УДК 65.01

БЛОКЧЕЙН — НОВАЯ РЕВОЛЮЦИЯ

© **Грошева Е. К., Невмержицкий П. И., 2018**
МАОУ Лицей ИГУ, г. Иркутск
Иркутский государственный университет, г. Иркутск

Технологии в наши дни непрерывно развиваются и привносят что-то новое в наши жизни. В современном мире существует быстро развивающаяся и набирающая популярность технология — блокчейн. Все в больших масштабах её начинают использовать, и её потенциал признаёт все больше людей и компаний по всему миру. Данная статья призвана не только описать эту технологию с помощью доступных слов и моделей, но и используя наглядные примеры объяснить, что такое блокчейн, и показать различные сферы применения этой технологии в будущем и настоящем. Кроме того, наша задача — показать, почему блокчейн является настоящей революцией в плане хранения и защиты информации.

Ключевые слова: блокчейн, технология, будущее, инновации, защита и хранение информации, сферы применения

Допустим, существуют абстрактные Алиса и Боб. Они — стандартная пара из криптографии. Допустим, Алиса хочет передать Бобу письмо. Какие у них варианты сделать это так, чтобы Ева, любительница посплетничать и почитать чужую переписку, не смогла прочитать письмо Алисы? Во-первых, Алиса и Боб могут встретиться лично в ближайшем парке и передать друг другу письмо. Но если это трудноосуществимо, например Боб уехал искать Атлантиду, а Алиса собирается покорять Эверест? Как вариант, Алиса может отправить письмо Бобу по электронной почте. Но, опять-таки, возникают препятствия, ведь что может помешать Еве, к примеру, взломать сайт почты, залезть в их банк данных и прочитать письмо? Конечно, можно использовать различные шифры и зашифровать письмо. А если Алиса не хочет тратить свое время на выбор самого безопасного шифра, а Боб не хочет заниматься расшифровкой? И, опять-таки, что мешает Еве, которая обладает весьма значительной вычислительной силой, взломать если и не саму организацию, которая будет доставлять письмо, то сам способ шифрования? Если взломан метод шифрования, то можно изменить содержание письма или вовсе подменить.

И именно здесь Алисе и Бобу на помощь придет блокчейн. Ева останется с носом, а Алиса и Боб смогут сколько угодно передавать друг другу условные конверты с почтой, зная, что никто не сможет их прочитать без ведома их самих.

Но, скажете вы, Алиса и Боб это один случай, и их переписка может интересовать только абстрактную Еву. Хорошо, рассмотрим другой пример. Рассмотрим более близкую к жизни ситуацию. Четыре человека решили сыграть в покер. Игра идет, и вот уже 1 игрок должен 3 денег, а 4 должен 2. Вполне вероятно, что эти 4 людей более или менее знакомы, и на встречи они деньги не берут, а записывают свои проигрыши и выигрыши в специальную тетрадь. И вот, в конце месяца настало время подводить итоги. Но игроки не настолько доверяют друг другу, чтобы верить записям в книге. Конечно, под каждым «действием» можно поставить свою подпись, но что мешает другим ее подделать? И пока дело не закончилось чем-нибудь плохим, предложим игрокам использовать блокчейн.

Но что это за панацея, которая может помочь и Алисе с Бобом, и клубу игроков?

Блокчейн — это хитрый механизм децентрализованного подтверждения операций, основанный не на доверии, а на основах криптографии и математических принципах. Рассмотрим по пунктам, как именно работает блокчейн, в чем его успех и инновация.

Блокчейн — это децентрализованная система, нет нужды в каком-либо центре обработки операций, и это сразу избавляет нас от посредников (например, банков). Условная схема сети при блокчейне выглядит как на рисунке 1, а централизованная система — на рисунке 2.

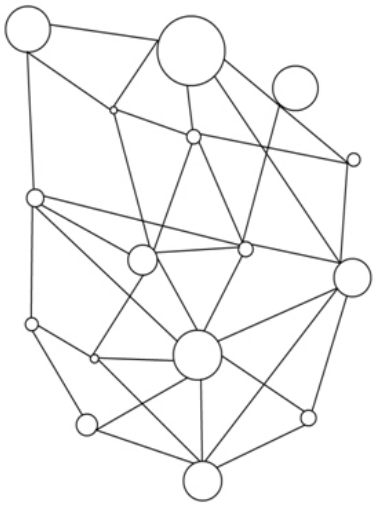

Рис. 1. Схема сети при блокчейне

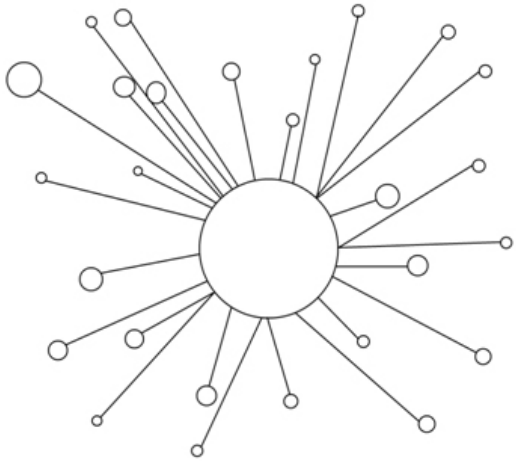

Рис. 2. Централизованная система

С децентрализованной системой все просто. Но как именно подтверждаются операции? Как без посредника обеспечивается (легальность)

операции? Что мешает некому злоумышленнику взломать эту децентрализованную систему и провести ряд (нелегальных) действий?

Именно механизм защиты блокчейна делает его инновацией. Рассмотрим последовательно, как это работает.

Первый шаг — это цифровые подписи, изобретение криптографии. К каждой операции ставится цифровая подпись, которую невозможно подделать. Она уникальна для каждого сообщения и основана на «секретном ключе» или пароле. Общая схема звучит таким образом: создается «секретный» и «публичный» ключи. Секретный ключ состоит из последовательности 256 единиц и нулей в особом порядке. С помощью математических операций из секретного ключа получается публичный ключ, или «адрес» операции.

Подтверждение операции выполняется последовательно — берется само сообщение, подпись (сообщение + секретный ключ) и публичный ключ. В результате этого можно получить либо «да», и тогда операция выполняется, либо «нет» и операция не проходит верификацию. Так как публичный ключ является производной от секретного, то любая операция таким образом легко проверяется. Смысл в том, что не зная секретного ключа невозможно провести операцию, так как вариантов секретного ключа 2^256 (на рисунке 3 представлена краткая схема работы механизма подтверждения (легальности) операции).

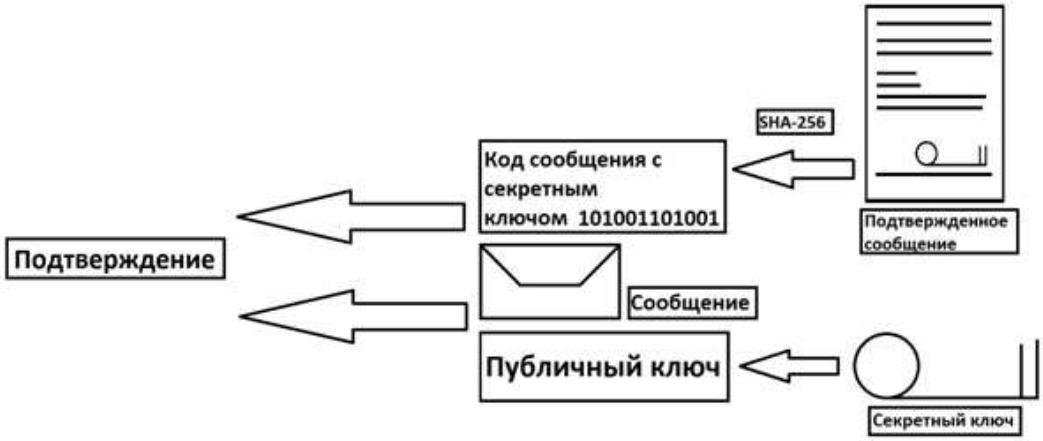

Рис. 3. Схема работы механизма подтверждения (легальности) операции

С этого момента все операции проводятся с вашего согласия и нельзя изменить ее содержание. Но как избежать недействительных операций, или, говоря иначе, как сделать так, чтобы нельзя было потратить больше, чем имеешь? Для этого все операции записываются в своеобразную «учетную книгу», и система проверяет возможность операции. Сумма на счете формируется из всех операций, что были совершены, и, анализируя эту сумму, система позволяет провести операцию или не позволяет. Система проводит операцию и возвращает на баланс «сдачу». Схема представлена на рисунке 4.

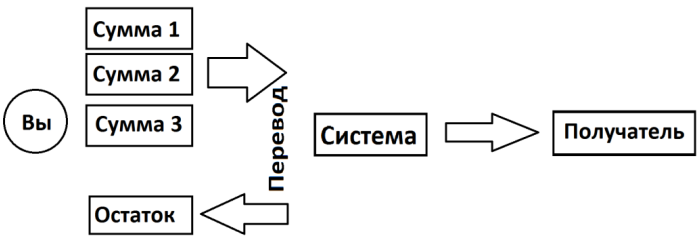

Рис 4. Система проведения операции

Все работает хорошо теперь, но остался последний шаг. В «учетную книгу» или блокчейн операции записываются любым человеком, если они подтверждены. Но кто следит за корректностью записи операций и где находится сам блокчейн? Кто контролирует заполнение книги? И именно это важнейшая особенность блокчейна — его заполнение полностью обеспечивается самими пользователями. Рассмотрим подробнее этот ключевой механизм регулирования всей системы.

Весь механизм основан на том, что записи операций есть у всех участников системы, и каждая новая запись синхронизируется с остальными. Но если взломщик решить добавить в запись что-то свое? Как защитить систему от таких случаев?

Это один из самых сложных моментов в системе. В самом деле, как добиться того, чтобы реестр у всех был одинаковый?

Общее решение таково, что нужно доверять цепи блоков с наибольшим количеством вычислений над ним. Безопасность такого метода основана на криптографической хэш-функции. Ее основная идея заключается в том, что подделка реестра потребует абсолютно невозможных затрат и вычислительных мощностей. Для того, чтобы понять этот принцип, рассмотрим как заполняется сам реестр и какую роль в этом процессе играют «майнеры».

Начнем с самого простого — понятия «хэш-функции». Ввод (например, картина или текст) зашифровывается специальным алгоритмом хеширования SHA-256 и в результате получается «хэш», который изменится, если ввод изменится. Следует отметить, что не имеет значения, как сильно изменяется ввод — значение хэша кардинально поменяется. Смысл применения хэш-функции состоит в том, что невозможно провести дешифровку и узнать объект, который зашифровывался, т.к. объекту присваивается «имя», состоящее из 256 единиц и нулей. Единственный вариант узнать исходный объект — перебрать все 2^{256} вариантов, что на данный момент не представляется возможным.

Но зачем это понятие хэш-функции? Все просто. Она используется при создании блока, который после того, как его подтвердят другие блоки, станет элементом реестра или блокчейна. Как конкретно это работает? В общих чертах у нас есть список операций, хэш предыдущего блока и некоторое число X. Когда все это обработают алгоритмом хеширования SHA-256 получится некоторое число. А система в свою очередь создаст другое число, которое будет начинаться с некоторого числа нулей, которые идут друг за другом. И теперь специальные люди или майнеры, которые обладают достаточной вычислительной мощью, будут искать такое число X, чтобы и число системы, и число, полученное в результате хеширования, сошлись. Это число можно легко проверить, просто использовав алгоритм хеширования. После этого блок записывается в реестр, формируя блокчейн. Наглядно этот процесс проиллюстрирован на рисунке 5.

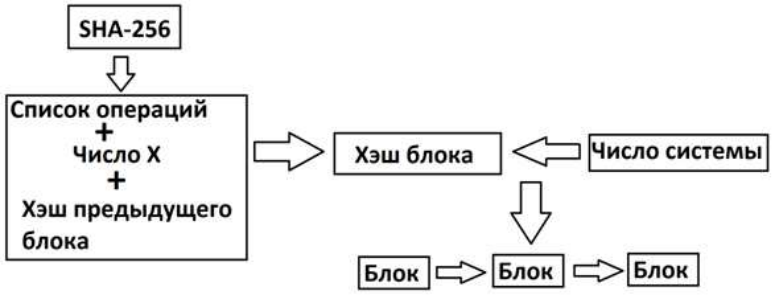

Рис. 5.

Осталось рассмотреть следующие вопросы — зачем майнерам высчитывать это число, как система регулирует себя, зачем это число нужно и возможно ли взломать систему на этом этапе?

Как уже сказано выше, хеширование записей операций и самого числа X дает нам некоторое число, которое должно совпасть с тем, которое предоставлено системой. Это число обеспечивает безопасность всей системы. Алгоритм разработан так, чтобы в среднем каждый блок добавлялся в реестр каждые 10 минут. Майнеры находят это число, и им за это предоставляется награда. Она формируется из награды за формирование блока по способу получения новых биткоинов. В систему заложен алгоритм выдачи награды за блок, так что общее число биткоинов равно 21-му миллиону, и превысить это значение больше не получится, и комиссии за операцию. С майнерами все понятно, они обеспечивают работу системы, так как они оформляют блок и пополняют реестр. Но как быть с тем, кто все-таки попытается изменить сам блок? Рассмотрим эту ситуацию.

Если кто-то захочет изменить содержимое блока, то он увидит, что его изменения одного блока вызывают изменения всех последующих блоков реестра. Это потребовало бы заново проделать всю работу по поиску числа X. На рисунке 6 изображен принцип отсеивания «ложных путей».

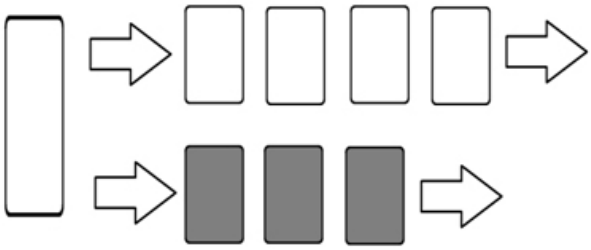

Рис.6. Принцип отсеивания «ложных путей»

Есть длинный исходный блок, а затем взломщик решил изменить один блок. Обозначим его серым цветом. Тогда хакеру придется находить решения для каждого блока раньше всех (серые блоки снизу). Так как он не может обладать половиной вычислительных мощностей мира, то через несколько блоков его линия начнет «отставать» от той линии, которую считают другие майнеры. Так

как в основе системы лежит принцип, согласно которому мы доверяем той цепи, над которой производилось больше всего вычислений, то линия взломщика автоматически отпадет, и безопасность системы не будет нарушена.

Таким образом, можно вывести основные особенности блокчейна:

- децентрализованность;
- доказательство работы;
- электронные подписи;
- цепочка блоков.

Теперь, вооружившись знаниями о работе системы блокчейна, перейдем к тем аспектам современной жизни, которые можно существенно упростить, добавив в них эту систему.

Применение блокчейна на практике не менее интересно, чем разбирать его схему работы. Основные элементы, как уже было сказано, за которые ценится блокчейн — независимость от центра и практически полная невозможность взломать данные. Отталкиваясь от этих двух опорных точек, можно сразу увидеть сферы применения блокчейна. Он будет нужен в тех местах, где необходима верификация чего-либо. Но перейдем от слов к делу.

Применение 1. Биржи статей.

Существуют биржи копирайтеров и рерайтеров, такие, например, как Advego и Etext (одни из крупнейших бирж в этой области). Эти биржи удерживают процент с продажи статей, а если рассматривать биржи поменьше, то они могут брать деньги за размещение статьи. И именно в такую ситуацию прекрасно вписывается концепция блокчейна.

На рисунке 7 представлена схема оптимизации размещения и продажи статей на биржах.

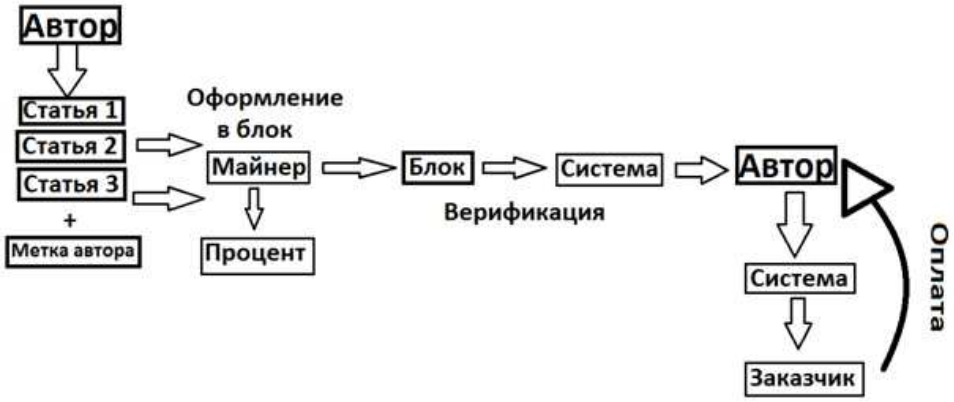

Рис.7. Схема оптимизации размещения и продажи статей на биржах

Автор загружает свои статьи в систему (для удобства стоит создать какую-нибудь систему проверки контента, которая сейчас есть на крупных биржах). Эти статьи группируются, к ним добавляется метка автора (которая будет состоять из его адреса или публичного ключа, которые в свою очередь будут формироваться из его закрытого ключа). Потом это все оформляется в единый блок, к которому добавляется небольшой процент для майнера. Собирается цепочка блоков (блокчейн), который работает по правилам описанным выше. После верификации статей автора они закрепляются в его профиле (аналогично действию биткойн-кошелька). Потенциальный покупатель сможет запросить систему и увидеть все работы автора. Обмен статьи на деньги осуществляется аналогично. Формируются блоки выплат, и они уже в свою очередь подтверждаются майнерами. Таким образом, создается прямое взаимодействие заказчик-продавец, где заказчик не может обмануть продавца (что случается на биржах копирайтеров), исключается третья сторона (биржа) и человеческий фактор, так как нередки случаи, когда администрация биржи сговаривается с заказчиком и авторы остаются без денег. Также, исключается и комиссия биржи, что всегда положительно для авторов. Взаимодействие покупатель-продавец происходит намного быстрее, чем цепочка покупатель-администрация-ожидание-автор.

Блокчейн на примере биржи продажи статей помогает оптимизировать процесс покупки и продажи статей, убрать «лишнее лицо».

Блокчейн также может оптимизировать и способ голосования, например можно создать базу голосов, которую будет намного удобнее подсчитывать, чем в бумажном виде. Она будет более безопасна и достоверна, чем та, которая оформлена в бумажном виде. Принцип работы блокчейна исключает возможность фальсификации выборов, что в любом демократическом государстве весьма важно. На рисунке 8 изображена схема новой системы обработки голосов.

Рис.8. Схема новой системы обработки голосов

Вполне возможно (и экономически выгоднее) создать электронную программу верификации паспортных данных и программу обработки голоса за кандидата. Избиратель заходит на официальный сайт выборов Российской Федерации, верифицирует свои документы и свой голос. Они формируются в блок, который впоследствии формируется в единый банк голосов по всей стране. И благодаря такой системе текущее множество проблем, связанных с выборами. Станет невозможной фальсификация голосов, повысится процент явки (процесс станет проще), будут весьма существенно сокращены издержки на создание избирательных пунктов и их правильное (оформление). И снова блокчейн оптимизирует процесс получения и обработки данных. Нужно упомянуть, что сильно сжатая база голосования будет, согласно алгоритму единого реестра хранится на всех компьютерах сети, что позволит абсолютно точно гарантировать легитимность выборов.

И самый масштабный проект применения блокчейна — это онлайн база всех документов граждан Российской Федерации. Суть проекта состоит в том, что будет формироваться база всех необходимых справок и документов на основе технологии блокчейна. Это позволит гражданам собрать все документы в одной базе, а затем использовать их во всех сферах жизни — в больницах, ЗАГСе, при получении прав и так далее. Эта база документов будет зашифрована с использованием закрытых и публичных ключей. Будет формироваться блок документов, которые будут подтверждаться соответствующими инстанциями и затем зашифровываться, чтобы обеспечить законность и безопасность системы. Эти документы будут прикрепляться к личному профилю гражданина, чтобы он мог ими воспользоваться везде. Сразу отпадает необходимость в хранении бумажных документов, ведь при необходимости можно будет сделать запрос в единую базу и получить необходимые бумаги или справки. Эту систему также стоит дополнить системой оповещений, которая будет напоминать о необходимости оформления нового документа или продлении старого. Также, каждый новый документ должен быть занесен в базу и прикреплен к личному профилю. Один из вариантов такой системы представлен на рисунке 9.

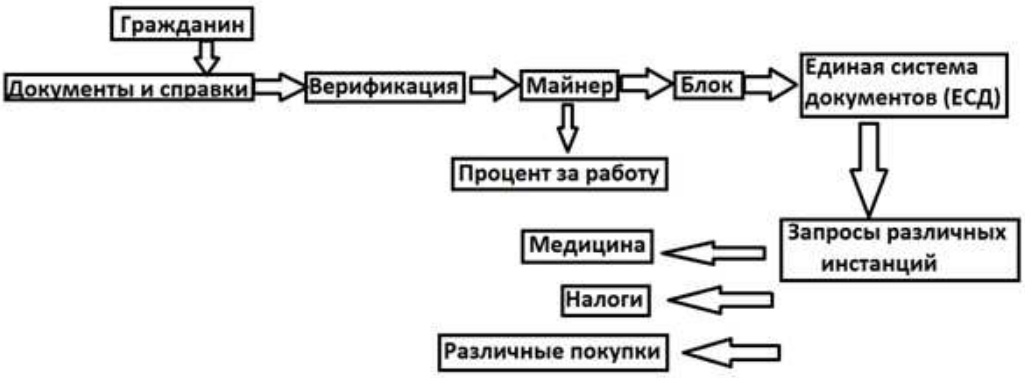

Рис. 9.

Таким образом, становятся практически не нужными бумажные копии документов, ведь если в сети будет хоть один компьютер, то и все данные будут целы. Единственный минус системы может заключаться в хранении большого объема данных. Но и такая проблема решаема — вполне возможно создать множество удаленных банков данных, защищенных с помощью шифрования, а в самой системе блокчейна передавать своеобразные ссылки на файлы, лежащие в этих банках. Таким образом сразу становятся не нужны различные пункты получения бумажных справок, экономится весьма значительное количество как финансов, так и природных ресурсов. Но эту схему можно усовершенствовать, присоединив к ней различные системы, основанные на блокчейне, которые сделают получение большинства справок намного быстрее, чем это происходит в данный момент.

В результате, блокчейн открывает перед человечеством множество путей оптимизации процессов.

Таким образом, новая децентрализованная система подтверждения операций или блокчейн открывает для всего человечества множество путей оптимизации для самых разных сфер жизни. Преимущество этой системы состоит в том, что ее практически невозможно взломать, в ней нет необходимости в третьих лицах для проведения операций, а также нет необходимости доверять другим участникам цепи. Вместо этого вся система основана на принципах математики и криптографии, что значительно повышает ее надежность и сферы применения. Постепенно блокчейн войдет в обиход человека, как это произошло с банковскими картами, и станет такой же незаменимой вещью. Из-за процесса оптимизации исчезнет большинство нотариусов, все станет доступно по «мановению руки». Действительно, блокчейн — это революция современного мира. ■

1. Marc Andressen. Why Bitcoin Matters [Электронный ресурс] // The New York Times, 2014- https://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/ (Дата обращения: 08.01.2018)

2. Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System [Электронный ресурс] // Satoshi Nakamoto- 2008.- https://bitcoin.org/bitcoin.pdf (Дата обращения: 05.01.2018)

3. Мелани Свон. Блокчейн: Схема новой экономики/ Мелани Свон : [перевод с английского]. – Москва : Издательство «Олимп-Бизнес», 2017. – 240 с., ил.

4. Don Tapscott. Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World/ Don Tapscott, Alex Tapscott : Portfolio, 2016. – 368 с.,

5. Andreas M. Antonopoulos. Mastering Bitcoin/ Andreas M. Antonopoulos. : Published by O'Reilly Media, Inc, 2010. – 282 с.,

6. Melanie Swan. Blockchain Blueprint for a New Economy/ Melanie Swan : Published by O'Reilly Media, Inc, 2015. – 129

7. Roger Wattenhofer. The Science of the Blockchain/ Roger Wattenhofer : Inverted Forest Publishing, 2016. – 123

8. Paul Vigna. The age of Cryptocurrency How Bitcoin and Digital Money Are Challenging the Global Economic Order/ Paul Vigna, Michael J. Casey: St. Martin's Press. - 414

9. Explain Bitcoin Like I'm Five [Электронный ресурс] / freeCodeCamp // - Электрон. дан. – URL: https://medium.freecodecamp.org/explain-bitcoin-like-im-five-73b4257ac833 (Дата обращения: 01.01.2018)

10. What is blockchain, really? (An intro for regular people) [Электронный ресурс] / Medium // - Электрон. дан. – URL: https://medium.com/@wen_xs/what-is-blockchain-really-an-intro-for-regular-people-e51578d98a96 (Дата обращения: 01.01.2018)

СПИСОК ЛИТЕРАТУРЫ

Andreas M. Antonopoulos. Mastering Bitcoin / Andreas M. Antonopoulos. : Published by O'Reilly Media, Inc, 2010. – 282 с.,

Marc Andressen. Why Bitcoin Matters [Электронный ресурс] // The New York Times, 2014- https://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/ (Дата обращения: 08.01.2018)

Don Tapscott. Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World/ Don Tapscott, Alex Tapscott : Portfolio, 2016. – 368 с.,

Explain Bitcoin Like I'm Five [Электронный ресурс] / freeCodeCamp // - Электрон. дан. – URL: https://medium.freecodecamp.org/explain-bitcoin-like-im-five-73b4257ac833 (Дата обращения: 01.01.2018)

Melanie Swan. Blockchain Blueprint for a New Economy/ Melanie Swan : Published by O'Reilly Media, Inc, 2015. – 129

Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System [Электронный ресурс] // Satoshi Nakamoto- 2008.- https://bitcoin.org/bitcoin.pdf (Дата обращения: 05.01.2018)

Paul Vigna. The age of Cryptocurrency How Bitcoin and Digital Money Are Challenging the Global Economic Order/ Paul Vigna, Michael J. Casey: St. Martin's Press. – 414

Roger Wattenhofer. The Science of the Blockchain/ Roger Wattenhofer : Inverted Forest Publishing, 2016. – 123

What is blockchain, really? (An intro for regular people) [Электронный ресурс] / Medium // - Электрон. дан. – URL: https://medium.com/@wen_xs/what-is-blockchain-really-an-intro-for-regular-people-e51578d98a96 (Дата обращения: 01.01.2018)

Мелани Свон. Блокчейн: Схема новой экономики/ Мелани Свон : [перевод с английского]. – Москва : Издательство «Олимп-Бизнес», 2017. – 240 с., ил.

Blockchain — new revolution

© **Grosheva E., Nevmerzhitskiy P., 2018**

Nowadays technologies develop really fast and they bring new ideas, break-throughs to our lives. In modern world there is one system that evolves and gains popularity unimaginably fast — it`s blockchain. It`s being used more and more frequently all over the world, and its potential is being admitted by many people and companies. This article is supposed not only to describe this technology using some understandable vocabulary and models, but also to show us different areas of application for this technology in present time and in future using clear samples. Moreover, the goal is to show why blockchain is actually a revolution in terms of protecting and storing data.

Keywords: blockchain, Technology, Revolution, Future, Innovation, data retention and protection, areas of application