

2. Указ Президента РФ от 10.08.2011 №1071 (ред. от 01.07.2014) «Об утверждении перечня информации о деятельности Федеральной службы исполнения наказаний, размещаемой в сети Интернет». //Доступ из СПС «КонсультантПлюс».

3. Приказ ФСИН России от 20.09.2011 №515 «О порядке работы интернет-портала ФСИН России и его технического сопровождения» (зарегистрирован в Минюсте России 29.12.2016 № 45038).

Для цитирования: Винда О.В., Критская С.Н. Знакомьтесь: сайт ФСИН России // Актуальные вопросы информатизации Федеральной службы исполнения наказаний на современном этапе развития уголовно-исполнительной системы: сборник материалов круглого стола (24 июня 2019 года). С. 217-221.

УДК 004+336.74

РОЛЬ И МЕСТО НОВЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРОИСХОЖДЕНИИ КРИПТОВАЛЮТ

Я. В. Долгов аспирант ФГБОУ ВО «Тверской государственный технический университет»

Аннотация Статья посвящена современной виртуальной валюте, криптовалюте, и особой роли информационных технологий при ее создании. Рассмотрены преимущества технологий блокчейн в сравнении с традиционными.

Ключевые слова информационные технологии, цифровая экономика, виртуальная валюта, криптовалюта, блокчейн, Blockchain.

Постановлением Правительства Российской Федерации от 28 июня 2017 года № 1632-р принята программа «Цифровая экономика Российской Федерации» с целью «создания экосистемы цифровой экономики Российской Федерации, в которой данные в цифровой форме являются ключевым фактором производства во всех сферах социально-экономической деятельности и в которой обеспечено эффективное взаимодействие, включая трансграничное, бизнеса, научно-образовательного сообщества, государства и граждан». Это означает внедрение цифровых технологий во всех видах деятельности граждан Российской Федерации. В ней указывается, что «основными сквозными технологиями, которые входят в рамки настоящей Программы, являются системы распределенного реестра». В соответствии с этим необходимо рассмотреть влияние данных технологий на экономическую и финансовую деятельность бизнеса, государства и граждан.

В современном мире появились и все более получают распространение виртуальные валюты, в основе которых лежат новые информационные технологии интернета и блокчейна.

Блокчейн (от англ. Blockchain – цепочка блоков) – база данных, которая хранится одновременно на множестве компьютеров. Новые блоки в базе-цепочке создаются постоянно. Каждый вновь созданный блок содержит группу накопившихся за последнее время и упорядоченных записей (транзакций), а также заголовок. Когда блок сформирован, он проверяется другими участниками сети и если все согласны, подсоединяется к концу цепочки. После этого внести в него изменения уже невозможно. Кроме новой информации блок хранит в зашифрованном виде данные о предыдущих блоках. База автоматически обновляется на всех компьютерах системы. Вероятность, что все они будут выведены из строя мала и пока хотя бы один компьютер сети работает, система, основанная на блокчейн, существует.

Таким образом, сущность технологии блокчейн – отсутствие центрального сервера, а хранение, пополнение и поддержание реестра пользователей обеспечивается за счёт одноранговых сетей. Это позволяет подтверждать подлинность источника, управлять идентификацией, легко регистрировать и обновлять события и т. п.

Из сказанного выше следуют основные принципы технологии блокчейн:

- децентрализация и распределенность;
- безопасность и защищенность;
- открытость и прозрачность;
- неизменность уже записанного.

Рассмотрим сущность данных принципов технологии блокчейн.

Любую централизованную базу данных можно внести несанкционированные изменения. Взломать один из блоков блокчейн и изменить в нем информацию не имеет смысла, так как необходимо ломать все блоки и их копии на всех компьютерах. Для этого нужны огромные вычислительные мощности. Препятствием является алгоритм шифрования с использованием хеш-функций и цифровой подписи. В подписи используется два ключа – открытый и закрытый. Первый необходим для проверки самой подписи, второй используется при ее создании и является секретным. Ключи обеспечивают доступ участникам к той или иной информации. Хеш-функция выглядит, как последовательность случайных цифр и букв, которая обеспечивает неизменность всех записанных данных. Каждый пользователь может изменять только ту часть цепочки, к которой имеет ключ. Без наличия такого ключа запись нового блока, подписанного пользователем, невозможна.

Блокчейн позволяет реализовать технологию токенизации, основной принцип которой заключается в подмене реальных конфиденциальных данных некими значениями-токенами. Этот способ считается наиболее безопасным, он обеспечивает сохранение конфиденциальных данных.

Токены предназначены для электронного удостоверения личности (например, клиента, получающего доступ к банковскому счету), при этом они могут использоваться как вместо, так и вместе с паролем. Токен - это электронный ключ для доступа к чему-либо. Назначение токенов заключается в оплате услуг сети по предоставлению конфиденциальности и защиты от слежки за личными данными и от действий ограничивающих свободу слова.

Вся база находится в публичном доступе и посмотреть данные того или иного блока может любой пользователь. О факте перевода денег может узнать каждый пользователь, а кто и кому перевел – тайна, доступная только участникам обмена.

Блокчейн позволяет напрямую обмениваться данными без участия каких-либо посредников. Подлинность транзакций в системе проверяют непосредственно ее участники.

Участников сети разделяют на пользователей и майнеров (строителей блоков). Чтобы стать майнером, достаточно выделить мощности своего компьютера для выработки новых блоков и подключиться к сети с помощью специального программного обеспечения. Пользователи создают в сети новые записи-транзакции, а майнеры из них формируют блоки. Записи подтверждаются и вносятся в блок только в том случае, если с этим согласно большинство пользователей. Остальные игнорируются и не считаются достоверными, пока не попадут в содержимое одного из последующих блоков. Воспользоваться той или иной записью может только владелец ключа, открывающего к ней доступ.

Выделяют несколько основных видов блокчейна.

1. Открытый блокчейн (public blockchain) – блокчейн, в котором нет ограничений на использование блоков, несмотря на то, что данные блоков зашифрованы, а также на отсылку транзакций для включения в блокчейн. Его разновидностью является общедоступный (инклюзивный) блокчейн (permissionless blockchain) – блокчейн, в котором нет ограничений на пользователей, которые могут создавать блоки и осуществлять транзакции.

2. Закрытый блокчейн (private blockchain, consortium blockchain platform) – это блокчейн, в котором доступ к данным и к отправке транзакций ограничен определенным кругом субъектов. Закрытый блокчейн более дешев и имеет более высокую производительность, чем открытый. Однако открытый блокчейн более эффективен и удобен в использовании.

3. Эксклюзивный блокчейн (permissioned blockchain) – это блокчейн, в котором размещение информации и обработка транзакций осуществляются определенным списком субъектов, личность которых с установлена. Доступ к эксклюзивному блокчейну может иметь разные степени открытости:

- чтение транзакций возможно с ограничениями (например, у клиента может быть доступ к транзакциям, которые затрагивают только его);
- предложение транзакций только для включения в блокчейн;

- создание только новых блоков транзакций и добавление блоков в блокчейн.

Выбирают разные варианты блокчейна с учетом требований, возникающих в каждом конкретном случае, например исходя из необходимости заключения умных контрактов и др.

На описанной выше технологии блокчейн строятся разные типы сервисов. Есть публичные наднациональные системы, присоединиться к которым и стать пользователем или майнером может любой желающий. Администрированием такой системы занимается само сетевое сообщество. Есть эксклюзивные блокчейн системы, которые поддерживаются и контролируются своими создателями. Чтобы стать их участником, нужно выполнить некоторые условия организаторов. Майнерами в таких системах могут быть четко определенный круг лиц определенной квалификации.

Исходя из вышесказанного, можно выделить преимущества технологии блокчейна, которые заключаются в следующем:

- отсутствие каких-либо посредников;
- контроль самих пользователей над транзакциями;
- высокая степень защиты и надежности транзакций;
- прозрачности любых изменений в сети для ее участников;
- малое время выполнения транзакций;
- низкие затраты на выполнение транзакций;
- сохранение анонимности при доступе ко всей необходимой информации;
- высокое качество данных, которые актуальны, достоверны и доступны всем пользователям сети.

Поэтому при решении различных практических задач технология блокчейн используется в качестве базовой платформы для практических приложений в различных видах деятельности. Ниже в таблице 1 приведен ряд блокчейн-проектов, отличительные свойства которых обусловили их перспективность.

Таблица 1- Блокчейн-проекты

Наименование проекта	Краткая характеристика проекта
Ethereum	Второй по капитализации проект криптовалют. Его основной идеей является использование умных контрактов, содержащих условия выполнения определенных действий, которые разработчик программирует с помощью встроенного языка сценариев. Каждая запись проверяется всеми заинтересованными сторонами. Недостаток – отсутствие понятных правил взаимодействия с некоторыми реальными процессами (нельзя отследить физическую передачу товара от поставщика к покупателю и т. д.)
Aragon	Реализует концепцию децентрализованных организаций, использующих только цифровые данные. Удобен для создания стартапов. Малые инновационные бизнесы стали первыми пользователями проекта. Планируется введение системы разрешения

	споров, которая позволит привязать исполнение умных контрактов к реальным бизнес-процессам. Позволяет существенно снизить издержки
NEM	Схож с Ethereum, но отличается высокой скоростью обработки транзакций (подтверждение действия занимает несколько секунд), что позволяет конкурировать с биткоином, имеющим меньшую скорость и более высокую стоимость совершения денежных переводов. В отличие от Bitcoin, ориентированного на переводы денег между частными лицами, позволяет осуществлять транзакций на межбанковском рынке. Разработчики работают над увеличением пропускной способности и снижением комиссий
Ripple	Конкурент проекта NEM. Его использование позволяет банкам существенно сократить время и снизить издержки транзакций. Недостаток – непрозрачная система распределения активов (более 50% капитала контролируется разработчиками)
Sia	Децентрализованное облачное хранилище зашифрованной информации на множестве независимых компьютеров, владельцы которых предоставляют часть своей памяти в аренду, создавая так называемую ноду. Доход владельца ноды зависит от стабильности работы его компьютера и сохранности файлов. Пользователь за плату загружает файл в распределенную сеть, файл шифруется и разбивается на блоки, которые загружаются на арендованные компьютеры. Информация многократно дублируется, а умный контракт автоматически выплачивает комиссию владельцам нод в собственной валюте – Siacoin. Стоимость хранения файлов в 10-15 раз ниже, чем у традиционных файловых хостингов, и зашифрованные файлы не могут быть вскрыты по требованию властей
Storj	Распределенное хранилище, практически идентичное Sia
DASH	Криптовалюта с улучшенными характеристиками конфиденциальности и анонимности по сравнению с Биткоином. Обеспечивает неопределенность источника и получателя денежных переводов на уровне протокола сети. Реализован механизм моментального подтверждения транзакций, а также уникальная модель управления и самофинансирования
Maidsafecoin	Предоставляет вычислительные мощности и услуги хранения в децентрализованной системе с оплатой в токенах этой же системы для неконтролируемых цензурой приложений и вебсайтов. Находится в процессе становления и управляется централизованной компанией. Планируется создать всемирную сеть, функционирующую на принципах битторрента
Bitshares	Использует токены для доказательства владения и обмена объектами, в том числе и физическими. Это позволяет торговать и отслеживать смену прав собственности в децентрализованной сети. При этом их текущую цену можно зафиксировать, выразив её в более стабильных единицах, таких как доллар или золото. Может стать платформой для электронной торговли следующего поколения для любого вида объектов.

Многие страны рассматривают возможности технологии блокчейн для использования в государственных учреждениях. Рассматриваются способы внедрения технологии блокчейн в систему голосования на выборах. Китай на блокчейн планирует перевести работу Национального фонда социального страхования и систему «умных городов». На основе технологии блокчейн создаются стартапы в сфере медицины, защиты интеллектуальной собственности, системы идентификации, веб-браузеры, децентрализованные облачные хранилища данных и т. д. Создана виртуальная нация — BITNATION, стать ее гражданином может каждый.

Все больше с использованием технологии блокчейн заключаются умные контракты (смарт-контракты), которые значительно упрощают процедуру подписания договоров, так как нет необходимости привлекать третью сторону, которая выступает гарантом соблюдения условий. Все участники в любой момент могут провести аудит сделки. "Умный контракт" означает событийно-управляемую программу, работающую на распределенном, децентрализованном, коллективно используемом и воспроизводимом реестре, в рамках которой может осуществляться контроль над активами и передачей активов в этом реестре. Это позволяет автоматизировать процесс заключения договора и его исполнения.

В Российской Федерации технологию блокчейн планируют узаконить в 2019 году, приняв необходимые нормативно - правовые акты. Крупные банки совместно с Центробанком уже создали платформу «Мастерчейн», проект «Активный гражданин» с использованием технологии блокчейн действует в Москве для голосования москвичей.

Таким образом, наблюдается широкое внедрение новых информационных технологий блокчейна в различных областях деятельности, что обусловлено рядом их существенных преимуществ перед традиционными. Очевидно, что криптовалюта обладает значительными преимуществами над классической финансовой системой. Поэтому появляются новые крипто-платформы, позволяющие дешевле и быстрее переводить деньги.

Для цитирования: Долгов Я.В. Роль и место новых информационных технологий в происхождении криптовалют // Актуальные вопросы информатизации Федеральной службы исполнения наказаний на современном этапе развития уголовно-исполнительной системы: сборник материалов круглого стола (24 июня 2019 года). С. 221-226.