕЧЕСОВ [01:12:33] : то есть я просто не вижу как раз про то что мы берем вообще первый блок другой просто с нуля начинаем то есть у вас как бы вы говорите что вы основывайтесь на предыдущих блоках да на репутации как бы которая хранится в предыдущих блоках я говорю взять просто с чистого листа новые мы строим новый блокчейн с репутационным консенсусом ваш в чем проблема почему пользователь консенсус, я же тоже могу быстро генерить блоки, там же нет трудоемкой задачи, получается она не возникает просто.

А.КОЛОНИН [01:13:08] : Вот такой вопрос. Ну, я не совсем все-таки понял вопрос, потому что пользователь имеет в виду, почему пользователь вместо proof-of-work должен выбрать proof-of-reputation?

А.НЕЧЕСОВ [01:13:20] : Нет, нет, про то, что proof-of-reputation, ну, я просто не говорю, не эксперт, да, вот у меня вопрос такой, что почему пользователь или Другой хакер, допустим, не может взять и с чистого листа создать параллельно такой же блокчейн Proof of Reputation и выдать этот блокчейн за реальный, а ваш за фейковый, например, вот так вот.

А.КОЛОНИН [01:13:45] : Я не знаю как. Я опять-таки не могу сказать, как он может это сделать. Я не знаю, как он может это сделать. У меня нет ответа на этот вопрос. Понял. Спасибо. Ага, ладно. Видимо, надо отдельно эту тему разбирать, если останется время. Спасибо, Андрей, за вопрос. Следующее слово предоставляю следующему спикеру. Дмитрий, пожалуйста. Дмитрий Пальчунов, Институт математики и Новосибирский государственный университет.

Д.ПАЛЬЧУНОВ [01:14:31] : Да-да-да, пожалуйста. Слышно. Значит, у нас немножко такой комплиментарный, на самом деле, доклад. Но оно скорее искусственный интеллект для блокчейна и для смарт-контрактов, на самом деле. Сегодня было упомянуто, что наличие смарт-контрактов – это такая важная вещь. и которая как раз выгодно отличила уже эфириум от биткоина. С одной стороны, с другой стороны тоже сегодня уже отмечали, что одна из серьезных проблем смарт-контрактов – необходимость их аудита. Причем это вещь дорогостоящая, и как вот там была некая

дискуссия со специалистами. Один человек говорил, что так можно их по дешевке сделать. Вот Виталий Гумиров, тоже многим известный. Саш, ну да, конечно, делать можно дешево, но потом очень дорого придется заплатить. Значит, вот. Айя, назад, наверно, пока первый слайд, надо пока. Значит, вот, дорого придется заплатить. И, собственно говоря... Одна из основных задач вот этого исследования – это как раз решение проблем, причем таким хитрым способом, с применением искусственного интеллекта. А именно, мы решаем проблему аудита, раскладывая на две задачи – валидация и верификация. Ну, валидация, я, как говорится, не нужно… в общем смысле, валидация, верификация. Но прежде чем объяснять, что это такое, еще один момент, для чего это нужно. То есть, на самом деле, вот давно уже идет этот разговор о цифровизации экономики, цифровизации бизнес-процессов и так далее. Вот даже как-то еще была Молчанова, замгубернатора, собирала встречу рукой для этих компаний, вот я там как раз тоже по этому поводу выступил. И идея в чем состоит? в одном предприятии, то есть в музее бизнес-процессов, то есть руководитель предприятий, и, собственно говоря, он все решает, он все определяет, как это происходит и так далее. И к нему можно обратиться, если кто-то с чем-то не согласен и так далее, да, то есть окончательное решение за ним. развертывание, значит, этого системы, и она работает, ну, с определенной поддержкой. Совсем другое дело, если мы хотим автоматизировать сложные бизнес-процессы между предприятиями, причем значительно более сложно, чем просто покупка токенов при помощи эфира, да, для, там, ICO. Вот, если мы действительно хотим сложный процесс, бизнес-процессы моделировать, нам нужны достаточно уже сложные смарт-контракты. И как раз здесь возникает тоже проблема, что здесь нет начальника, здесь нет начальника, хозяина, который скажет, что правильно, что неправильно. Есть различные хозяйствующие субъекты, есть различные юрлицы, и выяснять отношения они могут только в арбитраже. В 90-е годы выясняли отношения с помощью биты паяльников и утюгов, но сейчас, слава богу, выясняется в арбитраже. Но это тоже процесс очень неприятный, долгий, затратный, никому он не нужен. То есть нужно делать так, чтобы сразу все было хорошо и чтобы все были гарантированы. И здесь возникает какая проблема? Даже чтобы пойти в арбитраж, нужно иметь текст контракта, текст на естественном языке. Арбитраж не будет рассматривать смарт-контракт, с одной стороны. С другой стороны, текст на естественном языке, он достаточно сложный, если он юридически написан. И вопрос, как идентифицировать реализованность смарт-контракта с этим текстом. То есть, возникают, собственно говоря, две проблемы. Одна проблема – это соответствие смарт-контракта, то есть как программы, написанные, например, на Solidity, с текстом договора, который понятен заказчикам, они не программисты, они не понимают этих в Solidity, да. А с другой стороны, вторая проблема, то, что мы называем валидацией, что действительно смарт-контракт отражает то, о чем стороны на самом деле договорились. И второе, это уже верификация, это то, что, скажем, ну, например, в смарт-контракт не внесен какой-то вредоносный код, который будет деньги куда-то уводить в сторону. То есть это уже, скажем... реализация, проблема реализации, проблема безопасности при реализации, и собственно говоря блокчейн тоже сюда относится, что дальше это нужно будет размещать на блокчейне, но этот как раз вопрос мы не рассматриваем, почему я говорю, что это комплементарно, как бы дополняет, то есть есть блокчейн и есть отдельный смарт-контракт, который дальше при помощи блокчейна будут решаться проблемы его безопасности. То есть таким образом задача автоматизации по стороне семантического смарт-контракта заключается в том, что делать сразу смарт-контракт идентичный тексту на

естественном языке. Причем один из выходов – это рассматривать договор не в том виде, как его пишут юристы-адвокаты. а превращать его изначально в более простой текст, в котором устранены все, скажем, референтные индексы, то есть он, она и так далее. То есть предложения достаточно простые, понятные. Они, кстати, и сторонам, как говорится, будут более понятными, то, что называется стейкхолдером. И они как раз позволяют то, что мы можем уже локально, локально проверять соответствие. написанной программы и вот этого текста на естественном языке. То есть еще раз, цель сделать так, чтобы текст на естественном языке, который заключает стороны и который имеет юридическую силу, с которой можно идти по арбитражу, соответствовал тексту на солидитете, который будет дальше реализовываться. Это проблема валидации. И вторая проблема верификации – это уже отдельно, чтобы этот текст был правильным и не содержал каких-то, скажем так, Нарушение, мошенничество и так далее. Ну, теперь вот я Айе передаю слово, она дальше уже детально все расскажет.

А.ГАЛИЕВА [01:20:41] : Спасибо, Дмитрий Евгеньевич. Как уже было сказано, предлагается решить проблему аудита путем разделения его на валидацию и верификацию, где в соответствии с формальной спецификацией реальным ожиданием будет выполняться валидации, а уже... гарантии корректного запуска и исполнения смарт-контракта будет уже за это ответственной верификацией. И что касается спецификации смарт-контракта, она должна отражать правила взаимодействия сущности и бизнес-процесса. Для этого был разработан DSL-язык, а также сформулированы наиболее важные требования к функционалу разрабатываемой системы.

Д.ПАЛЬЧУНОВ [01:21:39] : Я всем поясню, DSL – Domain Specific Language, примета антигеронного языка.

А.ГАЛИЕВА [01:21:44] : К требованиям мы относим трансляцию спецификации бизнес-процесса в исполняемый смарт-контракт, генерацию представления контракта на языке, который будет приближен к естественному, для понимания... требований стейкхолдерами, а также гибкое моделирование бизнес-процессов с помощью концепции переиспользования, которая основана на онтологическом гомоморфизме. К этому мы попозже подойдем. При традиционном процессе разработки программного обеспечения возникает проблема разрушения семантики при конвертации спецификации в код. И это может привести к целому ряду проблем с поддержкой кода, с снижением эффективности системы и так далее. И одним из решений этой проблемы является семантическое моделирование. а именно использование семантических предметно-ориентированных языков для моделирования предметной области. В качестве языка, описывающего правила взаимодействия сущностей этой предметной области, будет выбран язык SDSL, и его концепт основан на семантической модели предметной области. И такой подход позволяет изменять бизнес-логику контракта через изменение только его асимметической модели, на основе которой, собственно, и генерируется формализованный текст договора. Таким образом, эксперты предметной области, которые не имеют навыков программирования, будут иметь возможность проверить смарт-контракт на соответствие тексту на естественном языке, который описывает суть этого контракта.

Д.ПАЛЬЧУНОВ [01:23:42] : Одну секунду, я тоже поясню еще. SDSL – это язык, разрабатываемый компанией Einlein, Виталием Гумировым. То есть он уже имеет там реализацию. То есть вот мы как раз используем их, это семантический язык. Кстати, он основан на, говорится, Sigma-программировании, который, естественно, делал вместе с нечестным предметом доклад, и основан он на Delta-0-формулах.

А.ГАЛИЕВА [01:24:09] : Семантическая модель представления данных имеет четыре уровня. Это антология предметной области, то есть набор понятий и их определений. Общие знания, то есть законы предметной области. Эмпирические знания, это случаи предметной области. А также оценочные знания, это вероятностные знания, которые мы берем из внешних источников. В качестве способа формализации описания бизнес-процессов предлагается использование модели ситуации, которая представляет из себя ориентированный граф, в вершинах которого расположены все возможные в данном бизнес-процессе ситуации, а ребрами являются условия перехода в эти ситуации. Существующие подходы к описанию моделей ситуации бизнес-процессов ограничены замкнутостью систем, которые они описывают. То есть в них не допускается недетерминированность сигналов, которые поступают в ситуации. Но для управления рисками необходимо как раз-таки обеспечить моделирование недетерминированных бизнес-процессов. при исполнении смарт-контракта будет выполняться тайлинг над спочкой ситуации в зависимости от последовательности недетерминированных событий в бизнес-процессе. Для автоматизации вывода цепочек исполнения предлагается использование аргументации на основе прецедентов, то есть частичных моделей всех возможных в данном бизнес-процессе ситуаций. Такое моделирование бизнес-процесса позволит использовать антологические гомоморфизмы частичных моделей при построении цепочек исполнения, благодаря чему станет возможным переиспользование описанных смарт-контрактов в качестве шаблонов для других подобных подпроцессов. Можно выделить три вида онтологических гомоморфизмов. Это, может быть, изменение номенклатуры, то есть объектов, изменение отношений и предикаты действия. Использование моделей ситуации можно проиллюстрировать на примере смарт-контракта поставки товара. Как на слайде, ситуации S1 и S4 в зависимости от приходящих сигналов могут переходить в разные ситуации, и это как раз иллюстрирует недетерминированность цепочки исполнения, а значит смарт-контракт, который имплементирует данную модель, будет учитывать соответствующие риски. В качестве примера использования онтологического гомоморфизма в случае с прадикатами можно привести пример того, что Вася Петя передает кабель, то есть прадикат передать кабель Вася Петя. USB будет онтологически гомоморфным предикату передать кабель Вася-Пете другого бизнес-процесса, в котором как раз уже будет неважно, какой именно кабель передается. Также онтологический гомоморфизм позволит в этот же предикат передавать другие предикаты. То есть, если ранее был определен унарный предикат USB тип, где в качестве параметра тип передается, собственно, тип USB кабеля, то есть Type C или Type B, мы можем создать вложенность, передав данный предикат в качестве третьего параметра. Замена онтологически-комаморфных предикатов происходит в зависимости от конкретной ситуации, которая необходима. в данном бизнес-процессе. Для упрощения процесса верификации контракта целесообразно декомпозировать его на составляющие, то есть на шаблоны. Это заранее верифицированные пары описания логики на естественном языке и соответствующего ему DSL-кода. Таким образом, процесс создания контракта

будет состоять из трех этапов. Это конструирование шаблонов, то есть создание составных частей спортконтракта, сборки шаблонов, а именно формирование общего шаблона из конструированных, а также наполнение шаблонов. то есть инициализация шаблонов конкретными данными. В процессе разработки условий и требований контракта с тейкхолдерами происходит унификация понимания контракта, валидация и согласование этого контракта, и использование шаблонов как раз позволит упростить эти процессы. В качестве одного из этапов валидации контракта может служить визуализация дерева разбора шаблонов готового смарт-контракта. Процесс аудита смарт-контракта итеративный, то есть после упрощения текста естественного языка, он преобразуется в набор фрагментов атомарных диаграмм, по которым происходит поиск подходящих шаблонов. с их последующей сборкой. Созданные шаблоны будут в той или иной мере приближенными к требованиям смарт-контракта, и далее по полученным шаблонам порождается текст естественного языка, который как раз валидирует пользователь. И если контракт на этом этапе соответствует ожиданиям пользователя, итеративный процесс валидации завершается, иначе пользователь вносит необходимые изменения во входные данные, запускает процесс сначала, и в результате такого итеративного редактирования шаблоны и приходят к абсолютному соответствию контракту. Также шаблоны должны создаваться в параметрическом виде и представлять набор предикатов, определяющихся через другие предикаты, то есть набор фрагментов атомарных диаграмм. Вместо констант должны использоваться одноместные предикаты, определяющие сущность с возможностью означения. Таким образом, мы будем иметь дело только с набором иерархически вложенных предикатов. Разработанная система создания и валидации смарт-контрактов включает в себя следующие компоненты. Это исполняемая программа, модель ситуации и генератор формализованного текста договора. При получении из внешних источников информации о происшествии определенного события программа обращается к ситуационной модели и, согласно написанным правилам, эта модель запускает необходимые функции программы, производящие полезные действия. А генератор текста отвечает за создание формализованного текста контракта, который поясняет стейкхолдерам суть договора. На слайде представлен интерфейс разработанной программной системы. Основными элементами здесь являются панель управления потоком исполнения смарт-контракта, также поле для ввода модели ситуации и панель, на которой отображается вывод языка, приближенного к естественному. Таким образом были подготовлены методы, алгоритмы автоматизации разработки смарт-контрактов, разработана программная система, которая позволяет формализовывать бизнес-процесс через построение моделей ситуаций и реализующая взаимодействие нескольких смарт-контрактов, а также предоставляющая возможность гибкого моделирования смарт-контрактов с помощью антологического гомоморфизма. Возможность переиспользования смарт-контрактов в качестве шаблонов бизнес-процессов позволит в дальнейшем создать децентрализованную систему моделирования. Каждый пользователь, который будет поддерживать исполнение смарт-контрактов, только собственных бизнес-процессов. Но в силу возможности создания шаблонов другие участники смогут использовать уже готовые и поддерживаемые смарт-контракты для моделирования. процессов, которые все более будут приближены к реальным бизнес-процессам, которые существуют в крупных компаниях или целых отраслях. Спасибо за внимание.

А.КОЛОНИН [01:33:26] : Ая, Дмитрий, спасибо большое за доклад. Коллеги, есть какие-то вопросы?

Д.ПАЛЬЧУНОВ [01:33:36] : Хорошо. В чате был вопрос насчет противоречия и пресечения шаблона. То есть в принципе да, это возможно. Такие средства есть. Ну сейчас, я думаю, в детали можно не вдаваться, но в принципе да. Причем заметим, что очень важно, что как раз то, что Виталий Бумеров разрабатывал. То есть заметим, что, скажем, а теория... Ну вообще у нас даже как правило будут все-таки даже формулы бесклантерные. но либо это а-теория, которая является разрешимой, здесь как раз вопрос разрешимости, они решаются просто, а уже, скажем, для более тонких вещей, в принципе, возможно трансляция и использование средств Semantic Web, то есть резонера, и написание каких-то частей антологии ноу-вейл, но это уже как бы отдельная задача, я думаю, сейчас не нужно в эти детали так

А.КОЛОНИН [01:34:37] : Спасибо за вопрос, спасибо за ответ. Еще один вопрос к Александру Науму, вопрос следующий. Хотел бы спросить, как Сбербанк собирается объединить блокчейн с ИИ, поскольку сам блокчейн это примитивная технология, а обучение ИИ это сложный процесс с множественными вычислениями. Тот же смарт-контракт это набор правил, который ограничен, нельзя просто пихать туда все подряд. Александр, можете ответить?

А.НАМ [01:35:06] : коллеги здесь вопрос наверное А такое, что мы действительно сейчас находимся на этапе исследований, то есть мы пытаемся понять, где будет польза, скажем, искусственному интеллекту от блокчейна, и наоборот, где блокчейн получает выгоды от искусственного интеллекта. Пока у нас все находится на этапе исследования, и мы какие-то конкретные кейсы не озвучиваем, но совершенно точно. одно направление, которое заслуживает внимания, это все, что касается безопасности пользователей, потому что это, на наш взгляд, это большая проблема сейчас на рынке. Вот и compliance, fraud detection, вот эти вот инструменты, которые могут превентивно определять мошеннические схемы, они сейчас у нас вот на повестке. В остальном, пока мы еще исследуем, у нас есть лаборатория искусственного интеллекта, мы с коллегами будем вместе обсуждать.

А.КОЛОНИН [01:36:19] : Хорошо, спасибо, Александр. Еще вопрос у Виктора Носко, еще два вопроса от участников и мы перейдем к нашей дискуссии прямо. Виктор, пожалуйста.

В.НОСКО [01:36:36] : Здравствуйте. Ну, на самом деле у меня может быть такой вопрос с черточка выступления, сколько у нас есть времени, или может быть потом в дискуссии?

А.КОЛОНИН [01:36:42] : Давайте, может быть, если у вас черточка выступления, то у вас будет очередь высказаться в ходе дискуссии. Хорошо, отвечаю. Тогда, если вопросы, то Анатолий Рейбольд, пожалуйста.

А.РЕЙБОЛЬД [01:36:56] : Да, спасибо. Даже не вопрос, а вопрос, на самом деле, Дмитрий Евгеньевич, следующего характера. Как активно вы исследуете тему того, что участники процесса не понимают язык, на котором формулируются? Есть такая в Германии популярная тема – простой язык, упрощенный язык, доступный язык и так

далее. Эта тема возникла в связи с большими проблемами, которые и в связи с криптографией возникли, Вот общение с чатами – вот мой вопрос, Дмитрий Евгеньевич.

Д.ПАЛЬЧУНОВ [01:37:39] : То есть вопрос в том, что какие-то тексты, может быть, слишком сложны для понимания и… Да, да, да.

А.РЕЙБОЛЬД [01:37:46] : Какую-то проблему решайте, да, именно этот вопрос.

Д.ПАЛЬЧУНОВ [01:37:49] : Как раз вот совершенно очень хороший вопрос. Как раз вот идея такая, что, скажем, если мы пытаемся брать тот договор, который написали юристы, И да, можно пытаться автоматически куда-то переводить, но это безумно сложно и нереально. Проще посадить девочку с теоретическим образованием и нормальным пониманием, которое все этот текст, я говорю, изложат очень простыми… В принципе, можно вообще попросить… У меня даже когда-то была статья опубликована еще в «Уч. Системы в истории математики». Очень простые, на самом деле, очень простые. Потом, кстати, показывали статью, вот некто Дмитрий Хромцов, небезызвестный, показал своей жене сапкардофилогию, она посмотрела, да, говорит, действительно, вот это верно. То есть переложить контракт, вот этот, юридический, простым языком, с простыми понятиями, где всё будет просто, но как бы без всяких сложных конструкций. С одной стороны, действительно, это упрощает понимание... к участникам процесса, потому что далеко не все люди очень образованы в экономике могут быть, которые занимаются бизнесом, а уж тем более в юридических вопросах. И вот этот простой текст, с одной стороны, он будет понятен стейкхолдерам, то есть участникам процесса, а с другой стороны, его как раз легко переводить. Причем, я опять же обращаю внимание, мы не изобретаем такой в полном объёме искусственный термин, который будет, текст гарантированно переводить в формальный вид. Здесь речь идёт о сборке. Какие-то кусочки шаблонов, самые минимальные, можно для них писать кусочки текста естественного языка. А вот когда происходит сборка, когда происходит онтологический гоморфизм, заменили номенкультуру краски на такую-то, заменили кирпичи на шлакоблоки, ничего формально, по сути, ничего не изменилось, То есть вот таким образом легко порождать правильный, нормальный текст естественного языка, который будет в точности соответствовать формальной спецификации. С одной стороны, с другой стороны, они будут полностью понятны людям. Спасибо.

А.РЕЙБОЛЬД [01:40:11] : Спасибо вам тоже. И, конечно, антологический геморфизм – это интересная тема, которая нас тоже интересует в Германии. Спасибо.

А.КОЛОНИН [01:40:20] : Спасибо, Антон, за запрос. Да, коллеги, спасибо. Еще вопрос от Алексея Удода. Короткий вопрос, короткий ответ, и переходим к дискуссии. Алексей, пожалуйста.

А.УДОД [01:40:32] : Спасибо, Антон. Этот вопрос скорее к вам. Тут полтора маленьких вопроса. Во-первых, репутация, как я понимаю, у вас – это некоторая агрегация каких-то действий условных агентов. Во-первых, есть ли многопараметрическая репутация, то есть для каждой ситуации используется своя репутация, которая по-своему рассчитывается, что-то типа мультиблокчейн-системы, про которые Андрей рассказывал?

А.КОЛОНИН [01:41:05] : Короткий ответ – да, есть, но мы должны понимать, что вычислительные затраты на мультипараметрическую репутацию, они существенно выше, я дал ссылки на статьи, можно почитать, что мы по этому поводу пишем, есть работы, они возможно не полностью опубликованы у нас с коллегами из Singularity. Нет, где мы вообще рассчитываем, предлагаем рассчитывать двумерную репутацию. Вот одна репутация, она тематическая, то есть за что мы оцениваем репутацию, а второе измерение – это какой аспект, допустим, дешевизна, качество, скорость, добросовестность, дружественность и так далее. Но есть понимание, что чем больше аспектов, тем выше вычислительные затраты и здесь возникает некоторое противоречие. Хочет ли сообщество той системы, в которой эта репутационная система используется, платить, внести дополнительные платы за более дорогостоящие расчеты, более многоаспектные репутации?

А.УДОД [01:42:08] : Спасибо. И еще маленький вопрос. Используется в качестве безопасности для предотвращения ситуации, когда кто-то приходит с новой сетью и начинает говорить, что у него большой рейтинг, система, в которой каждый агент хранит репутацию соседних агентов. И, соответственно, чтобы взломать такую систему, придется взломать сотню ближайших агентов из старой сети, которые будут подтверждать его высокий рейтинг.

А.КОЛОНИН [01:42:34] : Да, смотрите, здесь, я так понимаю, есть фундаментальное непонимание того, как это работает. Тоже вот коллеги задавали вопрос, и в чате тоже это прозвучало, я увидел. Есть почему-то иллюзия, что агент может сам себе назначить репутацию. Это невозможно. То есть, репутация, она вычисляется в ходе расчета репутационного снапшота или репутационного состояния системы в результате взаимодействия всех агентов системы по алгоритму, который является частью алгоритма. блокчейна, да, то есть вот у нас есть алгоритм консенсуса, есть алгоритм, по которому формируются блоки и есть алгоритм, по которому рассчитывается репутация. Этот алгоритм, это один код, да, это открытый код, который используется всеми участниками системы. Если участники системы используют другой код, то то, что они делают, расходится с... эти участники идентифицируются как нарушающие политику сети. Вот, при этом по этому коду он входит в систему с дефолтной репутацией, которая равна дефолтной репутации первых участников, которые вошли в систему. Единственное, что есть нюанс, что у нас есть вариант решения системы, когда эти дефолтные настройки, они могут по ходу системы меняться, то есть опять-таки в блокчейне лежит текущая... что называется параметры репутационной системы, частью которых являются, в том числе, дефолтные настройки. И существует алгоритм изменения политики governance системы. в рамках которого на основе голосования участников с учетом той же репутации можно поменять эти репутационные настройки. То есть, грубо говоря, все ученики системы в какой-то момент могут проголосовать за то, чтобы репутационная дефолтная репутация была там не 0,2, а 0,5. Тогда с этого момента все новые участники будут получать дефолтную повышенную репутацию. Как-то так. А вообще я рекомендую просто ознакомиться с материалами. Вот есть, я сейчас кину ссылку в группу, где эти вопросы можно пообсуждать и можно там задать вопросы, я дам более подробные ответы. Спасибо. Хорошо, коллеги, тогда я предлагаю перейти к нашему обсуждению. Сейчас я только кину ссылку в группу, где можно все, что касается репутационного консенсуса, обсудить. который у нас заявлен на этот семинар. Итак, у нас, правда,

остается не очень много времени, но хотелось бы, чтобы все спикеры, включая присоединившихся к нам Александра Балдачева и Виктора Носкова, высказались по всем озвученным четырем вопросам. Итак, вопрос первый. Есть ли будущие у технологии распределенного реестра из блокчейна, в частности, вообще? Александр, пожалуйста.

А.НАМ [01:45:41] : Это мне, да, вопрос?

А.КОЛОНИН [01:45:43] : Да, Александр, нам, пожалуйста, в том же порядке. Пойдем.

А.НАМ [01:45:47] : Да, коллеги, я, наверное, так скажу. Мы внутри Сбербанка тоже часто обсуждаем. Скорее, наверное, у нас сейчас такое мнение, что в отдельности технология блокчейн в корпоративном секторе, и мы скорее смотрим на набор нескольких технологий, здесь и блокчейн, и искусственный интеллект, и квантовые вычисления, которые вместе, скорее всего, дадут синергию, если говорить про вот наш финансовый рынок. Блокчейн здесь скорее имеет перспективы по созданию альтернативного метода платежей. То есть та инфраструктура банковская, которая выстроена, она никуда не денется. Она останется, но совершенно точно она потеряет какую-то часть транзакции. И эта часть транзакции уйдет в цифровые рельсы. ну, наверное, самые большие шансы часть этих транзакций забрать. Мы не верим в то, что вся инфраструктура банковская куда-то денется, испарится. Мы в это не верим. Или, допустим, фиатные деньги тоже исчезнут. Мы в это тоже не верим. Мы, скорее, говорим о том, что старые текущие методы платежей, они будут терять свою долю, и эта доля будет перетекать в альтернативные платежи. Это что касается технологии блокчейн, перспективы. Какие там еще вопросы были?

А.КОЛОНИН [01:47:42] : Давайте по этому первому вопросу сейчас пройдемся. Андрей Нечесов, пожалуйста. Есть ли будущие технологии распределенного реестра и блокчейна в частности вообще?

А.НЕЧЕСОВ [01:47:52] : Еще раз здравствуйте всем. Я, как уже сказал, конечно, оптимист в этом плане. Скажем так, с 2008 года, когда впервые был анонсирован биткоин, был же экспоненциальный рост, мы дошли до объема рынка в 1 триллион долларов, это огромный рынок, он обогнал по капитализации все коммерческие компании, то есть и Амазон и Эппл и так далее, то есть по объему капитализации Скажем так, в свое время, до 2017 года, вот эта экспонента росла и сейчас мы вышли на какое-то плато. То есть те, кто используют блокчейн, они его используют и уже никуда не денутся. То есть это криптоманы, которые уже будут в этом направлении работать. Новое поколение, бесспорно, будет тоже погружено. Видите, здесь вопрос обучения, использования этого направления. Если государство будет не заинтересовано и будет всячески пытаться заблокировать новые знания применения блокчейна, Конечно, люди будут сложнее понять, как этим пользоваться, где приложения скачать для этого и куча всего. Но с другой стороны, тем, кому надо, все-таки изучают эти направления. И я скажу так, просто я на своем живом примере, у меня есть несколько видов криптовалют. Там биткоин, эфириум, эфириум классик и монеро. Это вот анонимное, про что Александр нам говорил. И очень удобно на самом деле работать и переводить эти платежи. Если вы не попробуете, говорить удобно это неудобно, это как бы, ну, это примерно то же самое, что говорить, когда вы не катались

на велосипеде. Вот. Говорит, что велосипед это плохо. Ну, прокатитесь разочек, вы все поймете как бы. Конечно, есть. И огромные перспективы, спасибо.

А.КОЛОНИН [01:49:52] : Андрей, спасибо. Дмитрий Евгеньевич.

Д.ПАЛЬЧУНОВ [01:49:56] : Антон Германович, по идее, вы должны в следующем пути.

А.КОЛОНИН [01:50:00] : У нас осталось время, я уступаю.

Д.ПАЛЬЧУНОВ [01:50:03] : Хорошо. Вот здесь я бы немножко по-другому вопрос поставил. Во-первых, здесь есть две сущности, и на самом деле нужно их, мне кажется, отождествлять. Одна сущность – это криптовалюты, это биткоин, эфир и так далее. И, соответственно, криптовалюты, которые выпускает банк Китая, Вторая сущность – это распределённые реестры. На самом деле сущности совершенно разные, то есть то, что они возникли одновременно, это, говорится, вот. Теперь, дальше, опять распределённые реестры и блокчейн. А почему чейн? Я ещё, говорится, много лет назад, когда у нас в СССР, когда, кстати, была сквозная… Помните сквозные технологии? И мы, кстати, с Болдырем, со Свериденко, говорится, участвовали как эксперты, говорится, вместе с нашим институтом программных систем. Говорится, вот, они подавали заявку в этой заявке. Я в Ударе тогда еще говорил, а почему чей? Граф, граф-сеть, блок-нетворк, блок-граф, да? И теперь объясню, почему. Дело в том, в чем идея вот этого блокчейна, что эфира, что… Биткоина. Принципиально этот момент то, что все узлы равноправны. И вот ваш как раз консенсус, всевозможная, да, на этом основе. Хотя, кстати, Антон Германович, вы правильно заметили, что когда идет вопрос, как говорится, пруфов Стрейк, да, то богатые оказываются, хоть они тоже плачут, но оказываются главными здесь, тоже, получается, неравноправность, но в любом случае все-таки речь идет о равноправности. Почему? Потому что вначале манили биткоин, там тоже равноправность, кто больше манил, потом ICO, crowdfunding, понятно, тоже все узлы равноправных, все, говорится, покупает свои токены и так далее, но если мы берем ту проблему, которую я назначил, проблему цифрализации экономики, когда нужно делать, неважно, как назвать смарт-контракт, как угодно, формализацию, автоматизацию, полную автоматизацию, в чем доверенную, гарантированной правильности, защищенную автоматизацию бизнес-процессов между юридическими лицами и хозяйствующими субъектами, здесь нет равноправия, почему? Есть разные субъекты расы, кто выполняет логистику, производство и так далее. Есть банки, финансовая структура, это следующее. Есть, опять же, те же самые суды, есть органы государственного власти и управления. То есть, на самом деле, мы видим, что это более адекватно, вот красная сеть, граф, но в которой узлы будут немножко разные, будут классы разных узлов, которые будут иметь разный статус, разные возможности, адекватные своим полномочиям, ответственностям и так далее. И вот в этом смысле. Итак, первый ответ. Я думаю, что криптовалюты будут жить, и это, в принципе, вещь очень интересная, очень полезная. В какой-то стране латиноамериканской, я забыл в какой, уже же президент вел, что можно чуть ли не на улицах платить криптовалютой, Антон, это вам не напомните. Буквально, говорится… В Венесуэле, по-моему? Нет, не в Венесуэле, а в Венесуэле.

А.КОЛОНИН [01:53:18] : Ну, или в Сальвадор.

Д.ПАЛЬЧУНОВ [01:53:20] : А?

А.НАМ [01:53:21] : В Сальвадор, может.

А.КОЛОНИН [01:53:22] : Или в Сальвадор.

Д.ПАЛЬЧУНОВ [01:53:23] : Ну, в общем, я бы уже сказал, или в Сальвадор. Да-да-да, там просто уже все. Президент вел, пожалуйста, расплачивайтесь на улице в кафе криптовалютой. То есть криптовалюта, безусловно, будет иметь, говорится, будущее. Она нужна для разных целей. Там как-то все это будет регулироваться, меняться. И так далее. Это с одной стороны, с другой стороны, на мой взгляд, будут развиваться как раз вот именно распределённые реестры, где именно главный принцип распределённости, а вот равноправие узлов – это уже под вопросом, я думаю, будет разный вариант – и с равноправными узлами, и с неравноправными. И это тоже исключительно важно, как внутри одной страны, для автоматизации бизнес-процессов. Так и между разными странами, что еще более важно и полезно, особенно в условиях того, что имеются такие монополисты типа Слифт, от которых берут и кого-то в качестве санкции отключают. Спасибо.

А.КОЛОНИН [01:54:23] : Спасибо. Я, кстати, присоединяюсь. вашему высказыванию и хотелось бы услышать Александра Балдачева по этому поводу.

А.БАЛДАЧЕВ [01:54:34] : Добрый день, Александр Балдачев. Коротко представлюсь по данной теме, по теме блокчейна. Я работал системным архитектором блокчейн-платформы Аппла из Люксембурга. Сейчас она не функционирует по многим причинам. и разрабатывал много приложений, блокчейн-приложений для Эмиратов, Дубая, Аджмана, для Индии, для Люксембурга. Делали бы на нашей платформе торговую площадку для Газпромнефти МВП, они приняли, все хорошо было. Рестракции для голосования директоров Люксембурга делали, так что у меня очень большой опыт именно внедрения блокчейна. Чего, наверное, никто в словах похвастаться не может.

А.КОЛОНИН [01:55:19] : Да, я, Александр, извините, я вас перебью, я еще прокомментирую, почему Александр не был приглашен в сегодняшний ресторан.

А.БАЛДАЧЕВ [01:55:25] : А я сейчас могу сказать, да. А, да, хорошо, это красиво. Я потом объясню. Сейчас, когда будет вопрос конкретный, я объясню, почему я не выступал сегодня, да. Значит, и конкретный вопрос по поводу того, выживет или не выживет технология разбеленного реестра. на мой взгляд, обязательно выживут, если правильно сформулировать, что же это такое. То есть, по сути, мы имеем систему технологического управления доверием. То есть, когда доверие к транзакциям, доверие к данным, доверие к каким-то процессам регулируется не нормативными актами, а именно исключительно технологическими средствами, то есть блокчейн биткоина защищён сам своей технологией. И даже в своё время я ввёл такой термин как Trusted Digital System для замены всех систем, которые и DLT и блокчейна, чтобы подчеркнуть, что есть некие системы, которые специально работают на обеспечение доверия цифровому контенту. Вот ответ на пару вопросов.

А.КОЛОНИН [01:56:44] : И как я написал в группе, Александр у нас в прошлом месяце делал большой доклад как раз по своей системе на основе искусственного интеллекта и блокчейна. Можно ознакомиться с его материалами.

А.БАЛДАЧЕВ [01:56:57] : Это я потом на следующий вопрос отвечу.

А.КОЛОНИН [01:56:59] : Хорошо. И тогда теперь Виктор Носко, пожалуйста.

В.НОСКО [01:57:04] : здравствуйте, я тоже представлюсь. я сразу на все три хочу, на все четыре, наверное, ответить в том кейсе, в том вопросе. давайте все-таки будем соблюдать. так, хорошо. ну, точно да. в госуправлении и в бизнесе. и вот дальше я хочу раскрыть. в госуправлении и в бизнесе очень нужен блокчейн. все это знают, понимают. вопрос скорее такой управленческий. все.

А.КОЛОНИН [01:57:30] : Хорошо, тогда мы переходим к следующему вопросу, если он недостаточно раскрыт был, в частности, насколько, как вы видите, будущее у этих технологий как инструмента именно демократизации финансовой сферы. Александр, пожалуйста.

А.НАМ [01:57:48] : да и я здесь краски вижу большие перспективы когда мы говорим про демократизацию но мы говорим в первую очередь про те страны где проникновение банковских продуктов крайне низкая и здесь даже на примере того как развиваются цифровые валюты центральных банков себе диссис мы видим, что наибольший успех в тех странах, где люди не имеют банковского счета, а за счет того, что технология, интернет, мобильные устройства, они позволяют барьеры снизить, вот здесь как раз-таки у блокчейна, мне кажется, большие шансы, там 1,7 миллиардов людей, они не имеют сейчас доступа к банковским услугам. хороший правильный кейс, мне кажется, для развития блокчейна.

А.КОЛОНИН [01:58:47] : Александр, спасибо. Андрей Нечесов.

А.НЕЧЕСОВ [01:58:51] : Сейчас, минуточку. Так, ну вот у меня пока Александр говорил, возникла мысль, на самом деле, следующего плана. Сейчас из-за того, что на самом деле недостаточно как бы люди и погружены в это направление возникает очень много суррогатных валют, криптовалют, которые анонсируются как криптовалюты, ну типа цифрового юаня, цифрового рубля, еще что-то. То есть, зачем нужен там биткоин, если у нас есть цифровой юань или цифровой рубль. Поэтому вопрос даже и в финансах, я опять говорю, это вопрос регулирования государственного, очень серьёзная здесь помеха. Но, конечно, те, кто работает и понимает, что это такое, никогда биткоин и... Вообще блокчейн это децентрализация прежде всего, в чем его плюс, в чем его взрывной рост в том, что децентрализованное решение нет единого органа, который бы контролировал все процессы, а общий мировой консенсус достигается, это же очень важно на самом деле, а все вот эти цифровые, сама по себе структура блокчейна, ее можно вложить легко в любую реляционную базу данных, Таблично, на самом деле. Проблемы вообще нет. Ее основное преимущество, что она простая, но при этом, как бы, функциональная и привязывается децентрализация. То есть, вот в чем Сатоши Накамото, по сути, гений. В том, что он как раз вот этот механизм децентрализации придумал именно за счет экономической составляющей, что при майнинге блоков, кто смайнил блок, получает

деньги и решает криптографически сложную задачу. До этого все алгоритмы хеширования и другое, все это было уже более чем 20 лет назад разработано, но децентрализации не было. Поэтому, если мы говорим, есть ли будущее в финансах, надо смотреть, есть ли там децентрализация. Спасибо. Это такой вопрос риторический и философский больше на самом деле, чем сейчас сложно спрогнозировать, как это все пойдет, на мой взгляд.

А.КОЛОНИН [02:00:59] : Спасибо. Андрей, спасибо. Дмитрий, Ваше слово.

Д.ПАЛЬЧУНОВ [02:01:04] : Ну, я бы вот сказал, даже в первую очередь поставил, как важно, не столько демократизация финансовой сферы, сколько демократизацию бизнеса. Заметим, что вот в чем функция государства. Государство имеет репрессивную функцию, оно должно репрессировать мошенников. Понятно. Людей, которые нарушают законы, которые кого-то грабят и так далее. Но есть вторая сторона этой медали, что те ограничения, которые государство вводит, они часто бьют и по нормальным людям, по бизнесу создают очень тяжелые условия для работы, все эти аукционные требования, особенно бюджетный денег и так далее. Огромные проблемы. Непонятно же, кому больше проблем, жуликам или, как говорится, честным бизнесменам. И вот как раз доверенная система, возможность автоматизации, возможность введения доверенных бизнес-процессов, фактически может помочь уйти от необходимости обращаться к государству в функции защиты от мошенников. И тем самым резко облегчит ведение бизнеса, может резко ускорить всевозможные договоры, консорциумы и так далее. И, соответственно, как раз провести эту демократизацию. Причем, особенно это важно не для крупных корпораций, которые, понятно, легко, как мне вот сегодня сказали, что в Европе постоянно ведутся суды против Майкрософта, а Майкрософт по барабану, ну, штраф наложили, заплатили, все, и продолжают делать, как хотят. Это, кстати, особенно важно для мелких компаний, для стартапов. именно для тех компаний, которые могут создавать принципиально новые технологии и делать индустрию технологий будущего. И поэтому, на мой взгляд, это очень важно. И послушать демократизацию. Спасибо.

А.КОЛОНИН [02:02:59] : Спасибо, Дмитрий. Пожалуйста, Александр.

А.БАЛДАЧЕВ [02:03:04] : Я хотел бы здесь чуть-чуть вперед посмотреть и сказать, что блокчейн, технологическое управление доверием или DT-системой, частым случаем которой является блокчейн, не только способен демократизировать финансовую систему в местах, недоступных для обычных банковских услуг, что отмечал Александр. Но и вторе опять же Дмитрию, что может вообще исключить многие элементы финансовой системы в бизнесе за счет именно доверительных отношений и взаиморасчетов внутри самой системы. То есть не доводить отношения до финансовых отношений. что возможно и, в принципе, уже используется в некоторых приложениях и в некоторых направлениях, но это, скажем, такое будущее. Все, спасибо.

А.КОЛОНИН [02:04:01] : Александр, спасибо. Виктор?

В.НОСКО [02:04:05] : Да, на самом деле мы с 2018 года пытались внедрять блокчейн в бизнес, в частности сделали первый сервис по разметке данных, по получению датасетов на блокчейне, на блокчейне эфира. Вот такой сервис. Он, правда, был, он

опережал свое время. Теперь смотрите, вот по докладу Дмитрия Поличунова, доклад был, ну и коллеги, да, кейс был про смарт-контракты, но я считаю, что та проблема, которая озвучена в этом докладе, да, конечно, она существует, да, объяснение непротиворечивым образом в коде, а как это сделать нельзя, да, без нашего языка, без какой-то интеграции, перевода. законов в формальный вид. Эта проблема существует. Я считаю, что есть другая проблема более фундаментального характера. Она связана с тем, что, по сути, даже если эта проблема будет решена, озвученная в докладе, то мы все равно не сможем внедрить смарт-контракты в бизнес-процессы. Вот почему. Дело в том, что, ну, возьмем тот кейс, который там был, да? Две компании договорились о поставке одна другой. Ну, некоторого сырья одна компания оплатила, другая не поставила в срок, поставила некачественный и так далее, и так далее. Дальше, у вас контракт автоматически исполнился, это смарт-контракт автоматически исполнился. Вы потом только поняли задним числом, что у вас материалы там какие-то некачественные. Но дальше вам нужен какой-то инструмент, ну как в Paypal, допустим, да, как в обычных структурах, откатить. В Paypal это существует, вы можете написать куда-то. Но предположим, давайте мы зайдем немножко вперед на шаг, предположим, что такой инструмент у вас даже есть. Но это другая компания. Что она сделает? Она подделает накладные и скажет, что произошел форс-мажор, и это не она виновата в том, что товар был некачественный, а какие-то другие контрагенты. То есть у вас возникает цепочка, она попытается перекинуть ответственность, скинуть это на различные причины и тем самым доказать и показать, что штрафные санкции она оплачивать не будет. Здесь вопрос про синергию искусственного интеллекта и блокчейна. И здесь однозначно нужен искусственный интеллект для того, чтобы закрыть недостающую часть, которая вот существует, ну это реальный мир, то есть неоднозначность реального мира может быть решена, проблема неоднозначности решена с помощью нейросеток, которые могли бы. действительно достоверно подтверждать, что накладные правильные, что люди, которые их подписывали, что они действительно подписывали, да, и элементы этого, они у нас уже существуют. Есть электронные подписи там для компаний, там у нас она есть и так далее, но пока это все в единую систему не объединено. Есть, конечно, видеокамеры, но этого всего недостаточно для... для того, чтобы механизм действительно работал. Если он будет работать, если это все будет построена некоторая единая система, уж не знаю, как ее назвать, там единый правовой блокчейн, что-то в этом духе, то это будет означать, что мы существенно уменьшим количество времени на заключение договоров между компаниями и проблема газокупок уйдет. Вот к нам как стартапы обращаются уже большие компании, в том числе ГОСы. Проблема там 7 месяцев оформления. В частности, одна из проблем вот такого длительного срока, это то, что проблема безопасности. Нужно компанию проверить, что она способна исполнить контракт. Как проверить? Ну, только нейросетки. Потому что остальные способы являются все-таки субъективными. И нейросетки также должны быть объективны. Для этого они должны информацию, ту, которую они подают... как результат того, что у компании есть ресурсы, у компании есть работники, у компании есть технологии и так далее, это все также должно записываться в блокчейн, иначе мы столкнемся с тем, что будут фальсификации в этой части. То есть вот нужно в эту сторону работать, и здесь, конечно, однозначно СМВА есть.

А.КОЛОНИН [02:08:04] : Виктор, спасибо. Во-первых, мне кажется, что, если останется время, у Дмитрия Евгеньевича будет возможность возразить по поводу того,

что только сетки смогут валидировать смарт-контракты. во-первых, во-вторых, я услышал критические нотки и мне хочется вот тоже перед следующим ответом на следующий вопрос внести некоторый скепсис в части того, насколько технологии искусственного интеллекта могут демократизировать блокчейн или блокчейн может демократизировать искусственный интеллект, да, или они друг с другом могут помочь демаркетизируют друг друга. Вот смотрите же, что получается. Изобрели интернет. Компьютер – это сеть. На каждой станции можем развернуть свою собственную страничку. Каждый человек ходит друг другу, другому человеку в гости на его собственную веб-страничку. Кончилось все тем, что все веб-странички лежат либо на Фейсбуке, либо во ВКонтакте. Либо в инстаграме, и все это дело централизовано и антимонопольное законодательство, по сути, не работает в рамках не просто одного государства, а рамках всей планеты. Ладно, решили придумать semantic web. Каждый сайт может свою собственную семантическую подсеть на своем домене разворачивать. Ссылаемся друг на друга, получаем глобальную семантическую сеть. Кончилось все тем, что есть Google Knowledge Graph. который Гугл никому не показывает, на котором он исполняет свой семантический поиск, которым пользуется все население планеты, опять-таки никто, по большому счету, кроме Гугла, никакой поиск за исключением китайцев не использует. Антимонопольное законодательство в пределах планеты не работает от слова совсем. Почему то же самое не должно произойти с блокчейном? Почему в какой-то момент с помощью, извините, если не паяльника и биты, но миноносцев и авианосцев не будет приватизирован блокчейн или эфир, когда достигнет какого-то размера тем, кто будет иметь достаточное силовые ресурсы для этого. И почему мы считаем, что искусственный интеллект... Да, но искусственный интеллект то же самое. Хотели делать много разных искусственных интеллектов, в итоге все ходим, спрашиваем совета у ЧАД ЖПТ. Все. Кроме ЧАД ЖПТ у нас по большому счету ничего такого уровня нет. И скорость, с которой они двигаются, она не позволяет их обогнать. пока что никому. Как в этих условиях мы можем ответить на вопрос, есть ли будущее у блокчейна и распределенного реестра демократизировать искусственный интеллект и повысить уровень его безопасности? Пожалуйста, Александр, нам.

A.HAM [02:11:16] : Я бы сказал так, что надо вообще сейчас, наверное, посмотреть на вот эту вот бизнес-модель бигтехов, которые собирают данные у себя, хранят на центральных серверах и это монетизируют. понятно, что для бигтехов вообще блокчейн является угрозой и сейчас тема блокчейна, но она кем? она пушится обычными пользователями. У которых нет возможности конкурировать с такими гигантами. Есть венчурные фонды, которые заливали раньше деньги в стартапы. И понятно почему, потому что венчурные капиталисты, они всегда хотят заработать. И их задача поменять рынок, чтобы теперь появились другие компании. забрали долю у бигтехов, ну и венчурные инвесторы смогли выйти и заработать денег. Вот здесь как бы не надо передать иллюзий, когда мы говорим про технологию блокчейн, про демократизацию искусственного интеллекта, ну в конечном итоге все упирается в деньги. Кто сейчас там владеет рынком? Владеют рынком бигтехи. Почему БигТехи побежали там и начали разрабатывать свои большие языковые модели? Потому что появился OpenAI внезапно, который с меньшими ресурсами сделал такую модель. Сможет ли блокчейн как-то противостоять? Не знаю, вопрос. Я не уверен, что только одна технология смогла бы что-то демократизировать. Здесь вопрос комплексный. Вообще, сама вот эта вот история и тренд веб-3, про который сейчас говорят, в основе

которого тоже лежит децентрализация, смогут ли венчурные фонды, стартапы, И, конечно же, это очень важно, потому что, к примеру, если мы говорим о том, что мы хотим создать такие продукты, которые бы реально посигнули там сейчас на лидерство БигТехов. Вот здесь у меня пока вопрос большой, потому что развивались, и они сейчас огромные ресурсы вложили в свою бизнес-модель, и сломать это, сдвинуть с места будет очень тяжело. Поэтому, ну вот, сказал бы так, перспективы есть, но на каком горизонте, ну не уверен, что на ближайшем горизонте.

А.КОЛОНИН [02:13:53] : Александр, спасибо. Андрей Нечосов.

А.НЕЧЕСОВ [02:13:57] : Антон, а можете еще раз сформулировать третий вопрос?

А.КОЛОНИН [02:14:02] : Третий вопрос. Есть ли будущее у технологии распределенного реестра и блокчейна как инструмента демократизации искусственного интеллекта и повышения уровня его безопасности?

А.НЕЧЕСОВ [02:14:13] : На самом деле вот сейчас я активно занимаюсь искусственным интеллектом. У меня будет доклад в Майкопе по поводу задачного подхода. И сам по себе блокчейн никакой интеллектуальной составляющей, искусственному интеллекту не дает, это нужно понимать. Вопрос безопасности алгоритмов – да, но опять же, безопасность алгоритмов достигается только за счет децентрализации. Здесь кто-то правильно написал, что государство… невыгодно давать децентрализацию каким-либо проектам, то есть они будут бороться с этим, и тот же Сбербанк создат централизованные решения. Поэтому в общем случае блокчейн к интеллекту напрямую отношение не имеет, а имеют те технологии, которые позволяют интеллектуальному устройству высоко обучаться. Блокчейн напрямую единственное, что можно, это смарт-контракты погружать в них, которые по сути будут такими обучающимися вещами, но опять же сами алгоритмы в этих смарт-контрактах, они напрямую не имеют отношения к блокчейну, еще раз повторюсь, для безопасности он нужен, но только тогда, когда есть децентрализации, потому что, ну, а Сбербанку зачем блокчейн, если он может в релиционных базах данных централизованное решение построить? То есть здесь вопрос такой, открытый как бы блокчейн сам по себе просто, ну, хранилище данных. Какие алгоритмы, какая математика будет зашита в эти хранилища – это уже другой вопрос. И вот в первую очередь о повышении уровня интеллектуальных устройств нужно думать о математике. Либо это машинное обучение с нейронными сетями – новые подходы, либо это логика, либо это гибридные какие-то сети. Вот мы сейчас работаем над гибридными сосколковыми сетями, то есть центрами искусственного интеллекта. Возможно, что-то и получится, посмотрим. Сильный искусственный интеллект это как бы наша цель на самом деле, ну в наших исследованиях. Насколько получится его достичь, непонятно, а блокчейн здесь как средство зашивания математики и безопасности, все.

А.КОЛОНИН [02:16:23] : Спасибо. Андрей, спасибо. Дмитрий, пожалуйста.

Д.ПАЛЬЧУНОВ [02:16:28] : Ну, я, наверное, присоединюсь к скепсису, который Антон Германович высказал, но я бы проблему на нескольку тоже частей разделил. Ну вот, во-первых, действительно, уже упоминался о ГПТ, да, вот сейчас ГПТ-4, и что нужно отметить? Вот у нас был доклад от «Первый раз на конференции», доклад Мельникова, И он как раз, собственно, отметил, что, скажем так, я бы даже прежде,

чем сказать, что он отметил, немножко правильно преформулировал, что речь даже идет не о демократичности, как бы равенство людей, а даже демократический смысл, где сущности это государство. Вот он как раз отмечал, что мы не конкурентоспособны сейчас с ОПА на ИИ, потому что мощности, вычислительные, у нас просто на порядке меньше. Всё. Мы не можем создавать такие же большие языковые модели, как они. Причём это Россия, это всё-таки страна достаточно мощная. Реально США может конкурировать сейчас пока только Китай, но там может где-то ещё Япония отчасти. А все остальные огромное безумное количество стран, они всё, они, говорится, здесь вообще не участвуют. Это первый момент. Естественно, тут блокчейн ничем не поможет, потому что речь идет не о закрытости информации, а о, в смысле, не о защите информации, а о возможности ее перерабатывать, продуцировать, порождать и так далее. Но здесь есть еще два момента. тоже отмечают вот эти вот боты, да, это боты, которые, кстати, вот сейчас JPEG тоже сравнивают, вернее, не сравнивают, господи, ставят эту проблему, что порождается фейковое знание, да. То есть, в общем, он может порождаться в массовых количествах, люди уже могут его потреблять, и это огромная проблема. Причем здесь две проблемы, что и GPT может добросовестно порождаться, называется галлюцинацией, он несет всякий бред просто потому, что думает, что это не бред. И может, если он намерен, то специально порождается. вот специально порождается вот это вот неверное знание. И, кстати сказать, сейчас уже на западе, вот раньше были технологии, скажем, opinion mining, reputation mining, сейчас manipulation mining. То есть, смотрят вообще, пытаются найти, а где идут явные манипуляции, да? То есть вот это вот, ясно, что это некие блокчейны здесь помогут. И еще один момент, который почему-то все как-то не замечают. Ну, часть GPT, GPT, GPTuit, да? Ну, на самом деле, у нас есть Google. В принципе, когда это PHPrint его создали, да? Они получили первый экран. Кстати, кстати, 100 тысяч долларов, это вот бортник. нам дала такие же гранты, не так очень много, а потом, на самом деле, они начали уже интегрироваться в ЦРУ, и фактически, на самом деле, то информация, которую он нам выдаёт, Эта информация, она фильтруется, да, и Google, и Википедия, и так далее. И здесь о какой демократичности можно говорить, если там, ну, есть у нас еще Яндекс, да, так говорится, вот, контурент. Китайцы решают проблему демократизации железной стеной, да, просто отгораживаются и свои поисковики. Вот это огромная проблема, что фактически власть, сосредоточенная в очень небольшой группе компании, это власть над умами людей. А за счёт чего человек принимает решение? За счёт информации, которую он имеет. И даже очень умный человек, если ему давать неверную информацию, будет принимать неверное решение. И это как раз вот огромная проблема с искусственным интеллектом наравне и с GPT и так далее. То есть это еще раз и боты, которые порождают неверную информацию, и Google, которая эту информацию и Википедия фильтрует, ну и, собственно, GPT, которое может порождать уже то, что неотличимо практически от человека. Спасибо.

А.КОЛОНИН [02:20:36] : Спасибо, Дмитрий Евгеньевич. Пожалуйста, Александр Балдачев.

А.БАЛДАЧЕВ [02:20:41] : И вот сейчас я делаю маленькое замечание, почему я не участвовал с докладом, потому что свой доклад под названием «Новое поколение DLT – Trusted Semantic Network. DLT плюс семантик плюс языковые модели» я сделал несколько недель назад. И вот подробно на этот вопрос, который сейчас отвечают, я давал там. То есть именно взаимоотношения DLT и искусственного интеллекта и

языковых моделей. Сейчас я лишь скажу... Да, еще месяц до этого я делал доклад «Субъективный язык описания деятельности и как ему учился Чаджи Пити». То есть это доклад, пересекающийся с Дмитрием, как можно создавать семантические модели. И семантически исполняемые модели, не компилируемые в столе дети, а именно исполняемые как семантику. А язык описания деятельности, язык описания бизнес-процессов. А коротко на этот ответ у меня такой, что да, действительно, DLT-системы нужны для языковых моделей в частности, это прежде всего валидированный, не фальсированный контент. То есть нельзя давать языковой модели собой производить контент. Нужно всегда на основе какого-то контента, который может быть... Если особенно мы говорим не о ботах, а о бизнес-приложениях, то у нас должна быть система валидированного нефракционного контента, которая может обеспечить именно эти системы. Также то, что Александр в своем первом докладе говорил, что это подтверждение авторства, и авторства как человека, и авторства машины. То есть весь контент, который порождается в языковой модели, и плюс еще соединенность с DMT-системой, они должны быть подписаны ключом. То есть и неважно, кто произвел этот контент, главное, несет ответственность тот, кто подписал его ключом. Ну и, конечно же, обеспечение приватности данных. Для этого тоже нам нужны DLT-системы, соединенные с языковыми моделями.

А.КОЛОНИН [02:22:44] : Александр, спасибо. Виктор?

В.НОСКО [02:22:49] : Я в 2019 году делал доклад на конференции по искусственному интеллекту Data Start про безопасность контроля обучения моделей искусственного интеллекта. Тогда это еще не было в тренде, сейчас после принятия кодекса этики искусственного интеллекта об этом заговорили. Там я приводил в докладе, в частности, кейс, и всем известно этот кейс с Теслой, допустим, попала в аварию И, в принципе, это очень важный момент, потому что это очень важный момент для разработчиков, потому что это очень важный момент для разработчиков, потому что это очень важный момент для разработчиков, потому что это очень важный момент для разработчиков, потому что это очень важный момент для разработчиков, потому что это очень важный момент для разработчиков, потому что это очень важный момент для разработчиков, потому что это очень важный момент для разработчиков, какие, какова полнота, что такое полнота датасетов для обучения нейросети, вот это не было прописано, менеджмент это утвердил, они обучили, да, то есть, соответственно, здесь возникает проблема размытости вот этой ответственности, эту проблему нужно будет решать, я считаю, что ее нужно решать законами, потому что сейчас... все будет скинуто на разработчиков, то есть чем более будут сложные системы, тем больше в них будут ошибки возникать, ответят за все разработчики, они за это не захотят отвечать, потому что им менеджмент утвердил определенную стратегию обучения и сбора датасетов, существенно здесь есть проблема безопасности контроля моделей, поэтому нужно выпуск моделей. чекпоинтов, тех же JPT, неважно каких, по Vision, у которой модели, нужно эти чекпоинты сохранять в блокчейн для того, чтобы потом можно было обратиться к блокчейну и доказать, что менеджмент утвердил. Поэтому мы вот так обучили, и вот такие были объемы датасетов, и вот такая была полнота, и вот такая была точность утверждена. Если этого нет, то разобраться, то прав кто виноват будет совершенно невозможно. Ну и там второй кейс можно привести. Допустим, вот Антон, предположим, что через несколько лет будет внедрена proof of reputation. У нас все будет репутация, она у нас уже и так есть, но она будет

формализована очень круто, в виде графа там показана. Вот, допустим, где-то в чате вы взяли, использовали текст из chat.gpt, он оказался ложным, возник скандал, а репутация ваша упала. Вам хотелось бы доказать, что это не ваше было мнение, а что вы просто ошибочно опирались на ложные данные, которые сгенерировало chat.gpt. Как вы это докажете? Вы будете говорить, ну, извините, я взял из chat.gpt информацию, да, и ее предоставил сообществу. Нет, это вы сами. Вы сами вот такое вот сказали, и поэтому мы вам сейчас занижаем репутацию. То есть вам хотелось бы иметь вот этот инструмент действительно достоверности, о чем все говорят. Он должен быть, он однозначно будет.

А.КОЛОНИН [02:25:59] : Виктор, спасибо. Я отвечу на вашу ремарку в моем отношении. Смотрите, значит, я думаю, что если я... осознанно опубликовал какую-то неадекватную информацию, которая сгенерировала чат GPT, или если это сделали вы, я думаю, вся ответственность и соответствующие репутационные потери на мне, как на том, кто эту информацию зарепостил. То есть я как бы не считаю, что я имею моральное право искать какие-то отмазки, что я какую-то фигню запостил. потому что ее сгенерировал чат GPT, то есть я не вижу вообще никакой проблемы. Вот, хорошо, у нас остался один вопрос, значит, на него в какой-то степени участники ответили. Вот, времени у нас осталось немного, но тем не менее, точнее, мы его практически исчерпали. Тем не менее, давайте все-таки мы к последнему вопросу пройдемся. Вопрос звучит так, как технологии искусственного интеллекта могут помочь технологиям распределенного реестра и блокчейна в том числе? И тут на правах тоже участника я выскажу свою точку зрения. Во-первых, конечно же, это безопасность, и в частности это безопасность в части смарт-контрактов, то есть еще когда начинался проект Синкулярити.нет Дмитрий Иванович Савереденко помнит, что еще обсуждались вместе с организаторами Singularity.net совместные работы по разработке технологии валидации смарт-контрактов. Вот примерно в том же ключе, про который Дмитрий Евгеньевич сегодня рассказывал, тема мне кажется очень важная. Кстати, еще интересная тема, не связанная с блокчейном, а связанная с тем, чем я сейчас занимаюсь по основному месту работы – это автоматизация технологических процессов с помощью исполняемых спецификаций для управления объектами критической инфраструктуры, выявления безотказности, надежности, отсутствия дыр как с точки зрения безопасности, так и с точки зрения отказа устойчивости. в программах управления критической инфраструктурой. Это еще одна очень интересная задача, в том числе и для систем искусственного интеллекта. И, кстати, вот тоже заранее вопрос Дмитрию Евгеньевичу, насколько он считает, для обеспечения безопасности систем на блокчейне и смарт-контрактов в частности могут быть применимы либо нейросети, либо семантические технологии, либо какая-то комбинация их. Значит, второе направление, где искусственный интеллект мог бы помочь блокчейну, это опять-таки безопасность, с моей точки зрения, но безопасность уже с точки зрения вот той самой, того самого, той самой репутационной системы, про которую я сегодня говорил. Это выявление паттернов, дело в том, что кольцевые структуры, репутационные кольца, круговую поруку вычислять в условиях анонимных транзакций на блокчейне очень сложно, то есть кто-то может создать ботнет. через этот бутнет проводить какие-то транзакции, причем часть транзакций будет проводиться в off-chain или вообще в альтернативных валютах или в фиате, потом деньги будут возвращаться в блокчейн, то есть кольцо будет в блокчейне разрываться, а снаружи оно будет проходить в каких-то финансовых системах, которые не

отслеживаются репутационной системой. И выявление различного рода паттернов является очень важным. Второе, значит, интересное применение блокчейна – это выявление как раз паттернов типа FlashAttack или FrontRunning, про которые я говорил раньше, когда мы анализируем цепочки блоков и выявляем какие-то транзакции, которые потенциально... которые, по сути, являются вставленными, инъектированными в процессе анализа формируемого блока непосредственно тому, кто этот блок майнет. То есть, выявление таких паттернов и соответствующим образом блокирование рецидивов со стороны участников, если их удается идентифицировать, это тоже является важным. Даже придумали некоторый термин – reputation police. Это некоторая система искусственного интеллекта, которая мониторит сетевую активность и каким-то образом блокирует участки, сегменты сети или участников сети, которые с определенным уровнем достоверности превышают некоторые порог безопасного поведения или опасного поведения. Вот мой ответ и слово, Александр, нам вам, пожалуйста, с вашей точки зрения.

А.НАМ [02:30:56] : Да, Антон, я здесь полностью с вами согласен, как я говорил в начале своего доклада, как раз-таки безопасность блокчейна, но это, наверное, самый большой вызов. Для того, чтобы туда пришли обычные пользователи, как ни странно, нужно повысить доверие к самой технологии блокчейн. Вот люди, которые не разбираются в технологиях, они воспринимают блокчейн как что-то такое, мошенничество, скам и так далее. И цифры это подтверждают, потому что в этой сфере очень много денег пользователи теряют. И я думаю, что искусственный интеллект, он как раз таки даст инструменты по комплайенсу, по проверке транзакций, по превентивным фрод-мониторингам. Все это позволит нам обезопасить обычных граждан от недобросовестных игроков. И тогда и доверие поднимется. к самой технологии, и мы с вами быстрее увидим какие-то реальные применения в бизнесе. Вот это основной барьер сейчас, почему технология блокчейн активно не внедряется в бизнесе, потому что люди пока не доверяют. Искусственный интеллект мог бы нам здесь помочь.

А.КОЛОНИН [02:32:23] : Александр, спасибо. Андрей, Ваше слово.

А.НЕЧЕСОВ [02:32:29] : Здравствуйте еще раз. На самом деле я немножко хотел бы поспорить с Александром насчет того, что люди не доверяют и так далее. Самая надежная на сегодняшний день сеть в мире, которая не падала 15 лет уже, это сеть блокчейна, биткоина. С 2008 года это самая надежная. Все, кто хоть немножко понимает, на самом деле понимают, что это супер надежное решение на сегодняшний день. Но вопрос того, кому это выгодно, чтобы люди боялись таких технологий, я не буду называть, кому это выгодно, но я уже сказал, да, главный противовес всем этим технологиям – кто? Это раз. Во-вторых, как же все-таки искусственный интеллект может помочь блокчейн-сетям? Мое мнение – это то, мы вчера на семинаре на научном, который мы проводим в НГУ по средам. обсуждали, что нейронные сети, в принципе, уже неплохо научились генерить код, питонный код, программный питонный код и, в принципе, он корректный и можно его, вчера вот как раз верификация программ была, если прикрутить еще верификацию программ, да, то этот код можно сразу и верифицировать, то есть удобно, если зашить такие вот нейронные сети с верификатором прямо внутрь блокчейна, то, в принципе, Сами смарт-контракты, умные контракты могут порождать внутри блокчейна другие умные контракты под

различные требования пользователей. То есть это получается такая как бы щупальца растут во все стороны и создаётся куча смарт-контрактов умной системой внутри блокчейна, создаётся куча всего. В принципе, эта технология может быть интересна и каждому, допустим, надо создать свой сервис децентрализованный, он вбивает набор параметров, которые ему нужны. Система сама генерирует корректный смарт-контракт, который не надо уже аудировать, потому что он прошел процедуру аудита и верификации и просто размещает его внутри блокчейна. Я считаю, в этом может быть польза именно система искусственного интеллекта. Неважно, на каких там реализациях будут нейронные сети или просто логикой вероятность на какие-то подходы. Я думаю, что доверие здесь такое понятие относительно и как бы надо очень серьезно разбираться с этим вопросом. То есть это не от незнаний происходит, а наоборот иногда от запутываний людей и от подсовывания суррогатных криптовалют. Вот и все.

А.КОЛОНИН [02:35:14] : Спасибо. Андрей, спасибо. Дмитрий Евгеньевич, пожалуйста.

Д.ПАЛЬЧУНОВ [02:35:22] : Но на самом деле, вот если брать искусственный интеллект, ну, многие его отождествляют нейронными сетями с мышленного учения, но вот если брать чистые нейронные сети, то на мой взгляд они не могут помочь. Почему? Потому что они сами недостоверны. Они могут пропустить злоумышленника, с одной стороны. С другой стороны, недавно был эпизод, что где-то в Германии проходил фестиваль, и там куча народа, там было поиск контроля искусственного интеллекта, определяли людей, потенциально агрессивных, нехороших, террористов. Просто там сотни людей, совершенно необоснованно, были задержаны и так далее. То есть понятно, что если искусственный интеллект заблокирует вам транзакцию нейронной сети по какой-то причине, по причине сбоя, то это будет, мягко говоря, неправильно, если вы покупаете последний авиабилет, который кончается. Или еще хуже, если вы делаете какие-то банковские транзакции, а искусственный интеллект нейронной сети неправильно поняла и не заметила жулика, и он у вас украл все деньги. Это, как бы, скажем так, недопустимо такое присутствие нейронных сетей, а пока, как всем известно, мы в принципе не можем даже оценить с мира, оценить процент ошибок, который она может сделать, и ту ситуацию, в которой может сделать ошибки, с одной стороны. С другой стороны, если брать тоже чисто логико-семантические искусственные теории Тонцла, То есть его, если, скажем, решат довольно мощные задачи, то вряд ли он справится. На мой взгляд, как раз здесь может быть каком-то смысле спасения или решения проблемы, как скомбинирование. Комбинирование и нейронных сетей, и, соответственно, логика семантических методов основана на явном описании. Причем каким образом? На самом деле, кстати, когда биомедицинские системы какие-то, всегда встает вопрос, кто несет ответственность за диагноз пациента. И вот тут только что был хороший пример, что если сбил кого-то автомобиль беспилотник, то кто виноват. На самом деле, ответственность нейронная сеть нести не может. Но с другой стороны, здесь можно как раз разделять две вещи. А именно, с одной стороны, принятие предварительного решения и порождение гипотез, с которыми может справляться нейронная сеть. И второе – это уже принятие окончательного решения, которое доказательное. Собственно говоря, вот в чем сила логикосематических методов, что они могут давать решения, которые полностью доказаны. Ну, а слабость, повторяю, если вы будете строить доказательства чисто этими методами, вы сможете их очень долго строить и не получите. И вот как раз

комбинация ситуации, когда искусственный интеллект предлагает какое-то… в смысле нейронная сеть предлагает какое-то решение, а, соответственно, логико-семантический метод окончательно дает вердикт о том, что это решение верно, исходя уже из Аксиом. На мой взгляд, действительно можно решить проблему, и в частности, кстати, что интересно, можно решить проблему, не знаю, Антон Георгиевич согласится со мной или нет, решить проблему того самого репутационного консенсуса, который будет вообще полностью независим от участников, и будет адекватен, и, собственно говоря, нет реальной ситуации, будет работать очень быстро. не нужно будет ждать чашки кофе, подтверждение чашки кофе полчаса, и будет это делать быстро, и будет это делать гарантированно, и не будет зависеть от богатства или мощностей, которыми владеют отдельные участники процесса. Спасибо.

А.КОЛОНИН [02:39:31] : Дмитрий, спасибо, пожалуйста, Александр Балдачев.

А.БАЛДАЧЕВ [02:39:36] : Так, я коротко. В чем я вижу функцию, одну из важнейших функций искусственного интеллекта в DLT-системах, и даже уже, наверное, все-таки конкретно языковых моделей, это выполнение роли универсального адаптивного интерфейса. То есть замена всех веб-форм, замена всех отображений, которые генерятся какими-то веб-мастерами на адаптивные интерфейсы, генерируют непосредственно под запрос и непосредственно под конкретную деятельность. И именно языковые модели, которые понимают с одной стороны языки программирования, скажем, понимают некоторую семантику моделей бизнес-логики и понимают естественный человеческий язык, они могут стать вот этим универсальным адаптивным интерфейсом. И еще одну функцию могут выполнять языковые модели, которую проверено, то есть я уже это проверил, то есть генерация семантических моделей. То есть, когда есть некий язык описания деятельности, есть язык, на котором можно составлять бизнес-процессы, он формализован в некоторой степени, можно научить языковую модель. различными методами другую моделю и также какими-то формальными методами можно провалидировать модель, о чем говорил Дмитрий. Вот эти две функции и по сути сейчас они уже реально тестируются и особенно генерацию схематических моделей я реализовывал на GPT-4.

А.КОЛОНИН [02:41:22] : Александр, спасибо. Виктор.

В.НОСКО [02:41:30] : Да, вот сегодня мы, кстати, не затронули одну большую тему – это децентрализация самого обучения искусственного интеллекта, то есть не использования, а именно обучения, потому что действительно, как сказали там несколько спикеров, есть проблема того, что, ну и вы, собственно, Антон, да, тоже сказали, что у кого больше денег, ну тот и захватывает ресурсы и медийные и так далее, и модели вот этих OpenAI. Я думаю, что тренд будет следующий, что будут приняты законы. Мы видим, что сейчас уже в США пошло это движение, вызывают директоров компаний, там Конгресс, у нас тоже будут скоро вызывать, ну там через несколько лет вызывать и говорить, что как вы обеспечиваете, докажите обществу, что вы там за кулисами не обучили какую-то крутую модель, которая вам дает определенное супер преимущество в различных отраслях, безопасность, выхода этого искусственного интеллекта, вырывание его, то, что он вырвется и так далее. То есть докажите это, то есть будут приняты законы о контроле вот этих компаний, а следующий шаг – это в условиях, когда у нас централизация есть, а следующий шаг

будет – это децентрализация, когда будут созданы системы, где мы как обычные люди сможем сдавать в аренду свои GPU, ну видеокарты, будет распределенное обучение этих моделей, в том числе языковых и различных других. И вот здесь мы приближаемся к такому идеалу некоторого справедливого общества, когда все, кто дал GPU, в принципе причастны к тому, что что умеет в итоге эта модель, насколько она опасна, насколько она выровнена, относительно различных джелбрейков и прочее. И точно будет такая вещь, и уже есть опытные, они обсуждают ее выкатку, это водяные знаки в генерации. То есть вопрос в технологии этого, насколько ее можно обойти. обойденные знаки будут и думаю, что проблема будет решена. в общем, децентрализация многие-многие вопросы здесь решит.

А.КОЛОНИН [02:43:50] : Виктор, спасибо Вам, коллеги, всем спасибо за участие. У нас, очевидно, исчерпан лимит времени, нет больше времени на продолжение дискуссии, мне кажется, было очень интересно. Вначале было много оптимизма, потом оптимизм был осторожный. Поэтому давайте мы на ноте осторожного оптимизма завершим сегодняшний семинар. И огромное спасибо Александру, Андрею, Дмитрию, Александру и Виктору за участие. Всем большое спасибо за вопросы и ответы, и за доклады, и до новых встреч. До свидания. Всего доброго.

Д.ПАЛЬЧУНОВ [02:44:29] : Антон, вам большое спасибо за организацию. Спасибо. Все счастливо, всем до свидания.