

УДК 004.04

ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ BLOCKCHAIN ВНЕ ЗОНЫ ДЕЙСТВИЯ ЦИФРОВОЙ ЭКОНОМИКИ.

Дедаев М.А.

ФГБОУ ВО «Воронежский государственный университет инженерных технологий» (394036, Россия, г. Воронеж, проспект Революции, д. 19), e-mail: dedyaev-max1@yandex.ru

Коробова Л.А.

ФГБОУ ВО «Воронежский государственный университет инженерных технологий» (394036, Россия, г. Воронеж, проспект Революции, д. 19), e-mail: lyudmila_korobova@mail.ru

Аннотация: Статья посвящена общему обзору понятия Blockchain в разрезе доступных примеров. Формулируются проблемы, касающиеся общих понятий и определений данной технологии, с которыми сталкивается человек, при рассмотрении задачи. Поднимаются актуальные вопросы, касающиеся сложных сторон, понятий и определений, посредством которых, в последующем, формулируются ключевые черты рассматриваемой темы. Приводятся примеры развития этой технологии на базе сложных бизнес понятий, связанных, в первую очередь, с развитием информационной составляющей среды. А также формулировке возможностей применения ее на базе информационно технологической инфраструктуры предприятий и бизнес процессов, организованных с помощью усложненного взаимодействия между человеком и системой. Затрагиваются вопросы альтернативного применения инструмента хранения данных, в качестве основных примеров было выбрано несколько стратегий государственного развития оборота документов, в странах востока, а также ближнего зарубежья, где подобная практика уже имеет положительный результат, ярко отражающийся в удобстве использования государственных услуг в различных отраслях жизни. Кроме того, представлено рассмотрение потенциальных жизненных областей применения этой технологии, включающих в себя широкий спектр охвата повседневного быта современного человека.

Ключевые слова: Blockchain, цифровая экономика, цифровая подпись, свертка, хеш, хеширование, майнинг, майнеры, понятие «Смарт», смарт контракты.

POSSIBILITIES OF APPLICATION OF BLOCKCHAIN TECHNOLOGY OUT OF THE ZONES OF ACTION OF THE DIGITAL ECONOMY.

Dedyayev M.A.

FGBOU VO "Voronezh State University of Engineering Technologies" (394036, Russia, Voronezh, Revolution Avenue, 19), e-mail: dedyaev-max1@yandex.ru

Korobova L.A.

FGBOU VO "Voronezh State University of Engineering Technologies" (394036, Russia, Voronezh, Revolution Avenue, 19), e-mail: lyudmila_korobova@mail.ru

Annotation: The article is devoted to a general review of the concept of Blockchain in the context of available examples. Problems are formulated relating to the general concepts and definitions of this technology that a person encounters when considering a problem. Topical issues are raised concerning complex aspects, concepts and definitions, through which, subsequently, key features of the topic are formulated. Examples are given of the development of this technology based on

complex business concepts, primarily related to the development of the information component of the environment. And also the formulation of the possibilities of its application on the basis of information technology infrastructure of enterprises and business processes organized with the help of the complicated interaction between a person and the system. The issues of alternative use of the data storage tool are touched upon, several strategies for the state development of document circulation, in the countries of the east, as well as near abroad, where this practice already has a positive result, are reflected in the ease of use of public services in various sectors of life. In addition, consideration is given to the potential life-span of this technology, including a wide range of coverage of everyday life of modern man

Keywords: blockcahain, digital economy, digital signature, convolution, hash, hashing, mining, miners, the concept of "smart", smart contracts.

Наверняка, практически каждый человек сталкивался с понятием «Blockcahain», но, по всей вероятности, посчитав его очередным модным словечком, обещающим менеджерам по продажам увеличение стоимости проекта, решил, что оно не имеет под собой состоятельной основы. Я же считаю, что именно эта технология является настоящим прорывом в мировой технологической индустрии, и, потенциально, будет иметь крайне серьезное воздействие, как на мировую экономику, так и на протекание прежде обыденных жизненных процессов.

Начать, прежде всего, стоит, вероятно, с описания того, что же собой представляет упомянутая ранее «Blockcahain» технология. Термин Blockchain образован, фактически, из двух, связанных между собой английских слов block – оно переводится непосредственно, и chain – цепь. Последовательность блоков, а точнее сказать последовательность информационных блоков, содержащих в себе определенные сведения – вот самое простое определение, подходящее выражению Blockchain [1]. По своей сути, это просто инструмент, посредством которого можно хранить данные транзакций или непосредственно баз данных. Но все это, безусловно, лишь этимология и ничего больше. Поэтому для того, чтобы разобраться в процессе глубже, нам необходимо будет разобрать еще 2 определения.

Первое из них – цифровая подпись. Каждый человек в сети интернет может сформировать себе «цифровую фамилию». Он «показывает» ее всем, ее все знают, именно по «цифровой фамилии» можно определить человека в сети. Но существует более приватное понятие, которое «юридически» характеризует принадлежность субъекта – это «цифровая подпись».

[1] В отличие от предыдущего понятия, подпись не видит никто, она не доступна никому, кроме владельца. Благодаря этому, например, никто не сможет подделать ваше сообщение в сети.

Второе понятие называется хеширование. Не отходя далеко от «сообщений в сети», приведем простой пример. Допустим, вы отправляете сообщение, содержащее скажем 1

слово «слово». Но нам также необходимо понять, дошло ли оно до адресата или нет. Как это сделать? Самый простой и логичный вариант – попросить своего собеседника переслать текст в ответном сообщении и сравнить с исходным. Кстати, именно так многие и поступают, когда разговаривают по телефону, и просят продиктовать в ответ какие-то важные данные. Но, если что-то пойдет не так, то, по пути обратно, сообщение также может быть повреждено, да и мало кто отправляет такие короткие сообщения. А если в нем будет содержаться видео высокой четкости, не передавать же нам все гигабайты обратно? Во избежание подобных проблем используется свертка, или по-другому хеш. Свернем «Слово» в одно число. Сделаем это вот как, каждой букве в алфавите выдадим порядковый номер (пусть а – 1, я – 33), получится 19 13 16 3 16. Все эти числа мы перемножим и получим 189 616. Это и будет простейшей сверткой. Соответственно, после передачи сообщения, своему визави я отправлю еще и хеш, чтобы он убедился, что сообщение верное. Кстати, по сути, если поменять местами буквы, то, в данном случае, свертка не поменяется, и такое кодирование не будет иметь ни малейшего смысла. В реальной жизни используются гораздо более сложные алгоритмы, которые делают хеш «криптостойким».

На самом деле, два приведенных выше понятия, играют определяющую роль, в формировании фундамента технологии блокчейн. Первое, что действительно здорово удалось с ее помощью сделать, это криптовалюта [5]. Давайте разберемся и с ней.

Представим, что в студенческой аудитории находятся 20 человек, и им, для каких-то интересных целей понадобилось играть, и не просто играть, а платить игрушечными деньгами за что-либо. Есть условие, что деньги эти могут быть либо просто на бумажке, либо в интернете. Студентам приходит в голову классная идея – для прозрачности операций, писать их все на доске. Сверху – стартовое количество денег, снизу – дописывать, сколько и кому этих денег передается. Пишут все, естественно, своим подчеркиком, ставят подписи, чтобы никто и ничего на перерыве не дописал. Даже в таком виде эта система вполне эффективно работает. На самом деле до поры, пока не придет кто-то «сверху», предположим, преподаватель, и не заявит, что хочет контролировать все, потому что у него власть. И чтобы делами нехорошими не занимались. Умные студенты, как и полагается умным студентам, убирают доску, на которой все писали, и заводят большую тетрадь, только собственную, которую каждый пишет самостоятельно, и есть она у каждого. Принцип тот же – сверху стартовые позиции, снизу – все транзакции. Но при преподавателе кричать нельзя, все-таки пару никто не отменял. Тогда студенты начинают передавать друг другу записки (это, кстати, в реальной проекции и есть интернет). Теперь по классу гуляет минимум 20 бумажек с записанными на них транзакциями. Но, самое главное – абсолютно не понятно, переписал ли их студент себе в тетрадь, какие записки есть уже у всех и их можно выбрасывать, у кого

и сколько денег есть фактически. На самом деле и здесь решение есть. Студенты будут обмениваться не короткими записками с отдельными транзакциями, а сразу целыми страницами. Допустим, кто-то уже накопил много строчек, аккуратно записал их, проставил номера страниц, посчитал свертки предыдущих страниц и тоже их записал, а позже разослал по классу новую страницу. Условный Саша, получив эту страницу, проводит полную проверку: проверяет верность строчек, номера страниц, хеш, финансы, и, если верно, признает страницу правильной и переписывает ее себе в тетрадь. Если же что-то не так, то Вася со словами «Среди нас завелся вор», выкидывает подозрительную страницу, и все работают дальше. Как вы, наверное, уже поняли, страницы, это как раз и есть блоки, а их совокупность и отражает непосредственную суть Blockchain [4].

Давайте вернемся в наш класс. Если все в нем пустить на самотек, то каждый студент, как и подобает порядочному студенту, будет писать свою версию страницы, и в итоге по аудитории будет кочевать 20 версий одного блока, но как мы поймем какая правильная? Для этого необходимо установить какой-то порядок. Пусть страница оформляется каждые «N» минут, чтобы ее можно было разослать всем участникам, причем автор выбран случайно, а за сформированную страницу он сам получит «M» валюты. Для того, чтобы все имели право на такой «пассивный» заработок, введем еще одно правило. Пусть все решают задачки. Кто первый решит, тот и оформляет блок. Не страшно, если все время это будет делать один и тот же отличник, лишь бы делалось это регулярно и с нормальной скоростью. Тогда складывается еще один вопрос – зачем кому-то еще доверять это, если, опять же условный Миша с этим справляется? Ответ кроется в том, что если Миша, будет на постоянной основе решать задачки первым, т.е. его вычислительный ресурс будет выше остальных, то студент начнет оформлять страницы по своему, точнее свою часть данных будет выгодно писать. На практике, такое практически не возможно, поскольку для сбора такого количества вычислительных ресурсов требуется слишком много инвестиций, в тени которых такие кражи окажутся лишь мелким жульничеством. И еще одна особенность – отличник записывает на страницу решение задачи. Задача, по сути, не случайная, а связанная с самой страничкой. Это необходимо, чтобы свести к нулю риск подделки страниц – для такого подлога придется решить слишком много задач. Все описанное выше, кстати, называются словом майнинг, а люди, занимающиеся этим майнеры [4].

Получается, что сейчас, на основе этого примера, можно выделить несколько ключевых положительных сторон технологии блокчейн.

- 1) Масштабируемость – независимость системы от количества участников.
- 2) Децентрализованность – нельзя что-то сделать по своему, каждый участник все может проверить.

- 3) Анонимность, при условии «Цифровой фамилии», конечно.
- 4) Отсутствие комиссии. На самом деле это небольшое лукавство, потому что мы можем доплатить условному отличнику, чтобы он записывал наши транзакции первыми (ProofofWork).
- 5) Устойчивость к попыткам взлома. [5]

Разобравшись в этих непростых, по-настоящему непростых понятиях, перейдем к другому вопросу: «где и как это применить, если не в криптовалюте?». Начать, безусловно, стоит с анализа проблем, которые могут быть решены с помощью этой технологии:

- 1) упразднение архивов;
- 2) минимизация риска взлома серверов данных;
- 3) перевод бизнес деятельности на системы смарт контрактов.

И если с первыми двумя пунктами все приблизительно ясно, то понятие «Смарт», да еще и контракт, остается полной загадкой.

Смарт контракты, или по-другому, умные контракты позволяют производить обмен денежных средств, акций и других активов, не прибегая к помощи третьих лиц. Пойдем по порядку. Для заключения рядовой сделки нам необходимо пойти к юристу, потом к нотариусу, после заплатить им за «высокое качество в оформлении сложных услуг», а после еще и подождать «совсем немного». Умные же контракты меняют представление о том, как теперь будут вестись подобные дела. [2] Можно провести некоторую аналогию с торговым автоматом. Вы бросаете монету (валюту) в него, и необходимая услуга падает в корзину (ваш счет). Кроме того, в отличие от традиционных соглашений, смарты не только «знают» об условиях сторон, штрафах за их невыполнение, но и сами обеспечивают выполнение всех пунктов договора. Умный контракт переводится в скрипт, который следит за соблюдением условий договора. В определенный момент программа будет подтверждать выполнения договоренностей по контракту, и определять, должно ли указанное средство перейти к конкретному участнику процесса. [3] Условия могут быть гораздо сложнее, но это не меняет сути. Все это время документ хранится и дублируется по всем законам блокчейна.

Децентрализованность позволяет обеспечивать высокий уровень защиты данных, и практически гарантирует невозможность «переписки» кода.

На самом деле, если забыть о пользе для менеджмента слова блокчейн, то внедрение такой технологии может быть оправдано далеко не всегда. Уже существует масса примеров, где подобное решение, принятое из маркетинговых побуждений, ожидаемо провалилось, и ничем, кроме массы убытков, для компании это не обернулось. В качестве другого примера применения этой технологии, где явно просматривается польза от интеграции, можно рассмотреть задачу, в рамках которой, будет стоять создание системы, предоставляющей

услуги по электронным закупкам. Вообще, электронные торговые площадки, как метод прямого взаимодействия с поставщиками, в последнее время достаточно широко используется в работе закупочных отделов отраслевых предприятий. Как и любой процесс, он имеет множество недостатков, многие из которых связываются с бюрократизацией процесса, многократным повтором ввода данных контрагента, для последующей регистрации на других площадках, а также процесса делегирования полномочий и базы необходимых данных для поставщика. Если декомпозировать вопрос, то перед нами будет стоять задача создания децентрализованной системы обмена данных в рамках определенного консорциума, с последующим выделением доступа к определенным нодам системы. Посредством внедрения технологии блокчейн мы сможем получить очевидные достоинства решения.

Для начала стоит отметить, что теперь данные в сообществе будут распределяться между всеми участниками сети. Ни одному из участников системы не будет недоступна возможность диверсификации данных, а также их потенциальное удаление. Кроме того, даже при физическом отключении узла участника от сети, данные, полученные до момента отключения, будут оставаться на этом узле, и доступны для работы. Также к очевидным плюсам стоит отнести и то, что при подключении нового пользователя к консорциуму, поставщик сразу же получает все необходимые данные, требующиеся для последующей работы в системе. Еще, стоит отметить автоматическое обновление любых документов, которые были обновлены в системе тем или иным участником. Как говорилось ранее, для ликвидации многократной регистрации поставщика на разных торговых площадках, можно будет легко внедрить принцип KnowyourCustomer (знай своего клиента). Теперь, при однократной регистрации контрагент, за добавлением определенных документов, сможет быстро и удобно получить доступ к другим ЭТП консорциума. Помимо очевидного преимущества для поставщика, сама компания сможет собирать единые данные о контрагентах, работающих с системой. Не стоит забывать и о том, что при необходимости удалить поставщика из группы пользователей, будут нивелироваться проблемы, касающиеся последующего переприсвоения полномочий, поскольку теперь это будет делаться на основе смены, выданных заранее, ключей доступов к сети.

По своей сути, все приведенные выше решения и реализации открывают множество возможностей для многочисленных изменений в системе функционирования бизнес структур. Представьте, насколько прозрачнее и эффективнее можно было бы сделать современные бизнес-процессы. И, в данном случае, мы затрагиваем только коммерческую сферу. Так, например, правительство Грузии сосредоточило свое внимание на технологии блокчейн, для последующего его применения в области кадастрового учета. Объединенные

Арабские Эмираты планируют полный переход всего государственного документооборота на указанную технологию уже к 2020 году. Подтверждение авторства, здравоохранение, энергетика, образование – вот лишь небольшой список ниш, где главным драйвером, определяющим последующее развитие базы, будет именно блокчейн. Мы, безусловно, должны говорить о том, что эта технология еще недостаточно изучена, но недооценивать ее значимость, мы не имеем права. Давайте обратимся к истории, созданная когда-то в стенах пентагона, и предполагавшаяся лишь для внутреннего использования сеть интернет перевернула жизнь человека за каких-то несколько лет. Многие в нее не верили и пророчили скорую гибель. Результат мы все прекрасно знаем.

Подводя итог всему выше сказанному, следует отметить следующее. На основании имеющихся уже сейчас фактах о технологии блокчейн, можно смело говорить о том, что эта технология, если не сама по себе, то в купе с такими же передовыми инновациями сможет, возможно, уже через пару лет приоткрыть всем дверь в мир, который будет полностью функционировать благодаря информационным ресурсам.

Список литературы:

1. Свон М. Блокчейн: Схема новой экономики. М.: Олимп-бизнес, 2017. - 240 с
2. elibrary.ru/item.asp?id=9336699 научная электронная библиотека моделирование взаимодействия предприятия с внешней средой Черкасов О.Н., Ковалев Г.Е., Фортинский Ю.К., Коробова Л.А.
3. elibrary.ru/item.asp?id=23108634 научная электронная библиотека Оптимизация управления качеством производственных процессов на основе вероятностного подхода при взаимодействии стадий производства Сафонова Ю.А. Авсеева О.В. Коробова Л.А.
4. Kastelein R. UK Government Rolls Out Massive Blockchain Report Blockchain News. - URL: <http://www.the-blockchain.com/2016/01/19/uk-government-rolls-out-blockchain-report/> (изложение на русском языке: Великобритания: Опубликован толстый официальный отчет о технологии блокчейна и распределенных реестров
5. Nakamoto S. A Peer-to-Peer Electronic Cash System Bitcoin. -URL: <https://bitcoin.org/bitcoin.pdf>; Перевод статьи Сатоши Накамото. Биткоин: цифровая пиринговая наличность