УДК 009.338, 365

Макаров А.М.[1]
Киселев В.В.[2]
Голякова А.О.[3]
Осинин И.Д.[4]
Постовалов С.С.[5]

ВНЕДРЕНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ БЛОКЧЕЙН В СИСТЕМАХ ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА КАК ВОЗМОЖНОСТЬ СОЗДАНИЯ «УМНЫХ ГОРОДОВ» СЕВЕРНОГО КАВКАЗА

Аннотация. В предлагаемой статье рассмотрены общие принципы построения систем с распределенным реестром, в основе которых положены методы криптографии, созданы модели абонентов, которые состоят из определения сведений о том, что умеет (может) делать абонент и того, что абонент не умеет (не может) делать. Приведены примеры алгоритмов и моделей взаимодействия основных участников блок-хэшчейн сети, для регистрации оплаты ЖК услуг, составленные в результате исследований проведенных группой ученых студентов в течение 2016-2018 гг. в рамках инициативной научной работы под руководством профессора Пятигорского государственного университета Анатолия Макарова.

Ключевые слова: блокчейн сети, блокчейн, хэшчейн, распределенный реестр, цифровая экономика, цифровые технологии.

Makarov A.M.
Kiselev V.V.
Golyakova A.O.
Osinin I.D.
Postovalov S.S.

IMPLEMENTATION OF BLOCKCHAIN DIGITAL TECHNOLOGIES IN HOUSING AND COMMUNAL SERVICES AS AN OPPORTUNITY TO CREATE “SMART CITIES” IN THE NORTH CAUCASUS

Abstract. The present paper describes the general principles of constructing systems with a distributed registry, which are based on cryptography methods. Authors create subscribers’ models that

[1] *Макаров Анатолий Михайлович*, доктор технических наук, профессор кафедры инфокоммуникационных технологий, математики, информационной безопасности, Пятигорский государственный университет, e-mail: mellin_22@mail.ru
Anatoly Makarov, Doctor of Engineering Science, Professor, Department of Information and Communication Technologies, Mathematics, Information Security, Pyatigorsk State University, e-mail: mellin_22@mail.ru
[2] *Киселев Виктор Васильевич*, доктор биологических наук, профессор, профессор кафедры инфокоммуникационных технологий, математики, информационной безопасности, Пятигорский государственный университет
Viktor Kiselev, Doctor of Biological Science, Professor, Department of Information and Communication Technologies, Mathematics, Information Security, Pyatigorsk State University
[3] *Голякова Анна Олеговна*, ведущий инженер-программист ООО «Сервис-Инфо», г. Пятигорск, e-mail: anya_gol17@mail.ru
Anna Golyakova, Leading software engineer PLC “Service-Info”, e-mail: anya_gol17@mail.ru
[4] *Осинин Илья Дмитриевич*, магистрант кафедры систем управления и информационных технологий, Северо-Кавказский федеральный университет, г. Пятигорск, e-mail: leron.vinen@mail.ru
Ilya Osinin, Graduate Student, Department of Information Security, Systems and Technologies, North Caucasus Federal University, e-mail: leron.vinen@mail.ru
[5] ***Постовалов Степан Сергеевич,*** ведущий разработчик “Sigma-servis”, e-mail: poroh20100@yandex.ru
Stepan Postovalov, Leading developer “Sigma-servis”, e-mail: poroh20100@yandex.ru

define information about what the subscriber can do and what the subscriber cannot do. The paper gives examples of algorithms and models of interaction between the main participants of the block-hashchain network for registering payment for housing and communal services. These algorithms and models are the result of a scientific research carried out by a group of student-scientists during 2016–2018 within the limits of the initiative scientific work under the guidance of Anatoly Makarov, Professor of the Pyatigorsk State University.

Keywords: network, blockchain, hashchain, a distributed registry, and the digital economy, digital technologies.

Пространственные изменения в обществе состоят не только в системе расселения людей и экономической активности, но и в изменениях информационного пространства людей и регионов. Информационное пространство должно быть равномерно интегрировано и вширь, и вглубь всех слоев населения городов и регионов с целью объединения всевозможных аспектов обмена индивидуумов и властных структур достоверной информацией в распределенном информационном пространстве. При этом к нему предъявляются требования достоверности, прозрачности, верификации, целостности данных или в общем – информационной безопасности и защиты информации.

В настоящее время за рубежом интенсивно развивается подход, для решения такой всеобъемлющей задачи, основанный на цифровых технологиях блокчейн и хэшчейн [1–5].

Основным звеном «умного» города является жилищно-коммунальное хозяйство городов муниципальных образований. Предлагаемая работа и посвящена решению поставленной в работе задачи.

В начале XXI века вследствие нестабильного финансового положения возникла необходимость создания альтернативы всем существующим банковским традициям. Решение появилось в октябре 2008 г. и называлось «блокчейн» от английского «цепочка блоков» [1–3]. Некто под псевдонимом Сатоши Накамото, который переводится как «фундамент просветленного мышления», предложил миру алгоритм, не использующий посредников и не взимающий комиссий, предоставляющий анонимность, но при этом обеспечивающий прозрачность всех транзакций.

В 1983 году Дэвид Чаум, из Калифорнийского университета в Санта-Барбаре, предложил использовать алгоритм «слепой подписи», позволявший провести секретную сделку между двумя абонентами, сообщая при этом о самом ее факте всем участникам сети при сохранении приватности абонентов участников транзакции.

Британец Адам Бэк в 1997 г. изобрел механизм создания криптовалюты, используя систему защиты от спама Hashcash. В этом алгоритме отправитель совершает множество длительных по времени операций, а получатель быстро проверяет их подлинность.

В блокчейне все проведенные транзакции хранятся в блоках, связанных между собой специальным алгоритмом. Нельзя незаметно изменить информацию в блоке, так как изменение данных повлечет изменения во всей цепочке блоков. В системе существуют пользователи и майнеры. Пользователи создают блоки и внутренние хэши, а майнеры встраивают их в цепь и создают внешние межблочные хэши [4, 5].

Первым преимуществом блокчейна является то, что база блокчейна децентрализована, копии хранятся у каждого пользователя, что делает вмешательство в базу маловероятным, а так же используемые в соединении блоков хэш-функции являются односторонними и криптостойкими.

Вторым преимуществом является отсутствие посредников. Транзакция происходит на прямую от абонента А до абонента Б. Майнер только оказывает услугу, подтверждая транзакцию.

Третье преимущество – надежность. Блокчейн абсолютно прозрачен и хорошо защищен от фальсификации данных, так как используются технологии цифровой электронной подписи.

К недостаткам относится [6], трудности в

масштабируемости, огромные затраты электроэнергии и постоянно увеличивающийся вес базы. Также криптовалюта пока слабо регулируется законом, позволяя совершать нелегальные сделки.

В 2012–2017 г. интенсивно стали развиваться технологии блокчейн и хэшчейн. Не смотря на то, что блокчейн появился как решение в экономической сфере, он нашел применение и в других отраслях, в числе которых: организация частного и государственного управления, авторство и право владения, энергетика и т.д. Дальнейшее развитие применения технологии блокчейн получило в работах [7–10].

Успехи в государственном управлении с применением блокчейн-технологий показывает Эстония, где введена единая государственная электронная система. Децентрализованная структура сети соединяет между собой различные сервисы и базы данных. По данным на 2016 год: 94% граждан имеют электронное удостоверение; 2% ВВП страны сэкономлено на безбумажной работе государства; более 4000 сервисов предоставляются электронно.

Также в Эстонии реализуются проекты в сфере здравоохранения. На базе блокчейн-стартапа Guardtime создается единая медицинская база, которая помогает обмену информацией между больницами и страховыми компаниями. Аналогичными разработками занимаются компания Prescrypt в Нидерландах, и BitHealth в США.

Введение блокчейна в отрасли ведения земельного кадастра решает такие проблемы, как мошенничество, коррупция, наличие ошибок в документах т.д. Например, в Грузии при помощи компании BitFury уже существует блокчейн-система кадастрового учета, содержащая более 200.000 записей. Похожим образом обстоят дела в Швеции при помощи компании ChromaWay и в Гане, при помощи BitLand.

Пример, иллюстрирующий применение технологии блокчейн для цифровой идентификации пользователя приведен на Рис. 1.

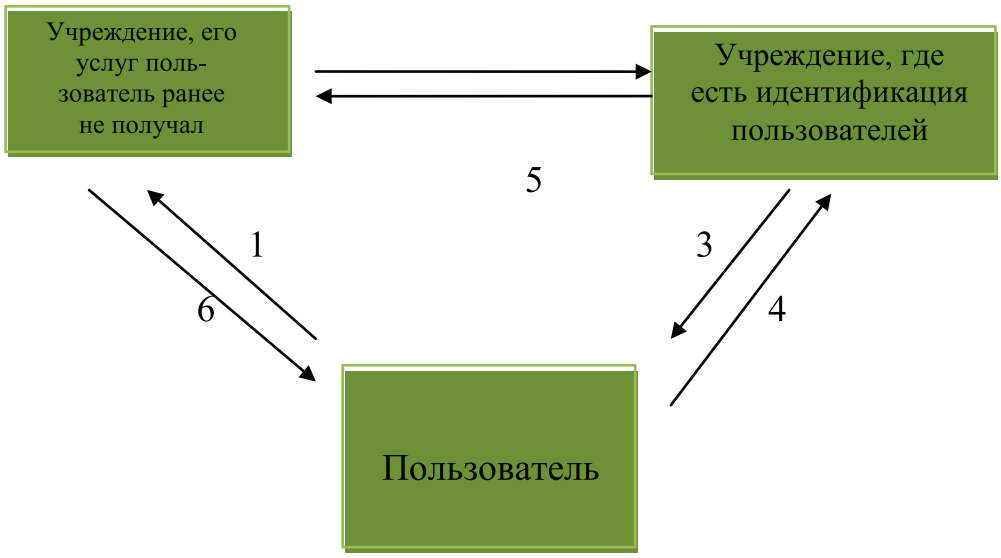


Рисунок 1 – «Алгоритм цифровой идентификации»

1. Запрос пользователя на услугу в учреждение, где его идентификация отсутствует.
2. Запрос этого учреждения на идентификацию в учреждение, где она имеется.
3. Запрос учреждения на подтверждение идентификации.
4. Подтверждение пользователем запроса.
5. Данные пользователя.
6. Предоставление услуги.

С применением блокчейн-технологий появились: цифровое голосование, умные контракты, цифровая идентичность, распределенное облачное хранение и многое другое. Список задач, с которыми могут справиться блокчейн-решения, огромен.

Существует также множество перспективных проектов, как и отдельных блокчейн-сетей, так и в сочетании с такими технологиями, как интернет вещей, обработка больших данных, искусственный интеллект и др. Например,

NASA выдало грант на исследование с применением анализа данных и блокчейн-технологий в области космических исследований. Сочетание блокчейна, интернета вещей и искусственного интеллекта используется при создании решений для «умных городов» (концепция информационно-коммуникационных технологий для управления городским имуществом с целью улучшения качества жизни).

Таким образом, весьма актуально решение задачи создания элементов теории технологий блокчейн-хэшчейн применительно не только к структурам банковской деятельности, но и применительно к технологиям, используемым в системах и структурах народного хозяйства, и одновременно несущими все полезные свойства технологии блокчейн-хэшчейн. Так как в настоящее время нет работ, в которых с единых позиций проводится анализ возможностей блокчейн технологий, с точки зрения их применений в различных областях получения услуг, продукции, товаров, то авторы взяли на себя труд по разработке элементов теории блокчейн-хэшчейн технологий.

В предлагаемой статье приведены результаты исследований проведенных группой ученых студентов в течение 2016–2018 гг. в рамках инициативной научной работы под руководством профессора Пятигорского государственного университета Анатолия Макарова [11].

Целью работы является разработка цифровой теории технологии блокчейн при условии, что абоненты сети не являются профессиональными криптографами и пользователями компьютерных технологий, а пользователи –это рядовые граждане, которые хотят пользоваться всеми преимуществами сервисного обслуживания современными цифровыми технологиями, основанные на методах криптографии и имеющие все вышеописанные преимущества.

Рассмотрим общие принципы построения систем с распределенным реестром, в основе которых положены методы криптографии.

В самом общем виде схема, поясняющая работу N абонентов, представлена на Рис. 1. Здесь цифровые объекты передаются от одного абонента другому с хэшем второго абонента, вычисляемому по хэшу первого абонента, вычисленному по хэшу первого, хэш третьего абонента вычисляется с учетом хэша второго абонента и т.д. Создается хэшчейн последовательность блоков, соединённых хэш-функциями. Хэш-функция, которую легко вычислить, но подобрать входные данные цифрового объекта к нему невозможно называют криптографическими хэш-функциями. Это так называемые односторонние функции:

$$x = f(y), \quad (1)$$

$$y = \varphi(x), \quad (2)$$

Через *y* легко вычислить *x*, но зная *x* невозможно вычислить *y*.

Из Рис. 2 следует, что вход последующего блока порождает *x* φ, связанную с *x* φi-1, предыдущего блока. Отсюда следует возможный вывод: если изменить данные то, необходимо изменить и хэш-функцию i-2, i-3, …, i-N блоков. Понятно, что такой вариант трудно выполним.



Рисунок 2 – «Блок-схема идеи блокчейн технологии» где, КА1 – компьютер первого абонента, КС – канал связи, КА2 – компьютер первого абонента

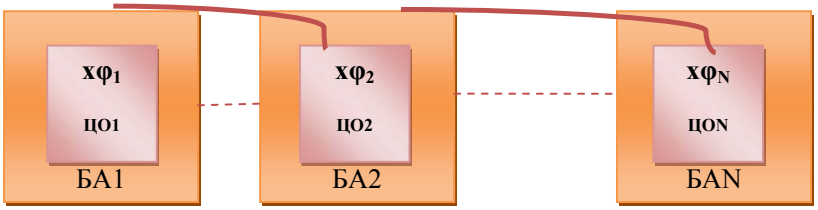


Рисунок 3 – «Блок-схема организации хэшчейна», где хφ1, хφ2… хφN – хэш-функции абонента 1, 2…N; БА1, БА2…БАN – блоки абонентов (полезное тело блока), ЦО1, ЦО2…ЦОN – цифровые объекты заголовка

Анализ приведенных структур показывает, что в общем случае необходимыми участниками сете являются следующие персонажи (рассмотрение структуры блокчейн сети будем вести на примере жилищно-коммунального хозяйства Российской Федерации [13]):

1. Абонент сети, который потребляет услугу.

2. Абонент сети, который оказывает услугу.

3. Абонент сети, который оказывает услугу абоненту потребителю услуги и абоненту, оказывающему услугу, для их комфортного функционирования в сети и исключения необходимости приобретать ими специфические знания профессиональной работы в блокчейн-хэшчейн сети. Этот абонент является аналогом майнера в сетях финансовых транзакций.

4. Абоненты сети, которые оказывают дополнительные услуги специфичные в конкретных ситуациях и конкретных видов применения технологий блокчейн-хэшчейн сетей. Например, отделы госуслуг, единые центры кассовых расчетов и т.д.

Во внутренней структуре блокчейн выделяются четыре основных действующих лица: Абонент-потребитель услуг (АПУ), абонент-оказывающий услугу (АОУ), Абонент, оказывающий услуги участникам сети: АПУ и АОУ – в силу общепринятой технологии назовем его майнером (АМ), удостоверительный центр или Трент (Т).

Для эффективного проектирования сетей необходимо создать модели абонентов, которые состоят из определения сведений о том, что умеет (может) делать абонент и того, что абонент не умеет (не может) делать. Исходя из этих условий, появляется возможность количественно оценивать внутренние и внешние параметры, после чего перекладывать модели абонентов на алгоритмы, которые в свою очередь позволяют писать программы на языках программирования для реализации алгоритмов блок-хэшчейн сети. Критерием принадлежности спроектированной сети к технологии блокчейн является обязательное присутствие таких свойств как:

1. Наличие распределенного реестра.

2. Децентрализация обработки информации.

3. Возможность свободного контроля достоверности данных любым участником (идентификация и аутентификация).

4. Практическая невозможность фальсификации данных любого абонента сети и нарушения их целостности.

Приведем описание моделей основных участников сети.

1. Абонент-потребитель услуг (АПУ) является рядовым потребителем услуг.

1.2. Навыки, которыми АПУ владеет: умеет пользоваться компьютером на базовом уровне, имеет поверхностное представление о работе системы распределённого реестра.

1.3. Навыки, которыми АПУ не владеет: не профессионал в цифровых технологиях, не владеет знаниями о криптографии, не способен создавать «правильные» ключи шифрования, не может самостоятельно защитится от хакерских атак.

1.4. АПУ должен: иметь ключи шифрования и ЭЦП, полученные от удостоверяющего центра, хранить личные ключи шифрования в тайне, быть ознакомлен со спецификой работы в приложениях связанными с блокчейн, и правилами безопасности, иметь компьютер (минимальной конфигурации) с доступом к сети интернет.

2. Абонент, оказывающий услуги (АОУ), является типовым предприятием.

2.1. Навыки, которыми АОУ владеет: владеет компьютером на уровне выше среднего, знает закон о персональных данных, имеет хорошее представление о работе распределенного реестра,

2.2. Навыки, которыми АОУ не владеет: не может создавать «правильные» ключи шифрования

2.3. АОУ должен: иметь ключи шифрования и ЭЦП, полученные от удостоверяющего центра, хранить личные ключи шифрования в тайне, быть ознакомлен со спецификой работы в приложениях связанных с блокчейн, и правилами безопасности, иметь дипломированного специалиста по информационной безопасности. Иметь рабочий сервер с защитой персональных данных и доступом в интернет.

2.4. АОУ имеет право: создавать (с помощью приложения) внутренние блоки и отправ-

лять их в сеть, принимать внутренние блоки от других абонентов, проверять подлинность автора любого внутреннего блока в сети, обращаться к Тренту для получения публичных ключей иных участников сети или личных для себя, хранить и обрабатывать персональные данные АПУ.

3. Абонент-майнер (АМ): является профессиональным криптографом-нотариусом, оказывает услугу другим абонентам сети в части криптографического оформления внешних блоков с включенными внутренними блоками абонентов.

3.1. АМ поддерживает децентрализацию сети блокчейн.

Майнер формирует хеш-функцию внешнего блока и включает его в блокчейн и хешчейн.

Навыки, которыми АМ владеет: профессиональные дипломированные навыки криптографии, полное понимание структуры блокчейн сетей, навыки электротехники и владение компьютером на высоком уровне.

3.2. АМ должен: иметь ключи шифрования и ЭЦП, полученные от удостоверительного центра, хранить личные ключи шифрования в тайне, знать полную структуру работы приложений и сети блокчейн в целом, иметь диплом специалиста по информационной безопасности, иметь сертифицированную технику для формирования внешних блоков, пройти аттестацию перед получением возможности формировать внешние блоки.

3.3. АМ запрещено: создавать внутренние блоки от своего лица, модернизировать данные внутренних блоков иных абонентов, получать конфиденциальную информацию, содержащуюся в зашифрованной части внутреннего блока, удалять блоки (как внешние, так и внутренние).

4. Абонент, оказывающий дополнительные услуги (АДУ) – это удостоверяющий центр или Трент: является государственной структурой занимающейся выдачей, хранением и аудитом ключей шифрования и ЭЦП. Им могут служить службы госуслуг.

4.1. Навыки, которыми владеет АДУ: профессиональные дипломированные навыки криптографии, полное понимание структуры блокчейн сетей, навыки цифровых технологий и владение компьютером на высоком уровне.

4.2. АДУ должен: иметь оборудование для генерации надежных ключей шифрования, предоставлять пользователям ключи шифрования и ЭЦП (как их личные, так и публичные других участников сети), хранить и защищать базу данных всех абонентов и соответствующим им ключей.

Из анализа описанных функций следует, что в любой блок-хэшчейн сети необходимо иметь автоматизированные рабочие места (АРМ).

1) АРМ абонента-потребителя услуг. Основные условия АРМ – абонент не является профессиональным криптографом и, тем более, криптографом-шифровальщиком.

2) АРМ криптографа-нотариуса. Основные условия: оказание услуги абонентам-пользователям и поставщикам услуг.

3) АРМ абонента поставщика услуг. Основное требование – это достоверность предоставленных данных по оплате услуг на основе нормативных документов и законов их регламентирующих.

Приведем пример алгоритм и моделей взаимодействия основных участников блок-хэшчейн сети, для регистрации оплаты ЖК услуг. Все действия выполняются от лица участников, но с использованием программных средств АРМ.

Для последующих выкладок целесообразно ввести следующие обозначения.

Общие параметры:

1. Множество «Абонентов» A_n – множество всех возможных абонентов-клиентов.

1.1. «KCs_{An}» – Закрытый ключ шифрования ЭЦП, используется для шифрации оригинальной стороной.

1.2. «KOs_{An}» – Открытый ключ шифрования ЭЦП, используется для дешифрации другой стороной.

1.3. «KC_{An}» – Закрытый ключ шифрования, используется для дешифрации сообщений оригинальной стороной.

1.4. «KO_{An}» – Открытый ключ шифрования, используется для шифрации сообщений второй стороной. Так же «адрес» абонента.

2. Множество «Поставщиков услуг» P_n

– множество всех возможных поставщиков услуг

2.1. «KCs_{Pn}» – Закрытый ключ шифрования ЭЦП, используется для шифрации оригинальной стороной

2.2. «KOs_{Pn}» – Открытый ключ шифрования ЭЦП, используется для дешифрации другой стороной.

2.3. «KC_{Pn}» – Закрытый ключ шифрования, используется для дешифрации сообщений оригинальной стороной.

2.4. «KO_{Pn}» – Открытый ключ шифрования, используется для шифрации сообщений второй стороной. Так же «адрес» поставщика услуг.

3. Множество «Майнеров» M_n – множество всех возможных майнеров.

3.1. «KCs_{Mn}» – Закрытый ключ шифрования ЭЦП, используется для шифрации оригинальной стороной

3.2. «KOs_{Mn}» – Открытый ключ шифрования ЭЦП, используется для дешифрации другой стороной.

3.3. «KCs_{Mn}» – Закрытый ключ шифрования, используется для дешифрации сообщений оригинальной стороной.

3.4. «KO_{Mn}» – Открытый ключ шифрования, используется для шифрации сообщений второй стороной. Так же «адрес» майнера.

4. Множество «Транзакций» tr_n – множество всех возможных транзакций

5. Множество блоков B_n – все возможные блоки

5.1. «N» – Номер блока цепи.

5.2. «$(tr_1, tr_2, \ldots tr_n)$» – Множество возможных массивов транзакций принадлежащих блоку n.

5.3. «T» – Время создания блока.

5.4. «r» – Случайный параметр.

5.5. «$f_{hasn}(B_{n-1})$» – значение хеша предыдущего блока.

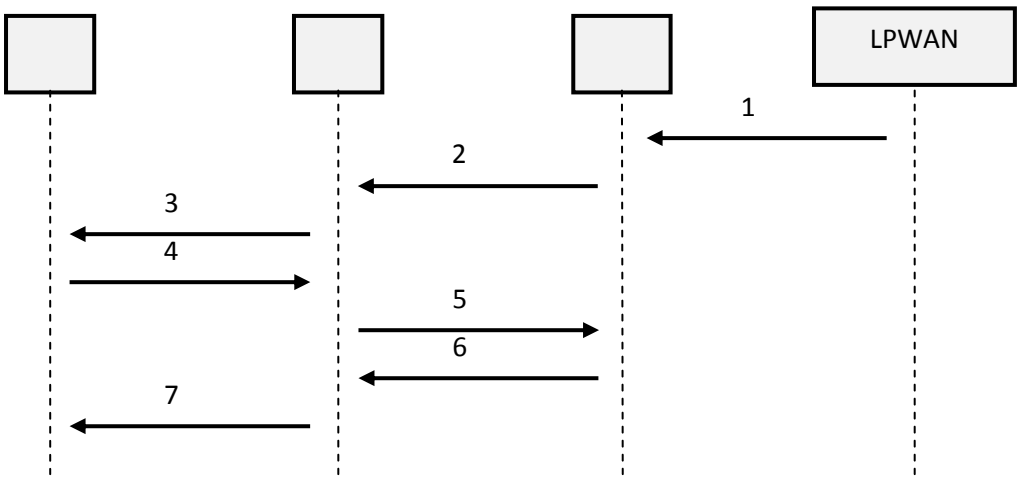


Рисунок 4 – «Алгоритм обмена данными в блокчейне»

1 – Со счетчиков абонента A_1 с радиоканалом снимаются данные с помощью мониторинговой системы LPWAN и передаёт поставщику услуг.

2 – Поставщик услуг P_1: запрашивает открытый ключ шифрования абонента KO_{A1}, формирует счет абонента в XML формате D_P1 и оформляет в свой закрытый блок данных:

$$b_{P1}=f_{ch}(D_{P1}, KO_{A1}) \quad (3)$$

где f_{ch} – функция шифрования,

создает подпись *sig*, генерируя хеш закрытого блока, и зашифровывая своим закрытым ключом ЭЦП KCs_{P1}:

$$sig = f_{ch}(f_{hash}(b_{P1}), KC_{SP1}), \quad (4)$$

где f_{hash} – функция хеширования,

завершает создание транзакции

$$\left["tr"\right]\downarrow P_1",$$

добавляя адреса и момент времени:

$$tr_{P1} = b_{P1} + sig + KO_{A1} + KO_{P1} + T, \quad (5)$$

где T – момент времени.

После, транзакция включается в очередь всех еще не оформленных во внешний бок цепи.

3 – Майнер M_n оформляет внешний блок B_n, в соответствии с правилами:

$$B_n = [N + T + KO_{Mn} + f_{hash}(B_{n-1}) + r + (tr_1, tr_2 \ldots tr_n)], \quad (6)$$

где r – случайный параметр,

для завершения формирования блока майнер, перебирает значения r до тех пор, пока, $f_{hash}(B_n)$ не будет удовлетворять условиям сложности сети (напр. первые 7 символов хеша должны быть нули). После формирования блок включается в общую, доступную для чтения сеть БЧ.

3 – Абонент *A1* находит транзакцию, адресованную ему, получает хеш из подписи, вскрывая ее отрытым ключом ЭЦП KOs_{P1}, формирует хеш блока данных и сравнивает оба хеша, для удостоверения в целостности данных, вскрывает своим закрытым ключом KC_{A1} блок данных и получает XML файл счета. Абонент заполняет счет и отправляет в сеть аналогично 2 пункту алгоритма, используя соответствующие ключи.

Параллельно с этим Абонент A_1 оплачивает счет на сайте государственных услуг, которые отвечают за передачу денег между абонентом и поставщиком услуг.

4 – Работа майнера M_n аналогично пункту 3 алгоритма.

5 – Поставщик услуг P_1 получает и вскрывает из сети подписанный счет абонента. После получения оплаты от государственных структур, поставщик услуг формирует квитанцию об оплате в формате XML аналогично 2 пункту алгоритма, и отсылает в сеть.

6 – Работа майнера M_n аналогично пункту 3 алгоритма.

7 – Абонент A_1 получает и вскрывает из сети квитанцию об оплате. Он точно знает, что счета оплачены и в любой момент может в этом удостоверится.

Примечание – все ключи шифрования участники сети получают от удостоверительного государственного учреждения, по защищенным каналам с меткой времени.

Оценивая итоги проведенной работы, авторы понимают, что в их попытке построения основ теории блок-хэшчейн технологий, изложены основы подхода к проектированию сетей, некоторые аспекты которой носят дискуссионный характер, требуют уточнения, раскрытия, дополнения. В новой науке всегда желательно иметь примерную структуру теории, чтобы теорию совершенствовать и развивать. Надеемся, что работа привлечет ученых для ее более тщательной проработки и развития. В этом и состояла цель работы. Авторы надеются, что свою задачу они в большей мере выполнили.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Nakamoto, S. Bitcoin: Apeer-to-Peer Electronic Cash System. 1st ed. URL: http://www.cryptovest.co.uk/resources/ (Дата обращения: 20.12.2017 г.)
2. Raval S. Decentralized Applications: Harnessing Bitcoin’s Blockchain Technology, O’reilly, Sebastopol, California.
3. Swan M. Blockchain blueprint for a new economy, O’reilly, Sebastopol, California.
4. Robinson A. What is Blockchain Technology, and What Is Its Potential Impact on the Supply Chain? URL: http://cerasis.com/2016/06/29/blockchain-technology/ (Дата обращения: 20.12. 2017 г.)
5. Houy N. The Bitcoin Mining Game. Ledger. p. 151. URL: http://www.ledgerjournal.org/ojs/index.php/ledger/article (Дата обращения 20.12.2017 г.)
6. Smart E. Top 5 Blockchain Technology Myths the Mainstream Has Fallen For. URL: https://bitconnect.co/bitcoin-news/ (Дата обращения: 20.12. 2017 г.)
7. Gilbert D. Blockchain Technology Could Help Solve $75 Billion Counterfeit Drug Problem. Ibtimes. URL: http://www.ibtimes.com (Дата обращения: 20.12.2017 г.)
8. ARMONK, Maersk and IBM Unveil First Industry-Wide Cross-Border Supply Chain Solution on blockchain. URL: https://www-03.ibm.com/press/us/en/pressrelease/51712.wss (Дата обращения 20.12.2017 г.)
9. BitFury Group Limited, Prof of Stake versus Proof of Work, White Paper. URL: http://bitfury.com/content/5-whitepapers-research/pos-vs-pow-1.0.2.pdf (Дата обращения: 20.12.2017 г.)

10. Dickson B. Blockchain has the potential to revolutionize the supply chain. Techcrunch
11. Walch A. The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk. Journal of Legislation and Public Policy. Том 18:837, pp. 851-852.
12. Vorobyev G.A., Ryndjuk V.A., Kozlov V.A., Makarov A.M. PROBABILISTIC MODELS OF CRYPTOGRAPHIC SYSTEMS AND THEIR APPLICATIONS, 3rd International Conference on Digital Information Processing, Data Mining, and Wireless Communications, pp. 160-163.
13. Кемайкин Н.К. Технология блокчейн в сфере жилищно-коммунального хозяйства Дзержинского филиала Нижегородского государственного университета им. Н.И. Лобачевского. URL: https://doi.org/10.24158/pep.2017.11.13 (Дата обращения: 20.12.2017 г.)