DOI 10.37882/2223–2966.2021.12–2.10

КРИТЕРИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ РАСПРЕДЕЛЕННОЙ СИСТЕМЫ ДОКУМЕНТИРОВАНИЯ ПРОЦЕССОВ МОРСКИХ ПЕРЕВОЗОК

INFORMATION SECURITY CRITERIA FOR A DISTRIBUTED DOCUMENTATION SYSTEM OF SEA TRANSPORTATION PROCESSES

E. Poleshchuk
S. Putilova
I. Shcherbinina

Summary. The digitalization of maritime transport is associated with a number of obvious features of ship transportation, which make it difficult or even impossible to exchange data with service consumers and situational centers. Accordingly, it is necessary to develop a technology that eliminates these shortcomings. This article discusses the information security criteria that must be taken into account when developing a distributed system for documenting shipping processes.

Keywords: information security, blockchain, smart contract, maritime logistics.

Полещук Евгения Михайловна
Аспирант, Морской Государственный Университет им. адм. Г.И. Невельского
poleshuk@msun.ru
Путилова Софья Евгеньевна
Аспирант, Морской Государственный Университет им. адм. Г.И. Невельского
Щербинина Инна Александровна
К.п.н., доцент, Морской Государственный Университет им. адм. Г.И. Невельского
shcherbinina@msun.ru

Аннотация. Цифровизация морского транспорта сопряжена с рядом очевидных особенностей перевозок на судах, которые затрудняют или вообще не позволяют осуществлять обмен данными с потребителями сервисов и ситуационными центрами. Соответственно необходимо разработать технологию, нивелирующую данные недостатки. В настоящей статье рассматриваются критерии информационной безопасности, которые необходимо учитывать при разработке распределенной системы документирования процессов морских перевозок.

Ключевые слова: информационная безопасность, блокчейн, смарт-контракт, морская логистика.

В процессе организации морских перевозок задействовано множество участников, выполняющих свои задачи на каждом определённом этапе логистической цепочки. В связи с чем для качественной разработки надежной системы документирования необходимо учитывать особенности документооборота морской логистики. Особенности инфраструктуры, условий работы таможни и других контролирующих органов, инспекционных комплексов, систем видеонаблюдения, автоматизации процедур, информационных систем также необходимо учитывать при переводе системы документирования процессов логистики на технологию блокчейн.

Предлагаемые прикладные решения адаптируют взятую за основы технологию к решению конкретной задачи, зачастую не исследуют ограничений и рисков применения этой технологии в отдельной предметной области. При этом потери, являющиеся следствием ограниченности применения технологии в конкретной предметной области, могут быть очень существенными.

Научная новизна настоящей работы заключается в анализе характеристик блокчейн-сети как распределенной системы с точки зрения возможности реализации на ее базе защищенной информационной системы документирования процессов морских перевозок.

В данном контексте необходимо рассматривать ряд критериев распределенных систем:

- Архитектура;
- Язык программирования;
- Наличие криптовалюты;
- Протокол консенсуса;
- Реализация смарт-контрактов;
- Обеспечение приватности и конфиденциальности данных;
- Идентификация пользователей.

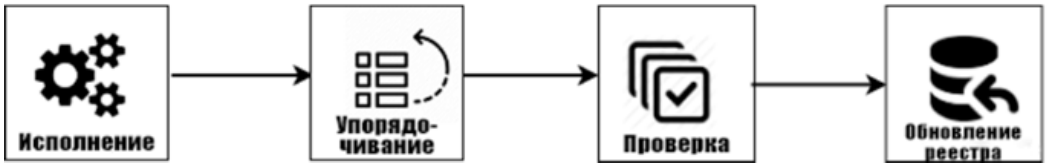

Рис. 1. Архитектура исполнения и распространения транзакций в permissioned-сетях

Архитектура

Архитектура блокчейн-среды подразумевает принцип формирования и распространения транзакций, формирование блоков в сети, поддержку СУБД, идентификацию пользователей, политику валидации и подтверждения.

В блокчейн-системах, поддерживающих permissionless архитектуру, подразумевается анонимность участников. В таких системах доверие основано только на неизменяемости состояния блокчейна.

Permissioned-блокчейны функционируют на модели управления с определенным уровнем доверия. Участники сети идентифицируемы и проверены. Это позволяет повысить безопасность взаимодействия между группой участников, а также исключает риск умышленного внедрения вредоносного кода через смарт-контракт. Все действия подвергаются проверке в соответствии с установленными для транзакций политиками подтверждения. Общая схема архитектуры исполнения и распространения транзакции в Permissioned-сетях представлена на рисунке 1.

Язык программирования

В блокчейн-сетях с архитектурой order-execute одним из требований является детерминизм смарт-контрактов. В противном случае консенсуса можно не достигнуть. Для исключения этой проблемы некоторые блокчейн-системы используют нестандартный язык или DSL для написания смарт-контрактов (таких, как Solidity) [1].

Такой подход не способствует распространению в сообществе разработчиков, поскольку им требуется потратить определенное время на изучение нового языка. Более того, данный подход может приводить к многочисленным ошибкам в коде. Существуют блокчейн-платформы (например, Hyperledger Fabric), которые поддерживают разработку смарт-контрактов на языках программирования общего назначения (Go, Java, Node.js), вместо использования DSL. Таким образом у организаций есть возможность разрабатывать смарт-контракты без необходимости изучения нового языка или DSL.

Наличие криптовалюты

Блокчейн-платформы, поддерживающие Permissioned-логику, характеризуются также отсутствием необходимости в использовании криптовалюты.

Основываясь на доверии к учетным записям пользователей в permissioned-сетях можно использовать более традиционные CFT или BFT консенсус-протоколы без необходимости в затратном майнинге. Отсутствие криптографических операций по производству криптовалюты (майнингу) позволяет развернуть платформу с приблизительно стандартными для любой распределенной системы операционными затратами. Отсутствие криптовалюты также исключает некоторые важные риски компьютерных атак [2].

Смарт-контракты

Бизнес-логика блокчейн-приложения заключается в смарт-контрактах. Смарт-контракты имеют сходство с объявлением классов в парадигме объектно-ориентированного программирования, состоят из набора переменных, которые используют для описания их состояний и набора функций, логика которых закладывается разработчиком таких контрактов [3].

Безопасность смарт-контрактов относительно атак является критически важной, поскольку смарт-контракты управляют ценными и важными ресурсами. При помощи атак возможна кража этих ресурсов или выведение контрактов из строя. Поскольку смарт-контракт исполняется на каждом узле, существует необходимость принятия комплексных мер по обеспечению безопасности всего блокчейна от таких контрактов, которые потенциально могут являться вредоносными.

Приватность и конфиденциальность

Блокчейн-сети, использующие public-permissionless архитектуру, работают по протоколу PoW, который подразумевает, что транзакции выполняются на каждом узле сети. Каждая транзакция и код, который ее осуществляет, видны каждому узлу в сети, что означает невозможность конфиденциальности ни самих контрактов, ни транзакционных данных, которыми они

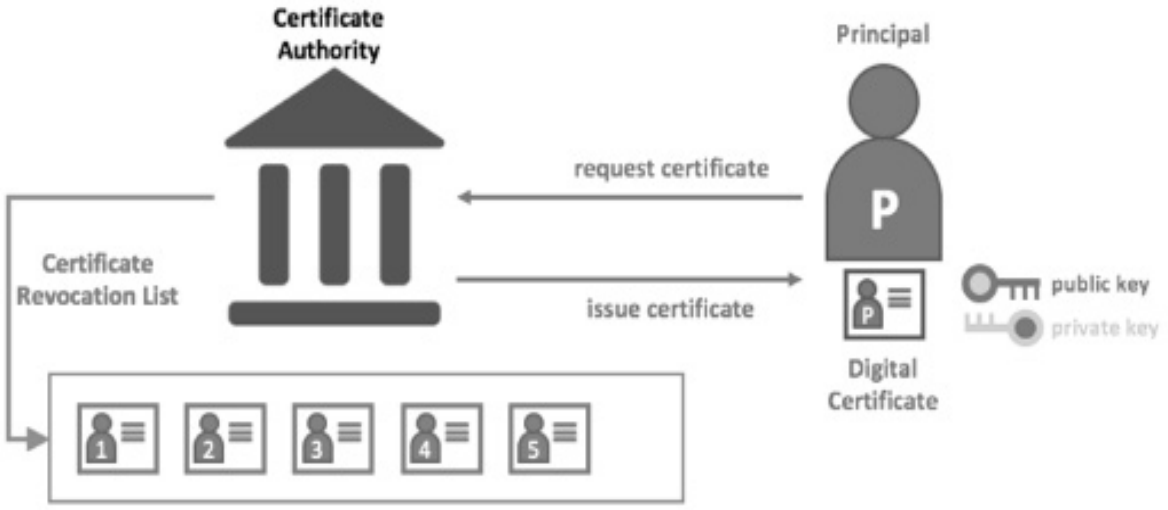

Рис. 2. Архитектура PKI

оперируют. Обладая достаточным количеством времени и вычислительных ресурсов, злоумышленник, вполне вероятно, может расшифровать такие данные.

Одним из способов обеспечения конфиденциальности является шифрование данных, в том числе доказательства с нулевым разглашением (Zero knowledge proofs, ZKP). Минус этого подхода состоит в том, что вычисление ZKP требует значительных временных и вычислительных ресурсов. Следовательно, в этом случае появляется вопрос соотношения производительности сети и конфиденциальности данных в ней.

В permissioned-архитектуре есть возможность реализовать альтернативные протоколы консенсуса, позволяющие распространять конфиденциальную информацию только на авторизованные узлы.

Аутентификация и целостность сообщений — важные концепции в области безопасной коммуникации. Аутентификация требует, чтобы стороны, которые обмениваются сообщениями были уверены в идентификации стороны, написавшей определенное сообщение. “Целостность” в контексте сообщения означает то, что оно не может быть изменено во время передачи.

Традиционные механизмы аутентификации основываются на цифровых подписях. Цифровые подписи также предоставляют гарантию целостности подписанного сообщения.

Получатели сообщений с цифровой подписью могут проверить автора сообщения и его целостность, проверив, что прилагаемая подпись валидна для публичного ключа ожидаемого отправителя.

Протокол консенсуса

Члены блокчейн-сети представляют собой узлы. Когда один из узлов хочет добавить данные в блокчейн, в сети формируется новый блок и при помощи алгоритма консенсуса добавляется в цепь. Подавляющее большинство блокчейн-платформ поддерживают архитектуру order-execure (упорядочить-выполнить). Протокол консенсуса валидирует и упорядочивает транзакции, а далее распространяет их на узлы сети, после чего все узлы сети обрабатывают транзакции в заданном порядке. Архитектура execute-order-validate (выполнить-упорядочить-валидировать) разбивает транзакционный поток на три шага:

- выполнить транзакцию и проверить ее корректность, запросив ее подтверждение;
- упорядочить транзакции с помощью (сменного) консенсус-протокола;
- валидировать транзакции через определенную для каждого типа транзакций политику подтверждения (endorsement policy), прежде чем занести их в реестр.

В блокчейн-сетях, работающих на execute-order-validate логике (например, Hyperledger Fabric), обязанность распределения (ordering) транзакций может быть передана модульному компоненту. Это сделано для того, чтобы консенсус был логически отделен от узлов, выполняющих транзакции и поддерживающих распределенный реестр. За ordering отвечает компонент под названием ordering service (служба распределения). Поскольку консенсус модульный, он может быть реализован с определенным уровнем доверия для конкретной системы. Такая модель позволяет использовать на платформе хорошо отработанные инструменты для CFT- или BFT-ordering’а [2].

Идентификация в блокчейн-сети. Цифровая личность

Участниками блокчейн-сети являются пиры, ordering-службы, клиентские приложения, администраторы и многие другие. Каждый участник — активный элемент, способный потреблять услуги, находящийся внутри сети или за ее пределами должен иметь цифровую личность (identity), инкапсулированную в цифровом сертификате X.509. Цифровая личность определяет разрешения на ресурсы и доступ к информации, которыми владеют участники блокчейн-сети. Помимо этого, identity имеет некоторые дополнительные атрибуты, которые используются для определения разрешений.

Чтобы цифровая личность была проверяемой, она должна исходить от trusted authority (доверенного органа). Это компонент, определяющий правила управления валидными identities для этой организации. Как правило, для этих целей можно использовать сертификаты X.509 в качестве identities, придерживаясь традиционной Public Key Infrastructure (PKI) иерархической модели [4].

Общая схема ассиметричной криптографии представлена на рисунке 2.

Ассимитричная криптография обеспечивает возможность шифровать и/ или подписывать сообщения электронной подписью. Для данных функций используется ключевая пара: открытый ключ используется для шифрования сообщения или проверки цифровой подписи, а закрытый — для расшифрования сообщений и для создания цифровой подписи. Ключевые компоненты связаны между собой однонаправленной функцией. Это означает что вычисление открытого ключа из секретного осуществляется за полиномиальное время, а вычисление секретного ключа по известному открытому является вычислительно сложной задачей [5].

На основании описанных критериев можно сформировать требования к распределенной системе для организации процессов документирования морских перевозок:

- Все пользователи должны быть идентифицированы в системе;
- Формировать транзакции могут только авторизованные пользователи, имеющие на это право;
- Пользователи могут вносить информацию в транзакции в соответствии с матрицей разрешений;
- Высокая производительность транзакций;
- Короткая задержка подтверждения транзакций;
- Приватность и конфиденциальность транзакций и связанных с ними данных;
- Никто не может сформировать транзакцию вместо другого пользователя (реализуется за счет асимметричной криптографии);
- Каждый пользователь может проверить, что его данные записаны в сеть;
- Каждый знает кто участвовал в цепочке, а кто нет.

Из-за децентрализованной топологии и криптографических механизмов, использовать информацию в преступных целях становится затруднительно и финансово-затратно, при этом сама информация должна оставаться доступной для авторизованных участников в соответствии политикой разрешений.

В отношении документирования процессов морских перевозок блокчейн позволяет эффективно реализовать ключевые аспекты информационной безопасности информации путем сочетания свойств распределенного реестра с блочной структурой данных, основанной на криптографической связанности.

ЛИТЕРАТУРА

1. Mayukh Mukhopadhyay. Ethereum Smart Contract Development — Packt Publishing Ltd., 2018–381 с., ISBN978–1–78847–304–0
2. Hyperledger Fabric documents. [Электронный ресурс] URL: https://hyperledger-fabric.readthedocs.io/
3. Прасти Н. П70 Блокчейн. Разработка приложений: Пер. с англ.— СПб.: БХВ-Петербург, 2018.— 256 с.: ил. ISBN978–5–9775–3976–0
4. Учебное пособие «Криптографические методы защиты информации» Владимиров С.М., Габидулин Э.М., Колыбельников А.И.
5. «Основы криптографии» Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В.— М.: Гелиос АРВ, 2001