

“Radio” is monthly publication on audio, video, computers, home electronics and telecommunication

УЧРЕДИТЕЛЬ И ИЗДАТЕЛЬ: ЗАО «ЖУРНАЛ «РАДИО»

Зарегистрирован Министерством печати и информации РФ 01 июля 1992 г.

Регистрационный ПИ № ФС77-50754

Главный редактор В. К. ЧУДНОВ

Редакционная коллегия:

А. В. ГОЛЫШКО, А. С. ЖУРАВЛЁВ, А. Н. КОРОТОНОШКО,
К. В. МУСАТОВ, И. А. НЕЧАЕВ (зам. гл. редактора),
Л. В. МИХАЛЕВСКИЙ, С. Л. МИШЕНКОВ, О. А. РАЗИН,
Б. Г. СТЕПАНОВ (первый зам. гл. редактора), В. В. ФРОЛОВ

Выпускающие редакторы: С. Н. ГЛИБИН, А. С. ДОЛГИЙ

Обложка: В. М. МУСИАКА

Вёрстка: Е. А. ГЕРАСИМОВА

Корректор: Т. А. ВАСИЛЬЕВА

Адрес редакции: 107045, Москва, Селивёрстов пер., 10, стр. 1

Тел.: (495) 607-31-18. Факс: (495) 608-77-13

E-mail: ref@radio.ru

Группа работы с письмами — (495) 607-08-48

Отдел рекламы — (495) 608-99-45, e-mail: advert@radio.ru

Распространение — (495) 608-81-79; e-mail: sale@radio.ru

Подписка и продажа — (495) 607-77-28

Бухгалтерия — (495) 607-87-39

Наши платёжные реквизиты:

получатель — ЗАО “Журнал “Радио”, ИНН 7708023424,
р/сч. 40702810438090103159

Банк получателя — ПАО Сбербанк г. Москва

корр. счет 3010181040000000225 БИК 044525225

Подписано к печати 16.09.2016 г. Формат 60×84 1/8. Печать офсетная.

Объём 8 физ. печ. л., 4 бум. л., 10,5 уч.-изд. л.

В розницу — цена договорная

Подписной индекс:

по каталогу «Роспечати» — 70772;

по Объединённому каталогу «Пресса России» — 89032;

по каталогу Российской прессы ПОЧТА РОССИИ — 61972.

За содержание рекламного объявления ответственность несёт рекламодатель.

За оригинальность и содержание статьи ответственность несёт автор.

Редакция не несёт ответственности за возможные негативные последствия использования опубликованных материалов, но принимает меры по исключению ошибок и опечаток.

В случае приёма рукописи к публикации редакция ставит об этом в известность автора. При этом редакция получает исключительное право на распространение принятого произведения, включая его публикации в журнале «Радио», на интернет-страницах журнала, CD или иным образом.

Авторское вознаграждение (гонорар) выплачивается в течение двух месяцев после первой публикации в размере, определяемом внутренним справочником тарифов.

По истечении одного года с момента первой публикации автор имеет право опубликовать авторский вариант своего произведения в другом месте без предварительного письменного согласия редакции.

В переписку редакция не вступает. Рукописи не рецензируются и не возвращаются.

© Радио®, 1924—2016. Воспроизведение материалов журнала «Радио», их коммерческое использование в любом виде, полностью или частично, допускается только с письменного разрешения редакции.

Отпечатано в АО «ПОЛИГРАФИЧЕСКИЙ КОМПЛЕКС «ЭКСТРА М»,
143400, Московская обл., Красногорский р-н, а/м «Балтия», 23 км.
Зак. 16-09-00223.

Луч света в царстве Интернета

А. ГОЛЫШКО, канд. техн. наук, г. Москва

“Состоятельный человек может находиться одновременно в нескольких местах. Например, на Гавайских островах и в федеральном розыске”.

*(из методички
по финансовому мониторингу)*


Что есть блокчейн?

Не секрет, что Интернет — одно из выдающихся изобретений второй половины прошлого века — называют как невероятным прорывом в будущее, так и всемирной помойкой. Последнее заслуженно получено за глобальный фрод (мошенничества в области информационных технологий), за спам, за воровство, за троллинг, за незаконное проникновение в неприкосновенное, за площадки для преступников и, конечно же, за горы “социального мусора”. Никто не может быть уверен, что не украдут, не обманут, не подменят и не обольют. Кажется, что так будет всегда, но вот в помощь этике подтянулись кое-какие технологии, и перед прогрессивным человечеством забрезжила надежда...

В роли надежды выступает модная в последнее время технология блокчейн (blockchain — цепочка блоков), за которую сегодня и “ухватилось” всё ответственное человечество в лице бизнеса и особенно финансового сообщества. Крупные компании, вроде Microsoft и IBM, взяли эту технологию на вооружение из-за её возможности совершить переворот в плане обработки транзакций и управления ими. Более 20 банков, среди которых Goldman Sachs, JP Morgan, Credit Suisse и Barclays, уже объединились в консорциум R3 для пристального изучения работы блокчейна. Причём в последний год отмечается просто взрывной рост интереса к этой технологии. Говорят даже, что блокчейн — это революция на уровне изобретения сети Интернет.

Прежде всего, идея технологии максимально проста — это огромная база данных общего пользования, которая функционирует без централизованного руководства (собственно, как и Интернет, который в одной из своих ипостасей также является распределённой базой данных). Однако блокчейн — не просто единая база данных, хранящаяся целиком у каждого узла в сети. Её уникальная особенность заключается в том, что любой участник может самостоятельно удостовериться в том факте, что его копия совпадает с копиями большинства других узлов. Причём совпадает полностью, до единого бита. Конечно, всегда есть некоторая вероятность ошибки, но её можно сделать сколь угодно малой. Ключевое слово — “самостоятельно”, а это значит, что для работы сети не нужно доверять другим узлам. На практике это является решением “задачи византийских генералов” или “механизмом распределённого консенсуса”. Есть такая задача, как группе генералов, каждый из которых находится в своей действующей армии, договориться о совместных действиях, если известно, что среди них есть “предатель”, который не должен понять совместного плана, тогда как “честные генералы” должны договориться. И поскольку в варианте блокчейна “честные генералы” достигли своего, “генералам от бизнеса” это понравилось.

К сказанному следует добавить, что технология блокчейн “пришла” из мира криптовалют (а это ни что иное, как биты, собранные определённым образом), о чём уже шла речь на страницах журнала. В разных местах отношение к криптовалютам, как известно, меняется от бурных восторгов до желания сажать в тюрьму, но собственно к технологиям это не имеет отношения. Могут быть разные мнения о самих криптовалютах, но система их передачи (собственно блокчейн) считается безупречной по части точности и достоверности. Технология биткоина подразумевает проверку транзакций, которой занимаются так называемые майнеры — участники криптовалютной системы, которые подтверждают подлин-



Компьютерная сеть редакции журнала «Радио» находится под защитой Dr.Web — антивирусных продуктов российского разработчика средств информационной безопасности — компании «Доктор Веб».

www.drweb.com

Бесплатный номер службы поддержки в России:
8-800-333-79-32

ИНФОРМАЦИОННАЯ ПОДДЕРЖКА — КОМПАНИЯ «РИНЕТ»



Телефон: (495) 981-4571
Факс: (495) 783-9181
E-mail: info@rinet.ru
Сайт: <http://www.rinet.net>

Internet Service Provider

ность совершенных действий, а затем формируют из записей транзакций блоки. Поскольку сам процесс майнинга сопряжен со сложными математическими задачами, майнеры должны иметь в своём арсенале довольно мощные компьютеры. Поэтому у этих участников и находится распределённая база данных, состоящая из "цепочки блоков". В свою очередь, распределённый характер базы данных на основе блокчейна и позволяет контролировать достоверность транзакций без надзора каких-либо финансовых регуляторов. Кстати, первые адепты биткоинов утверждали, что, мол, они помогут избавиться от банков и государств. В свою очередь, отдельные бизнесмены считают, что биткоины — это нечто вроде очередной финансовой пирамиды, в то время как исследователи продолжают погружаться в возможности новой технологии, которая стоит за всеми электронными валютами.

Независимо от мнений разных людей по поводу биткоина, практически каждый солидарен с тем, что фундаментальная технология, на которой он работает, безупречна. С её помощью любой может не только хранить деньги, но и совершенно прозрачно совершать денежные транзакции, без необходимости доверять друг другу или какому-либо централизованному посреднику (вопрос доверия, к примеру, долго тормозил внедрение ЭЦП — электронной цифровой подписи).

Блокчейн — это одновременно и крайне простая технология, и одновременно сложная, и самая защищённая технология (взломать почти невозможно). По-простому, блокчейн — это система передачи информации, уникальность которой состоит в том, что в ней нет искажений — что на входе, то и на выходе. И это крайне важно, например, для банковских транзакций, когда в ходе операции не без помощи мошенников могут вклиниваться дополнительные опции, которые извращают входящую информацию со всеми возможными последствиями. Кстати, можно даже не хранить весь блокчейн у себя. Информация внутри блоков хранится в виде дерева, поэтому можно удостовериться, что "лист" дерева (транзакция или любые другие данные) содержится в цепочке, не скачивая её всю. И пока в сети есть хотя бы один узел, можно говорить о том, что существует и блокчейн. То есть, иными словами, это напоминает вечный двигатель, который никто и ничто не сможет остановить.

Как работает?

Блокчейн является всего лишь очередной базой данных для записи и хранения данных о транзакциях, которые копируются на каждый компьютер, участвующий в процессе их передачи по сети. Поэтому блокчейн ещё называют распределённым журналом для записи транзакций. Записи в него можно вносить только с согласия большинства пользователей, а однажды записанная информация уже никогда не может быть изменена или стёрта. Данные в блокчейнах состоят из фиксированных структур (блоков), которые, в

свою очередь, состоят из следующих важных частей:

— заголовок блока, он включает в себя метаданные, вроде уникальной контрольной суммы, времени создания и ссылки на предыдущий блок;

— содержимое блока — это список цифровых активов и команд вроде совершенных транзакций, их объёмов и адресов участников сделок.

Таким образом, если у вас есть последний блок, вы можете получить доступ ко всем предыдущим в цепочке. База данных блокчейна сохраняет всю историю транзакций, включая данные о всех цифровых активах и командах, которые были заданы со времени создания самого первого блока. Вот так информация в блокчейне доступна и проверяема в любой момент времени. И с ростом числа участников потенциальному "шпиону" становится всё труднее отслеживать деятельность всей цепочки. Именно благодаря этой особенности цепочка блоков транзакций является очень жизнеспособной и защищённой структурой данных. Кстати, большинство систем обработки транзакций работают не так, как функционирует децентрализованная и распределённая система блокчейна. Также блокчейн можно разрабатывать в контексте публичного или частного доступа, или создавать блокчейн-консорциумы. Для каждого вида применения нужно выбрать подходящий тип этой технологии.

Мало того, в определённых сферах блокчейн-процессы куда более безопасны и прозрачны, чем традиционные модели создания стоимости. Возможно, самое интересное его применение — объединение вместе разрозненных частей предприятия или даже разных организаций, функционирующих в одном секторе. Всё это может иметь невероятный эффект — нацонец-таки, люди смогут с уверенностью знать, что именно происходит в цифровом мире.

На текущий момент каждая интернет-транзакция опирается на какой-либо центральный институт, которому доверяют. Каждый раз, когда вы присутствуете в Интернете, вы вынуждены полагаться на кого-либо, кто сообщит вам достоверную информацию. Идёт ли речь о банке, сообщаемом данные о вашем текущем счёте или о сообщении от вашего почтового провайдера о том, что письмо было доставлено, или о вашем антивирусе, заверяющем, что с безопасностью вашего компьютера всё в порядке. Однако всегда есть доля вероятности, что какой-либо информационный провайдер сообщает ложную информацию, не важно, по злому умыслу или в результате ошибки. Именно поэтому информационная безопасность в сети Интернет находится в весьма плачевном состоянии, когда мы вынуждены доверять сервисам, которые могут быть взломаны или попасть под контроль злоумышленников. И этому "тёмному царству" Интернета доверяют даже самую ценную личную информацию. А вот блокчейн может всё это изменить. Сделав доступной эту систему распределённого консенсуса, он позволяет создать истинную цепочку запи-

сей о прошлых и настоящих событиях в цифровом мире. Причём принципиально важно, что он делает это без вторжения в ваше личное пространство. Вы можете зафиксировать сам факт того, что событие случилось, и даже тот факт, что оно случилось надлежащим образом, не раскрывая конфиденциальную информацию относительно предмета или сторон-участников.

Сказанное, кстати, объясняет, почему биткоин стал так хорош для чёрного рынка (и именно это вызывает его неприятие в ряде стран), ведь несмотря на то что по своей природе это открытая система, её пользователи могут оставаться полностью анонимны. Однако в итоге положительные моменты всё-таки значительно перевешивают отрицательные. К примеру, один из ключевых способов использования блокчейна — это так называемые "умные контракты", когда вы можете погрузиться на децентрализованную сеть, которая подтвердит, что контракт любого типа был выполнен должным образом (выполнение может быть осуществлено в автоматическом режиме), не раскрыв при этом никакой конфиденциальной информации об участниках или самой транзакции.

Возможные проблемы

Конечно, никогда и нигде не бывает так, чтобы совсем не было проблем. Проблема блокчейна в том, что для большинства людей сама его концепция неразрывно связана с криптовалютой биткоин, которая действительно сложна и крайне неоднозначна, а её курс в последние годы, по сравнению с другими валютами, колебался очень сильно. К тому же в массовом сознании биткоин имеет неважный имидж, поскольку способствовал развитию многомиллиардного рынка анонимных покупок, где в том числе продавались и покупались запрещённые вещества и оружие. Поэтому человека со стороны участие в спорах на подобные темы приводит в замешательство.

С развитием экосистемы и возникновением новых сфер применения блокчейна появятся и новые задачи, и новые проблемы. Прежде всего, необходимо повышение осведомлённости людей и институтов о блокчейн-технологии и её понимании. Важным вопросом её применимости будет стоимость и эффективность использования вкупе с обеспечением безопасности и конфиденциальности. Обязательно будет также необходимо наличие механизма управления и регулирования на государственном уровне, а также готовность к межотраслевому сотрудничеству.

Ни для кого не секрет, что технология блокчейн проникает всё глубже в разные сферы нашей жизни. И если раньше блокчейн был просто базой данных, то теперь с его помощью можно совершить переворот в системах хранения и обработки данных, о чём свидетельствуют более тысячи стартапов, планирующих использовать новую технологию. Правда, реальных сервисов на блокчейне не так уж и много. Большинство разработчиков пока только говорят о том, что планируют сделать



или как это будет выглядеть. Но есть и приятные исключения. Специалисты говорят, что блокчейн — это совершенно новая категория базы данных и применять его там, где применяются классические решения, нет никакого смысла. По их словам, блокчейн — это как алмазный сейф, в который может любой положить что угодно, любой будет видеть, что туда положено, но забрать или изменить может только хозяин предмета. В общем, главные свойства — распределённость, публичность и математическая достоверность, которыми надо суметь воспользоваться. Сумма этих свойств открывает бизнесу дорогу к очень низким издержкам в ряде областей, в том числе к удешевлению персонализированных сервисов.

Перспективы

Помимо повышения уровня доверия блокчейн-технологии, дополнительную ценность её "цепочки" могут представлять для происходящей на наших глазах повсеместной цифровизации всех бизнес-процессов. В связи с широким внедрением этой технологии кое-кто даже предсказывает сегодняшним финансовым институтам смерть в течение нескольких лет. Другие же считают, что блокчейн не сможет сильно повлиять на банковскую сферу, кроме как стать ещё одним способом оплаты, и почему бы финансовым институтам не взять его на вооружение. Предполагается, что в базах данных, созданных на основе блокчейна, можно будет хранить не только информацию о платежах, но и данные о кредитах, заключённых браках или даже вести миграционный учёт, словом, выстроить систему нового образца. Крупнейшие банки мира начали изучать саму возможность применения технологии блокчейна. В частности, Эстония обеспечивает безопасность своей банковской инфраструктуры, в основном используя блокчейн, и может похвастаться самым низким уровнем мошенничества с кредитными картами во всей Еврозоне. Или стартапы, вроде Bitreserve, предоставляют полностью бесплатные онлайн транзакции без волатильности и рисков, которые свойственны биткоину.

Кстати, блокчейн — это не только прямая оплата без посредников, но и молодая технологическая экосистема, которая сегодня играет всё большую роль в развитии общества. Она включает в себя такие сферы, как искусственный интеллект, робототехнику, повышая как минимум общий уровень доверия между участниками. Блокчейн, несомненно, повлияет на сотрудничество организаций и бизнеса, на прозрачность данных и процессов и, в конце концов, на продуктивность и устойчивость экономики в целом. Вокруг этой технологии давно ходит мнение о том, что она может облегчить обмен средствами по всему миру с помощью криптовалют, однако банки могут найти и другие применения цепочкам транзакционных блоков в лице многочисленных банковских услуг или юридического сопровождения финансовых сделок. В целом, используя блокчейн, банки могут приостановить отток капитала и

клиентов. Страховщики, как и банки, — тоже своего рода посредники в финансовом мире. С помощью блокчейн-технологий они могут ускорить выплату взносов и возмещение ущерба.

Можно представить перспективы использования блокчейна для хранения медицинских записей, при проведении голосований, при ведении учёта прав собственности, при регистрации браков и судебного делопроизводства. Со временем каждый набор данных и каждая цифровая транзакция может оставить свой уникальный, как отпечаток пальцев, след, создавая возможность для аудита любого цифрового события, не нарушая при этом чьей-либо приватности. С помощью блокчейна планируется защищать данные атомных электростанций в Великобритании, механизмы предупреждения наводнений и другие важные объекты инфраструктуры.

Если обратиться к такому сложному механизму, как государственный сектор, то, с одной стороны, он отличается централизацией с точки зрения ответственности перед гражданами за качественные госуслуги и управление страной. С другой стороны, госсектор фрагментарен и разобщён, если говорить о его организационных структурах и межведомственном обмене данными, и в нём блокчейн можно использовать для борьбы с неэффективностью бюджетных организаций в оказании публичных услуг.

В XXI веке цифровые технологии кардинально изменили развлекательную индустрию и медиасферу. Проблемы дистрибуции продуктов, соблюдения авторских прав и свободного копирования медиаконтента также могут быть решены с помощью блокчейна. Например, путём сведения напрямую музыкантов, писателей и прочих креативщиков с их клиентами, так и путём реструктуризации процессов внутри главных игроков медиарынка.

Проекты

Исторически первым проектом на базе блокчейн был проект DNS Namecoin (DNS — Domain Name System — система доменных имён), который позволяет реализовать возможность регистрировать стандартные DNS-записи, производить над ними обычные операции (типа обновления) и, разумеется, получать к ним доступ. Тогда любой клиент, обладая копией актуального блокчейна, легко сможет проверить, какой IP-адрес в данный момент соответствует такому-то адресу сайта.

В проекте хранения данных Datacoin реализована простая возможность прикреплять за определённую стоимость к своей транзакции файлы до 128 килобайт. И теперь в любой момент можно получить доступ к этому файлу.

Блокчейн-платформа Emer включает в себя уже работающие сервисы для электронного бизнеса и обеспечения сетевой безопасности. Совокупность этих базовых сервисов позволяет легко создавать любые блокчейн-ориентированные приложения с крайне высокими показателями надёжности и быстродействия.

Сервис EmcSSL — это расширение для стандартного пользовательского протокола SSL, которое хранит цифровые отпечатки сертификатов пользователей в блокчейне, авторизует пользователей и делает доступ к удалённым сайтам полностью защищённым. Когда человек входит на сайт (например, сайт банка), информация, передаваемая к пользователю и от него, может быть украдена (например, могут быть украдены пароли). EmcSSL делает передачу данных полностью безопасной и непереживаемой, даже если вся сеть находится под контролем злоумышленника. Сильно упрощаются и ускоряются действия при потере клиентом сертификатов (например, при похищении компьютера или ключа).

Сервис EmcTTS позволяет фиксировать в блокчейне время размещения любых документов. Это незаменимый сервис для размещения страховых и других подобных контрактов, который решает вопросы приоритетов авторского права, патентные вопросы и пр. Например, если зарегистрировать документ в блокчейне так, что можно будет легко проверить его существование на указанную дату. Можно будет легко проверить, что документ действительно существовал на дату регистрации и был именно таким, как представлен. Работа нотариальных и патентных ведомств заметно упрощается, ускоряется и удешевляется, а главное, исключается любая возможность фальсификации. Теперь, просто разместив любой документ в блокчейне, можно зарегистрировать приоритет изобретения или дату заключения контракта. В этом случае как сам документ, так и дата и время его размещения будут записаны навсегда, без малейшей возможности фальсификации.

Сервис EmcDPO может быть использован для подтверждения прав на любые виды собственности, за которыми закреплены уникальные номера — VIN номера автомобилей, кадастровые номера земельных участков, номера квартир в доме, лицензионные номера программного обеспечения и многое другое. При продаже или передаче актива владелец автоматически лишается прав владения, и оно переходит к новому хозяину.

Концепция виртуальных транзакций основана на технологии вероятностной агрегации виртуальных микротранзакций в реальные. Все платёжные системы имеют стоимость транзакций, выражённую либо в деньгах, либо в потреблённых материальных ресурсах. В свою очередь, данная технология позволяет совершать микроплатежи на сверхмалые суммы (скажем, в доли копейки), с минимальными транзакционными издержками. Так можно оплачивать поточный трафик — телефонно, видеоуроки, видеофильмы, консультации в реальном времени, и всё это без подписки и без создания аккаунта.

Власти штата Делавэр (США) разработали блокчейн с "умными" контрактами для регистрации компаний, мониторинга цен на их акции и поддержания контактов с учредителями. Министерство обороны США разрабатывает

безопасный сервис обмена сообщениями на базе блокчейн, который отделяет процесс создания сообщения от процесса его передачи и приёма. Министерство внутренней безопасности США использует блокчейн для защиты цифровых идентификационных характеристик IoT-устройств, управления идентификацией, обеспечения конфиденциальности и анализа данных о безопасности. Почтовая служба США оценивает перспективы использования блокчейн для организации системы снабжения, службы идентификации и управления устройствами. В России главными лоббистами технологии блокчейн стали платёжная система Qiwi и Сбербанк.

В будущем государства могут взять на вооружение данные, заверенные с помощью блокчейна, как доказательства в различных процессах, в том числе и в судебной практике, поскольку технология не предусматривает какую-либо фальсификацию.

Разумеется, как и любое новшество, технология блокчейн вызывает множество споров в мировом сообществе. Но многие соглашаются в одном — эта технология является одним из важней-

ших изобретений за последние десятилетия, которое способно перевернуть не только финансовую индустрию, но и другие сферы жизни, такие как кибербезопасность или образование.

Если блокчейн полностью раскроет свой потенциал, он сможет породить такой уровень демократии и объективной "правды" в цифровом мире, на какой окружающий нас физический мир оказался неспособен. Это также обещает нам будущее, в котором ни у кого не будет абсолютной силы в Интернете и где никто не сможет сфальсифицировать информацию о прошлых или текущих событиях. Всё это пока что только возможное будущее, но с каждым днём всё больше и больше умных людей, разбирающихся в технологиях, присоединяются к этой системе, веря, что однажды всё, о чём мы здесь говорили сегодня, станет возможным. А общей проблемой станут тогда те, кому правда не нужна.

По материалам PCWeek, gazeta.ru, rusbase.com, walter-simons.livejournal.com, bolshoyvopros.ru, futurebanking.ru, bitcoininfo.ru

МОДУЛЬНАЯ РЕКЛАМА

FLCG "Берёзка" — многофункциональный измерительный комплекс:

- ✓ измерение частоты (до 2 ГГц);
- ✓ генератор (до 1 МГц);
- ✓ измерение ёмкости и индуктивности;
- ✓ измерение напряжения;
- ✓ проверка кварцевых резонаторов.

Цена — 4499 руб.!

www.FLCG.ru

8(495) 781-59-24 8(985) 924-34-35
info@icdarom.ru

* * *

НОВЫЕ НАБОРЫ
на российском рынке!
Свыше 200 моделей!
Для дома, бизнеса и офиса.
8-495-545-92-41
WWW.RADIO-KIT.RU