УДК 004.7

ТЕХНОЛОГИЯ BLOCKCHAIN ИЗНУТРИ: НОВАЯ ТЕХНОЛОГИЧЕСКАЯ РЕВОЛЮЦИЯ

Зоткина А.А., Маркин Е.И., Бершадская Е.Г.
Пензенский государственный технологический университет, Пенза, e-mail: Alexey314@yandex.ru

Технология блокчейн (blockchain) появилась недавно, но уже набрала популярность и обладает потенциально большой значимостью для проведения различных операций благодаря своей защищенности и надежности. В статье рассматриваются перспективы развития технологии блокчейн путем исследования данной технологии в современном мире. Анализируются преимущества и недостатки блокчейна, как универсального инструмента для построения различных баз данных. В статье дан краткий обзор технологии, принципов ее работы и возможное применение в различных сферах жизни человеческой деятельности. Особое внимание уделяется технологической модели рассматриваемой распределенной системы хранения данных. Данная технология может применяться в различных сферах, в том числе в качестве основы для социальных сетей, при создании и управлении крупных баз данных, в логистике, медицине, страховании и многих других областях, где требуется надежный способ обработки и хранения массивных объемов информации. Показана перспективность, которая ее состоит еще и в том, что любые инициативы могут быть начаты небольшой группой или даже одним участником для своих клиентов, а потом без особого труда распространены на весь рынок.

Ключевые слова: Blockchain, Bitcoin, блок, майнинг, майнер, хэш – функция, P2P

TECHNOLOGY BLOCKCHAIN FROM INSIDE: NEW TECHNOLOGICAL REVOLUTION

Zotkina A.A., Markin E.I., Bershadskaya E.G.
Penza State Technological University, Penza, e-mail: Alexey314@yandex.ru

The blockchain technology appeared not so long ago but it has already become very popular and potentially significant for carrying out various operations because of its reliability and security. The article presents the prospects for the development of technology. The advantages and disadvantages of blockchain as a universal tool for building various databases are analyzed. The article gives a brief overview of the technology, its principles and possible application in various spheres of human activity. Special attention is paid to the technological model of the considered distributed data storage system. This technology can be used in various fields, including as a basis for social networks, in the creation and management of large databases, in logistics, medicine, insurance and many other areas where you need a reliable way to process and store massive amounts of information. It shows the prospects, which it consists also in the fact that any initiatives can be started by a small group or even one participant for their customers, and then easily distributed to the entire market.

Keywords: Blockchain, Bitcoin, block, mining, miner, hash function, P2P

Не секрет, что индустрия информационных технологий в современное время развивается очень стремительно, и новые технологии появляются настолько быстро, что специалисты зачастую не успевают среагировать на их появление. Так произошло и с Blockchain – разработанной в рамках криптовалюты Bitcoin, впервые выпущенной еще в 2009-м году Сатоши Накамото, она долгое время оставалась незамеченной, однако в последнее время нарекшей себя на популярность.

Технологию Blockchain пытаются применить в различных областях. Мир без банков, нотариусов, регистраторов, регуляторов – технология Blockchain заставляет иначе взглянуть на обмен ценными бумагами, деньгами, информацией. Она, убирая посредников, позволяет пользователям напрямую отправлять друг другу важные данные. Некоторые люди восхваляют Blockchain, другие, в свою очередь, критикуют. К нему можно относиться по-разному, считая его самым важным технологическим нововведением после создания интернета или технологией, который способен породить множество других проблем.

Эпоха интернета принесла нам новое явление, известное как криптовалюта. Технологическая модель Blockchain была разработана в рамках криптовалюты Bitcoin [1]. Bitcoin – Blockchain – это открытая, децентрализованная веб – система учета, которая содержит все когда-либо совершенные Bitcoin – транзакции. Идея протокола Blockchain состоит в том, чтобы обеспечить возможность подтвердить прозрачное проведение транзакций между двумя незнакомыми сторонами без привлечения центральной инстанции [2].

В общем случае, Blockchain – это база данных, в которую записываются факты, объединенные в блоки, содержащиеся на всех компьютерах, объединенных в P2P-сеть.

P2P-сети – это распределенные системы, которым необходимо решить одну из сложнейших проблем информатики – разреше-

ние конфликтов (the resolution of conflicts) или согласование (reconciliation). Факты, которые заносятся в базу данных, могут быть различными, например, денежные транзакции или подписи содержимого и т.д. Члены сети – анонимные субъекты, называемые узлами сети. Новый узел, присоединяющийся к сети, обязан загрузить полную копию Blockchain. Все коммуникации внутри сети используют инструменты криптографии для точной и безопасной идентификации отправителя и получателя. В случае того, если узел хочет добавить информацию в базу данных, в сети должен быть сформирован консенсус, определяющий, где будет размещен факт. Данный консенсус называется блоком [3].

Блоки – это способ организации фактов в сети недоверенных пользователей (network of non-trusted peers). В их основе лежит простая идея: сгруппировать факты в блоки, составить из блоков единственную цепочку, которая будет передана по всем узлам сети. Блоки связаны друг с другом с использованием хэша. Каждый блок ссылается на предыдущий, так может быть прослежено происхождение каждого факта. А новые блоки всегда включаются в конец цепочки. Блок в системе Blockchain включает заголовок и тело блока. Тело блока содержит список транзакций. Блоки в системе blockchain связываются между собой при помощи хэша идентификатора блока. В каждом заголовке блока содержится хэш ID предыдущего блока. Соответственно, в ID каждого блока кодируется информация о всех предыдущих блоках и данных. Из этого следует, что отследить хоть какое-либо изменение данных в любом блоке не составит труда. Соответственно, имея цепочку транзакций и ключ одного из блоков можно проверить: корректность информации в блоке, настоящая ли это цепочка, есть или нет пропущенные блоки, возможное наличие «левых» блоков в цепочке [4].

Майнингом называется процесс поддержания деятельности распределенной платформы и "поиска" блоков. Майнинг заключается в выборе транзакций (фактов) из числа ожидающих и последующем получении хэш-значения, сформированного блока транзакций. Блок считается успешно подтвержденным, если его хэш-значение начинается с определенного количества нулей, однако, большую часть времени полученные хэш-значения не являются успешными, блок немного меняется и хэш-значение генерируется заново. Успешно подтвержденный блок включается в цепь и становится видимым для всех узлов сети. Благодаря сложности данного процесса, шанс "найти" успешное хэш-значение является крайне низким, следовательно, предотвращается возможность мошенничества (никто не в состоянии контролировать, какие именно транзакции (факты) пройдут в майнинг) и повышается безопасность сети. Исключением является ситуация, когда мошенник владеет более чем половиной узлов сети. За каждый созданный блок майнер получает небольшой процент. Это такое поощрение, за выполнение ресурсоёмкой задачи [5].

Майнинг имеет следующую особенность: независимо от количества перерасчётов, которые были исполнены, вероятность расчета необходимого хэша примерно равна. В свою очередь, становится невозможным провести предварительный расчёт или запись результата расчётов для последующего, возможно мошеннического использования. Поэтому все майнеры равноправны между собой.

Известным мифом о Blockchain, который обеспечил ей множество как сторонников, так и противников, является ее анонимность. С точки зрения Bitcoin (и криптовалют в целом), Blockchain – это эффективный инструмент для построения распределенной децентрализованной экономики. В то же время, существует много возможностей для различного рода мошеннической деятельности, например, отмывания денег [6].

Использование такой децентрализованной системы имеет свои преимущества и недостатки. К преимуществам применения Blockchain можно отнести:

• повышает уровень защиты от подделок за счет отслеживаемых цепочек происхождения;

• сокращает или помогает избежать ненужных затрат IT-инфраструктуры;

• помогает обезопасить огромное количество транзакций, т.к. хранящиеся в реестре данные нельзя изменить (без согласия более половины майнеров);

• сокращает расходы на проведение транзакций за счет их прямого проведения;

• предоставляет возможность контроля переводов внутри системы.

• Кроме того, следует отметить следующие недостатки:

• сильная зависимость от надежности криптографических функций;

• затрудненное регулирование из-за отсутствия центральных адресатов;

• с ростом количества транзакций возрастает объем Blockchain, и она занимает всё больше места на компьютерах-узлах;

Энергозатратность. В результате работы можно сделать вывод, что блокчейн, как универсальный инструмент обладает

высокой степенью криптографической защиты, ввиду того что каждый блок состоит из хеш-сумм, по которым невозможно точно определить предмет транзакции или иные входные данные. Благодаря перечисленным возможностям, технология Blockchain может сделать прорыв в следующих отраслях [7, 8]:

Финансы – система сделает ненужными традиционные банки и финансовые институты, заменив бэк-офисные системы системой P2P;

Контракты – **умные контракты** найдут применение в качестве сетевых э счетов, деньги с которых будут отправляться получателям в зависимости от реализации запланированного события. Контракты, сделки, титульные права и прочая важная документация будет храниться в открытом реестре [9];

Патенты и авторское право – Blockchain может обеспечить соблюдение авторских прав на новые технологии, игровые приложения, музыкальные произведения и т. п.;

Голосование – Blockchain позволяет защитить волеизъявление людей в процессе выборов;

Коллекционирование – Blockchain можно использовать для отслеживания и валидации редких предметов, например произведений искусства;

Товарные накладные – использование криптографических подписей поможет повысить доверие к поставляемым товарам и отслеживать их происхождение.

Данная технология может применяться в различных сферах, в том числе в качестве основы для социальных сетей, при создании и управлении крупных баз данных, в логистике, медицине, страховании и многих других областях, где требуется надежный способ обработки и хранения массивных объемов информации. Перспективность ее состоит еще и в том, что любые инициативы могут быть начаты небольшой группой или даже одним участником для своих клиентов, а потом без особого труда распространены на весь рынок. Поэтому blockchain – это больше, чем просто система денежных переводов. Технология Blockchain – это будущее человечества. Но все же современные компьютеры пока не способны обеспечить Blockchain вычислительными мощностями в необходимом объеме, согласно этому повсеместное внедрение системы еще продлится неопределенное время. Блокчейн превосходит другие технологии по обеспечению безопасности. Он обладает высокую степенью криптографической защиты, ввиду того, что каждый блок состоит из хеш-сумм, по которым невозможно точно определить предмет транзакции или иные входные данные.

Однако технология имеет и недостатки:

1. Производительность блокчейна ниже, если сравнивать ее с традиционными централизованными базами данных.

2. Полноценная реализация технологии требует больших трудозатрат и инвестиций в инфраструктуру, безопасность, в том числе разработку и систему хранения приватных ключей и так далее.

Таким образом, использование блокчейна как децентрализованного хранения, например, достижений студентов хотя и предполагает большую надежность, но ввиду небольшого количества участников сети в одном университете, не может обеспечить ту безопасность, которая могла бы обеспечиваться в более глобальных масштабах. Это должен быть региональный или всероссийский уровень. Наибольшая эффективность технологии может быть отражена в банковских операциях, медицине, организации электронных голосований и других сферах, где требуется повышенная надежность и отсутствие централизованного контроля.

Список литературы

1. Форк А. Bitcoin. Больше чем деньги. – М.: Изд-во Продюсерский центр Александра Гриценко. 2014. – 290 с.

2. Тапскотт А., Тапскотт Д. Технология блокчейн – то, что движет финансовой революцией сегодня. – М.: Изд-во Эксмо. 2016. –150 с.

3. Zebus – A lightweight Peer to Peer Service Bus [Электронный ресурс]. – URL: http://github.com/Abc-Arbitrage/Zebus/ (дата обращения: 15.11.2019).

4. Блокчейн простыми словами [Электронный ресурс]. – URL: https://prostocoin.com/blog/blockchain-guide/ (дата обращения: 21.01.2019).

5. Токены vs Пароли [Электронный ресурс]. – https://habrahabr.ru/post/126828/.

6. Как понять, нужно ли интегрировать blockchain в ваш продукт? [Электронный ресурс]. – URL: https://habrahabr.ru/company/web_payment_ru/blog/301972/ (дата обращения: 20.12.2018).

7. Как blockchain изменит нашу жизнь? [Электронный ресурс]. – URL: http://rb.ru/opinion/blockchain/ (дата обращения: 20.12.2018).

8. Евтушенко А., Поляков Е. По цепочке до России // Газета.ru [Электронный ресурс]. – URL: http://www.gazeta.ru/tech/2016/02/01/8038769/blockchain.shtml/ (дата обращения: 21.01.2019).

9. Как блокчейн изменит способы хранения документов об образовании? [Электронный ресурс]. – https://vc.ru/crypto/32267–kak-blokcheyn-izmenit-sposoby-hraneniya-dokumentov-ob-obrazovanii/ (дата обращения: 20.02.2019).