ЦИФРОВАЯ ТРАНСФОРМАЦИЯ

УДК 004.056

Макаров А.М.[1]
Киселев В.В.[2]
Писаренко Е.А.[3]
Пономаренко И.А.[4]

ИСПОЛЬЗОВАНИЕ БЛОКЧЕЙН-ТЕХНОЛОГИЙ В СОЦИАЛЬНО-ЭКОНОМИЧЕСКОЙ СФЕРЕ

Аннотация. С проникновением информационных технологий во все сферы жизни и деятельности человека появилась и возможность совершения преступлений в информационной сфере – кражи персональных данных, коммерческой информации, модификации и подтасовки данных и т.п. Поэтому особую роль в современных информационных системах играют средства обеспечения целостности и достоверности данных при их хранении, обработке и передаче по сетям. К таким средствам относятся, в первую очередь, технологии блокчейн. В работе предложено решение задачи адаптации двухключевой системы шифрования при использовании блокчейн-технологий в информационных системах, обеспечивающих процессы в социально-экономических сферах: в ЖКХ, фармацевтическом производстве, в медицинском документообороте и др.

Ключевые слова: информационная безопасность; технологии блокчейн; криптография; защита информации.

---

[1] *Макаров Анатолий Михайлович*, доктор технических наук, профессор кафедры информационно-коммуникационных технологий, математики и информационной безопасности, Пятигорский государственный университет, г. Пятигорск, e-mail: mellin_22@mail.ru, т. (879)3400-000

Anatoly Makarov, Doctor of Technical Sciences, Professor of the Department of Information and Communication Technologies, Mathematics and Information Security, Pyatigorsk State University, Pyatigorsk, e-mail: mellin_22@mail.ru, t. (879)3400-000

[2] *Киселев Виктор Васильевич*, доктор биологических наук, профессор кафедры информационно-коммуникационных технологий, математики и информационной безопасности, Пятигорский государственный университет, г. Пятигорск, e-mail: vikkiselev@yandex.ru, т. (879)3400-000

Victor Kiselev, Doctor of Biological Sciences, Professor of the Department of Information and Communication Technologies, Mathematics and Information Security, Pyatigorsk State University, Pyatigorsk, e-mail: vikkiselev@yandex.ru, t. (879)3400-000

[3] *Писаренко Елена Анатольевна*, кандидат педагогических наук, доцент кафедры информационно-коммуникационных технологий, математики и информационной безопасности, Пятигорский государственный университет, г. Пятигорск, e-mail: gmu41@mail.ru, т. (879)3400-000

Elena Pisarenko, Candidate of Pedagogical Sciences, Associate Professor of the Department of Information and Communication Technologies, Mathematics and Information Security, Pyatigorsk State University, Pyatigorsk, e-mail: vikkiselev@yandex.ru, t. (879)3400-000

[4] *Пономаренко Ирина Алексеевна*, магистрант кафедры информационно-коммуникационных технологий, математики и информационной безопасности, Пятигорский государственный университет, г. Пятигорск, e-mail: irina_20011997@mail.ru, т. 89054104355

Irina Ponomarenko, Graduate Student, Departament of Information and Communication Technologies, Mathematics and Information Security, Pyatigorsk State University, Pyatigorsk, e-mail: irina_20011997@mail.ru, t. 89054104355

Makarov A.
Kiselev V.
Pisarenko E.
Ponomarenko I.

USING BLOCKCHAIN TECHNOLOGIES AND CRYPTOGRAPHY METHODS TO ENSURE THE INTEGRITY AND RELIABILITY OF DATA IN THE SOCIO-ECONOMIC SPHERE

Abstract. With the penetration of information technology in all spheres of human life and activity, the possibility of committing crimes in the information sphere appeared – theft of personal data, commercial information, modification and manipulation of data, etc. Therefore, a special role in modern information systems is played by means of ensuring the integrity and reliability of data during their storage, processing and transmission over networks. Such tools include, first of all, blockchain technologies. The paper proposes a solution to the problem of adapting a two-key encryption system when using blockchain technologies in information systems that support processes in the socio-economic spheres: in housing and communal services, pharmaceutical production, in medical workflow, etc.

Keywords: information security; blockchain technology; cryptography; protection of information

Практически во всех отраслях, куда пришли информационные технологии, возникли и угрозы информационной безопасности. Данные, которые хранятся в электронном виде, легко скопировать, переслать, модифицировать, заменить. Поэтому вместе с удобством, скоростью передачи и огромными объемами накапливаемой и передаваемой информации современные технологии несут с собой и проблемы обеспечения безопасности и достоверности данных [1–3]. Для решения этих проблем в любой отрасли, где требуется верификация и протоколирование определенных действий, можно использовать технологии блокчейн [4].

Особую роль играют технологии блокчейн в экономике, где они тесно связаны с понятием криптовалюты [5, 6]. Однако цифровая экономика не ограничивается цифровой валютой, а обеспечивает безопасность и удобство финансовых сделок [7] и заключения контрактов [8].

В частности, при изготовлении лекарственных средств блокчейн позволяет решать проблему аутентификации лекарственных средств и их компонентов, что обеспечивает защиту от подделок и контрафактных лекарств. В медицинском документообороте использование блокчейна позволит каждому человеку всегда иметь при себе в зашифрованном виде полную электронную медицинскую карту с информацией обо всех заболеваниях, результатах обследования и лечения, аллергических реакциях, группе крови и т.д. [3]. По желанию владельца карты эту информацию сможет увидеть любой врач в любом медицинском учреждении страны. А поскольку информация зашифрована, то без ведома пациента никто не сможет получить к ней доступ. В системе жилищно-коммунального хозяйства блокчейн-процедуры могут использоваться при заключении контракта на поставку коммунальных услуг, при учете потребления, формировании счета на оплату, а также для оплаты услуг и разрешения проблем. Технологии блокчейн позволяют как поставщикам, так и потребителям коммунальных услуг гарантировать точность и достоверность получаемых данных, а также их защиту и неуничтожаемость.

Испанские исследователи предложили использовать IT-инфраструктуру для создания «умных кампусов» и «умных университетов», которые должны быть подключены к узлам интернета вещей [14]. Несмотря на вычислительную сложность и ограниченную масштабируемость, блокчейн-технологии используются для обеспечения безопасности и надежности интернета вещей [15, 16].

Несомненны перспективы применения технологии блокчейн в энергетике [17, 18] и нефтедобывающей отрасли [19], где нужен постоянный жесткий контроль за добычей, передачей и использованием ресурсов.

Представляет интерес идея использования блокчейна для защиты авторских прав [20].

Однако во всех перечисленных моделях применения блокчейн-технологий существуют общие проблемы: обмен ключами шифрования между участниками сети и определение роли майнера в функционировании системы с распределенным реестром. Большинство участников такой сети не являются профессиональными криптографами и вообще ничего не знают о методах шифрования. Но внедрение новых технологий, практически тотальная цифровизация общества во многом меняет уклад жизни людей, делает их зависимыми от качества систем шифрования информации и умения ими пользоваться. Таким образом, возникает общая проблема адаптации человека к новым технологиям и технологий к нуждам и возможностям пользователей. Все это в полной мере относится и к блокчейн-технологиям.

В данной работе сделана попытка решения задачи адаптации двухключевой системы шифрования к процессам передачи и хранения информации на объектах социально-экономической сферы.

Как показал анализ, основную трудность в решении поставленной задачи представляет процедура обмена ключами между участниками сети и определение роли майнера в функционировании системы с распределенным реестром. Критерием качества разработанной системы должна стать не только техническая сторона разработки, но и дружественный интерфейс, удобный как для потребителя, так и для поставщика услуг.

Для создания общей схемы использования блокчейн-технологий в социально-экономических процессах были разработаны модели потребителя услуг, поставщика услуг и майнера.

Для профессиональной деятельности в социально-экономических системах майнер должен получить новую специальность – нотариуса-криптографа. Именно такой специалист будет оказывать услуги по встраиванию внутренних блоков абонентов сети во внешнюю блокчейн-сеть и формировать распределенный реестр.

Разработанные модели ключевых участников блокчейн-сети с распределенным реестром позволяют сформулировать задание на проектирование сетевых криптографических протоколов и мер защиты информации. Должны быть созданы автоматизированные рабочие места абонентов сети, имеющие дружественный и понятный интерфейс. Далее необходимо создать модель Злоумышленника в сети, подобно известной модели Долево-Яо и проработать возможные атаки на протоколы обмена данных сети и меры их ликвидации. В результате появляется возможность создания протоколов двухключевого шифрования и цифровой подписи с хешированием внешних блоков.

Общий принцип встраивания технологии блокчейн в систему документооборота заключается в том, что в распределенном реестре фиксируется вся информация о происходящих транзакциях, и эту информацию уже невозможно будет изменить. Например, в блокчейне должны фиксироваться все предоставленные услуги, выполненные работы, произведенная оплата и т.д.

Схема формирования блоков внутреннего блокчейна и внешнего блока внешней сети блокчейна показана на рисунке 1.

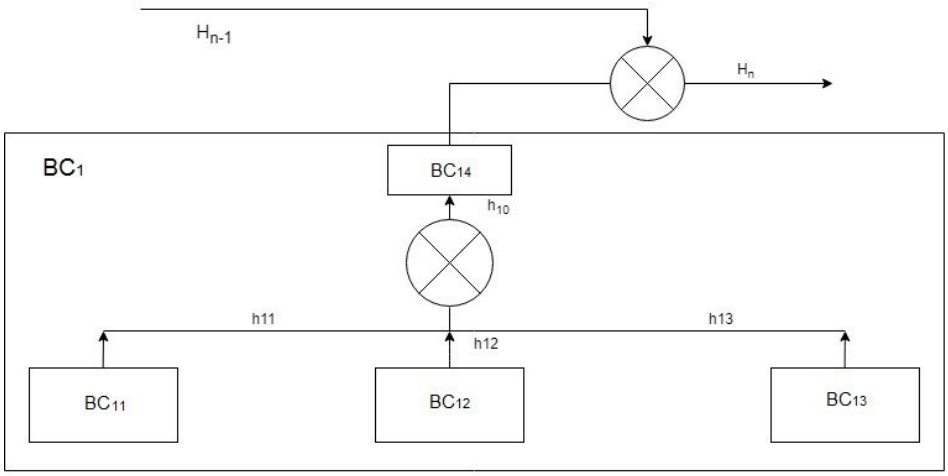


Рисунок 1 – Состав блока внутреннего блокчейна во внешнем блоке сети с распределенным реестром

Обозначения на схеме:

$ВС_{11}$ – блок данных произведенных работ или услуг;

$ВС_{12}$ – блок состава оборудования, участвующего в работах;

$ВС_{13}$ – блок аппаратуры измерения основных параметров произведенных работ и услуг при передаче в следующее звено;

h_{11}, h_{12}, h_{13}, h_{10}, h_{14} – внутренние хэши блоков $ВС_{11}$, $ВС_{12}$, $ВС_{13}$, $ВС_{14}$;

h_{10} – хэш, объединяющий блоки $ВС_{11}$, $ВС_{12}$, $ВС_{13}$;

h_{14} – внутренний, обобщающий хэш блока $ВС_{14}$;

h_n – хэш конечного блока $ВС_{14}$;

H_{n-1} – внешний хэш предыдущего блока;

H_n – n-й внешний хэш нового блока сети.

В результате формируется внутренний блок, который затем будет встроен во внешний блок сети. При изменении каждого бита блоков $ВС_1$, $ВС_2$, $ВС_3$ сразу же изменяется соответствующий хэш, что гарантирует достоверность передаваемых сведений. Таким образом, решается задача отслеживания всех работ, произведенных в соответствующей социально-экономической системе.

Далее на основе внутренних блоков формируется структура внешнего блокчейна (рисунок 2).

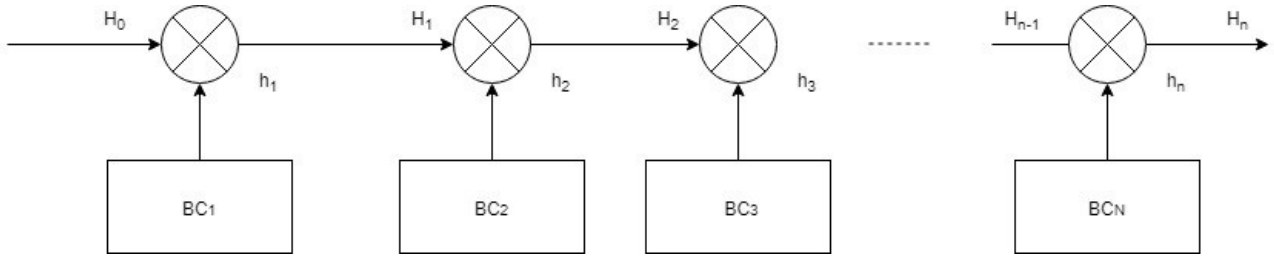


Рисунок 2 – Пример внешней сети формирования хэшей Hn на основе внутренних hn

В приведенной структуре данные в блоках связаны хэш-функциями. Для их изменения необходимо изменить хэш-функции всех предыдущих блоков, что практически невозможно. Распределенный реестр хранится у каждого участника сети, поэтому его практически невозможно модифицировать или уничтожить.

Рассмотренные схемы могут быть положены в основу проектирования сетей с распределенным реестром с использованием методов криптографии для контроля всех процессов, требующих учета в социально-экономических системах.

Взаимодействие между поставщиками и потребителями услуг жилищно-коммунального хозяйства происходит через посредника – управляющие компании. В этой схеме возможны как ошибки, так и различные махинации. Поэтому внедрение технологии блокчейн в систему учета полученных услуг и оплаты за них является, безусловно, актуальным.

На основе анализа работы жилищно-коммунального хозяйства была смоделирована система автоматизированного контроля, учета и оплаты услуг. Данная система моделировалась на основе применения систем распределенного реестра и методов криптографии (технологии блокчейн). Были разработаны алгоритмы подключения нового абонента к сети, автоматизация учета, оплата услуг, формирование счета за пользование услугой, дублирование настоящего договора на оказание услуг [4].

Для того чтобы разработать проект цифровых технологий для организации жилищно-коммунального хозяйства на основе систем распределенного реестра и методов криптографии, нужно для начала схематически представить автоматизированную систему учета, контроля и оплаты услуг. Данная система изображена на рисунке 3.

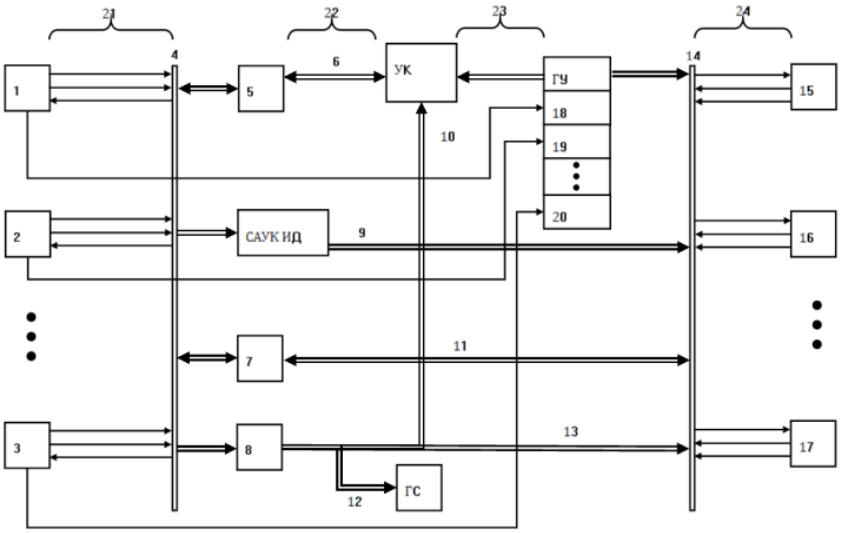


Рисунок 3 – Система автоматизированного учета, контроля и оплаты услуг ЖКХ на основе технологий блокчейн

Обозначения на схеме:

УК – управляющая компания;

ГУ – государственные услуги;

ГС – городские службы;

САУКиИД – система автоматизированного учета по контролю за измерительными датчиками, передачи информации с них по радиоканалу на сервера структур, оказывающих услуги.

1. К i-х абонентов-потребителей услуг 1,2,…,k – рядовые граждане, которые привыкли видеть в своем доме электричество и горячую воду;

2. Блокчейн-сеть 5, или блокчейн контрактов, которые содержат данные обмена между абонентами и управляющей компанией, данные контрактов абонентов и показания со счетчиков при оплате по контракту;

3. Абоненты, оказывающие услуги: 15, 16, м – компании, готовые предоставлять рядовым гражданам вышеописанные удобства за оплату;

4. Блокчейн-сеть 7, которая содержит данные о счетах на оплату от абонентов, предоставляющих услуги и факт оплаты этих счетов абонентами-получателями;

5. Блокчейн-сеть 8, которая дублирует показания счетчиков абонентов в формате, пригодном для считывания управляющей компанией, сервисом государственных услуг и абонентами, предоставляющими услуги;

6. Управляющая компания (УК), выполняющая роль, схожую с ролью майнера. Различие в том, что УК в рамках сети находится в единственном экземпляре и не имеет конкурентов. В дальнейшем она будет называться УК либо просто майнер.

Блокчейн-сеть – совокупность распределенных реестров различных систем, взаимодействующих друг с другом.

При этом создаются распределенные реестры абонентов, потребляющих услуги (21), управляющей компании (22), государственных услуг (23) и абонентов, оказывающих услуги (24).

Алгоритм подключения нового абонента к сети, заключение договора на техническое обслуживание показан на рисунке 4.

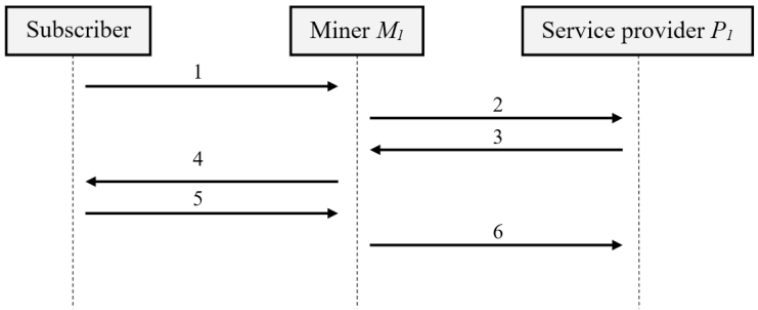


Рисунок 4 – Алгоритмы заключения контракта абонента и поставщика услуг

Обозначения на схеме:

1. Абонент заполняет данные бланка контракта поставщика услуг, зашифровывает их с помощью открытого ключа поставщика, создает электронную цифровую подпись.

2. Майнер оформляет внешний блок с учетом предыдущего хеша внешнего блока цепи блокчейн и данных всех внутренних находящихся в очереди.

3. Поставщик услуг находит в данных внешних блоков сети блокчейн адресованный ему от абонента внутренний блок. Вскрывает его своим секретным ключом шифрования, дополняет свою часть в данные контракта, оформляет свой внутренний блок и посылает его в сеть блокчейн, где блок попадает в очередь всех еще не оформленных во внешний блок цепи.

4. Майнер оформляет внешний блок с учетом предыдущего хеша внешнего блока цепи блокчейн и данных всех внутренних находящихся в очереди. Далее посылает внешний блок по реестру, где тот становится частью блокчейн контрактов.

5. Абонент находит в данных внешних блоков сети блокчейн адресованный ему от поставщика услуг внутренний блок. Вскрывает своим секретным ключом, подписывает данные контракта, оформляет новый внутренний блок. После, направляет в сеть блокчейн, где блок попадает в очередь всех еще не оформленных во внешний бок цепи.

6. Майнер оформляет внешний блок с учетом предыдущего хеша внешнего блока цепи блокчейн и данных всех внутренних находящихся в очереди. После успешного формирования, посылает внешний блок по реестру, где тот становится частью блокчейн контрактов.

Алгоритм оплаты счета поставщика услуг показан на рисунке 5.

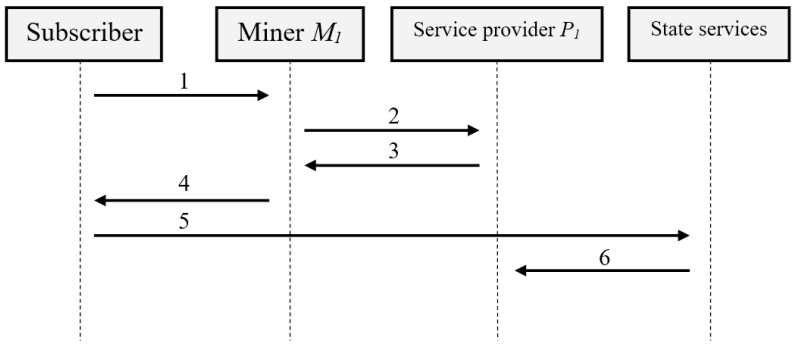


Рисунок 5 – Алгоритм оплаты счета поставщика услуг

Обозначения на схеме:

1. Абонент записывает данные счетчика либо счетчик, поддерживающий автоматическую передачу показаний по сети, считывается ПО. Данные шифруются и подписываются электронной цифровой подписью.

2. Майнер оформляет внешний блок с учетом предыдущего хеша внешнего блока цепи блокчейн и данных всех внутренних находящихся в очереди. После успешного формирования, посылает внешний блок по реестру, где тот становится частью блокчейн контрактов.

3. Поставщик услуг находит в данных внешних блоков сети блокчейн адресованный ему от абонента внутренний блок его своим секретным ключом шифрования. На основании данных поставщик услуг формирует счет на оплату услуг для абонента, шифрует их открытым ключом и подписывает электронной цифровой подписью. После блок попадает в очередь всех еще не включенных во внешние блоки цепи.

4. Майнер оформляет внешний блок с учетом предыдущего хеша внешнего блока цепи блокчейн и данных всех внутренних находящихся в очереди. После успешного формирования посылает внешний блок по реестру, где тот становится частью блокчейн контрактов.

5. Абонент находит в данных внешних блоков сети БЧ адресованный ему от поставщика услуг внутренний блок. Вскрывает своим секретным ключом счет от поставщика услуг

и проводит оплату через Госуслуги посредством личного кабинета.

6. Госуслуги переводят деньги поставщику услуг.

Данная система автоматизированного учета, контроля и оплаты услуг ЖКХ на основе технологий блокчейн позволит организовать взаимодействие между поставщиками и потребителями напрямую, без посредников. Данная система позволит избежать различного рода махинаций.

Для защиты фармацевтического рынка от подделок лекарств необходимо контролировать весь процесс производства и поставок лекарственных средств от заготовки сырья до доставки лекарств в аптеки. Для этого логично использовать технологию блокчейн. Распределенный реестр позволит решить проблему аутентификации лекарственных средств и их компонентов. При заключении договора на поставку лекарственной продукции и обмене контрактами между аптекой и аптечным складом должны заключаться блокчейн-контракты (рисунок 6).

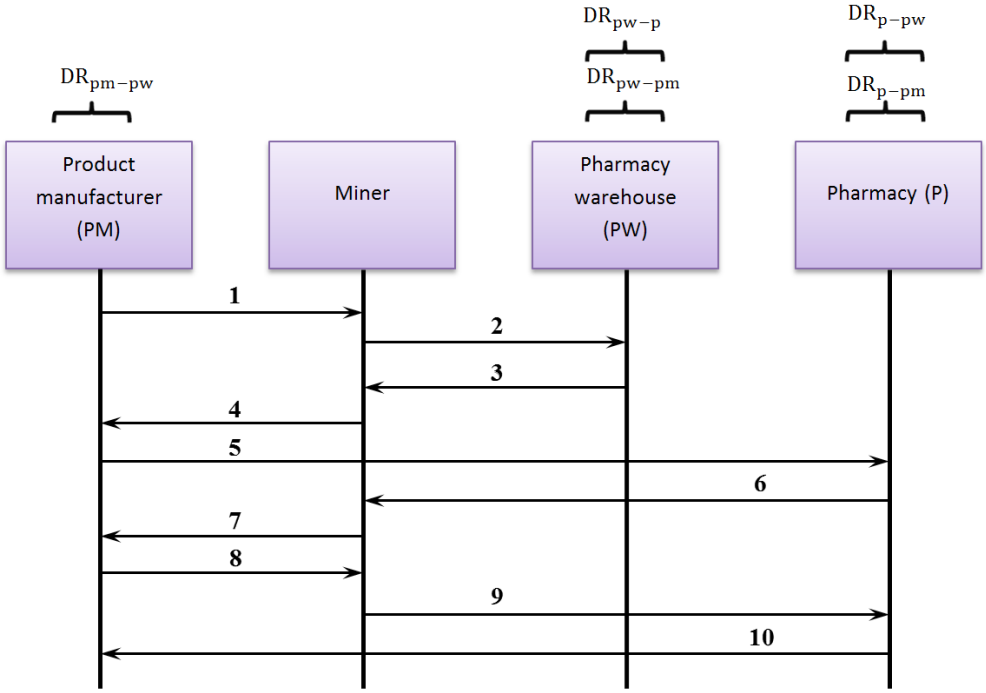


Рисунок 6 – Структурная схема договора на поставку продукции

DRwp-p-распределенный реестр между аптекой и складской аптекой

1. Производитель продукта формирует свой внутренний блок с внутренним хэшем:

$$h_{pm} = f(D, K_{pub(pm)}, K_{pr(pm)}, S_{pm}, Z_{pm})$$

D – блок данных;

Kpub (pm) – открытый ключ PM;

КПР(ПМ) – ПМ закрытый ключ;

Цифровая подпись Spm – PM;

МНТ – заголовок блока.

Затем он отправляет внутренний блок в сеть для встраивания во внешнюю блокчейн-сеть.

2. Майнер, приняв блок, формирует внешний хэш:

$$H_{pm} = f(h_{pm}) = f(h_{pm}, D, K_{pub(pm)}, K_{pr(pm)}, S_{pm}, Z_{pm})$$

Этот хэш является функцией внутреннего хэша и внешнего хэша предыдущего сетевого блока.

Майнер отправляет его на аптечный склад (PW).

3. Аптечный склад подписывает его своей цифровой подписью Spw, формирует внутренний хэш hpw и отправляет его майнеру.

$$h_{ppm} = f(H_{ppm}) = f(h_{pm}, D, K_{pub(pm)}, K_{pr(pm)}, S_{pm}, Z_{pm}, H_{ex}, h_{pw})$$

4. Майнер, основанный на hpw, формирует окончательный внешний хэш, используя информацию из предыдущего блока.

$$H_{pw} = f(h_{pw}, H_{ex})$$

Затем он отправляет его поставщику продукта и внедряет его во внешнюю сеть blockchain.

5. Производитель продукции отправляет этот блок во все аптеки в виде распределенного реестра.

6. Аптека заключает прямой договор с поставщиком продукции, производит внутренний блок с хэш:

hp = f(Dp, Kpub(p), Kpr(p), Sp, Zp)

Затем аптека отправляет его майнеру. Майнер генерирует внешний хэш и отправляет его поставщику продукта.

$$H_p = f(h_p)$$

7. Производитель формирует внутренний блок со своим хэшем и отправляет его майнеру.

$$h_{pm} = f(H_p, H_{previous})$$

8. Майнер формирует внешний конечный хэш и внедряет его в блокчейн-сеть.

$$H_{pp} = f(H_p, H_{previous})$$

9. Майнер отправляет блок в аптеку.

10. Аптека отправляет блок поставщику продуктов.

Далее происходит обмен контрактами между аптекой и аптечным складом. Он должен проходить по схеме, показанной на рисунке 7.

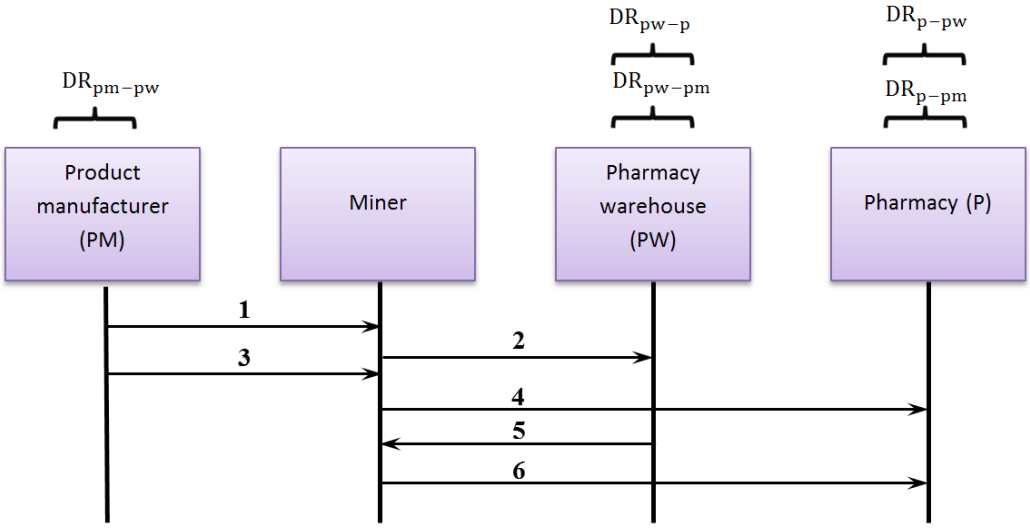


Рисунок 7 – Схема обмена блокчейн-контрактами между аптекой и аптечным складом

$DR_{wp\text{-}p}$ – распределенный реестр между аптекой и складской аптекой

1. Производитель продукта создает внутренний блок с хешем h_{pm1}:

$$h_{pm1} = f(D_1, K_{pub(pm)}, K_{pr(pm)}, D_{pm}, Z_{pm1})$$

D_1 – данные о продукте;

$K_{pub(pm)}$ – открытый ключ PM;

$K_{pr(pm)}$ – ПМ закрытый ключ;

D_{pm} – ПМ цифровой подписи;

Z_{pm1} – заголовок внутреннего блока с продуктами.

Затем он посылает его майнеру.

2. Майнер находит внешний хэш предыдущего блока и формирует внешний хэш H_{pm1}:

$$H_{pm1} = f(h_{pm1}, H_{previous})$$

Затем он отправляет его на аптечный склад.

3. Производитель продукта создает внутренний блок с хэш-h_{pm2}:

$$h_{pm2} = f(D_2, K_{pub(pm)}, K_{pr(pm)}, D_{pm}, Z_{pm2})$$

D_2 – данные о продукте;

$K_{pub(pm)}$ – открытый ключ ПМ;

$K_{pr(pm)}$ – ПМ закрытый ключ;

D_{pm} – ПМ цифровой подписи;

Z_{pm2} – заголовок внутреннего блока с продуктами.

Затем он посылает его майнеру.

Технология, которая была описана выше, позволяет гарантировать защиту от попадания в аптеки и к пациентам поддельных и контрафактных лекарств. Однако следует сказать, что пока внедрение такой технологии возможно только в границах одного государства, т.к. предполагает ведение единой базы лекарственных средств для всех аптек, находящихся в подчинении одной фармацевтической управленческой структуры.

В процессе работы создана примерная схема формирования распределенного реестра для социально-экономических систем. В рам-

ках этой схемы обеспечивается компромисс между открытостью абонента в открытой сети и одновременной закрытостью его персональных сведений и приватной информации. Это достигается путем использования цифровой подписи абонента сети.

Таким образом, разработана общая схема использования технологии блокчейн для различных типов социально-экономических систем.

Отличие от существующих разработок заключается в использовании двухключевой системы криптографического шифрования. Для реализации такой схемы в ней в качестве майнера должен выступать профессиональный криптограф, который одновременно является специалистом в соответствующей предметной области. Например, криптограф-нотариус, криптограф-энергетик, криптограф-фармацевт и т.д. Такой подход обеспечит, с одной стороны, корректную работу блокчейн-сети и формирование блокчейн-цепочки, с другой – соответствие всех транзакций нормативно-технической и нормативно-правовой документации, существующей в данной сфере. Это даст возможность всем остальным участникам и пользователям блокчейн-сети работать в ней комфортно и надежно.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. D.A.Lipinsky, A.A.Musatkina and K.N. Evdokimov, “Actual problems of international cooperation of Russia in the sphere of cyber security. Lecture notes in networks and systems”, V. 57, 2019, pp. 495–504.
2. Yazdinejadand A. Dehghantanha, “P4-to-blockchain: a secure blockchain-enabled packet parser for software defined networking”, Parizi R.M., Choo K.-K.R. Computers & Security. 2020. V. 88. P. 101629.
3. Q. Lyu, X. Zhang, Q. Wang, N. Zheng, Y. Qi and H. Liu, “SBAC: a secure blockchain-based access control framework for information-centric networking”, Journal of Network and Computer Applications. 2020. V. 149. P. 102444.
4. A.M.Kudin, B.A.Kovalenko andI.V.Shvidchenko, “Blockchain Technology: Issues of Analysis and Synthesis”(Article). Cybernetics and Systems Analysis, Volume 55, Issue 3, 15 May 2019, Pages 488–495.
5. A. Klarin, “The decade-long cryptocurrencies and the blockchain rollercoaster: Mapping the intellectual structure and charting future directions”, Research in International Business and Finance. 2020. T. 51. C. 101067.
6. Lazarenkoand S. Avdoshin, “Financial risks of the blockchain industry: A survey of cyberattacks”, Advances in Intelligent Systems and Computing. 2019. T. 881. C. 368–384.
7. N. Kabra, P. Bhattacharya, S. Tanwar and S. Tyagi, “MUDRACHAIN: blockchain-based framework for automated cheque clearance in financial institutions”, Future Generation Computer Systems. 2020. T. 102. C. 574–587.
8. M. J.J. Gul, A. Paul, A. Ahmad, M. Khan and G. Jeon, “Smart contract’s interface for user centric business model in blockchain”, Proceedings of the ACM Symposium on Applied Computing 34. 2019. P. 709–713.
9. S. Khezr, M.Moniruzzaman, A.Yassine and R.Benlamri,“Blockchain technology in healthcare: A comprehensive review and directions for future research” (Article). Applied Sciences (Switzerland)Volume 9, Issue 9, 1 May 2019, Article number 1736.
10. R. Casado-Vara, F. De la Prieta, S. Rodriguez, J. Prieto and J.M. Corchado “Cooperative algorithm to improve temperature control in recovery unit of healthcare facilities”, Advances in Intelligent Systems and Computing. 2020. T. 802. C. 49–62.
11. V. Menshikov and O. Volkova, “Digitalization for increased access security to healthcare services in Latvia”, Journal of Security and Sustainability Issues. 2019. T. 9. № 1. C. 171–183.
12. S. Avdoshin, E. Pesotskaya, “Blockchain revolution in the healthcare industry”, Advances in Intelligent Systems and Computing. 2019. T. 880. C. 626–639.

13 A.M. Makarov, A. O. Golyakova, I. D. Osininand S. S. Postovalov “Fundamental design of blockchain – hashchain networks with a decentralized register based on cryptography methods”. Advances in Intelligent Systems and Computing. 2019. V. 726. P. 620–629.
14. T.M. Fernández-Caramés and P. Fraga-Lamas, “Towards next generation teaching, learning, and context-aware applications for higher education: A review on Blockchain, Iot, Fog and Edge computing enabled smart campuses and universities”, Applied Sciences (Switzerland). 2019. V. 9. № 21. P. 4479.
15. X. He, S. Alqahtani, R. Gamble, M. and Papa, “Securing over-the-air iot firmware updates using blockchain”, ACM International Conference Proceeding Series 2019. P. 164–171.
16. S.N. Mohanty, K.C. Ramya, S.S. Rani, D. Gupta, A. Khanna, K. Shankarand S.K. Lakshmanaprabu, “An efficient lightweight integrated blockchain (ELIB) model for iot security and privacy”, Future Generation Computer Systems. 2020. V. 102. P. 1027–1037.
17. N.Wang, X.Zhou, X.Lu, Z.Guan, L.Wu, X.Du and M.Guizani, “When energy trading meets blockchain in electrical power system: the state of the art”, Applied Sciences (Switzerland). 2019. V. 9. № 8. P. 1561.
18. V.Denisova, A.Mikhaylov and E.Lopatin, “Block chain infrastructure and growth of global power consumption”, International Journal of Energy Economics and Policy. 2019. V. 9. № 4. P. 22–29.
19. R.Kh.Azieva, M.I. Chazhaev, Kh.G.Chaplaev, S.U.Gapaeva and K.Kh.Mazhiev, “Innovative breakthrough of blockchain technology in oil and gas industry”, In the collection: “The European Proceedings of Social & Behavioural Sciences EpSBS Conference: SCTCGM 2018 – Social and Cultural Transformations in the Context of Modern Globalism. Conference Chair(s): Bataev Dena Karim-Sultanovich – Doctor of Engineering Sciences, professor, director of the Complex Scientific Research Institute n. a. H.I. Ibragimov of the Russian Academy of Sciences”. 2019. P. 142–149.
20. C.Zhao, M.Liu, Y.Yang, F.Zhao and S.Chen, “Toward a blockchain based image network copyright transaction protection approach”, Advances in Intelligent Systems and Computing. 2020. V. 895. P. 17–28.