УДК 004:338 + 004.738.5:336.743 Вестник УрФО № 4(26) / 2017, с. 21–24

Осипов Н. Р., Кротова Е. Л.

БЛОКЧЕЙН – ПЛАТФОРМА ДЛЯ ИННОВАЦИЙ

В настоящее время жизнь человека связана с новыми технологиями, информацией, деньгами и многочисленными бумагами. Для достижения тех или иных задач приходится привлекать многочисленных посредников, сотрудничество с которыми подразумевает проведение десятков разных операций. Также это накладывает временные и материальные ограничения в виде комиссии посредников и бумажной проволочки. Задача технологии блокчейн — исправить проблему, которая связана со значительными материальными (оплачиваемые посреднические услуги) и временными затратами.

Ключевые слова: *Блокчейн, криптовалюта, цепочки блоков транзакций, биткоин.*

Osipov N. R., Krotova E .L.

BLOCKCHAIN – A PLATFORM FOR INNOVATION

At the now day, a person's life is connected with new technologies, information, money and numerous papers. To perform different tasks, it is necessary to involve numerous intermediaries, cooperation with which implies performing different operations. It also imposes temporary and material restrictions in the form of a commission of intermediaries and "paper" delay. The task of blocking technology is to fix a problem that is associated with significant material (paid intermediary services) and time costs.

Keywords: *Blocking, crypto currency, chain of transaction blocks, bitcoin.*

Что такое блокчейн и его актуальность

Блокчейн означает «цепь блоков». Блоком называют такой информационный пакет, содержащий в себе все предыдущие сведения и часть новых. А вся цепочка представляет собой распределенную между множеством участников базу данных, работающую без централизованного управления.

Отсутствие централизации - важный элемент технологии. Все сведения хранятся на компьютерах пользователей, которые видят одно и то же. Поэтому взломать или «выключить» блокчейн невозможно: если есть хотя бы один компьютер, включенный в сеть, технология будет работать.

Кроме того, система организована так, что каждый ее участник постоянно проверяет поступающие к нему сведения. В итоге при любой операции подтверждается целостность и достоверность хранящихся в сети материалов.

Новая информация записывается в конец цепочки поверх уже проверенной и частично основывается на ней. Если изменить какую-то

часть материалов, например, путем взлома, то это должно привести к изменению последующей цепочки информации, иначе эта ошибка будет видна всем участникам. А изменить данные сразу, например, на десяти тысячах компьютеров очень сложно и дорого. Этим гарантируется сохранность и точность сведений.

Сегодня мы уже все привыкли делиться информацией через децентрализованную интерактивную платформу Интернета. Но когда речь заходит о пересылке ценностей (денег), мы обычно вынуждены снова пользоваться услугами старых централизованных финансовых учреждений (банков). Да, методы платежей через Интернет появились сразу же в момент рождения этой сети (наиболее очевидный пример — это PayPal), но они, как правило, требуют интеграции с банковским счетом или кредитной картой, иначе их нельзя реально использовать.

Технология блокчейн предлагает заманчивую возможность избавиться от этого «лишнего звена». Она может взять на себя все три важные роли, которые традиционно играет сектор финансовых услуг: регистрация сделок, подтверждение подлинности личности и заключение контрактов.

Это будет иметь огромное значение, поскольку во всем мире рынок финансовых услуг — самый большой по рыночной капитализации. Перевод хотя бы части этой системы на технологию блокчейн приведет к разрыву большого числа связей в сфере финансовых услуг, но одновременно позволит значительно повысить эффективность этих услуг.

Возможности этой технологии в заключении контрактов могут оказаться очень полезными и вне сектора финансовых услуг. Помимо ввода в обращение еще одной валюты (биткоина), технология блокчейн может использоваться также для хранения любого вида цифровой информации, включая компьютерный код.

Этот фрагмент кода можно запрограммировать так, чтобы он выполнялся, только когда обе договаривающиеся стороны вводят свои ключи, тем самым соглашаясь на заключение контракта. Этот же код может получать информацию из внешних потоков данных (цены на акции, метеорологические сводки, заголовки новостей и все остальное, что может быть проанализировано компьютером) и составлять контракты, которые будут *автоматически* регистрироваться при выполнении определенных условий.

Этот механизм называется «умные контракты», и возможности их применения практически бесконечны.

Например, интеллектуальная система терморегуляции может передавать данные об энергопотреблении в интеллектуальную электрическую сеть. При потреблении определенного количества электроэнергии другая цепочка блоков автоматически переводит нужную сумму с вашего счета на счет энергетической компании. В результате автоматизируются работа счетчика и процесс выставления счетов.

Можно также использовать этот подход для контроля использования интеллектуальной собственности, определяя, сколько раз пользователь может получить доступ к информации, поделиться ею или скопировать ее. Еще его можно использовать для создания систем голосования с защитой от фальсификаций, распространения информации без цензурных ограничений и многого другого.

Принцип работы

Иногда технологию блокчейн называют «Интернетом ценностей», и мы считаем, что это хорошая метафора.

Каждый человек может разместить в Интернете информацию, а затем другие люди могут получить к ней доступ из любой точки мира. Цепочки блоков позволяют отправлять в любую точку мира, где будет доступен файл блокчейна, какие-либо ценности. Но у вас должен быть закрытый ключ, созданный по криптографическому алгоритму, чтобы разрешить вам доступ только к тем блокам, которыми вы «владеете».

Предоставляя кому-либо ваш закрытый ключ, вы, по сути, передаете этому лицу денежную сумму, которая хранится в соответствующем разделе цепочки блоков.

В случае биткоинов такие ключи используются для доступа к адресам, по которым хранятся некоторые суммы в валюте, представляющие прямую финансовую ценность. Этим реализуется функция регистрации перевода средств, обычно такую роль выполняют банки.

Кроме того, реализуется еще одна важная функция: установка отношений доверия и подтверждение подлинности личности, потому что никто не может изменять цепочку блоков без соответствующих ключей. Изменения, не подтвержденные этими ключами, отклоняются. Конечно, ключи (как и физическая валюта) теоретически могут быть украдены, но

защита нескольких строк компьютерного кода обычно не требует больших затрат.

Это означает, что основные функции, выполняемые банками: проверка подлинности личности (для предотвращения мошенничества) и последующая регистрация сделок (после чего они становятся законными) — могут выполняться цепочкой блоков быстрее и точнее[1].

Итак, из чего же состоит технология блокчейн?

1. Участники

Все участники системы делятся на 2 категории:

– рядовые пользователи, создающие записи (операции, действия, транзакции);

– майнеры, которые формируют из них блоки (пакеты, конверты) данных. Это очень сложная и ресурсоемкая процедура, и не каждый участник имеет техническую возможность ее реализации.

Обычный пользователь записывает в систему сообщение, например, о том, что «X взял кредит у Y». Оно зашифровано. Причем X и Y имеют свои ключи[2].

Каждый участник, получив эти сведения, проверяет шифры и распространяет сообщение по сети. Если в шифровке обнаружена ошибка, данные остальным пользователям не отправляются.

2. Формирование блоков

Майнеры, получив записи, проверяют их, пакуют в блоки и также рассылают по сети. Пока данные не запакованы, они считаются недостоверными.

Блок состоит из 2 частей: тела и заголовка. Тело — это набор записанных сообщений. Заголовок — связующее звено цепи. Он содержит 2 ключа:

– предыдущего набора материалов;

– и текущего блока, который рассчитан на основе содержащихся в нем записей, и шифра предшествующего конверта.

Таким образом, в каждом запакованном наборе материалов закодирована вся предыдущая информация. Любое изменение сведений потребует корректировки ключа текущего пакета и всех последующих. Другими словами, видя систему и зная коды, можно понять, не нарушен ли порядок конвертов, не удалены или не добавлены ли новые наборы, соответствуют ли сведения шифровке и т. п.

4. Формирование ключей

Ключи получаются путем хэширования или свертки — преобразования информации в число. Проиллюстрируем простым примером. Вместе со словом «деньги» передается его код, представляющий собой произведение чисел - порядковых номеров букв, из которых состоит слово «деньги». Получатель слова перемножает номера букв и сверяется с кодом. Так происходит проверка. Если в процессе передачи «деньги» трансформировались в «денги», то получатель, увидев несоответствие между полученным кодом и рассчитанным им самим результатом поймет, что данные искажены.

Это самый простой пример, приведенный для наглядности. Более сложную защиту в блокчейн дает криптографическое шифрование, которое применяется в электронной подписи. В итоге код может представлять собой число, состоящее из нескольких десятков цифр.

Кроме того, для повышения безопасности, создатели сетей блокчейн разрабатывают дополнительные условия кодировки. Так, в сети биткоин, каждый ключ начинается с десяти нулей. Поэтому майнеры должны проводить сотни и миллионы вычислений для соответствия требованиям формирования кода.

5. Зашифровка записей

Записи также объединены в цепочки. Никто не может создать злонамеренное сообщение «перечислить все средства Y на счет X, открытый в оффшорном банке», так как все операции содержат в себе ссылку на предшествующее сообщение (источник).

Запись имеет 2 части: источник и результат. Источник включает в себя шифр предыдущей операции и разблокирующее правило. Результат — содержание текущей операции и блокирующее условие. Создать следующее сообщение и продлить цепь записей сможет только тот, кому известно разблокирующее правило.

Например, предыдущая операция (источник) имела результат «перевести компании X сумму, равную 1000 денег». Блокирующее условие было таким: «код пароля — 56739209871...». Для того чтобы получить и потратить эту сумму, компания X должна создать следующее сообщение, включив в ее разблокирующее правило этот пароль. А само это правило будет гласить «Рассчитать ключ пароля NNNN». Майнер, получив запись, подставляет результат расчета в предыдущее сообщение цепочки, и если все сходится, включает ее в пакет[3].

Заключение

Таким образом, технология блокчейн делает возможным хранение данных о финансовых операциях, юридических обязательствах, правах собственности, обеспечивая полную прозрачность и всеобщую доступность для ознакомления, но при этом надежно защищая от любого подлога, взлома и так далее. В еще более простом варианте можно сказать, что технология блокчейн — это некий стеклянный куб с постоянно включенной камерой наблюдения — в него можно (под присмотром) положить что-то новое, но при попытке изменения или подмены содержимого это тут же станет видно любому наблюдателю.

Также он может применяться не только в описанных сферах, но и в страховании, налогообложении, риэлтерских услугах, сделках с имуществом, логистике, избирательной системе и других сферах, что делает эту технологию платформой для дальнейших инноваций.

Литература

1. Что такое Блокчейн? // 24PAYBANK. URL: https://24paybank.com/faq/chto-takoe-blockchain.html (дата обращения 10.06.2017)

2. Блокчейн - это… Как работает блокчейн, преимущества, применение, перспективы. // fb.ru URL: http://fb.ru/article/261672/blokcheyn---eto-kak-rabotaet-blokcheyn-preimuschestva-primenenie-perspektivyi (дата обращения 11.06.2017)

3. Технология Блокчейн (blockchain) – что это такое простыми словами. // real-investment.ru URL: http://real-investment.ru/finansovaja_gramotnost/blokchejn_blockchain_chto_ehto_takoe_prostymi_slovami (дата обращения 15.06.2017)

4. Что такое блокчейн? Расскажем простыми словами. // Coinspot URL: https://coinspot.io/beginners/chto-takoe-blokchejn-rasskazhem-prostymi-slovami/ (дата обращения 17.06.2017)

5. Что такое блокчейн и зачем он нужен // Хабрахабр URL: https://habrahabr.ru/company/bitfury/blog/321474/ (дата обращения 20.06.2017)

References

1. Chto takoye Blokcheyn? // 24PAYBANK. URL: https://24paybank.com/faq/chto-takoe-blockchain.html (data obrashcheniya 10.06.2017).

2. Blokcheyn - eto… Kak rabotayet blokcheyn, preimushchestva, primeneniye, perspektivy. // fb.ru URL: http://fb.ru/article/261672/blokcheyn---eto-kak-rabotaet-blokcheyn-preimuschestva-primenenie-perspektivyi (data obrashcheniya 11.06.2017).

3. Tekhnologiya Blokcheyn (blockchain) – chto eto takoye prostymi slovami. // real-investment.ru URL: http://real-investment.ru/finansovaja_gramotnost/blokchejn_blockchain_chto_ehto_takoe_prostymi_slovami (data obrashcheniya 15.06.2017).

4. Chto takoye blokcheyn? Rasskazhem prostymi slovami. // Coinspot URL: https://coinspot.io/beginners/chto-takoe-blokchejn-rasskazhem-prostymi-slovami/ (data obrashcheniya 17.06.2017).

5. Chto takoye blokcheyn i zachem on nuzhen // Khabrakhabr URL: https://habrahabr.ru/company/bitfury/blog/321474/ (data obrashcheniya 20.06.2017).

ОСИПОВ Никита Романович, студент кафедры Автоматики и телемеханики Пермского национального исследовательского политехнического университета. 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. E-mail: nikita.osipov.96@yandex.ru

КРОТОВА Елена Львовна, кандидат физико-математических наук, кафедра Высшей математики Пермского национального исследовательского политехнического университета, доцент. 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. E-mail: lenkakrotova@yandex.ru

OSIPOV Nikita, student of the Department of Automation and Telemechanics of the Perm National Research Polytechnic University. 29 Komsomolsky prospekt, Perm, Perm krai, Russia, 614990. E-mail: nikita.osipov.96@yandex.ru

KROTOVA Elena, candidate of physico-mathematical sciences, Department of Higher mathematics, Perm National Research Polytechnic University, docent. 29 Komsomolsky prospekt, Perm, Perm krai, Russia, 614990. E-mail: lenkakrotova@yandex.ru