Секция «Компьютерное право и информационная безопасность»

Использование смарт-контрактов в государственном секторе

Научный руководитель – Зуева Анна Сергеевна

Боброва Екатерина Олеговна

Студент (магистр)

Московский государственный университет имени М.В.Ломоносова, Высшая школа государственного аудита, Кафедра информационной безопасности и компьютерного права, Москва, Россия

E-mail: cat.katrin@rambler.ru

В последние годы наблюдается тенденция применения технологии блокчейн в самых разных сферах: экономика, производство, образование, здравоохранение, бизнес. При этом, движущим механизмом бизнес-логики в блокчейне являются смарт-контракты [1]. В эпоху цифровизации заключение договорных отношений между сторонами при помощи нотариусов становится все менее актуально. В статье ГК РФ 141.1 определены такие понятия, как «цифровые права», «токены», а также ряд других терминов в цифровой экономике, вследствие чего становится возможным использование смарт-контрактов вместо существующих стандартных рукописных договоров. Как одним из вариантов обмена, для выполнения обязательств между двумя сторонами, используют относительно новую технологию, которая называется смарт-контракты.

Цель: определить уровень безопасности использования смарт-контракта в государственном секторе.

Задачи:

1. Проанализировать существующие критерии определения безопасности использования смарт-контракта в государственном секторе.

2. Провести сравнительный анализ существующих алгоритмов определения безопасности смарт-контрактов.

3. Разработать рекомендации по оптимизации использования смарт-контракта в государственном секторе.

Наличие уязвимостей в смарт-контрактах является фундаментальной проблемой большинства использующих их систем на основе технологии распределенных реестров, поскольку эксплуатация злоумышленником даже самой незначительной уязвимости в смарт-контракте может привести к сбою всей функциональности системы.

Результатом анализа исходного смарт-контракта по предложенной методике является генерация детального отчета на основе результатов расчетов и определения уровня безопасности смарт-контракта. В данном отчете содержится такая полезная информация, как уровень безопасности смарт-контракта, выявленные уязвимости и ошибки в процессе анализа, а также меры по устранению найденных уязвимостей.

К возможным подходам применения смарт-контрактов в сфере государственных услуг можно отнести проведение процедуры голосования на основе смарт-контрактов, организацию хранения электронных документов, в том числе нормативно-справочного характера. В перспективе применение смарт-контрактов позволит повысить прозрачность работы государственного сектора, снизить риски коррупции и искажения информации, увеличить эффективность взаимодействия с государственными органами.

Наличие уязвимостей в смарт-контрактах является фундаментальной проблемой большинства использующих их систем на основе технологии распределенных реестров, поскольку эксплуатация злоумышленником даже самой незначительной уязвимости в смарт-контракте может привести к сбою всей функциональности системы.

Смарт-контракт не обладает функциональной гибкостью. При использовании традиционных механизмов заключения соглашения всегда есть возможность договориться или изменить его условия, но при использовании смарт-контрактов реализовать такие изменения в ходе его исполнения затруднительно [3].

Отсутствие в мировой законодательной практике официально закрепленного статуса смарт-контракта может затруднить решение спорных вопросов, возникающих при нарушении условий его исполнения.

Для того, чтобы смарт-контракт получился безопасным и не содержал уязвимых конструкций, следует придерживаться следующих правил:

1. Необходимо выбрать разработчика для написания смарт-контракта. Большинство компаний, которые хотят использовать смарт-контракты в коммерческих отношениях, не разрабатывают контракты сами, а прибегают к помощи специализированных организаций.;
2. Рекомендуется использовать среду для разработки и тестирования смарт-контрактов (например, IDE Remix), которая позволяет выявлять мелкие ошибки и неточности, а также проверять, компилируется ли код вообще [2];
3. Не стоит использовать лишние переменные или функции, которые никак не влияют на работоспособность контракта;
4. После написания смарт-контракта, необходимо перейти к полноценному тестированию. В качестве инструмента возможно использование такой среды, как Truffle, DApple, EmbarkJS;
5. Проверив смарт-контракт силами разработчика на ошибки и возможные уязвимости, также необходимо прибегнуть к аудиту контракта сторонними специалистами. Аудиторы осуществят проверку смарт-контракта и затем отправят отчет заказчику;
6. Завершающим этапом перед погрузкой смарт-контракта на блокчейн-платформу, рекомендуется прибегнуть к использованию Bug Bounty - схеме, при которой код выкладывается в git-репозиторий и всех желающих приглашают за вознаграждение (обычно токенами) найти ошибки.

Только пройдя все стадии разработки, начиная от выбора языка программирования, написания контракта и заканчивая тестированием, независимым аудитом и использованием подхода Bug Bounty, можно с уверенностью сказать, что разработанный смарт-контракт полностью соответствует требованиям безопасности и готов для дальнейшей погрузки на блокчейн-платформу для выполнения функций, которые заложены внутри него.

Источники и литература

1) Вашкевич А. М. Смарт-контракты: что, зачем и как. — М.: Симплоер, 2018.
2) Осмоловская А.С., Смарт-контракты: функции и применение. Иркутский государственный университет, г. Иркутск. 2018
3) Аналитический обзор по теме «смарт-контракты», Центральный банк Российской Федерации. [Электронный ресурс], 2018, URL: https://www.cbr.ru/Content/Document/File/10.*pdf*