УДК 004.62

Галиуллина Юлия Фанилевна

бакалавр направления «Государственное и муниципальное управление»
Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации
Россия, Челябинск

julia.g2@mail.ru

Никулин Владимир Максимович

бакалавр направления «Государственное и муниципальное управление»
Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации
Россия, Челябинск

ПЕРСПЕКТИВЫ РАЗВИТИЯ ТЕХНОЛОГИИ БЛОКЧЕЙН И «КВАНТОВЫЙ БЛОКЧЕЙН» В СОВРЕМЕННОЙ ЭКОНОМИКЕ[1]

Аннотация

Статья посвящена внедрению технологии блокчейн и квантовый блокчейн во все отрасли экономики, инфраструктуру, систему органов государственной власти, а также в остальные социальные институты с целью мобильности транспортировки информации из одного устройства другому, что позволит сократить существенную долю потраченных ресурсов: время, финансы, человеческий капитал, и т.д. Также блокчейн-технология позволяет надёжно защитить свои личные данные каждого участника системы. Целью исследования является анализ перспектив развития технологий блокчейн и «квантовый блокчейн» в различных элементах экономики. Методологической основой работы является системный подход. Методы научного исследования: метод анализа и синтеза, метод анализа документов, контент-анализ СМИ. В статье рассмотрены преимущества и недостатки применения технологии блокчейн, а также проведен анализ перспектив развития «квантового блокчейна». Сделан вывод о необходимости использования технологии блокчейн и квантовый блокчейн в современной экономике.

Ключевые слова:
блокчейн, биткойн, квантовый блокчейн, суперкомпьютер, эмитент, фиатные деньги

Yulia F. Galiullina

Bachelor of "State and Municipal Management"
Russian Academy of National Economy and Public Administration under the President of the Russian Federation
Russia, Chelyabinsk

julia.g2@mail.ru

Vladimir M. Nikulin

Bachelor of "State and Municipal Management"
Russian Academy of National Economy and Public Administration under the President of the Russian Federation
Russia, Chelyabinsk

PROSPECTS FOR THE DEVELOPMENT OF TECHNOLOGY BLOCKCHAIN AND "QUANTUM BLOCKCHAIN" IN THE MODERN ECONOMY

Abstract

The article is devoted to the implementation of the blockchain and quantum blockchain technologies in all sectors of the economy, infrastructure, government system, as well as in other social institutions for the mobility of transporting information from one device to another, which will reduce a significant proportion of resources spent: time, finance, human capital, etc. Also blockchain - technology allows you to reliably protect your personal data of each participant in the system. The aim of the study is to analyze the prospects for the development of blockchain and "quantum blockchain" technologies in various elements of the economy. The methodological basis of the work is a systematic approach. Research methods: analysis and synthesis method, document analysis method, media content analysis. The article discusses the advantages and disadvantages of using the blockchain technology, as well as an analysis of the prospects for the development of the "quantum blockchain". It is concluded that it is necessary to use the blockchain and quantum blockchain technologies in the modern economy.

Keywords:
blockchain, bitcoin, quantum blockchain, supercomputer, issuer, fiat money

[1] Научный руководитель: Солодовникова М.В., старший преподаватель, Российской академии народного хозяйства и государственной службы при Президенте РФ, Челябинский филиал

Стремительное развитие цифровых технологий, как в мире, так и в России послужило появлению новых инструментов реализации экономической политики. Переход в эру цифровых технологий ознаменовался появлением программы цифровой экономики, которая должна охватывать все сферы жизнедеятельности человека. Но с появлением новых инструментов экономической политики возрастает и потребность в защите этих данных.

Механизм защиты информации может быть реализован с помощью новейшей технологии блокчейн (block chain). Блокчейн – это распределенная, непрерывная цепочка блоков, которые содержат данные о проведенных участниками транзакциях. Как правило, данные цепочки блоков хранятся на нескольких разных компьютерах независимо друг от друга, что говорит о распределенности данной системы. При этом доступ к данным в этих блоках есть у всех участников данной системы.

Дон и Алекс Тэпскотт, авторы книги «Революция блокчейна дали свое определение блокчейна. Так, они считают, что блокчейн – это вечный, цифровой распределенный журнал экономических транзакций, который может быть запрограммирован для записи не только финансовых операций, но и практически всего, что имеет ценность [7].

Блокчейн значительно снижает вероятность внесения изменений в данную систему, путем введения несанкционированных блоков и хакерских атак. Так, каждый новый блок в данной системе, взаимосвязан с предыдущим, и в его названии существуют ссылки на прошлый блок. Процесс хеширования в данной системе также не может быть изменен и в случае смены данных в документах происходит трансформация в цифровых подписях.

Таким образом, блокчейн – технология позволяет передавать данные быстрее, безопаснее и дешевле, так как исключает участие посредников, действует автоматизировано и практически исчезает вероятность человеческой ошибки.

Впервые термин блокчейн появился под названием полностью синхронизированной распределенной базы данных, которая была реализована в системе криптовалют «Биткойн» в 2009 году. В данном случае, она исполняет роль единого реестра всех операций с валютой.

Биткойн – это децентрализованная платежная система, использующая одноименную единицу учета операций. Чтобы обеспечить защиту данной системы, используют криптографические методы шифрования, но при этом все данные

транзакций участников системы доступны в открытом доступе. Биткойн действует без какого–либо контролирующего органа или центрального банка, а обработка транзакций и эмиссия осуществляется коллективно участниками сети. Также биткойн имеет открытый исходный код и его система известна каждому, но при этом никто не контролирует его.

Биткойн имеет уникальные свойства и открывает для своих участников новые и уникальные возможности, которые до этого не могла сделать ни одна платежная система. Но отличительным минусом биткойна можно считать то, что он до сих пор не закреплен законодательно и из-за этого существуют проблемы в его использовании. Поэтому, при всем многообразии преимуществ, многие фирмы и люди не решаются использовать биткойн повсеместно.

Появление криптовалюты с внедрением блокчейн – технологии произвело фурор на финансовом рынке. Так, данную тематику начало рассматривать все большее количество людей. Основными авторами книг про криптовалюту стали Натаниел Поппер – «Цифровое золото», Мелани Свон – «Блокчейн. Схема новой экономики», Руслан Акст – «Маркетинговые фокусы криптовалют», Дон Тапскотт и Алекс Тапскотт – «Технология блокчейн» и компания Prypto – «Биткойн для чайников».

Биткойн был первым применением блокчейн – технологии и в настоящее время блокчейн – технология имеет перспективные шансы на внедрение в повседневную жизнь. Так, данная технология может применяться в экономике, государственном управлении, банковском и финансовом секторе и т.д. Примером может служить, лондонский филиал Deutsche Bank Innovation Lab. Он разрабатывает систему инвестиций на основе технологии блокчейн, которая значительно упрощает, ускоряет и снижает стоимость инвестирования за счет исключения или полного сокращения роли посредников в данных операциях

Блокчейн – технологии имеют как преимущества, так и недостатки. Можно привести несколько примеров преимуществ и недостатков блокчейна.

Первым преимуществом является защищенность данных от хакерских атак, мошенничества и кражи персональных данных благодаря распределенности данных по блокам и криптографической защите по произведенным транзакциям. Данные механизмы делают финансовую систему более защищенной. А сама же подлинность транзакций проверяется непосредственно самими участниками системы.

Вторым преимуществом, является проведение операций без посредников, брокеров и т.д. Вместо обращения к третьим лицам по вопросам инвестирования или проведения транзакций, в системе присутствует специальный протокол консенсуса для согласования содержимого реестра, а также криптографические алгоритмы хеширования и электронно–цифровые подписи для обеспечения целостности транзакций и передачи ее параметров. За счет этого повышается скорость проведения транзакций и частота обмена информации [4].

Третьим преимуществом можно считать применение технологии блокчейн в разработке платежных систем с использованием цифровых валют, подкрепленных фиатными деньгами. Фиатные или фидуциарные деньги – это деньги, которые не обеспеченны ни золотом, ни другими драгоценными металлами, номинальная стоимость которых устанавливается и гарантируется государством вне зависимости от того сколько вышло затрат для их изготовления. Сеньораж при эмиссии таких денег в таком случае почти равен их номиналу. Блокчейн – технология в таком случае позволяет значительно упростить взаимодействие главных банков стран и обеспечивает мгновенное проведение трансграничных платежей при партнерстве с коммерческими банками.

Вышеперечисленные преимущества являются не единственными, но основными преимуществами данной технологии, позволяющими значительно упростить и обезопасить транзакции между участниками системы.

Недостатки технологии блокчейн:

Первым и главным недостатком является деятельность блокчейн – технологии вне правового поля. Так, в нашей стране до сих пор нет нормативно–правовой базы регулирующей технологию блокчейн и криптовалюту. Такая проблема существует не только в России, но и в других странах. Например, Центральный Банк Англии так и не разрешил использовать блокчейн, но неформально попросил банки о содействии в реализации блокчейн – проектов [10].

Вторым недостатком является потребность в больших вычислительных мощностях и в связи с этим получаются большие затраты на электроэнергию. По данным ученых, уже к 2020 году для поддержки биткойна потребуется такое количество энергии, которое потребляет в день небольшая страна. На данный момент эта проблема еще не решена, но ученые активно работают над ней.

И третьим недостатком является высокая стоимость внедрения данной технологий и достаточно малое количество специалистов разбирающихся в блокчейне. Для решения этой проблемы в 2017 году на базе НИЯУ МИФИ открыли «Центр развития блокчейн технологии MEPHIUS» центра будет создана своя блокчейн – платформа MEPHIUS, позволяющая разрабатывать на ее основе бизнес – предложения для реального сектора экономики и выпускать криптографические активы. Часть штаба разработчиков будет состоять из студентов старших курсов, магистрантов и аспирантов, которые получили знания в различных областях IT – технологий.

Перспективы развития квантового блокчейна в современной экономике

Квантовый блокчейн – это система распределённого хранения данных, реализованная с помощью квантового распределения ключа.

Квантовое распределение ключей – это метод транспортировки ключа, который использует квантовые явления для гарантии безопасности связи. Данный метод позволяет двум сторонам, соединенным по открытому потоку связи, создать общий случайный ключ, который известен только им, и использовать его для шифрования и расшифрования сообщений.

Данная технология квантового блокчейна была разработана группой Е.О. Киктенко. Для её создания была использована стандартная система квантовой криптографии швейцарской компании ID Quantique. В ее основе лежит упоминавшаяся выше схема, в которой каждая пара узлов соединяется с помощью линии распределения квантового ключа. Фактически всё дело сводится к квантовой подписи, которая привязана к каждой транзакции, и передаваемой в виде квантовых частиц (фотонов). По законам физики, данные сигналы невозможно скопировать подслушивающими устройствами. В результате этого воздействия они разрушаются.

Квантовые угрозы блокчейну

Возникновение, такого явления как «Квантовая опасность» связано с появлением информации о том, что квантовый компьютер способен оказать воздействие «грубой силой» на блокчейн. Эта атака заключается в том, что изменение в теле транзакции не будет отражено в изменении хэша.

Однако, основная функция такой электронно-вычислительной машины как квантовый компьютер, способен производить одновременные расчёты в

параллельных вселенных, с целью вычислить все возможные значения переменной, а потом выбрать необходимое.

Ещё одной актуальной проблемой может быть вычисление закрытого ключа по открытому, общедоступному ключу. Эти угрозы можно отнести к внешним воздействиям среды. Однако есть вероятность и внутренних опасностей.

Если теоретически смоделировать ситуацию, квантовый компьютер станет майнить в блокчейне. В этом случае очень актуально станет проблема 51% мощности. Майнер, использующий квантовый компьютер, монополизирует запись блоков, сможет по своему желанию управлять цепочкой, поддерживать ту или иную ветвь.

Какие же есть способы защиты квантовой блокчейн-технологии? Появление рабочих версий квантовых компьютеров в корне изменит мир. Это существенно затронет криптографию в том состоянии, в котором она действует сейчас. Поэтому параллельно с разработкой квантовых технологий идёт интенсивное развитие систем криптографической защиты информации. Также это касается непосредственно и самого блокчейна.

В настоящее время можно наблюдать поэтапное совершенствование криптографической защиты блочной цепи и транзакций:

Усложнение алгоритмов шифрования, использование их комбинаций:

- использование других альтернативных математических зависимостей между открытым и закрытыми ключами;

- разработка практических реализаций уже известных теоретических криптографических алгоритмов;

- создание квантового блокчейна;

- использование квантовых компьютеров для криптографической защиты информации;

- усложнение алгоритмов шифрования.

Ярким примером из первого пункта можно считать компанию QBit. Данная фирма предлагает использовать алгоритм шифрования X11 вместо SHA-256 (алгоритм шифрования X11и SHA-256 – это безопасный алгоритм хеширования, семейство криптографических алгоритмов – однонаправленных хэш-функций), на котором работает Биткоин. Новый алгоритм использует 11 функций хэширования и позволяет значительно быстрее вычислять хэши. Разработчики заявляют о снижении энергозатрат и значительно более высокий скорости обработки транзакций.

Реализацией второго пункта на данный момент может быть проект The Quantum Resistan Ledger (QRL). Данная компания предлагает использовать для усложнения определения взаимосвязи между открытым и закрытыми ключами алгоритм XMSS (eXtended Mergele Signature Scheme).

Схема использует одноразовые закрытые ключи, которые генерируются каждый раз, когда нужно подписать сообщение. Принцип «Одно сообщение – один ключ» на данный момент значительно усиливает безопасность подписи транзакций.

На данный момент чётко не определён алгоритм для квантового компьютера, позволяющий подобно алгоритму Шора, вскрывать закрытые ключи, сгенерированные с помощью ECDSA (SHA-256) для Биткоина. Однако, если появилась методика Шора, то затруднительно с уверенностью говорить о невозможности появления другого алгоритма для квантового компьютера.

Разработка новых алгоритмов шифрования

Наиболее привлекательно перспективным для защиты от квантового компьютера сейчас выглядят алгоритмы, основанные на многомерных решётках. Нужно знать секретный маршрут движения по узлам многомерной пространственной сетки, с возможностью прочитать зашифрованную информацию. Не имеет существенного значения, какой тип информации: закрытый ключ, транзакция или текст.

В недавнем времени было заявлено, о возможности уязвимости данных алгоритмов, однако, впоследствии выяснилось, что это касается упрощённых схем, созданных для более быстрого процесса шифрования.

Использование квантовых компьютеров для криптографической защиты информации.

Появление в сети квантового компьютера, генерирующего закрытые ключи или какие-то ещё криптографические структуры, разрушает основную целостность блочной цепи. Чтобы миссия блокчейна была сохранена, актуальна и на высоком уровне востребована, должна быть сформирована сеть квантовых компьютеров, соединенных с помощью квантового интернета.

Физики из Российского квантового центра сформировали и проверили на практической задаче первый в мире «Квантовый блокчейн» - невзламывемую систему распределенного хранения определённых данных, защищённую при помощи методов квантовой криптографии.

Как поясняют учёные, данный вид блокчейна был протестирован на недавнем времени созданной трёхузловой квантовой сети между отделениями «Газпромбанка» в Москве. Все попытки «злоумышленника», роль которого играл один из участников сети, внесли ложные транзакции в базу данных – провалились, что подтвердило работоспособность блокчейна.

«По прогнозам экспертов на основе блокчейна к середине 2020-х годов будет создаваться порядка 62 триллионов долларов услуг. При этом эффект от нашей разработки может многократно увеличить объём рынка. Не маловажным считается, что эта технология создана и впервые обработана в России в реальных жизненных условиях», – заключают Фёдоров и его коллеги.

Таким образом, исходя из данных по актуальной инновационной теме, можно сделать вывод, что квантовая блокчейн технология имеет широкий потенциал в будущем начиная с экономических процессов в банковской системе постепенно трансформируя своё влияние в экономику в целом как систему.

Список использованных источников

1. Пряников М.М., Чугунов А.В. // Блокчейн как коммуникационная основа формирования экономики: преимущества и проблемы // International Journal of open Information Tehnologies. 2017. vol.5, no.6.
2. Апатова Н.В., Королев О.Л., Круликовский А.П. // Анализ блокчейн – технологии на финансовую систему // Научно – технические ведомости СПбГПУ // Экономические науки. 2017.Т.10. №6. С.31-39.
3. Ковальчук А.В., Сайбель Н.Ю. // Блокчейн – технологии в финансовом секторе экономики: преимущества и проблемы использования // Научно-методический электронный журнал «Концепт». 2018. №4.
4. Аксенов Д.А., Куприков А.П., Саакян П.А. // Направления и особенности применения блокчейн – технологии в экономике // Научно – технические ведомости СПбГПУ // Экономические науки. 2018. Т.11. №1. С.30-38.
5. Енгисаев М.А., Малёва У.И., Солодовникова М.В. Криптовалюта: экономическая перспектива или угроза экономической безопасности? // Вестник Московского университета// государственный аудит 2018. №3. С.198-209.
6. Бабкин А.В.Буркальцева Д.Д.,Пшеничников В.В., Тюлин А.С., Криптовалюта и блокчейн – технология в цифровой экономике: генезис развития //

Научно – технические ведомости СПбГПУ // Экономические науки. 2017.Т.10. №5. С.9-22.

7. Заколдаев Д.А., Ямщиков Р.В., Ямщикова Н.В., Технология блокчейн в России: достижения и проблемы // Вестник Московского государственного областного университета (Электронный журнал) №2. 2018.

8. Электронный ресурс: https://bitcoin.org/ru/ (Дата обращения 15.11.2018)

9. Электронный ресурс: https://forklog.com/sostoyalsya-zapusk-marketplejsa-blokchejn-instrumentov-ot-kaleido-pri-podderzhke-amazon-web-services/ (Дата обращения 15.11.2018)

10. Электронный ресурс: https://rb.ru/opinion/crypto-law/ (Дата обращения 15.11.2018)

11. Электронный ресурс: https://bits.media/gruppa-kompaniy-m9-sovmestno-s-mifi-otkroyut-tsentr-razvitiya-blokcheyn-tekhnologiy-mephius/ (Дата обращения 15.11.2018)