УДК 336.717

А.К. СУПИБЕКОВА
КЫРГЫЗСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СТРОИТЕЛЬСТВА, ТРАНСПОРТА И АРХИТЕКТУРЫ ИМЕНИ Н. ИСАНОВА, Г. БИШКЕК, КЫРГЫЗСКАЯ РЕСПУБЛИКА
E-MAIL: <ALTYNAYS@MAIL.RU>
A. K.SUPIBEKOVA
KYRGYZ STATE UNIVERSITY OF CONSTRUCTION, TRANSPORT AND ARCHITECTURE NAMED AFTER N. ISANOV, BISHKEK, KYRGYZ REPUBLIC
E-MAIL: ALTYNAYS@MAIL.RU

Г.А. ЭСЕНАЛИЕВА
КЫРГЫЗСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СТРОИТЕЛЬСТВА, ТРАНСПОРТА И АРХИТЕКТУРЫ ИМЕНИ Н. ИСАНОВА, Г. БИШКЕК, КЫРГЫЗСКАЯ РЕСПУБЛИКА
E-MAIL: ALTYNAYS@MAIL.RU
G. A.ESENALIEVA
KYRGYZ STATE UNIVERSITY OF CONSTRUCTION, TRANSPORT AND ARCHITECTURE NAMED AFTER N. ISANOV, BISHKEK, KYRGYZ REPUBLIC
E-MAIL: ALTYNAYS@MAIL.RU

E.mail. ksucta@elcat.kg

ПРИМЕНЕНИЕ SMART-CONTRACT В ПЛАТФОРМЕ ETHEREUM

USAGE OF SMART-CONTRACT IN THE ETHEREUM PLATFORM

Макалада финансылык технологиялар, Blockchain технологиясы, Эфириум платформасы жана Smart-contract каралган. Аталган технологиялардын ар кандай класстагы маселелерде колдонулушунун өзгөчөлүктөрү жана кемчилдиктери. Аталган технологиялардын артыкчылык жактары жана колдонулушу боюнча жалпы бүтүмдөр талкууланган.

Чечүүчү сөздөр: *финансылык технологиялар, Blockchain, Эфириум, Smart-contract.*

В статье рассматриваются финансовые технологии, технология- Blockchain, Эфириум - платформа на базе блокчейна и Smart-contract. Приводятся преимущества и недостатки каждой из технологий для разных классов задач и общие выводы о применимости технологий.

Ключевые слова: *финансовые технологии, Blockchain, Эфириум, Smart-contract.*

Financial technologies are examined in the article, Blockchain technologies, Ethereum and Smart - contract. Advantages over and lacks of each of technologies for the different classes of tasks and general conclusions are brought about applicability of technologies.

Key words: *financial technologies, Blockchain, Ethereum, Smart-contract.*

Технология Blockchain — это технология распределенного реестра, которая использует распределенный, децентрализованный, разделенный между пользователями и воспроизводимый реестр[1]. Такой реестр может быть частным или публичным, открытым или закрытым, основываться на криптоэкономике токенов или функционировать без токенов. Данные внутри реестра защищены методами

криптографии. На каждом узле (нода) храниться полная база транзакций, проц… вычисления блока называется майнинг (шахтерство, добыча). Связь основана на протоколе Peer-to-peer.

Каждая сделка или транзакция записывается и добавляет в цепочку распределенной базы данных новый фрагмент, который хранит данные о времени, дате, участниках, сумме сделок и, что важно, информацию о всей сети. Сложные математические алгоритмы и специальные программы следят за целостностью и общедоступностью системы.

Следует уточнить, что в этой сети может осуществляться трансфер не только валюты, но и других ценностей. К примеру, блокчейн позволит отследить всю цепь поставки того или иного товара от производителя, до потребителя, позволяет заключать смарт-контракты, хранить распределённые базы документов, проводить подсчет голосов избирателей и много другое.

Данная технология заинтересовала и активно финансируется крупными мировыми банками. Такая заинтересованность основана на доверии участников сети, прозрачности операций, сокращении бумажной и документной волокиты, сохраняет время для обработки всех операций. Во многом, участники транзакций смогут отказаться от услуг третьих сторон,

Основное преимущество блокчейна перед традиционными банковскими транзакциями — отсутствие посредников[1].

Умный контракт (англ. *Smart contracts*) — электронный алгоритм, описывающий набор условий, выполнение которых влечет за собой некоторые события в реальном мире или цифровых системах[2]. Для реализации умных контрактов требуется децентрализованная среда, полностью исключающая человеческий фактор, а для возможности использования в умном контракте передачи стоимости требуется криптовалюта.

Объекты умного контракта:

- подписанты — стороны умного контракта, принимающие или отказывающиеся от условий с использованием электронных подписей. Прямым аналогом является подпись отправителя средств в сети Bitcoin, которая подтверждает внесение транзакции в цепочку блоков.
- предмет договора. Предметом договора может являться только объект, находящийся внутри среды существования самого умного контракта, или же должен обеспечиваться беспрепятственный, прямой доступ умного контракта к предмету договора без участия человека.
- условия. Условия умного контракта должны иметь полное математическое описание, которое возможно запрограммировать в среде существования умного контракта. Именно в условиях описывается логика исполнения пунктов предмета договора.

Для того, чтобы умные контракты[3] могли существовать, требуются определенные условия:

1. Использование широко распространенных методов электронной подписи на основе публичных и приватных ключей (асимметричное шифрование).
2. Существование открытых, децентрализованных и доверительных сторонам контракта баз данных для исполняемых транзакций, работа которых полностью исключает человеческий фактор. Как пример: цепочка блоков в Bitcoin.
3. Децентрализация среды исполнения умного контракта. Как пример: Ethereum, Codius.
4. Достоверность источника цифровых данных. Как пример: корневые центры сертификации SSL в базах современных интернет-браузеров.

Ethereum (от англ. *ether* —«эфир»), **Эфириум-** платформа для создания децентрализованных онлайн-сервисов на базе блокчейна, работающих на базе умных контрактов [4]. Реализована как единая децентрализованная виртуальная машина. Был предложен Виталиком Бутериным в конце 2013 года, сеть была запущена 30 июля 2015

года. Являясь открытой платформой (*open source*), Ethereum значительно упрощ… внедрение технологии блокчейн, что объясняет интерес со стороны не только у новых стартапов, но и крупнейших разработчиков ПО, таких как Microsoft, IBM и Acronis. Заметный интерес к платформе проявляют и финансовые компании, включая Сбербанк.

Цель Эфириума — создание альтернативного протокола для децентрализованных приложений, обеспечивающего набор компромиссов, полезных для большого класса децентрализованных приложений, с особым акцентом на тех ситуациях, когда скорость развития, безопасность для малых и редко используемых приложений, а также способность различных приложений очень эффективно взаимодействовать.

Эфириум достигает этого, обеспечивая фундамент: блокчейн с функционально полным языком программирования. Этот фундамент позволяет любому писать смарт-контракты и децентрализованные приложения, где можно реализовать произвольные правила собственности, форматы сделок и правила регистрации [4].

Экономический смысл. Технология Ethereum дает возможность регистрации любых сделок с любыми активами на основе распределенной базы контрактов типа блокчейн, не прибегая к традиционным юридическим процедурам. Эта возможность является конкурентной по отношению к существующей системе регистрации сделок. Блокчейновые технологии могут быть успешно совмещены с банковскими услугами удаленного типа, предоставляемыми через СМС-сообщения[4].

Программная реализация. Умные контракты в Ethereum представлены в виде классов, которые могут быть реализованы на различных языках, включая визуальное программирование и компилируются в байт-код для виртуальной машины Эфириума (Ethereum Virtual Machine, EVM) перед отправкой в блокчейн. Изменение состояния виртуальной машины может быть записано на полном по Тьюрингу языке сценариев [4].

Блок транзакций — специальная структура для записи группы транзакций.

Чтобы транзакция считалась достоверной («подтверждённой»), её формат и подписи должны проверить и затем группу транзакций записать в специальную структуру — блок. Информацию в блоках можно быстро перепроверить. Каждый блок всегда содержит информацию о предыдущем блоке [4]. Все блоки можно выстроить в одну цепочку, которая содержит информацию обо всех совершённых когда-либо операциях в этой базе. Самый первый блок в цепочке — первичный блок — рассматривается как отдельный случай, так как у него отсутствует родительский блок. Блок состоит из заголовка и списка транзакций. Заголовок блока включает в себя свой хеш, хеш предыдущего блока, хеши транзакций и дополнительную служебную информацию. В системе Биткойн первой транзакцией в блоке всегда указывается получение комиссии, которая станет наградой пользователю за созданный блок. Далее идут все или некоторые из последних транзакций, которые ещё не были записаны в предыдущие блоки. Для транзакций в блоке используется древовидное хеширование (рис.1).

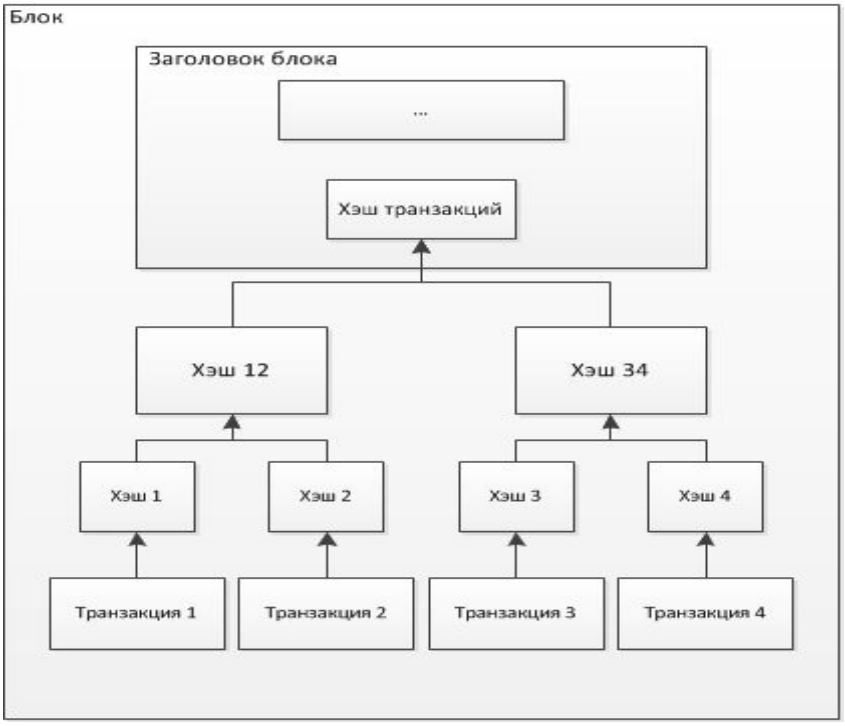

Рис.1. Схема получения хеша транзакций

Умные контракты можно использовать в разных финансовых продуктах:

- партнерские программы;
- страхование;
- периодические платежи;
- торговля.

Можно привести простой пример того, как умный контракт[5] может использоваться уже сейчас. Например, два человека хотят сыграть в тотализатор и поставить на один и тот же матч. Их ставки сохраняются в блокчейне. После окончания матча смарт-контракт проверяет результат и передает выигрыш победителю.

В будущем подобные контракты смогут легко контролировать исполнение и более сложных обязательств. Например, человек снимает жилье, но вовремя не успел заплатить за аренду. Компьютерная программа блокирует замок в квартиру и арендатор не может открыть ее. Перспективы развития действительно огромные.

На рис. 2. представлена схема работы умных контрактов.

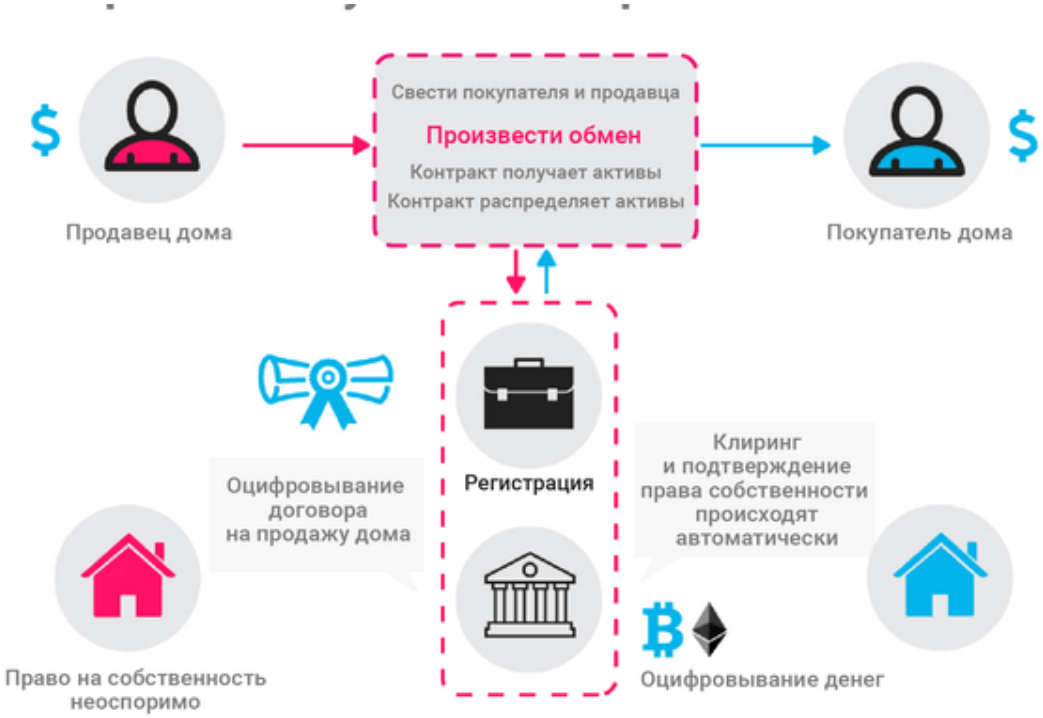

Рис. 2. Схема умных контрактов

Возможности распределенного реестра. Реестр[6] помогает пользователю определить размеры еще не использованных ресурсов. Для криптовалют это его баланс. Информацию о ресурсах, которыми может оперировать пользователь, получают все участники сети.

Технология криптовалют может использоваться для подтверждения права пользования ресурсом. Это криптографическая задача, которая, как правило, заключается в демонстрации знания пары криптоключей, связанных с этим ресурсом.

Кроме того, реестр позволяет указывать правила для следующего владельца передаваемого ресурса, которые он должен выполнить, чтобы подтвердить свое право на владение. Это может быть криптографическая задача из предыдущего пункта, а может быть что-то другое. Для криптовалют типа биткоин в общем случае это выглядит следующим образом: «Вот биткоины, которые я хочу переместить (например, оплатить покупку). Вот доказательство моих прав на перемещение, а вот то, что должен сделать получатель, если хочет их потратить». Напомним, что распределенный реестр обладает механизмами, поддерживающими согласие всех узлов относительно хранимых в нем данных (рис.3).

Для ускорения процесса предлагается использовать так называемые сайдчейны[6] (sidechain) — централизованные кошельки, в которые можно переслать криптовалюту и использовать ее уже по правилам этого кошелька. Сайдчейны отличаются от простых кошельков тем, что проводят проверку вашей цепочки блоков и сами тоже представляют собой цепочки блоков.

Использование сайдчейнов позволяет для некоторых вариантов перевода использовать механизмы, отличные от базовой системы, гибко настраивая соотношение скорости перевода средств и уровня безопасности.

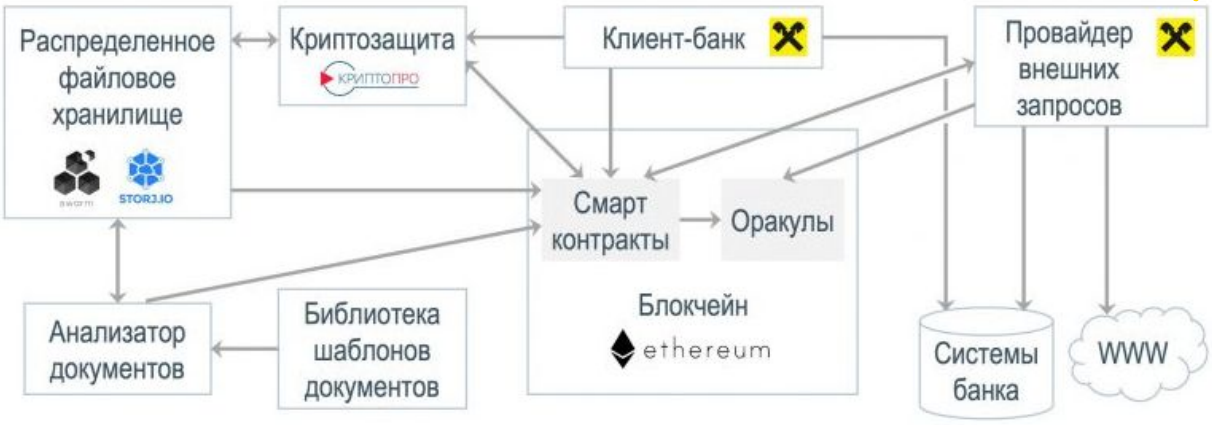

Рис. 3. Технологическая платформа для торгового финансирования

Умные контракты (Smart contracts) могут кардинально изменить взаимоотношения сторон в области права и финансов[7]. С развитием «интернета вещей», когда почти все бытовые устройства будут подключены к общей сети, Ethereum за счет смарт-контрактов может войти в жизнь обычных пользователей. Среди его особенностей стоит выделить:

- высокая степень защиты пользователя за счет авторизации через криптографические подписи, при условии, что он хранит их на записывающих устройствах, которые не подключены к сети, например, обычных флешках;
- устойчивость к DDoS-атакам[7];
- история всех транзакций хранится в блокчейне.

Технологические возможности экосистемы блокчеина позволяют реализовать платформу автоматического исполнения операции торгового финансирования на базе смарт-контрактов.

Список литературы

1. Технология Blockchain [Электронный ресурс] Режим доступа: http://blockchain.info
2. Что такое умные контракты [Электронный ресурс] Режим доступа: http://prizm24.ru
3. Умный контракт[Электронный ресурс] Режим доступа: http://bankir.ru
4. Эфириум [Электронный ресурс] Режим доступа: https://www.ethereum.org/
5. Умный контракт: биткоин как двигатель банковских технологий [Электронный ресурс] Режим доступа: http://bankir.ru
6. Концепции развития умных контрактов: биткоин и Ethereum [Электронный ресурс] Режим доступа: http://forklog.com
7. Децентрализованные платформы для смарт-контрактов [Электронный ресурс] Режим доступа: http://forklog.com