

Технология блокчейн в фармацевтической цепочке поставок. Исследование примера бизнес-модели на основе Hyperledger Fabric

С.Р. Брятов¹, А.А. Бородинов¹

¹Самарский национальный исследовательский университет имени академика С.П. Королева 34, Московское шоссе 34А, Самара, Россия, 443086

Аннотация. Фармацевтические компании, производящие, отгружающие и поставляющие продукцию, сталкиваются с трудностями при отслеживании своих товаров, что позволяет фальшивомонетчикам внедрять поддельные лекарства в систему. Данная ситуация наблюдается, в частности, на Российском рынке оборота фармацевтических средств, хотя проблема носит давно уже глобальный характер. Способность blockchain-систем точно устанавливать происхождение данных делает их особенно подходящими для применения в сфере фармацевтической цепочки поставок. Хранимые в общем распределенном реестре данные об идентификации произведенных заводом препаратов, а также записи об их перемещениях по всей цепи поставок могут позволить с точностью определить подлинность фармацевтических товаров, лежащих на прилавках аптек. Разработка и внедрение данной системы может стать большим шагом к победе в изнурительной борьбе с легкой доступностью поддельных лекарств и медицинских продуктов, как на локальных, так и мировых рынках. В первой части данной работы будут исследованы основные характеристики и особенности функционирования blockchain-систем. Во второй, и заключительной, части будет исследован спроектированный концепт системы контроля оборота фармацевтических средств на основе blockchain-технологии Hyperledger Fabric с использованием среды разработки Hyperledger Composer.

1. Введение

В недавнем докладе Всемирной Организации Здравоохранения контрафакция лекарственных препаратов была квалифицирована как глобальная проблема. По его оценкам, в странах с низким и средним уровнем дохода каждый 10-й препарат, находящийся в рыночном обороте, является фальсифицированным или некачественным [1]. Использование таких некачественных изделий может негативно сказаться на показателе смертности населения.

Лекарственные препараты перемещаются по цепочке поставок, в которой участвуют несколько участников. К ним, как правило, относятся производитель, оптовик и розничный торговец. Они занимаются производством, транспортировкой и продажей данных изделий. Также в данных системах имеется наличие ключевого участника - регулирующего органа, отвечающего за каждый этап перемещения партий изделий по всей цепи. В частности, на государственном уровне данным участником может являться некоторый уполномоченный орган государственного аппарата, к примеру, специальное ведомство по контролю оборота лекарственных изделий. Его главная задача - делегирование прав на производство

лекарственных препаратов по государственным стандартам, а также контроль за перемещением всех когда-либо произведенных единиц товара.

Что же касается потребителя, здесь возникает еще одна проблема - контроль лекарств, отпускаемых только по рецепту врача. Отпуск лекарств без рецепта является подсудным делом, однако контроль за честностью розничных продавцов, также, как и с поддельными лекарствами, является непростым делом, требующим особого продуманного подхода.

Некоторые фармацевтические компании уже начали внедрение технологии blockchain в управление цепочками поставок лекарств. Blockchain - это электронный криптографический реестр, основанный на децентрализованной сетевой модели, в котором информация распределяется и синхронизируется между всеми узлами в сети. Такое функционирование обеспечено алгоритмом консенсуса, развёрнутым в системе для устранения проблемы дублирования транзакций, позволяющим узлам проверять истинность информации перед её непосредственной записью в реестр. Кроме того, данная система обладает высокой отказоустойчивостью. Пороговое значение числа отказавших узлов до полного отказа сети зависит от общего числа узлов, подключенных к сети. Таким образом, чем больше узлов функционирует в blockchain сети, тем меньше вероятность полного отказа системы.

Правильно спроектированная система на основе технологии blockchain сможет существенно упростить процесс контроля оборота лекарственных средств для уполномоченных государственных органов. Наряду с этим, децентрализованный подход имеет ряд преимуществ, повышающих информационную безопасность таких систем по сравнению с централизованными аналогами.

В разделе 1 данной работы будут исследованы основные характеристики и методы функционирования blockchain-систем. Раздел 2 посвящен исследованию концепта проектируемой системы по контролю оборота лекарственных средств с регуляцией на государственном уровне.

2. Blockchain сети

2.1 Технология blockchain

Blockchain - выстроенная по определённым правилам непрерывная последовательная цепочка блоков, содержащих информацию. Чаще всего копии цепочек блоков хранятся на множестве разных компьютеров независимо друг от друга. [2]

Совокупность таких компьютеров, собранных в сеть, работающую по единому протоколу добавления новых блоков в цепочку, т.е. проведения транзакций, образует сеть Blockchain [3].

Таким образом, сеть Blockchain - это распределенная информационная система, являющаяся как базой данных, так и вычислительной системой, которая содержит информацию обо всех транзакциях, когда-либо выполненных в прошлом и работающая по заранее выбранному протоколу, определяющим ход проведения и валидации транзакций, и работы всей сети и её участников, в целом [4]. Также, данную сеть обычно называют распределенным реестром, так как данные о каждой транзакции такой сети хранятся на каждом узле, оперирующем в ней.

Всего можно выделить 3 типа blockchain-систем:

1. Публичный blockchain (Public Blockchain или Permissionless Blockchain)
2. Blockchain Консорциума (Consortium Blockchain)
3. Частный blockchain (Private Blockchain)

В публичном blockchain каждый участник имеет возможность увидеть и проверить любую транзакцию, проходящую в сети, а также может участвовать в процессе достижения консенсуса. В публичном blockchain нет администрирующего узла, проверяющего транзакции, валидность достигается консенсусом между участниками. Bitcoin и Ethereum - яркие примеры данного типа сетей.

В blockchain консорциума существует администрирующий узел, которой выбирается участниками сети изначально исходя из оптимальных путей достижения своих бизнес-целей, например, в случае с партнерством. Данные в таких сетях могут быть общедоступными и закрытыми (например, конфиденциальная информация), поэтому сама сеть может быть

расценена как частично децентрализованная. Примером такой сети может послужить платформа Hyperledger.

Частный blockchain схож с предыдущим типом за исключением одного аспекта. Все данные такого распределенного реестра являются строго закрытыми от общего обозрения, то есть частными. Только уполномоченные административным узлом участники могут получить доступ к разрешённой им информации. Платформы Multichain или Hyperledger могут быть использованы для построения таких решений [5][6].

Выбор определенного типа сети зависит от поставленной задачи. Например, для малых бизнесов, где между филиалами ведётся бухгалтерский учёт отдельным учреждением, подходящим вариантом будет использовать частную blockchain сеть, в которой распределённый реестр станет единым источником правды. А в ситуации, например, с цепью поставок, где потребитель хочет знать всё о полученном продукте, подойдёт сеть с консорциумом. Данные о продукте являются доступными всем участникам, однако их запись ведётся уполномоченными лицами-узлами, например, продавцом, заводом и поставщиком сырья.

2.2 Функционирование blockchain систем. Консенсус-механизмы.

Группы транзакций в сетях blockchain объединяются в блоки транзакций, соединяемые друг за другом по цепочке с помощью хеш-записей о предыдущем блоке (рисунок 1).

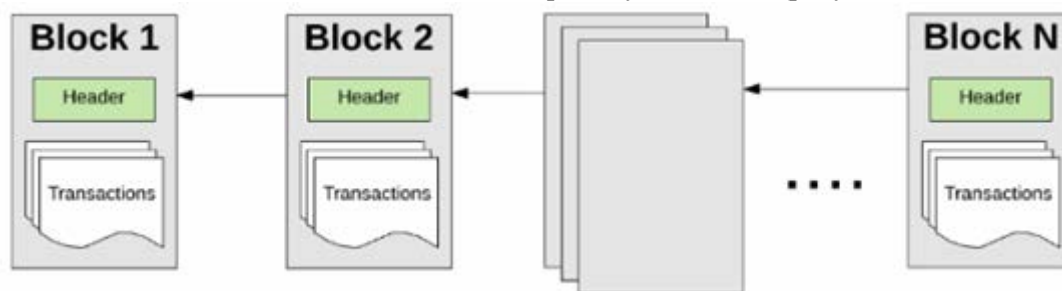


Рисунок 1. Структура цепи blockchain –систем.

Таким образом, реализуется основной механизм безопасности сетей blockchain в виде свойства неизменности. Чем дальше блок располагается по цепочке (чем он старше), тем более защищенными от изменения являются данные, заключённые в нём. Если узел злоумышленника попытается изменить какой-либо из блоков, его локальный реестр автоматически перестанет быть валидным, так как хеш-значения внутри заголовков следующих блоков будут уже совершенно иными, исходя из механизма работы хеш-функций.

Blockchain системы не нуждаются в доверенном третьем лице для достоверной регистрации транзакций в реестре. Вместо этого используются децентрализованные механизмы консенсуса, гарантирующие выполнение транзакций надлежащим образом. В существующих blockchain -сетях одними из наиболее популярных являются следующие [7]:

1. Proof of Work (PoW)
2. Proof of Stake (PoS)
3. Practical Byzantine Fault Tolerance (PBFT)
4. Delegated Proof of Stake (DPoS)

На практике также часто применяются решения, совмещающие в себе комбинацию таких механизмов.

В рамках исследования остановимся на алгоритме Practical Byzantine Fault Tolerance (PBFT), который основывается на известной задаче о Византийских генералах [8]. Для достижения согласия в сети данный алгоритм предполагает, что не более 1/3 узлов будут недоброжелательными. Весь процесс можно разделить на три этапа: подготовка, подготовленное состояние и фиксация консенсуса. На каждом этапе узел вступает в следующую фазу, если он получил голоса более чем от 2/3 всех узлов. Таким образом PBFT

требует, чтобы каждый узел был известен в сети. В итоге, финальное решения о валидации блока предоставляется трети доверенным по итогам всеобщего голосования узлам.

Платформа Hyperledger Fabric[9], которая будет рассмотрена в следующей главе, использует PBFT в качестве алгоритма консенсуса.

3. Проектирование информационной системы контроля оборота лекарственных средств

3.1 Платформа Hyperledger Fabric

Государство играет ключевую роль в цепочке поставок лекарственных препаратов, являясь всеобщим регулятором взаимодействия между участниками системы. Только государство имеет право устанавливать нормы взаимоотношений между организациями и потребителями, а также только его органы могут заниматься регистрацией лекарственных препаратов и выдачей лицензий на их производство, а также продажу и выписку рецептов. Поэтому при проектировании системы контроля оборота лекарственных средств было решено взять частную модель blockchain-сети и сделать её администратором подконтрольное государству ведомство. Таким образом, платформа Hyperledger Fabric, предлагающая широкий набор инструментов для построения решений на основе частных blockchain сетей стала основой данного проекта.

Так как сети на основе Hyperledger Fabric являются частными, все их узлы имеют разные роли в системе. Всего существует 3 типа узлов:

- Клиентские узлы. Они являются конечными пользователями и имеют право совершать заказ исполнения транзакций.
- Основные узлы. Данный тип узлов занимается управлением исполнением и проверки транзакций. Однако, не все узлы данного типа непосредственно принимают участие в исполнении кода умных контрактов. Для этого существуют специальные узлы-поручители, которые выбираются исходя из условий выполняемого контракта.
- Сервисные узлы. Занимаются формированием блоков транзакций и обновлением состояния распределенного реестра. Также используются при проведении конфигурационных транзакций администраторами сети. Созданы для упрощения изменения алгоритма консенсуса в сети при необходимости.

Текущий проект базируется на использовании фреймворка Hyperledger Composer, созданного для упрощения разработки blockchain-систем на основе Hyperledger Fabric. С помощью него, можно получить единый конфигурационный файл системы, который впоследствии может быть использован администратором для перепрограммирования поведения всей сети. Для успешного создания конфигурации требуется 4 различных источника:

1. Файлы моделей.
2. Файлы скриптов транзакций.
3. Список контроля доступа.
4. Скрипты запросов.

Файлы моделей определяют структуру основных сущностей, создаваемые в распределенном реестре: ассетов, участников и описаний транзакций. Ассеты представляют собой цифровое имущество и документы, в данном случае это могут быть единицы лекарств, выдаваемые лицензии и договоры между участниками оборота. Участниками же являются ассеты-карточки, содержащие основную информацию о пользователях системы и их принадлежности к другим ассетам. Описания транзакций содержат данные, передаваемые как аргументы функций скриптов транзакций.

Файлы скриптов транзакций описывают код умных контрактов (chaincode), исполняемый узлами-посредниками. В данном фреймворке скрипты должны быть написаны на популярном языке JavaScript.

Списки контроля доступа определяют права участников на доступ к определённым ресурсам системы, права на чтение, запись и изменение ассетов, а также исполнение как системных транзакций, так и созданных на основании скриптов транзакций при разработке бизнес-модели. С помощью скриптов запросов данные могут быть легко извлечены из реестра blockchain. Обычно они используются для отображения данных во front-end приложениях, либо в коде

создаваемых скриптов транзакций, увеличивая тем самым эффективность повторного использования уже разработанного кода.

3.2 Архитектура предлагаемого решения

На следующей схеме представлено взаимодействие участников сети с распределенным реестром Hyperledger Fabric в рамках разрабатываемого проекта (рисунок 2):

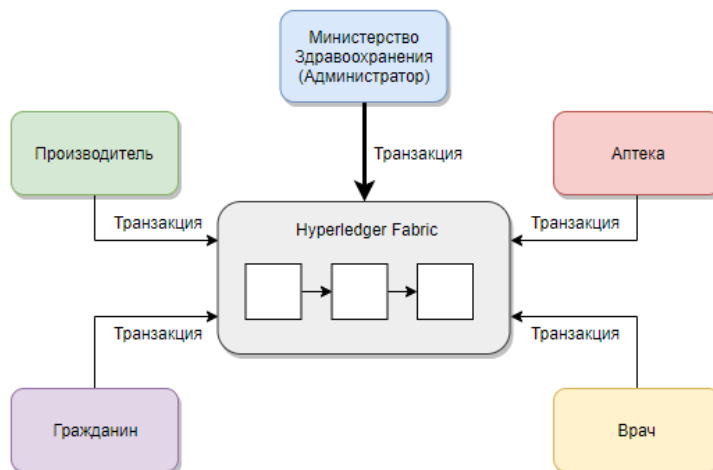


Рисунок 2. Участники информационного обмена.

Каждый участник системы обладает своими определёнными правами на чтение данных из реестра и выполнение транзакций для его модификации. Для доступа к карточке участника оператор клиентского приложения должен быть идентифицирован в системе на основе закрытого и открытого ключей.

Таким образом, в разрабатываемой системе можно выделить следующие виды участников информационного обмена:

1. Государство. Является как администратором, так и разработчиком сети, владеет всеми узлами реестра. Аккаунт Государства имеет возможность регистрировать остальных участников сети и производить транзакции по выдаче лицензий на производство лекарств производителям. Также регистрирует новые лекарства в информационной системе.

2. Производитель. Производит товар и принимает заказы со стороны аптеки. Аккаунт производителя имеет возможность производить регистрацию единиц лекарств в системе на основе уникального идентификатора (uuid), а также создавать транзакции о передаче прав на владение единицей лекарства аптеке.

3. Аптека. Продаёт товар гражданам. Аккаунт аптеки имеет возможность создания транзакции на передачу прав владения лекарств гражданину. Если лекарство отпускается без рецепта, делает отметку о том, что лекарство было продано, в другом случае обязуется внести в реестр данные о продаже лекарства гражданину, аккаунт которого имеет право на покупку определенного типа лекарства. Транзакция одобряется узлами, если в системе существует рецепт врача с ссылкой на данный тип лекарства и аккаунт покупателя, а также поле количества возможных покупок единиц лекарств в рецепте больше 0. С каждой продажей данный счетчик убывает.

4. Врач. Выписывает рецепт своим пациентам (гражданам), в котором производит отметку о видах лекарств и их количестве, необходимых для излечения, а также ссылку на аккаунт гражданина и заносит эти данные в распределённый реестр Hyperledger Fabric.

5. Гражданин. При покупке лекарств по рецепту обязательно должен предъявить свой виртуальный идентификатор, ссылающийся на его аккаунт в государственном реестре. Таким образом, конец жизненного цикла ресурса единицы лекарства в системе - отметка аптекой о продаже определенной единицы в виртуальном рецепте врача, а также отметка на единице

лекарства последнего владельца - Гражданина или Государства, если лекарство было продано без рецепта.

Далее приведена упрощённая реляционная модель связей между ассетами системы (рисунок 3):

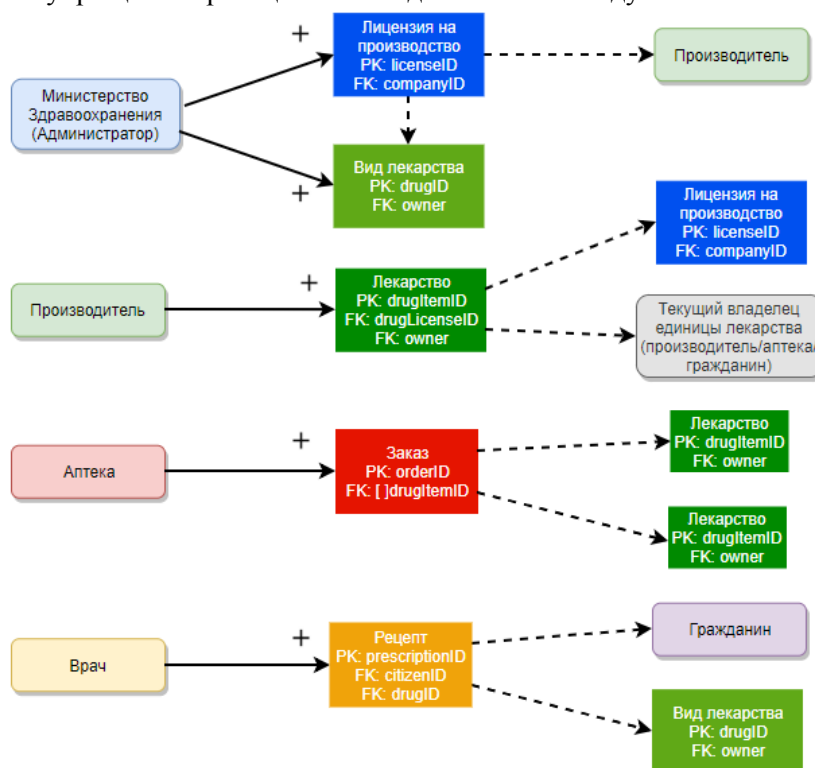


Рисунок 3. Упрощенная реляционная модель предлагаемого решения.

Обычные стрелки со знаком “+” на схеме выше определяют транзакции по созданию указанного ассета определенным участником сети. Пунктирные стрелки обозначают связи ассетов между собой по внешнему ключу.

3.3 Принципы работы проектируемой информационной системы. Сильные и слабые стороны.

Система контроля оборота лекарственных средств все еще находится в разработке, поэтому на данном этапе невозможно предоставить финальный список основных транзакций системы. Однако можно выделить основные из них, приведя примерную картину функционирования рабочего прототипа. Для наглядности, проследим за полным жизненным циклом фармацевтического препарата:

1. Государство разрабатывает спецификацию лекарственного средства и регистрирует новый препарат в распределенном реестре с помощью транзакции создания ассета “Тип лекарства”. Для предоставления возможности производства оно также регистрирует “Лицензию на производство” и выдает её зарегистрированному участнику-производителю, указывая ссылку на его аккаунт. В случае отзыва лицензии, существует транзакция, помечающая лицензию как “недействительная”. Также есть необходимость в транзакции о её продлении.
2. Производитель создаёт “Лекарство”, идентифицируя его уникальным кодом, заносит ссылку на “Тип лекарства” и заполняет поля о сроке годности.
3. Аптека производит “Заказ” и отмечает в нем количество необходимого товара и его тип. По ходу выполнения заказа, производитель привязывает к данному ассету ссылки на уникальные номера единиц товара со склада. Также он производит транзакции об изменении статуса заказа. При доставке, поле “собственник” на единице лекарства становится равным идентификатору получателя, т.е. аптеки.

4. Врач выписывает “Рецепт” своему пациенту. Гражданин покупает лекарство, предоставляя свой цифровой медицинский полис, который в данном случае привязан к ассету его аккаунта. Там же содержится ссылка на предоставленный рецепт. В аптеке происходит транзакция продажи, которая становится успешной только в случае остатка баланса счётчика по данному типу лекарства в рецепте клиента. Гражданин становится владельцем как реальной, так и виртуальной единицы лекарства. Лекарство без рецепта отпускается свободно, его ассет помечается флагом “продано”, а последним владельцем становится государственный аккаунт.

Таким образом, каждая лицензированная единица лекарства оставляет за собой уникальный след в реестре, который без труда можно отследить при возникновении спорных ситуаций.

Применение данной системы на практике должно упростить процесс контроля за официальными цепочками поставок лекарственных средств. Прозрачность системы будет мотивировать её участников соблюдать установленные законом нормы.

К слабым сторонам данного проекта можно отнести следующие ограничения:

- Предлагаемая система будет способна выявлять только те перемещения лекарственных препаратов, которые следуют официальными цепочками поставок, известными регулирующему ведомству. Она не может отслеживать фальсифицированные лекарства, которые распространяются по маршрутам за пределами официальных цепочек оборота.
- Предлагаемая система будет разрабатываться и тестироваться в контролируемой моделируемой сети; поэтому результаты, полученные в результате следующих исследований, могут не отражать фактическую производительность при развертывании в реальных условиях.

4. Заключение

На данном этапе реализована реляционная модель, продуманы основные участники системы и их роли. Разработка проекта продолжается. Следующим этапом станет разработка скриптов транзакций умных контрактов и списков разграничения доступа. После завершения разработки прототипной модели системы предполагается проведение нескольких тестов на виртуальных машинах под управлением ОС Ubuntu 18.04. В случае успеха, следующим этапом станет создание front-end архитектуры для удобства доступа пользователей к работе с проектируемой системой.

Blockchain технологии являются ещё довольно молодыми и с точностью нельзя сказать, приживутся ли они в дальнейшем ввиду многих своих концептуальных ограничений. Однако подобные исследования, как система контроля оборота лекарственных средств, могут впоследствии стать примером для появления более продвинутых решений по автоматизации процессов деятельности государственного аппарата с обеспечением максимального уровня информационной безопасности обрабатываемых данных.

5. Литература

- [1] World Health Organization. 1 in 10 medical products in developing countries is substandard or falsified: WHO urges governments to take action [Electronic resource]. – Access mode: <http://www.who.int/en/news-room/detail/28-11-2017-1-in-10-medical-products-in-developing-countries-is-substandard-or-falsified> (19.01.2018).
- [2] Википедия, Блокчейн [Электронный ресурс]. – Режим доступа: <https://ru.wikipedia.org/wiki/%D0%91%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD> (21.04.2018).
- [3] Dennis, R. A temporal blockchain: A formal analysis / R. Dennis, G. Owenson, B. Aziz // International Conference on Collaboration Technologies and Systems, 2016. – P. 430-437.
- [4] Singh, S. Blockchain: Future of financial and cyber security / S. Singh, N. Singh // 2nd International Conference on Contemporary Computing and Informatics, 2016. – P. 463-467.
- [5] Hackernoon [Electronic resource]. – Access mode: <https://hackernoon.com/3-popular-types-of-blockchains-you-need-to-know-7a5b98ee545a> (21.04.2018).

- [6] Zheng, Z. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends / Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang // IEEE 6th International Congress on Big Data, BigData Congress, 2017. – P. 557-564.
- [7] Zheng, Z. Blockchain challenges and opportunities: A survey / Z. Zheng, S. Xie, H.-N. Dai, H. Wang, // Internat. J. Web Grid Serv, 2016. DOI: 10.1504/IJWGS.2018.095647.
- [8] Wikipedia, Byzantine fault tolerance [Electronic resource]. – Access mode: https://en.wikipedia.org/wiki/Byzantine_fault_tolerance. (21.04.2018).
- [9] Hyperledger Project [Electronic resource]. – Access mode: <https://www.hyperledger.org/>. (16.05.2018).

Blockchain technology in the pharmaceutical supply chain: researching a business model based on Hyperledger Fabric

S.R. Bryatov¹, A.A. Borodinov¹

¹Samara National Research University, Moskovskoe Shosse 34A, Samara, Russia, 443086

Abstract. Pharmaceutical companies that manufacture, ship and supply products face difficulties in tracking their products, allowing counterfeiters to inject counterfeit drugs into the system. This situation is observed, in particular, in the Russian market of turnover of pharmaceutical products, although the problem has long been global. The ability of blockchain systems to pinpoint the origin of data makes them particularly suitable for pharmaceutical supply chain applications. The data stored in the blockchain distributed register on the identification of drugs produced by the plant, as well as records of their movements throughout the supply chain, can accurately determine the authenticity of pharmaceutical products lying on the shelves of pharmacies. The development and implementation of such a system can be a big step towards winning the exhausting fight against the easy availability of counterfeit drugs and medical products. In the first part of this work, the main characteristics and features of the functioning of blockchain systems will be studied. In the second and final part, the designed concept of the pharmaceutical turnover control system based on the blockchain technology Hyperledger Fabric using the Hyperledger Composer development environment will be investigated.