

Blockchain, как новая технология для разработки

Д.А.Кирилова, Н.С.Маслов, А.Д.Рейн

Аннотация – В настоящее время происходит повсеместная цифровизация, в связи с этим, всё более популярной становится технология Blockchain. Данная технология, представляет интерес для многих отраслей в Европе и за ее пределами. Являясь относительно новым направлением в информатике, блокчейн становится глобальной, межотраслевой технологией, которая, как прогнозируется, поспособствует росту мировой экономики в течение следующих нескольких десятилетий.

С начала 1990-х годов проводились эксперименты с технологией блокчейн, но широкое распространение он получили только в 2008 году, после выпуска «Белой книги» отдельным лицом или группой лиц, работающих под псевдонимом Сатоши Накамото. Первой известной разработанной технологией блокчейн, стал протокол Биткойн, который также является именем первой широко используемой, децентрализованной криптовалютой. Термин блокчейн становится все более популярным среди населения и автоматически ассоциируется с «цепочкой блоков» и платформой биткоин.

Blockchain быстро становится общественно доступным, и все же технология остается трудной для понимания многими людьми.

В работе дано определение технологии Blockchain, с точки зрения авторов. Разобраны главные принципы работы технологии, представлена структура реестра. Описаны типы записей, которые блокчейн использует для хранения, такие как: транзакции, умные контракты, цифровые подписи и сертификаты.

Ключевые слова— цифровизация, блокчейн, реестр, транзакции, умный контракт, криптовалюта.

I. ВВЕДЕНИЕ

Технология Blockchain является растущей областью, представляющей интерес для многих отраслей в Европе и за ее пределами. Будучи относительно недавним нововведением в информатике, блокчейн является глобальной, межотраслевой технологией, которая, как прогнозируется, поспособствует росту мировой экономики в течение следующих нескольких десятилетий.

Уже сегодня, блокчейн дает возможность всему человечеству оптимизировать самые различные сферы жизни. Одним из преимуществ этой технологии является то,

что её практически невозможно взломать и нет необходимости в привлечении третьих лиц [1].

Blockchain быстро становится общественно доступным, и все же технология остается трудной для понимания многими людьми. Поэтому необходимо сформулировать определение блокчейн:

Блокчейн – это распределенная книга, которая дает способ записывать информацию и делиться ей в сообществе. В этом сообществе каждый член поддерживает свою собственную копию информации, и все участники должны проверять все обновления в совокупности. Информация может представлять собой транзакции, контракты, активы, удостоверения личности или практически все, что можно описать в цифровой форме. Записи являются постоянными, прозрачными и доступными для поиска, что позволяет просмотреть истории транзакций в полном объеме.

Каждое обновление представляет собой новый «блок», добавленный в конец «цепочки». Протокол управляет тем, как иницируются, проверяются, записываются новые записи и распределяет их. В blockchain, криптология заменяет сторонних посредников в качестве доверительной стороны, при этом все участники блокчейна, выполняющие сложные алгоритмы, удостоверяют единство в целом.

С начала 1990-х годов проводились эксперименты с технологией блокчейн, но широкое распространение он получили только в 2008 году, после выпуска «Белой книги» отдельным лицом или группой лиц, работающих под псевдонимом Сатоши Накамото. Первой известной разработанной технологией блокчейн, стал протокол Биткойн, который также является именем первой широко используемой, децентрализованной криптовалютой. «Биткойн» также относится к сетевому протоколу, лежащему в основе криптовалюты. Термин блокчейн становится все более популярным среди населения и автоматически ассоциируется с «цепочкой блоков» и платформой биткоин, однако существуют и другие блокчейн платформы, например, Ethereum.

II. РЕЕСТР

В основе технологии блокчейн, лежит реестр. Реестр – это инструмент, с помощью которого можно определить владельца актива на любом момент времени. Он выполняет эту функцию, выступая в качестве центрального достоверного списка передачи данного актива.

В системе или обществе, которое согласилось использовать блокчейн, реестр отвечает за то, чтобы определить право собственности на конкретный актив, все, что требуется для передачи права собственности между

Статья получена 8 октября 2018

Кирилова Дарья Александровна, Нижегородский государственный инженерно-экономический университет (e-mail: dasha.kirilova.96@bk.ru).

Маслов Никита Сергеевич, Нижегородский государственный инженерно-экономический университет (e-mail: j-knaginino@yandex.ru).

Рейн Андрей Давыдович, Нижегородский государственный инженерно-экономический университет (e-mail: ndr18@yandex.ru).

двумя сторонами, – это сделать запись в реестре, указав, что произошла транзакция.

С технической точки зрения, реестр представляет собой просто список последовательностей, с отметкой времени транзакции, структурированный следующим образом (рисунок 1).

Транзакция №	Дата и время	Отправитель	Активы	Получатель
#	ДД-ММ-ГГ ЧЧ:ММ	Человек 1	Описание передаваемого актива, например, денежная единица, акт передачи имущества или сертификат	Человек 1
#	ДД-ММ-ГГ ЧЧ:ММ	Человек 2	Описание передаваемого актива, например, денежная единица, акт передачи имущества или сертификат.	Человек 2

Рис. 1 Структура реестра

Эта простая концепция сохранения достоверного списка передач актива/активов, которая позволяет систематизировать передачу и накопления капитала.

Лицо или организация, которые физически владеют или контролируют публичную регистрацию (включая сервер, на котором находится реестр, в случае онлайн-публичного реестра) находится в положении значительного влияния. В частности, владелец реестра может:

- решить, следует ли записывать транзакцию, которая, в свою очередь, предоставляет этому лицу возможность накладывать ограничения для регистрации физических лиц и принимать решение о системе контроля, которая будет применяться для проверки точности этих сделок;

- полностью уничтожить реестр или разрешить его уничтожение.

В такой системе запись, изменение или удаление транзакции в реестре изменяет право собственности на объект, определенного лица или организации, которые контролируют такие реестры. Кроме этого, эти действия оказывают значительное влияние, эффективно контролируя тех, кто является хранителем списка транзакций.

Ответственность за сохранение реестров традиционно была отнесена к разнообразным учреждениям:

- правительства контролируют владение землей, контролируя реестр;
- банки контролируют денежную систему мира, держа реестр за валюту;
- фондовые биржи контролируют крупные акции делового мира путем ведения реестра.

Поскольку капиталистические общества строятся вокруг концепций продажи и владения (передачи и накопления капитала), есть большая ответственность, связанная с хранением реестра. В частности, этим центральным органам доверяют:

- предоставлять свидетельские показания, то есть удостоверить личность и обеспечивать, чтобы зарегистри-

рованные лица в реестре являлись теми, кем они назвались, и что переданные активы существуют;

- обеспечение прозрачности всех транзакций, то есть не лишать пользователей своих активов путем создания поддельных транзакций или незаконного изменения транзакций после того, как они были созданы;

- безопасность, то есть гарантию того, что несанкционированные третьи стороны не смогут читать или писать в реестре;

- лицам совершать сделки, то есть предоставлять доступ всем, у кого есть законный интерес к совершению операции, перечисляя их в реестре.

В результате, что эти учреждения могут индивидуально или коллективно нанести вред или даже создать социальный хаос, злоупотребляя доверием, оказанным им, чтобы поддерживать эти реестры. Вывод состоит в том, что эти учреждения имеют право использовать или злоупотреблять своим контролем над реестром и осуществлять значительный контроль над отдельными лицами и организациями в рамках их непосредственной компетенции.

III. БЛОКЧЕЙН КАК ПУБЛИЧНЫЙ РЕЕСТР

Наиболее широко известное применение блокчейна это публичный реестр транзакций для криптовалюты, таких как биткойн и эфириум. Как и в случае с другими государственными реестрами, blockchain предоставляет отчет о происхождении и передаче права собственности на актив. Транзакционная структура протоколов блокчейна облегчает не только передачу криптовалюты, но и других цифровых активов. Актив может быть осязаемым, например, дом, автомобиль, деньги, земля или нематериальные активы, такие как патенты, авторские права или брендинг. Поскольку блокчейн предназначен для записи и хранения транзакций, все блоки традиционно имеют цифровую валюту какого-либо вида, связанного с ними, как самого основного актива.

Блокчейн - это, следовательно, реестры, записывающие группы транзакций, иначе известные как блоки, которые связаны криптографически в линейной временной последовательности. Другие ключевые свойства, блокчейна – безопасность, неизменность, программируемость зависят от архитектуры цепочки блоков и харак-

тера консенсусного протокола, который управляется этим блокчейном. Некоторые блоксхемы структурированы для облегчения одноранговых транзакции через неиерархические узлы – это называется «распределенной» сетью. Некоторые блоксхемы, такие как блокчейн-биткойн, также обеспечивают неизменность их реестров через их уникальный консенсусный протокол. Чтобы определить, кто владеет определенным активом, сторона должна просто проконсультироваться с регистратором, чтобы проверить кто является его последним владельцем.

IV. ПРИНЦИП ПРОЗРАЧНОСТИ

Простота обмена и прозрачность являются важными особенностями блокчейна, отсутствие одной или другой функций в современных системах часто являются центральным драйвером принятия технологии блокчейн. Они становятся особенно важными в транзакциях, в которых многие организации делают записи блок-цепи.

Blockchain дает участникам возможность получить информацию о происхождении каждого актива или записи, и как его собственность изменилась с течением времени. Однако эта прозрачность работает, только если транзакции цепочки связаны с идентификатором. Без общедоступного идентификатора, такого как связанный документ или серийный номер, транзакции цепочки отслеживаются и могут быть декодированы. Таким образом, блокчейн - даже «публичный» блокчейн - являются закрытыми по умолчанию, но также может использоваться для отслеживания транзакций отдельных лиц с течением времени через связанные данные «закрытые цепи».

Технология Blockchain предоставляет неоспоримый механизм для проверки того, что данная транзакция существовала в определенное время. Каждый блок в цепочке содержит информацию о предыдущем блоке: историю, должность, более того каждый блок ещё и автоматически аутентифицируется и не может быть изменен. Один общий реестр предоставляет место для определения права собственности на актив или завершения транзакции.

V. ТИПЫ ЗАПИСЕЙ, ХРАНЯЩИХСЯ В БЛОКЧЕЙН

Блокчейн обычно используют для хранения:

1. Транзакций, записи которых обычно имеют две формы:

- деньги, выраженные в единицах валюты: каждая единица одной валюты имеет одинаковое значение, как и каждый другой отдельный блок в любой момент времени. Кроме этого, валюты внутриконвертируемые по обменному курсу. Наиболее распространенная форма валюты, использованная в технологии blockchain - биткойн.

- документальные доказательства прав собственности, юридически известные как документы о праве собственности. Это обычно используемые представления недвижимого имущества, такие как земля или неосвоенные, такие как права интеллектуальной собственности.

2. Умных контрактов. Умные-контракты – это фактически небольшие компьютерные программы (программный код), хранящиеся в блокчейне, которые будут выполнять транзакцию в определенных условиях. То есть, умный контракт – обычно декларация, такая как «перевод X в Y, если происходит Z».

Преимущества, представленные умными контрактами, заключаются в том, что важные цифровые записи подлежат проверке на каждом узле блокчейна, поэтому начинает развиваться совершенно новая система технической автоматизации, происходит создание новой социальной структуры, которая позволила бы повысить гражданскую эффективность, личную мобильность и институциональную трансформацию. Поэтому в этом контексте умные контракты представляют собой автоматизированный взгляд на будущее.

3. Цифровых подписей и сертификатов.

В своей наиболее важной форме сертификация – это вопрос утверждения одной стороной того, что определённый набор факторов другой стороны верен.

Также, блокчейн может использоваться для хранения криптографических хэшей «цифровых отпечатков пальцев» или сертификатов. Таким образом, блокчейн может выполнять функции открытого реестра сертификатов.

VI. ЗАКЛЮЧЕНИЕ

Полные преимущества технологии blockchain достигаются только благодаря прозрачности транзакций. Под этим мы подразумеваем решения, основными компонентами которых являются:

- а) право собственности на получателя;
- б) независимость поставщика;
- с) децентрализованная проверка.

Если это все не достигнуто, использование блокчейна, вероятно, будет пустой тратой усилий и ресурсов для всех заинтересованных сторон.

Технология Blockchain имеет потенциал для завершения бумажного документооборота. За счет того, что блокчейн предоставляет организациям возможность выпускать неизменяемые цифровые сертификаты, которые действительно неограниченный срок, поскольку их подлинность может быть проверена в блокчейне. Эти преимущества по сравнению с существующими системами значительно увеличивают стоимость цифровых сертификатов и, скорее всего, будут внедрять цифровую сертификацию в основное русло.

БИБЛИОГРАФИЯ

- [1] Kirilova D., Maslov N., Astakhova T. Prospects for the introduction of blockchain technology into a modern system of education // International Journal of Open Information Technologies, 2018. Т. 6. №. 8.
- [2] Грошева Е. К., Невмержицкий П. И., Блокчейн - новая революция // Бизнес-образование в экономике знаний, 2018. №1. URL: <https://cyberleninka.ru/article/n/blokcheyn-novaya-revolutsiya> (дата обращения: 28.09.2018).
- [3] Шевченко К.В., Корсукова Н.Д. Блокчейн, как новый этап в развитии цифровой экономики // Актуальные проблемы авиации и космонавтики, 2017. №13. URL: <https://cyberleninka.ru/article/n/blokcheyn-kak-novyuy-etap-v-razvitiit-sifrovoy-ekonomiki>.
- [4] Власов А. И., Карпунин А. А., Новиков И. П. Системный анализ технологии обмена и хранения данных blockchain // Современ-

ные технологии. Системный анализ. Моделирование, 2017. №3 (55). URL: <https://cyberleninka.ru/article/n/sistemnyy-analiz-tehnologii-obmena-i-hraneniya-dannyh-blockchain> (дата обращения: 01.10.2018).

- [5] Handbook of blockchain, digital finance, and inclusion / David Lee Kuo Chuen, Robert H. Deng Amsterdam: Academic Press, 2017. 197 p.
- [6] Мезенцева Е. М., Шубин А. А. Технология блокчейн // Экономика и социум, 2017. №12(43). С. 712–714.
- [7] Савенков Д. М., Мезенцева Е. М. Как изменит нашу жизнь блокчейн // Экономика и социум, 2017. №12(43). С. 1969–1970.

Кирилова Дарья Александровна родилась в Княгинино, Россия, в 1996 году. В 2017 году закончила бакалавриат в Нижегородском государственном инженерно-экономическом университете и поступила в магистратуру. С 2018 года является сотрудником кафедры «Информационные системы и технологии» Нижегородского государственного инженерно-экономического университета, Княгинино, Россия. Текущие научные интересы включают: цифровую экономику, технологию блокчейн, разработка и применение программных продуктов.



Маслов Никита Сергеевич родился в Княгинино, Россия, в 1992 году. В 2015 году окончил специалитет в Нижегородский государственном педагогическом университете имени Козьмы Минина. С 2015 года является сотрудником кафедры «Информационные системы и технологии» Нижегородского государственного инженерно-экономического университета, Княгинино, Россия. Текущие научные интересы включают: цифровую экономику, развитие телекоммуникационных услуг, разработка и применение программных продуктов.



Рейн Андрей Давыдович родился в России, г. Княгинино, Нижегородской области в 1991 году. В 2013 году окончил специалитет в Нижегородском государственном инженерно-экономическом институте. С 2012 года является сотрудником кафедры «Информационные системы и технологии» Нижегородского государственного инженерно-экономического университета, Княгинино, Россия. Текущие научные интересы включают: цифровая экономика, анализ больших данных, разработка и внедрение программных продуктов.



Blockchain as a new technology for development

D.Kirilova, N.Maslov, A. Reyn

Abstract - currently, there is a local digitalization, in this regard, the Blockchain technology is becoming more popular. This technology is of interest to many industries in Europe and beyond. As nongym innovation in Informatics, the blockchain becomes a global, cross-sectoral technology, which Proglaziruetsya, promotes the growth of the world economy over the next several decades.

Since the early 1990s, experiments with blockchain technology have been carried out, but it became widespread only in 2008, after the release of the White Book, to be picked up by the pseudonym Satoshi Nakamoto. The first known blockchain technology developed was the Bitcoin protocol, which is also the name of the first widely used, decentralized cryptocurrency. The term blockchain is becoming more popular among the population and is automatically associated with the "block chain" and bitcoin platform.

Blockchain is fast becoming publicly available, and yet the technology remains difficult for many people to understand.

The paper defines Blockchain technology from the author's point of view. The main principles of the technology are analyzed, the structure of the register is presented. It describes the types of records that the blockchain uses for storage, such as transactions, smart contracts, digital signatures and certificates.

Keywords— digitization, blockchain, roster, transactions, smart contracts, cryptocurrencies.

REFERENCES

- [1] Kirilova D., Maslov N., Astakhova T. Prospects for the introduction of blockchain technology into a modern system of education // International Journal of Open Information Technologies, 2018. T. 6. #. 8.
- [2] Grosheva E. K., Nevmerzchickij P. I., Blokchejn - nova-ja revoljucija // Biznes-obrazovanie v jekonomike znaniy, 2018. #1. URL: <https://cyberleninka.ru/article/n/blokcheyn-novaya-revoljutsiya> (data obrashhenija: 28.09.2018).
- [3] Shevchenko K.V., Korsukova N.D. Blokchejn, kak novyj jetap v razvitii cifrovoj jekonomiki // Aktual'nye problemy aviacii i kosmonavtiki, 2017. #13. URL: <https://cyberleninka.ru/article/n/blokcheyn-kak-novyy-etap-v-razvitii-tsifrovoy-ekonomiki>.
- [4] Vlasov A. I., Karpunin A. A., Novikov I. P. Sistemnyj analiz tehnologii obmena i hranenija dannyh blockchain // Sovremennye tehnologii. Sistemnyj analiz. Modelirovanie, 2017. #3 (55). URL: <https://cyberleninka.ru/article/n/sistemnyj-analiz-tehnologii-obmena-i-hraneniya-dannyh-blockchain> (data obrashhenija: 01.10.2018).
- [5] Handbook of blockchain, digital finance, and inclusion / David Lee Kuo Chuen, Robert H. Deng Amsterdam: Academic Press, 2017. 197 r.
- [6] Mezenceva E. M., Shubin A. A. Tehnologija blokchejn // Jekonomika i socium, 2017. #12(43). S. 712–714.
- [7] Savenkov D. M., Mezenceva E. M. Kak izmenit nashu zhizn' blokchejn // Jekonomika i socium, 2017. #12(43). S. 1969–1970.