УДК 004.7.056.5

Н.Г. Лабутин

АНАЛИЗ ВОЗМОЖНОСТЕЙ ТЕХНОЛОГИИ БЛОКЧЕЙН ПО ЗАЩИТЕ ОТ СЕТЕВЫХ АТАК

Приволжский институт повышения квалификации Федеральной налоговой службы

В статье проведен анализ возможностей блокчейн-технологии по защите от основных видов атак в компьютерных сетях. С помощью функциональной модели рассмотрены механизмы, встроенные в блокчейн, позволяющие надежно аутентифицировать участников системы, обеспечить целостность и аутентичность информации, таким образом, защищать ее от подделки и других угроз безопасности информации.

Ключевые слова: блокчейн, моделирование процессов, методология IDEF0, целостность и аутентичность информации, электронная подпись, хеширование данных, проверка подлинности.

Введение

Блокчейн-технология за последние несколько лет обрела большую популярность в различных сферах деятельности человека. Во многом это объясняется использованием принципов децентрализованного обмена данными в распределенных системах, то есть отсутствием посредника, выполняющего функции центра, подтверждающего подлинность участников обмена и передаваемой ими информации [1]. Популярность блокчейн в значительной степени связана также с тем, что она разработана как защищенная технология: в ней применяются, как криптографические способы защиты информации, так и другие способы обеспечения аутентичности, конфиденциальности и целостности информации. Конечно, блокчейн обладает и определенными ограничениями по сравнению с технологиями централизованного обмена. В данной статье не преследуется цель выявления данных позитивных и негативных аспектов; блокчейн-технология рассматривается с позиций защиты информации: функционирование механизмов защиты и предотвращение угроз безопасности информации. В работе представлен вариант анализа механизмов защиты информации, реализованных в блокчейн-системах, который произведен при помощи функционального моделирования IDEF0 [2].

Анализ защитных механизмов блокчейн-технологии важен для определения ее возможностей противостоять известным типам сетевых атак не только в платежных системах, подобных «Биткоин», но и в любых информационных системах с децентрализованным хранением и обработкой данных в компьютерных сетях. Необходимость данного анализа также связана с тем, что, несмотря на большое количество различных данных по рассматриваемой тематике, очень мало источников, в которых представлено формализованное описание работы защитных механизмов блокчейн.

Анализ защитных механизмов блокчейн при помощи функционального моделирования IDEF0

Заложенные в технологию блокчейн принципы, позволяющие обеспечить целостность и аутентичность данных, передаваемых по сети, могут применяться для защиты информации не только в электронных платежных системах, но и в любых децентрализованных распределенных системах.

Сформулируем основные принципы технологии блокчейн, позволяющие защитить данные участников системы:

1) децентрализация хранения данных о транзакциях (децентрализованный реестр транзакций) при использовании технологии одноранговой (P2P) сети;
2) использование криптографической защиты информации с помощью электронной подписи транзакций и хеширования транзакций и блоков, с помощью чего достигается надежная аутентификация участников обмена, обеспечение целостности информации в блоках и в цепи блоков;
3) практическая невозможность подделки транзакций, сохраненных в цепочке блоков и невозможность, точнее вычислительная сложность подделки цепочки блоков – реестра проведенных операций, так как полная копия текущего реестра сохраняется на всех компьютерах участников сети.

Как на основании этих принципов работают защитные механизмы блокчейн? Для ответа на этот вопрос проанализируем основные процессы в блокчейн-системе (БЧ-системе), направленные на обеспечение безопасности информации в ней. Анализ проведем с использованием функциональных моделей процессов при создании блока и формировании цепочки блоков в БЧ-системе, построенных по методологии IDEF0 [2] и рассмотренных в [3].

Согласно методологии IDEF0, процессы функционирования системы представляются в виде диаграмм, основными элементами которых являются функциональные блоки (функции, процессы). Функциональные блоки должны быть сформулированы как действие, то есть с помощью глаголов и обозначаются в диаграмме прямоугольниками. Каждая сторона прямоугольника играет свою роль: верхняя – управление (управляющее воздействие), нижняя – механизм реализации данной функции, левая – вход, правая – выход. Блоки соединяются интерфейсными дугами, представленными в виде стрелок. Интерфейсная дуга (стрелка) предназначена для отображения элемента системы, который или обрабатывается блоком (вход), или является результатом обработки (выход) или оказывает другое воздействие на функцию, отображенную данным блоком [2].

Модель любой системы представляется сначала в виде основной целевой функции, затем с помощью декомпозиций детализируется до состояния, определяемого разработчиком [2]. На рис. 1 представлена диаграмма с целевой (контекстной) функцией системы, отображающая в общем виде предметную область блокчейн – формирование цепи блоков [3].

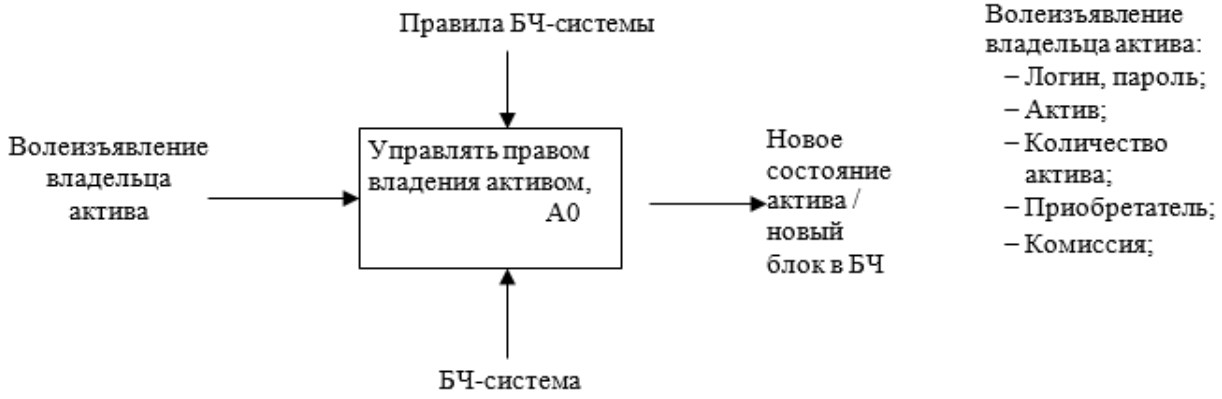

Рис. 1. Контекстная диаграмма функции «Управлять правом владения активом», A0

Проведем декомпозицию функции (процесса) A0 для детализации работы защитных механизмов блокчейн-технологии. Первый уровень декомпозиции представлен на рис.2.

В общем виде декомпозицию целевой функции представим в виде трех процессов:

- «Получить доступ к системе», A1;
- «Подготовить транзакцию для записи в блок», A2;
- «Сформировать блок и добавить его в цепь», A3.

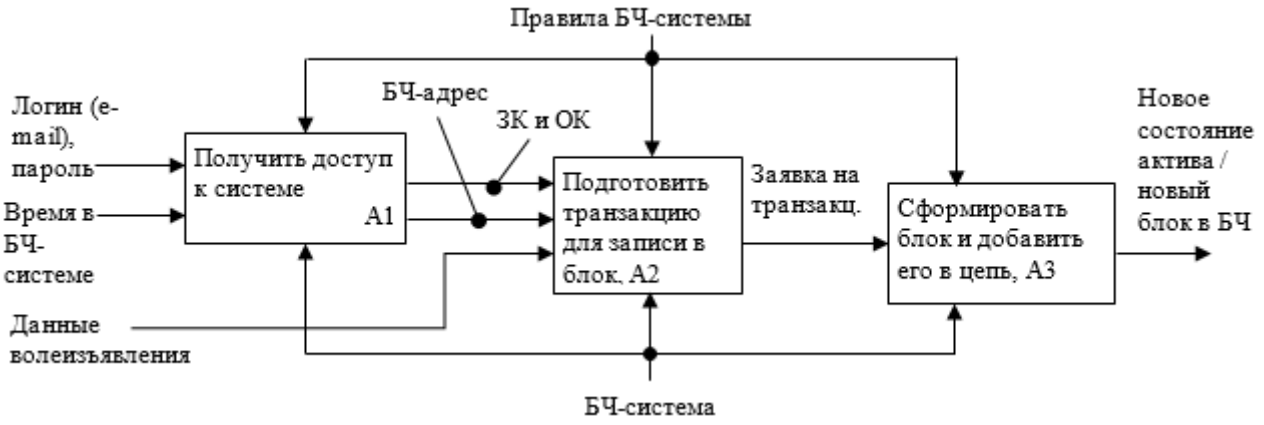

Рис. 2. Декомпозиция целевой функции БЧ-системы, A0

Для получения доступа к активам пользователя и действиям, предоставляемым БЧ-системой, необходимо сначала зарегистрировать пользователя. Декомпозиция функции (процесса) *«Получить доступ к системе», A1* может быть представлена в виде двух процессов: «Зарегистрировать нового пользователя в системе», A11 и «Авторизоваться в системе», A12 (рис. 3).

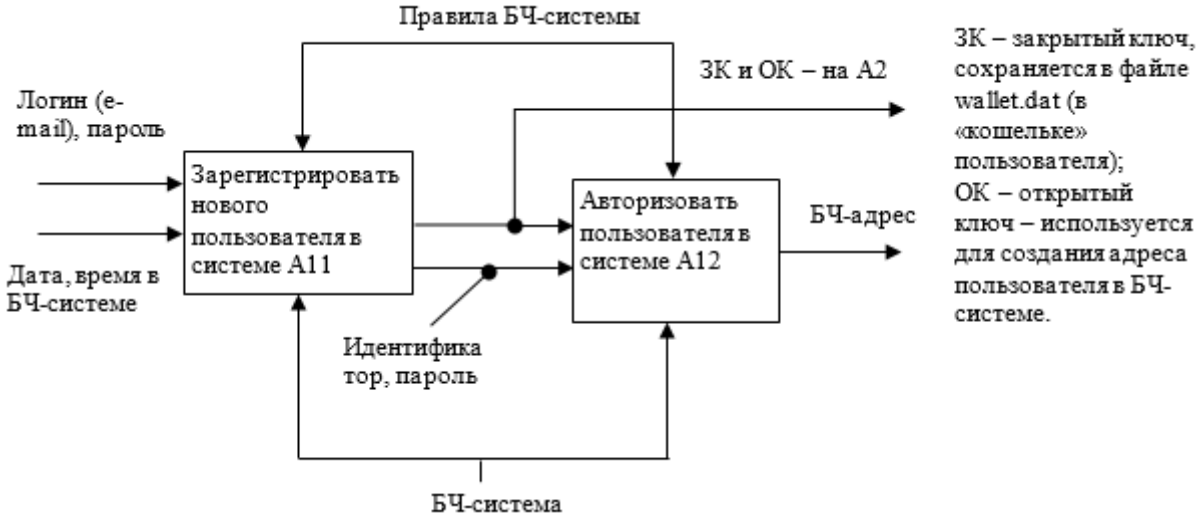

Рис. 3. Декомпозиция функции «Получить доступ к системе», A1

Регистрация нового пользователя является необходимым процессом в работе блокчейн-системы (БЧ-системы), так как при регистрации формируется пара криптографических ключей, являющихся основой криптографической защиты информации, используемой в БЧ-системе.

Для обеспечения аутентичности и целостности данных пользователей в системе применяется асимметричная криптография, основанная на паре ключей. Для каждого пользователя ассиметричной криптосистемы должна быть создана уникальная пара ключей: открытый (публичный) и закрытый (приватный), которые связаны между собой математическими зависимостями таким образом, что к закрытому ключу (ЗК) может подойти только открытый ключ (ОК) из этой пары.

Закрытый (секретный) ключ применяется для:

- доступа к своим активам (в Биткоине – для доступа к электронному кошельку);
- постановки криптографической электронной подписи (ЭП) в заявке на транзакцию.

ЭП подтверждает подлинность авторства заявки на транзакцию, то есть подтверждает факт того, что заявка на транзакцию составлена именно тем участником, который поставил подпись. ЗК также обеспечивает защиту доступа к своим активам (кошельку), так как к кошельку можно получить доступ только по ЗК данного пользователя, с которым ассоциирован кошелек при его создании в системе.

ОК используется для проверки ЭП, а также для формирования адреса узла в БЧ-системе. Как формируются криптографические ключи пользователей БЧ-системы? Представим этот процесс в виде диаграммы А11, являющейся декомпозицией процесса А1 (рис. 3).

Процесс *«Зарегистрировать нового пользователя в системе», А11* описывает действия, осуществляемые при регистрации пользователя в БЧ-системе, например, в системе Биткоин – во время создания биткоин-кошелька. При этом в БЧ-системе происходит генерация пары криптографических ключей и из них формируются идентификатор пользователя для входа в систему и адрес кошелька.

На входы процесса А11 поступают:

- логин, как правило, в различных БЧ-системах это e-mail;
- пароль, созданный пользователем;
- дата, время в БЧ-системе.

Выходами процесса А11 является пара ключей данного пользователя: ЗК и ОК, а также идентификатор (имя пользователя) для входа в систему (для доступа к кошельку). Таким образом, БЧ-система переходит в новое состояние, при котором в P2P-сети появился новый узел. ЗК и ОК используются в дальнейшем для создания и проведения транзакции от имени пользователя – владельца пары ключей. ЗК используется для постановки электронной подписи на заявку на транзакцию, ОК, точнее вычисленный хеш ОК передается вместе с транзакцией для проверки электронной подписи.

Управляющие воздействия на диаграмме процесса обозначены в общем виде как правила БЧ-системы. *Механизм*, используемый в процессе обозначим «БЧ-система», под которой понимается совокупность вычислительных устройств и пользователей вычислительных устройств, объединенных в одноранговую (P2P) сеть. Пользователя, зарегистрированного на вычислительном устройстве, будем называть узлом сети блокчейн.

Описание процесса: при регистрации в системе, новый пользователь предоставляет системе следующие данные: адрес электронной почты, пароль и подтверждение пароля. По этим данным генерируется пара ключей. Пара ключей состоит из закрытого ключа (ЗК) и открытого ключа (ОК). ЗК надежно хранится у пользователя системы (в Биткоин – в кошельке) и никому не предоставляется, ОК является публичным, он используется для проверки ЭП, из него с помощью хеш-функции вычисляется *адрес пользователя*. После регистрации в системе (создания кошелька) на почтовый адрес пользователя приходит письмо со ссылкой, по которой надо перейти для верификации пользователя, и его персональным идентификатором, который в дальнейшем будет использоваться для входа в систему – подключения к кошельку, то есть в качестве имени пользователя в системе. Таким образом, учетной записью для входа в систему служит связка «персональный идентификатор – пароль»; пароль выбирается пользователем при регистрации в БЧ-системе.

Процесс *«Авторизовать пользователя в системе», А12* происходит по персональному идентификатору в качестве имени пользователя и паролю (*входы* процесса), который задавался при регистрации. *Выходом* процесса А12 является *БЧ-адрес пользователя*, по сути – учетные данные пользователя, используемые для адресации пользователя в БЧ-сети и перевода активов на его кошелек. После авторизации в системе пользователю доступен его кошелек с закрытым ключом и возможностью переводить активы другим пользователям, то есть создавать заявки на транзакции. Так как в системе блокчейн используется одноранговая сеть, то новый пользователь сети становится полноправным членом системы сразу после его авторизации в БЧ-системе.

Результатом процесса *«Получить доступ к системе», A1* является то, что у пользователя системы (владельца актива) сформированы закрытый и открытый ключи и он авторизован в системе, он может инициировать транзакции, то есть создавать заявки на транзакции, которые затем должны быть проверены другими пользователями БЧ-системы для включения их в блок для дальнейшего формирования цепочки блоков (блокчейн). С помощью процесса *«Получить доступ к системе», A1* в БЧ-системе обеспечивается важный защитный механизм – предотвращение несанкционированного доступа к активам пользователя.

Транзакцией в блокчейн будем называть процедуру передачи актива, подтвержденную участниками БЧ-системы, по сути, являющуюся записью в децентрализованном реестре всех действий, производимых в системе с начала ее работы. Под *заявкой на транзакцию* будем понимать оформленное по правилам БЧ-системы волеизъявление владельца актива на его передачу новому владельцу, которое требует дальнейшей проверки участниками БЧ-системы для включения его в блок.

Процессы, моделирующие действия по формированию заявки на транзакцию, ее проверку для включения в блок и формирования цепочки блоков в БЧ-системе, с использованием функционального моделирования IDEF0 подробно описаны в [3], в данной статье детализацию этих процессов произведем только до уровня, необходимого для понимания работы механизмов защиты информации в БЧ-системе.

Подлинность и неотрекаемость инициатора транзакции, целостность и валидность транзакции проверяется всеми участниками (пользователями) БЧ-системы, у которых имеется экземпляр всей цепи (полные узлы), с помощью криптографической электронной подписи и открытого ключа ее владельца. Сформированная инициатором заявка на транзакцию широковещательным запросом транслируется в P2P-сети блокчейн и становится доступной для ее проверки всеми участниками системы.

Чтобы лучше понимать процесс формирования и проверки транзакции, рассмотрим упрощенную структуру транзакции с одним входом (input) и одним выходом (output), а также связи между предшествующей, текущей и следующей транзакциями.

В каждую транзакцию включены следующие параметры:

- Previous tx=Hx – хеш предыдущей транзакции, из которой берется актив для текущей транзакции;
- Index – номер выхода предыдущей транзакции, для наглядности *Previous tx и Index* вместе будем называть *ссылкой на транзакцию*;
- ScriptSig- PKx – открытый ключ создателя текущей транзакции;
- ScriptSig- Sigx – ЭП текущей транзакции, созданная на ЗК создателя данной транзакции;
- Value – сумма (количество актива);
- ScriptPubKey- Ax – адрес получателя актива текущей транзакции, представляющий хеш его ОК;
- ScriptPubKey-правила – скрипт на языке БЧ-системы.

Значения параметров ScriptSig и ScriptPubKey участвуют в проверке валидности транзакции. В простейшем виде эта проверка заключается в следующем: если текущая транзакция указывает на «правильную» предыдущую транзакцию, то в результате выполнения скрипта над ScriptSig и ScriptPubKey получится значение *«Истина»*, что означает равенство хеша ОК, указанного в текущей транзакции, и хеша ОК в параметре ScriptPubKey предыдущей транзакции.

Для моделирования процесса формирования заявки на транзакцию с ЭП, представим декомпозицию процесса *«Подготовить транзакцию для записи в блок», A2* (рис. 4), состоящего из трех процессов:

- «Сформировать заявку на транзакцию», A21;
- «Подписать ЭП заявку на транзакцию», A22;
- «Записать заявку на транзакцию в мемпул», A23.

Описание процесса *«Сформировать заявку на транзакцию», А21*. *Входами* процесса являются:

- данные волеизъявления – информация, указываемая владельцем актива в клиентской программе для доступа к активам БЧ-системы, например, в кошельке Биткоин: сумма перевода, из каких «поступлений» он хочет осуществить перевод;
- БЧ-адрес получателя – адрес получателя в БЧ-системе, например, в Биткоин – это хеш от ОК получателя;
- ОК владельца – открытый ключ владельца актива, который добавляется в транзакцию в параметр ScriptSig;
- системное время – текущее время БЧ-системы, необходимо для привязки транзакции к системному времени и фиксации хронологии действий в системе.

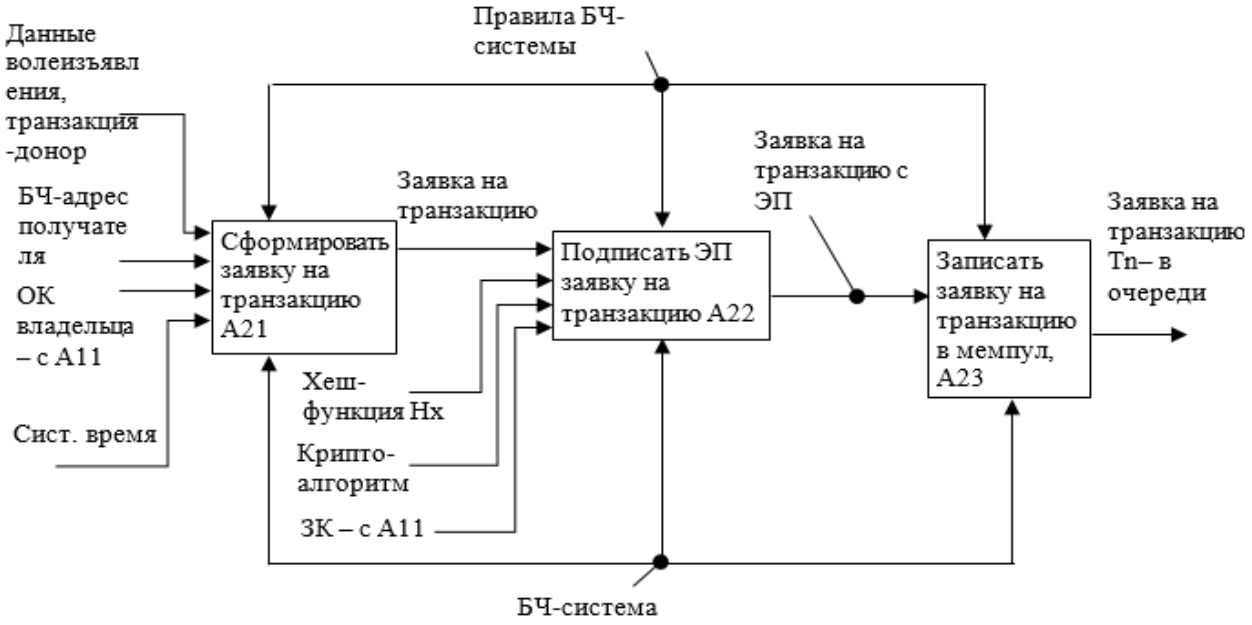

Рис. 4. Декомпозиция процесса «Подготовить транзакцию для записи в блок», А2

Выходом процесса А21 является заявка на транзакцию без электронной подписи в параметре ScriptSig. Разделение процесса А2 на два процесса: «Сформировать заявку на транзакцию», А21 и «Подписать ЭП заявку на транзакцию», А22 выполнено для наглядности работы криптографических защитных механизмов.

Управляющие воздействия на рис.4 обозначены как «Правила БЧ-системы», *механизм* процесса – «БЧ-система». Заявка на транзакцию формируется под управлением функционала программного обеспечения, которое применяется пользователем БЧ-системы.

Декомпозиция процесса *«Подписать ЭП заявку на транзакцию», А22* представлена на рис.5.

Описание процесса А22:

На *входы* процесса *«Вычислить хеш заявки на транзакцию», А221* поступает заявка на транзакцию без ЭП и хеш-функция Нх, применяемая в БЧ-системе, как правило, это SHA-256, SHA-512 или иная. На этой хеш-функции вычисляется хеш-транзакции, которая является уникальным для данной транзакции.

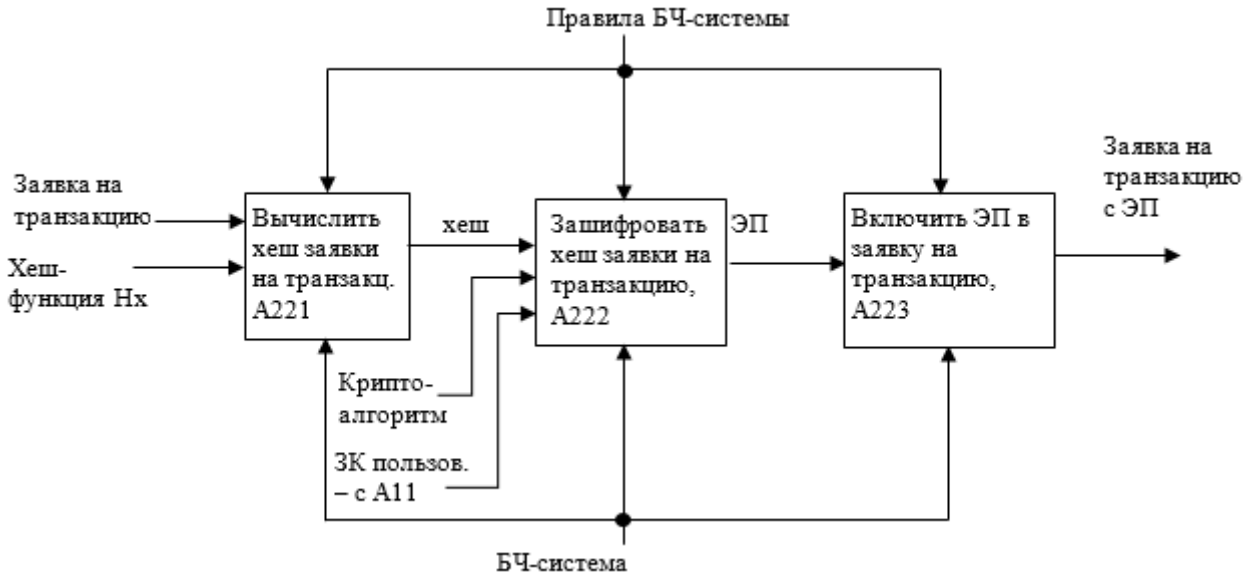

Рис. 5. Диаграмма процесса «Подписать ЭП заявку на транзакцию, А2

Хеш-функции широко используются в БЧ-системах по нескольким причинам:

- любая хеш-функция необратима, это значит, что по известному хешу задача нахождения исходных данных является вычислительно сложной, то есть это практически невозможно;
- хеш-функция формирует хеш-данные строго фиксированного размера, независимо от размера исходных данных, причем хеш намного меньше самих данных;
- хеш-функция создает уникальный хеш для каждого блока исходных данных, при мельчайшем изменении этих данных значение хеша радикально изменяется;
- эти три свойства хеш-функции определили их использование для защиты данных в БЧ-системах.

Выходом процесса А221 является вычисленный с помощью функции хеширования Нх-хеш заявки на транзакцию. Далее с помощью процесса *«Зашифровать хеш-заявки на транзакцию»*, *А222* хеш зашифровывается на закрытом ключе пользователя, осуществляющего данную транзакцию, с помощью встроенного в БЧ-систему криптоалгоритма. Как правило, используется алгоритм AES, но это может быть любой надежный алгоритм асимметричного шифрования.

Выходом процесса А222 является ЭП заявки на транзакцию.

Созданная ЭП поступает на *вход* процесса *«Включить ЭП в заявку на транзакцию», А223. Выходом* данного процесса является заявка на транзакцию с электронной подписью владельца актива-инициатора данной транзакции. Подписанная заявка на транзакцию автоматически распространяется в одноранговой сети, каковой является БЧ-система.

Все узлы одноранговой сети, на которых имеется полная копия цепочки блокчейн, получают подписанную заявку на транзакцию и сохраняют ее в *мемпуле* – распределенной между узлами сети области памяти, предназначенной для хранения непроверенных транзакций. В результате выполнения процесса *«Записать заявку на транзакцию в мемпул», А23* заявка на транзакцию с ЭП передается в мемпул, где ожидает своей очереди на дальнейшую обработку и включение ее в блок.

В результате анализа процесса «Подготовить транзакцию для записи в блок», А2 с помощью моделирования IDEF0 становится очевидным тот факт, что подделать транзакцию в БЧ-системе фактически невозможно, то есть в БЧ-системе обеспечена защита от сетевых атак, связанных с модификацией данных.

Фактическая невозможность подделки транзакций вытекает из того, что все транзакции каждого участника системы взаимосвязаны между собой с помощью хеширования и выстраиваются в цепочку, проверенную всеми полными узлами БЧ-сети. Все проведенные транзакции хранятся в блоках, которые также защищены с помощью хеширования. Децентрализация блокчейна также значительно снижает вероятность фальсификации хранимых данных. Для модификации данных в централизованных системах злоумышленники обычно атакуют сервера или майнфреймы, на которых хранятся данные системы. В блокчейне это практически невозможно.

Подписанная заявка на транзакцию поступает на вход процесса *«Сформировать блок и добавить его в цепь», А3,* декомпозиция которого представлена на рис.6 для понимания работы защитных механизмов по обеспечению аутентичности и целостности транзакции при добавлении ее в блок.

На рис. 6 и далее стрелки, обозначающие управляющие воздействия в виде правил БЧ-системы, не отображены для того, чтобы не загружать диаграмму.

Из *мемпула* заявка на транзакцию выбирается узлами БЧ-системы, называемыми майнерами, которые одновременно проверяют ее на аутентичность и валидность. Заявка считается проверенной, если ее проверили и подтвердили не менее определенного количества майнеров. Это количество определяется параметрами БЧ-системы. Например, в Биткоин оно равно 6. Таким образом, обеспечивается фактическая невозможность подделки транзакции.

Если заявка на транзакцию проходит проверку, то она включается в текущий блок в качестве транзакции. Основной задачей майнера является формирование блока определенного формата, в качестве записей которого выступают проверенные транзакции.

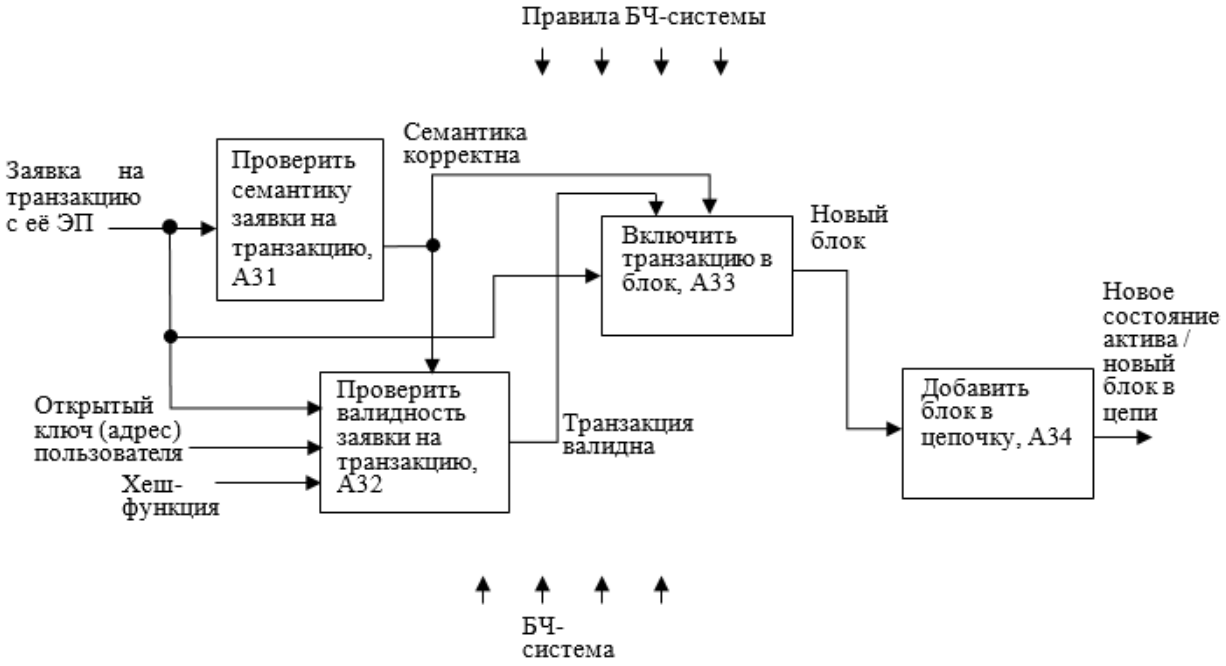

Рис. 6. Декомпозиция процесса «Сформировать блок и добавить его в цепь, А3

При выполнении процесса *«Проверить семантику заявки на транзакцию», А31* осуществляется проверка семантической корректности заявки на транзакцию, которая заключается в проверке формата заявки и ее верификации. Верификация заключается в проверке выполнения следующих правил БЧ-системы:

- количество передаваемого актива не должно превышать количество актива, взятого из источника, или некоторого значения;

- количество передаваемого актива не должно превышать некоторого значения за определенное время;
- количество транзакции данного пользователя не должно превышать установленного значения и т.д.

Выходом процесса А31 является команда *«Семантика корректна»*, которая будет являться управляющей для процессов *«Проверить валидность заявки на транзакцию»*, А32 и *«Включить транзакцию в блок», А33*.

После семантической проверки заявки на транзакцию, т.е. ее верификации, для включения в блок майнер осуществляет валидацию – проверяет ЭП инициатора данной транзакции. Такие проверки происходят одновременно на всех узлах-майнерах БЧ-системы, на каждом их которых хранится свой экземпляр цепи блокчейн. И только блок того майнера, который первый решит вычислительно сложную задачу формирования нового блока, будет добавлен в цепочку блокчейн. Остальные блоки будут игнорированы системой.

Описание процесса *«Проверить валидность заявки на транзакцию», А32.*

Входами являются: заявка на транзакцию с открытым ключом инициатора заявки на перевод актива, а также хеш-функция, встроенная в БЧ-систему.

С помощью процесса А32 рассмотрим одну из важнейших функций механизма проверки аутентичности и валидности транзакции, происходящей с помощью проверки ЭП владельца актива, на узле майнера. Декомпозиция процесса «Проверить валидность заявки на транзакцию», А32 представлена на рис.7.

В данном случае, ЭП обеспечивает несколько защитных функций:

- подтверждает подлинность владельца актива, осуществляющего данную транзакцию;
- обеспечивает неотрекаемость подписанта от подписанной им транзакции;
- обеспечивает целостность подписанной транзакции.

Выходом процесса *«Проверить валидность заявки на транзакцию», А32* является управляющая команда *«Транзакция валидна»*, которая является разрешающей для выполнения процесса *«Включить транзакцию в блок», А33.*

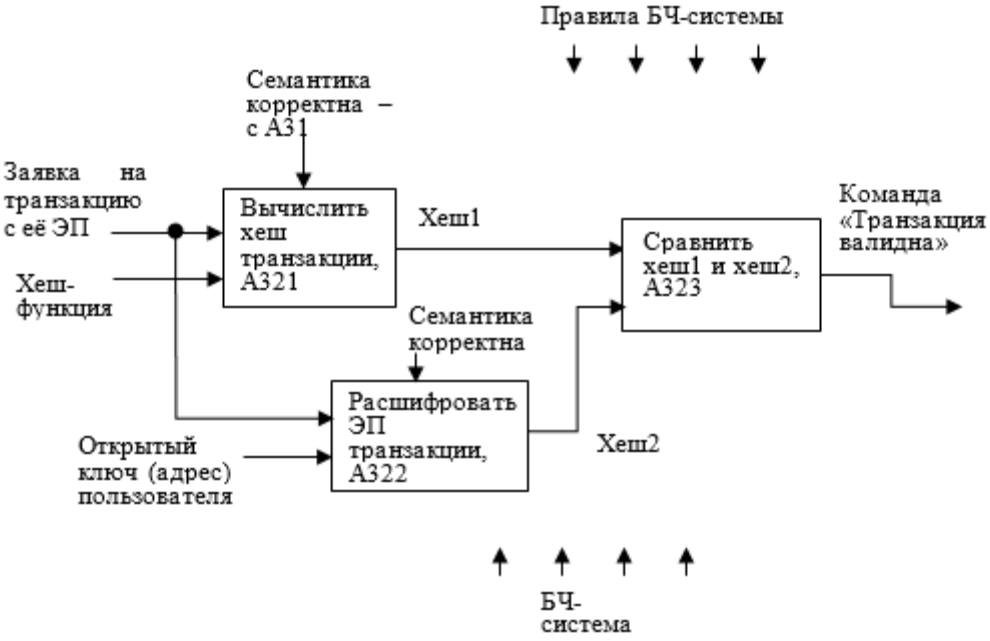

Рис. 7. Диаграмма процесса «Проверить валидность заявки на транзакцию, А32

При выполнении процесса «Включить транзакцию в блок», А33 осуществляется формирование блока, состоящего из заголовка и определенного, заданного правилами

БЧ-системы, количества транзакций. При этом данные о транзакциях защищаются с помощью криптографических функций хеширования следующим образом. *Входом* процесса А33 является очередная проверенная транзакция, *управляющими воздействиями*, кроме правил БЧ-системы, служат разрешающие команды *«Семантика корректна»* и *«Транзакция валидна»*. *Выходом* процесса А33 является очередной сформированный блок, который добавляется в цепочку по правилам БЧ-системы. Правила добавления блока в БЧ-системе в рамках данной статьи не рассматриваются.

Описание процесса *«Включить транзакцию в блок», А33.*

После добавления каждой новой транзакции в блок майнер вычисляет хеш – контрольную сумму от всех транзакций по специальному алгоритму, называемому деревом Меркла. Для вычисления хешей используется одна из популярных хеш-функций, например, SHA-512. По этому алгоритму сначала вычисляются хеши от каждой транзакции в блоке, затем вычисляются хеши от пар хешей и так до тех пор, пока не будет сформирован один общий хеш всех транзакций.

Хеш по дереву Меркла (Merkle Root) пересчитывается каждый раз после добавления очередной транзакции. Пустой блок, в который по мере поступления добавляются транзакции, предварительно создается майнером.

Наиболее интересными с позиций анализа работы защитных механизмов БЧ параметрами и данными блока являются следующие.

1. Хеш открытого ключа майнера, являющийся его адресом.
2. Транзакции.
3. Метка времени и рост блока, которые, по сути, идентифицируют блок, то есть являются номером блока.
4. Хеш всего блока (Hash).
5. Хеш от предыдущего блока – последнего на данный момент времени в цепочке блоков (Previous Block).
6. Хеш, вычисленный от всех транзакций в текущем блоке по дереву Меркла.
7. Bits – параметр, от которого зависит сложность расчета, по специальной формуле из него высчитывается максимально возможный хэш блока и, по правилам системы, принимается только тот блок, хэш которого меньше этого значения.
8. Nonce – параметр, который вычисляют майнеры с помощью сложных расчетов: он обеспечивает вычислительную сложность подделки блока.

Анализ структуры блока и процесса его формирования А33 показывает, что с помощью хеша транзакций и хеша всего блока обеспечивается взаимосвязь и целостность информации в блоке: хеш всего текущего блока вычисляется от хеша транзакций по дереву Меркла, хеша предыдущего блока и служебных параметров текущего блока. При любой несанкционированной модификации данных, хранящихся не только в текущем блоке, но и в предыдущих блоках, хеши также изменятся, что сразу будет определено всеми участниками БЧ-системы. Эти особенности БЧ-системы с успехом защищают от сетевых атак типа «человек посередине» [4].

В результате выполнения процесса *«Добавить блок в цепочку», А34* очередной блок добавляется к цепи, продублированной на каждом полном узле БЧ-системы. Так как одинаковые экземпляры БЧ хранятся на разных узлах сети и регулярно синхронно перезаписываются при добавлении нового блока, то организовать атаку типа «отказ в обслуживании» [5] на ресурсы БЧ-системы весьма проблематично, фактически невозможно. Действительно, количество полных узлов в сети БЧ исчисляется тысячами и десятками тысяч, например, в сети Биткоин около 10 тыс. полных узлов [6]. Заблокировать одновременно несколько тысяч полных узлов в сети блокчейн, в настоящее время представляется нереальным.

Заключение

Представленная в статье функциональная модель, по мнению автора, наглядно отображает принципы работы защитных механизмов БЧ-системы, но не претендует на завершенное решение. Моделирование процессов, используемых для защиты информации в БЧ, произведено с точки зрения автора и по тем описаниям блокчейн-технологии, которые были доступны автору статьи. Проведенный при помощи моделирования IDEF0 анализ защитных механизмов блокчейн-технологии позволил сделать выводы о возможности ее применения для защиты от наиболее распространенных в настоящее время сетевых атак, таких как: «распределенный отказ в обслуживании», «подмена или модификация данных», «человек посередине».

Применяемые в блокчейн способы криптографической защиты информации: электронная подпись, хеширование – не новы. Они широко применяются в различных централизованных системах, например, в виртуальных частных сетях организаций, в современных клиент-серверных банковских и платежных системах и т.д. Но, в отличие от них, в блокчейн-системах нет необходимости в едином центре управления ключевой информацией участников сети, который должен быть в любой централизованной системе, защищенной с помощью криптографии. Таким образом, значительно упрощается криптографическая система без снижения ее защищённости. Следует отметить, что применение в блокчейн в комплексе криптографических механизмов защиты и структурных решений децентрализованной обработки данных позволяет достигнуть высокой защищенности информации.

Предполагается, что рассмотрение темы защиты информации при помощи технологии блокчейн будет продолжено автором в следующих публикациях.

Библиографический список

1. **Лелу, Л.** Блокчейн от А до Я. Все о технологии десятилетия / Л. Лелу. – М.: Эксмо, 2018, – 256 с.
2. Integration DEFinition for function modeling (IDEF0). Draft Federal Information Processing Standards Publication 183, 1993 December 21. – URL: http://idef.com/wp-content/uploads/2016/02/idef0.pdf. (дата обращения 19.02.2019 г.).
3. **Карпычев, В.Ю.** Функциональное моделирование (IDEF0) как метод исследования блокчейн-технологии / В.Ю. Карпычев // Труды НГТУ им. Р.Е. Алексеева. – 2018. – № 4 (123). – С. 22-32.
4. **Иванов, О.** Все об атаке «Человек посередине» (Man in the Middle, MitM). – URL: https://www.anti-malware.ru/analytics/Threats_Analysis/man-in-the-middle-attack (дата обращения 29.03.2019 г.).
5. DOS и DDoS-атаки: понятие, разновидности, методы выявления и защиты. – URL: https://compconfig.ru/net/dos-i-ddos-ataki.html (дата обращения 29.03.2019 г.).
6. **Дрешер, Д.** Основы блокчейна: вводный курс для начинающих в 25 небольших главах / Д. Дрешер. – М.: ДМК Пресс, 2018, – 320 с.

Дата поступления
в редакцию: 09.04.2019

N.G. Labutin

ANALYSIS OF OPPORTUNITIES OF BLOCKCHAIN TECHNOLOGY ON PROTECTION AGAINST NETWORK ATTACKS

Volga institute of advanced training of the Federal Tax Service

Purpose: the analysis of protective mechanisms a blockchain with use of functional modeling.
Methodology: the functional model offered for the analysis of protective mechanisms a blockchain systems is based on the known methodology of SADT/IDEF0
Value: the model developed for the analysis of security a blockchain can be used in fundamental researches of blockchain technology.
Research implications: the formalized description of work of protection gears a blockchain on counteraction to widespread network attacks can be detailed further.

Keywords: blockchain, modeling of processes, IDEF0 methodology, integrity and authenticity of information, digital signature, hashing of data, authentication.