УДК 004.043

БЛОКЧЕЙН И ЕГО ПРИМЕНЕНИЕ В СОВРЕМЕННЫХ ТЕХНОЛОГИЯХ

Вольнова В.А., Соловей К.В.

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники» филиал «Минский радиотехнический колледж»
г. Минск, Республика Беларусь

Научный руководитель: Сальникова Е.А. – преподаватель первой категории дисциплин общепрофессионального и специального циклов

Аннотация. *Исследована технология блокчейн, ее принцип работы, преимущества и недостатки. Установлено, что данная технология будет востребована и имеет тенденцию к развитию и усовершенствованию в будущем, но также уже находит применение в различных областях жизнедеятельности на сегодняшний день. Объясняется принцип работы блокчейна на наглядных и простых примерах, а также рассматриваются существующие сферы применения и потенциал дальнейшего внедрения в данную сферу.*

Ключевые слова: *блокчейн, применение, криптовалюта, биткоин.*

Введение. Нельзя точно сказать, кто и где придумал технологию блокчейн. Вспышка популярности данной технологии началась в 2008 году, с момента опубликования статьи неизвестным человеком или группой людей под именем Сатоши Накамото.

С того времени прошел довольно большой промежуток времени, однако популярность блокчейна только возрастает.

В данной статье автором объясняется принцип работы блокчейна, почему данная технология не утрачивает свою популярность столь долгое время и рассказывает про применение блокчейна в различных областях деятельности человечества.

Основная часть. Блокчейн представляет собой децентрализованную базу данных, в которой хранится специально организованная информация о всех транзакциях и которая используется одновременно несколькими нодами компьютерной сети. Блокчейн отличается от обычной базы данных способом хранения информации, которая обеспечивает максимальную точность и безопасность операций [1].

Принцип работы данной технологии не так и сложен для понимая. Можно рассмотреть на примитивном примере. Допустим, есть журнал учетов всех денежных переводов, которые происходят в нашей организации. Однажды к нам проникает человек из организации конкурента, и изменяет одну строчку в журнале так, чтобы деньги данной операции присваивались ему. Штаб замечает что-то неладное и программистам дается задача: защитить журнал. Программисты решают каждой строчке присвоить свое хеш-значение. Хеш-значение – это преобразованный массив входных данных произвольной длины в выходную битовую строку установленной длины с помощью определенного алгоритма. Это значит, что одна и таже запись будет иметь одинаковый хеш, если же запись изменяется, то и хеш соответственно. Однако на следующий день этот человек опять пробирается в организацию и уже в журнале его встречают хеши. Он определяет, каким алгоритмом высчитывались данные хеши и затем меняет запись и хеш соответственно. Штаб опять замечает подделку, и программисты придумывают новый метод защиты записей: теперь хеш для каждой записи будет рассчитываться с учетом всех вышестоящих записей. В следующее проникновение человек из организации конкурента замечает изменение в журнале, и спустя время замечает, что хеши рассчитываются с учетом предыдущих, и для изменения записи в этот раз ему потребовалось изменить не только текущую запись на и все нижестоящие. Потратив больше времени ему все же, удалось справиться и с этой защитой. Тогда программисты добавили новый столбец со случайными значениями nonce, которое будет использоваться для подсчета нового хеша записи. Nonce – это аббревиатура от «числа, используемого только один раз», то есть числа, добав-

ляемого к хешированному или зашифрованному блоку в блокчейне, который при повторном хэшировании соответствует ограничениям уровня сложности. Также было добавлено правило, что необходимо найти такой хеш, чтобы он начинался с 0. Это значит, что для зашифровки записи мы берем саму запись и nonce (например, цифра 1) и рассчитываем хеш для комбинации. Если значение хеша начинается не с нуля, выбирается некоторое новое случайное число nonce, и хеш рассчитывается заново. Не стоит забывать, что данный хеш рассчитывается с учетом предыдущих хешей. Человек из организации конкурента снова пробовал изменить записи в журнале, ему удалось высчитать хеш и подобрать nonce, который удовлетворяет закономерности, однако так надо было подобрать nonce и подсчитать хеши для всех нижестоящих записей – времени ему не хватило. Данный алгоритм можно усложнить, установив условие соответствия хеша, если он начинается с 00. В результате вероятность подделки данных станет приблизительно равна 0.

Данная таблица-журнал и является блокчейном. Таким образом, блокчейн – это принцип хранения информации, в котором записи представляют собой цепочку, так как каждая новая запись зависит от предыдущей (рисунок 1).

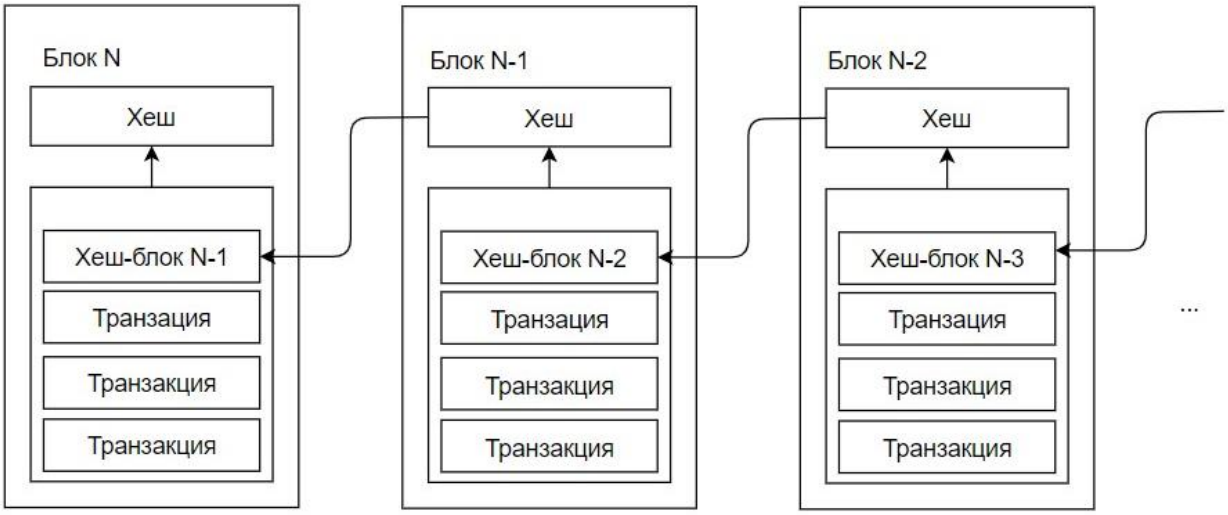

Рисунок 1 – Организация блокчейн

Из всего вышерассмотренного можно вывести основные преимущества:

- прозрачность транзакций за счет открытого доступа блоков;
- сохранность данных за счет хранения в блоках на различных компьютерах;
- безопасность за счет различных методов криптографии;
- независимость за счет децентрализованной организации системы [3].

Однако у данного принципа есть и свои недостатки. Большой расход электроэнергии, поскольку каждый пользователь хранит информацию о всех транзакциях. Если рассмотреть, например биткоин в ноябре 2021, размер его блокчейна превышал 360 ГБ. Еше одной проблемой является атака 51% – когда группировка пользователей, обладающая достаточно большой мощностью компьютеров, может изменить запись в блокчейне, однако согласно исследованиям данный тип атаки не является осуществимым, поскольку данная атака требует одобрение транзакции 51% пользователей, что почти невозможно в настоящих реалиях Также прозрачность транзакций можно отнести как к преимуществу, так и к недостатку, поскольку это означает наличие возможности просмотра истории транзакции пользователя при наличии адреса кошелька владельца. Например, если фальсификатор и есть тот единственный человек, который управляет работой блокчейна, тогда подделать данные будет не так затруднительно. Данный недостаток можно избежать распределить управление системой между большим количеством человек, то есть децентрализовать систему.

Хорошим примером децентрализованного блокчейна является криптовалюта. Данная платежная система получила большую популярность за счет ее организации. Она представляет собой цепочку блоков, в каждый из которых записана информация о осуществленной транзакции. Физически криптовалюта не хранится, она существует в электронных кошельках. Однако «существует» она образно, поскольку для просмотра остатка денег программа просматривает все транзакции осуществления перевода криптовалюты на ваш счет, который представляет собой открытый ключ.

Одной из самых популярных криптовалют является биткоин, которая была создана в 2009 году. Операции осуществления перевода биткоинов на другой счет происходит следующим образом, необходимо сгенерировать новую транзакцию и подписать ее своим закрытым ключом, для подтверждения личности, осуществляющую данную операцию. Затем, перед попаданием в блокчейн, запись попадает в очередь, ожидая, пока ей не подберут подходящий nonce и хеш один из участников блокчейна, за что в результате получит награду в размере небольшого количества виртуальных денег. Это и называется майнинг биткоинов: совместная работа участников для обеспечения транзакций и поддержания сети.

Тем самым множество криптовалют, включая биткоин, функционируют без управления, представленного в лице одного человека или малой группы заинтересованных человек, что обеспечивает безопасность транзакций, а также единственным источником эмиссии являются майнеры, которые получают небольшое вознаграждение, за использование ресурсов их компьютеров. Также стоит учитывать, что эмиссия у различных криптовалют ограничена, что дает возможность понять, сколько виртуальных денег будет создано в конечном счете, из чего следует то, что ни у кого не будет возможности просто напечатать новых виртуальных денег.

Таким образом криптовалюта помогает решить проблему неограниченной эмиссии, помогает защитить наши средства и операции с ними благодаря блокчейну и секретным ключам, а также данная система не может подвергаться контролю, например проверки денег у определенного пользователя или когда и кому были осуществлены транзакции. Неустойчивость курса данной валюты на сегодняшний день обуславливается тем, что в настоящей реальности не так много услуг и товаров можно приобрести за криптовалюту, что в свою очередь приводит к меньшему числу пользователей, а как известно, любая валюта подкрепляется доверием людей к ней. Чем больше услуг и товаров поддерживают расчет в криптовалюте, тем больше участников, спрос и транзакций с данной валютой, что приводит к большей устойчивости курса.

Еще одной глобальной сферой применения блокчейна является удостоверение личности или же идентификационные системы. Сначала рассмотрим какие есть проблемы хранения личной информации в настоящее время, а затем преимущества и недостатки использования блокчейна в данной сфере.

Проблема хранения данных у различных организаций встречается повсеместно: постоянно нам необходимо предоставлять свои данные различным веб-ресурсами для получения возможности пользования каким-либо сервисами, тем самым оставляя цифровой след. Чем больше происходит взаимодействие с интернетом, тем глубже цифровой след, который остается. Вся личная информация, которая храниться в базах данных различных сайтов, может быть украдена или же база данных может быть взломана, что в лучшем случае приведет к рекламе и спаму на почту, например, в худшем случае для других мошеннических манипуляций. Также есть проблема юзер экспириенса, которая говорит о том, что пользователям сети приходится создавать множество аккаунтов в сети и запоминать все логины и пароли, что приводит к использованию одинаковых паролей для различных платформ.

Существует три метода аутентификации личности в сети:

- нечто, что известно только вам (пароль, вопрос, фраза);
- нечто, что есть только у вас (кредитная карта);
- нечто, чем вы является (биометрические данные).

Чем может помочь в данном случае блокчейн? Блокчейн может позволить нам хранить данные в единой блокчейн системе, а не на централизованных серверах третьих сторон. Так-

же личная информация о пользователе не может быть просто изменена или удалена, благодаря организации блокчейн и вся информация надежно зашифрована.

Хорошей идеей использования блокчейна для удостоверения личности является использование электронных карт вместо привычного бумажного паспорта. Данный вид хранения данных о граждане государства избавляет людей от хранения и заполнения большого количества бумаг. Эта система уже выходила в оборот в Эстонии и ОАЭ. Широко используемая платформа e-Residency простыми жителями Эстонии и людьми в бизнес-интересах, представляет собой электронную систему идентификации, позволяющая владельцам специальных карт и цифровых ключей получать доступ к различным услугам. Также есть Follow My Vote, которая предоставляет платформу для анонимных онлайн-голосований, использующую технологию блокчейн и эллиптическую криптографию, чтобы гарантировать точность и достоверность результатов.

Одним из наиболее известной реализацией внедрения блокчейна в данную сферу стала платформа для идентификации беженцев, разработанная совместно компаниями Microsoft и Accenture. Данная платформа решает проблему того, что люди, неумеющие удостоверение личности оказываются абстрагированными от общества и не имеют тех возможностей, которые есть у большинства населения. Она занимается непосредственно идентификацией таких граждан и записывает это все на блокчейн.

Еще одним примером является ProximaX Identity, которая была разработана для Филиппинского государства для идентификации граждан. Принцип работы данной системы заключается в том, что граждане имеют карты, на которых записаны публичный и приватный ключ. И далее, для подтверждения своей личности или для подписи документов гражданин прикладывает карту и систему находит информацию по данному пользователю. При утере карты организовывается новая карта, и генерируются новые ключи данной программой, что означает, нашедший карту не сможет сделать ничего со старой картой. Блокчейн для данной системы обеспечивает децентрализованное хранение данных и логирование всех изменений в программе. Однако недостатками данного решения на сегодняшний день является проблема утери карты, поскольку при утере неизвестно, через какое время удастся перезаписать ключи гражданина и что может успеть за это время нашедший карту.

Следующей сферой применения блокчейна является авторство и право владения. Такие платформы как Blockai, Stampery позволяют людям по всему миру подтверждать и сохранять право авторства с помощью блокчейн. Данные платформы позволяют создавать цифровые издания с помощью идентификаторов и цифровых сертификатов для подтверждения авторства подлинности. Также организована передача права владения от создателя к покупателю или коллекционеру, включая юридические аспекты [2].

Управление данными также возможно пропустить через технологию блокчейн. Factom – одна из наиболее известных блокчейн-компаний, применяющая распределенные реестры для управления данными. Различные компании используют Fatcom для упрощения ведения записей, фиксирования информации о бизнес-процессах. Метки времени и хранение в блокчейне позволяет снизить стоимость и сложность управления ими.

Блокчейн захватил и сферу видеоигр. Примерами являются Etheria, First Blood, Etheramid, CoinPlace, Rolling и другие. Суть игры Etheria заключается в том, чтобы завладеть ячейками игрового поля, добывая их за блоки, и что-нибудь на них построить. Все данные, описывающие мир и его состояние, также и все действия игроков хранятся в распределенном Ethereum-блокчейне [2].

Блокчейн может быть применен не только для повышения прозрачности и целостности политических систем. В частности, существует целая международная виртуальная нация под названием BITNATION. У нее есть свои граждане, послы, партнеры и физические места по всему миру. Присоединиться к ней может каждый желающий без каких-либо ограничений.

Заключение. Несмотря на некоторые недостатки, в настоящее время технологии блокчейн прочно укореняются в нашей повседневной жизни. Блокчейн находит применение не только в переводе цифровых денег, но и во многих сферах деятельности, таких как область кибербезопасности, в банковской сфере, в помощи удостоверения личности и многих других и с годами данная технология имеет потенциал развиваться и совершенствоваться.

Список литературы

1. *Что надо знать о блокчейн в 11 карточках [Электронный ресурс]. – 2020. – Режим доступа: https://trends.rbc.ru/trends/industry/5f05c0a79a7947aac5c7577a – Дата доступа: 25.03.2022.*
2. *20 областей применения Блокчейн вне финансовых сервисов [Электронный ресурс]. – 2017. – Режим доступа: https://habr.com/en/company/wirex/blog/397999/ – Дата доступа: 25.03.2022.*
3. *Преимущества и недостатки блокчейна [Электронный ресурс]. – 2022. – Режим доступа: https://aussiedlerbote.de/2022/01/preimushhestva-i-nedostatki-blokchejna/ – Дата доступа: 25.03.2022.*

UDC 004.043

BLOCKCHAIN AND ITS APPLICATION IN MODERN TECHNOLOGIES

Volnova V.A.,Solovey K.V.

Educational Institution "Belarusian State University of Informatics and Radioelectronics" branch "Minsk Radio Engineering College"
Minsk, Republic of Belarus

Salnikova E.A. – teacher of the first category of disciplines of general professional and special cycles

Annotation. Annotation. Blockchain technology, its principle of operation, advantages and disadvantages have been investigated. It has been established that this technology will be in demand and tends to develop and improve in the future, but is also already being used in various areas of life today. The principle of operation of the blockchain is explained with clear and simple examples, as well as the existing areas of application and the potential for further implemen-tation in this area.

Keywords. blockchain, application, cryptocurrency, bitcoin.