УДК 004.056.55

МАТЕМАТИЧЕСКИЕ ОСНОВЫ СМАРТ-КОНТРАКТОВ

Данильченко Д.И., Хралович Ю.А.

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники» филиал «Минский радиотехнический колледж», г. Минск, Республика Беларусь

Тынкович В.В., преподаватель высшей категории дисциплин естественно-математического цикла

Аннотация. Исследована подчинённость технологии смарт-контрактов к математическим наукам. Описаны методы шифрования в смарт-контрактах, которые осуществляются с помощью криптографии, и разобраны их преимущества. Установлено, что применение шифрования гарантируют максимальную надежность исполнения смарт-контрактов. Так же рассмотрены основные принципы работы технологии смарт-контрактов.

Ключевые слова: смарт-контракты, криптография, шифрование.

Введение. В сегодняшнем мире широкое распространение получили криптовалюты. Криптовалюты являются разновидностью цифровой валюты, однако в отличии от фиатных цифровых валют (валют, номинальная стоимость которых устанавливается и гарантируется государством), криптовалюты основаны на децентрализованных системах, работающих в автономном, или почти автономном режиме. В основе принципа работы этих механизмов лежат смарт-контракты. Принципы работы смарт-контрактов в свою очередь тесно связаны с математическими науками, что и будет являться темой данной статьи.

Основная часть. Определение и история смарт-контрактов. Смарт-контракт – это компьютерная программа или протокол транзакции, предназначенный для автоматического выполнения, контроля или документирования юридически значимых событий и действий в соответствии с условиями контракта или соглашения [1]. Целями смарт-контрактов являются сокращение потребности в доверенных посредниках, снижение расходов на арбитраж и правоприменение, убытков от мошенничества, а также сокращение злонамеренных и случайных исключений.

Смарт-контракты были впервые предложены в начале 1990-х годов Ником Сабо, который придумал этот термин, используя его для обозначения «набора обещаний, указанных в цифровой форме, включая протоколы, в рамках которых стороны выполняют эти обещания». В 1998 году этот термин использовался для описания объектов на сервисном уровне управления правами системы The Stanford Infobus, которая была частью проекта Stanford Digital Library Project.

Практические реализации смарт-контрактов стали возможными благодаря появлению в 2008 году технологии блокчейн. Некоторые принципы умных контрактов были заложены уже в первом протоколе такой криптовалюты как Bitcoin, однако они не были реализованы в клиентском программном обеспечении, не обладали полнотой по Тьюрингу из соображений безопасности и широко не использовались на практике.

Смарт-контракты впервые получили широкое распространение с появлением криптовалюты Ethereum.

«White paper» 2014 года о криптовалюте Ethereum описывает протокол Bitcoin как слабую версию концепции смарт-контракта. Начиная с этого момента, различные криптовалюты поддерживают языки сценариев, которые позволяют использовать более продвинутые смарт-контракты между сторонами. Смарт-контракты следует отличать от смарт-юридических контрактов. Последнее относится к традиционному юридически обязывающему соглашению на естественном языке, в котором определенные условия выражены и реализованы в машиночитаемом коде.

Основные принципы работы смарт-контрактов. Если сравнивать работу смарт-контрактов с повседневными для нас вещами, то мы бы могли представить их в роли нотариусов, которые гарантируют надлежащее исполнение условий, заключенного договора. Главным отличием является автоматизация процесса, которая позволяет существенно увеличить скорость совершения сделки.

Смарт-контракты не требуют участия человека в их исполнении. На этапе создания достаточно корректно прописать обязательства его выполнения и дальше процесс будет развертываться автоматически. Как и в версии традиционных реальных контрактов, смарт-контракты имеют возможность регламентировать санкции в случае невыполнения условий договора.

В современном мире идет активная цифровизация всех процессов, благодаря чему смарт-контракты могут стать неотъемлемой частью нашего общества. Фактором такого явления является улучшенный процесс выполнений обязательств, нежели физические аналоги. Поскольку смарт-контракты обеспечивают максимальную безопасную среду для хранения, которая обуславливается шифрованием большего количества информации, риски взлома сведены к минимуму.

Участие человека в жизненном цикле смарт-контракта имеется только на этапе его программирования. Остальное время он полностью автономен, что позволяет избежать задержек в его работе. Также избежание вмешательства третьих лиц позволяет избежать комиссию за их работу. Это дает возможность экономить значительную часть денег как юридическим, так и физическим лицам.

Автономность и надежность смарт-контрактов обеспечивается благодаря различным методам криптографии. Для шифрования смарт-контрактов в зависимости от назначения и сферы могут применятся различные криптографические методы, однако среди них есть и обязательные [2]:

– приватная Blockchain-сеть;

– электронная подпись;

– договор, утвержденный подписями сторонами, между которыми производится транзакция;

– предмет договора и инструментарий для выполнения условий и обязательств между сторонами;

– математический алгоритм с ясной логикой и последовательностью действия, который представляет собой условия для совершения транзакции.

Уже сейчас начинается переход на смарт-контракты в различных отраслях нашей жизни. Особое внимание стоит уделить решению вопроса, который присуще большинству демократических государств – выборы. Используя преимущества технологий блокчейна, смарт-контракты позволяют использовать максимальный уровень защиты, что делает невозможным декодирование и доступ к данным третьих лиц. Скорость проведения вы боров, которую обеспечивают высоконадежное кодирование результатов голосования, а также высокую вычислительную способность, в разы превышает, в разы превышает обычную систему.

Обязательно нужно учитывать, наличие и недостатков технологии, большинство которых вытекает из ее преимуществ. Прозрачность действий, которую гарантирует блокчейн, исключает возможность на конфиденциальность. Любой участник сети может узнать полную информацию о смарт-контракте. Однако, появляются платформы, которые дают возможность создания частного смарт-контракта, который гарантирует конфиденциальность.

Хоть смарт-контракты и обладают высокой надежностью защиты, но уязвимость могут создать сами программисты на этапе разработки. Это деятельность требует больших навыков и опыта, иначе в случае неисправного кода может появится возможность взлома или средства, фигурирующие в смарт-контракте, все будет заблокированы. Необходим ответственный подход при поиске специалистов для написания смарт-контракта. Если такой человек окажется мошенником, то он сможет скомпрометировать код так, что одна из сторон понесет убытки при осуществлении сделки.

Исполнение смарт-контракта. Смарт-контракты развертываются в пределах определенного блокчейна. Существует возможность переноса смарт-контракта из одного блокчейна в другой в другой, но самостоятельное существование без блокчейна невозможно.

Существует множество платформ, которые обеспечивают смарт-контрактам, которые предлагают разную функциональность в его работе. Из основных платформ можно выделить Ethereum, Solana, Avalanche, Tron и многие другие. Все приложения, присоединенные к сети, должны использовать одну и ту же версию смарт-контракта, чтобы совместно реализовать идентичные совместно используемые бизнес-процессы и данные.

На данный момент Ethereum является лидером рынка, если мы говорим про развертывание смарт-контракта. Solidity является языком написания смарт-контрактов в сети Ethereum.

Криптография. Шифрование является способом способ сокрытия и раскрытия, в котором применяется сложная математика. Изначально мы имеем незашифрованные данные, которые представлены в виде какого-либо фрагмента текста, который преобразуется в шифр. Для пользователя этот шифр не сможет предоставить информации и будет бесполезен. Такой метод именуется как шифрование с симметрическим ключом.

На рисунке 1 показано, как выглядел один из первых шифров. Он использовался для сокрытия военных тайн армией Римской империи. Сутью его являлось смещение каждой буквы на три пробела в правую или левую сторону, исходя из их порядка в алфавите. Это позволяла сохранить уверенность в недосягаемости информации, если она будет перехвачена.

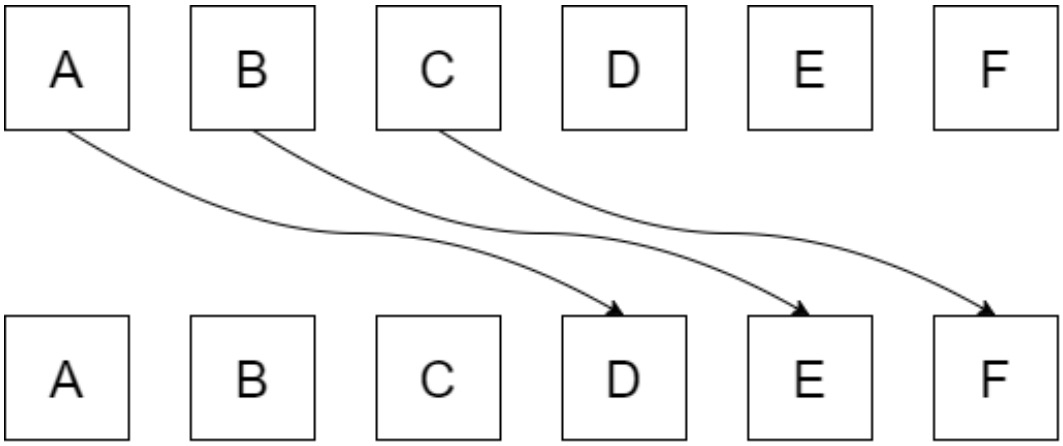

Рисунок 1 – Пример шифра Юлия Цезаря

В наше время используется тот же принцип, хотя и с гораздо большим уровнем сложности. Наиболее широко используемый шифр в мире называется AES и является примером использования метода криптография с открытым ключом [3]. Не выявлено никаких уязвимостей, что подтверждает полную безопасность данных, хранящихся в блокчейне.

Криптография с открытым ключом (асимметричная криптография) – метод, который позволяет передавать информацию с помощью открытого ключа любому пользователю. Используется два ключа: открытый и закрытый. Открытый ключ используется в качестве адреса для передачи активов в блокчейне, а закрытый хранит информацию, появляющаяся в виде строки случайных чисел и букв, давая контроль над всем, что связано с ключом. В итоге у получателя и отправителя есть своя связка ключей, которая расшифровывает друг друга. На рисунке 2 представлена иллюстрация криптографии с открытым ключом.

Хеш-функции – существуют разные виды криптографических хеш-функций, и каждая из них работает по-разному. SHA-256, хеш-функция, наиболее применяемая в технология блокчейна, – работает на основе формулы, связанной с отражением света от эллипсов. Суть заключается в том, что криптографическую хеш-функции можно понять только, при отличном понимании математических наук.

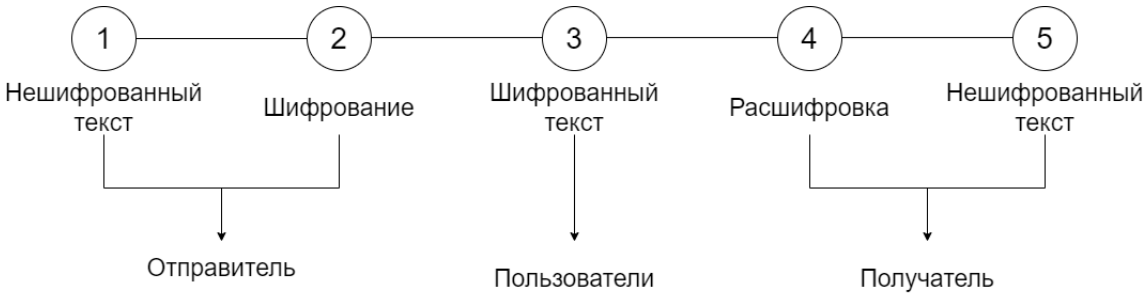

Рисунок 2 – Криптографии с открытым ключом

Именно при обновлении транзакционной информации любая аутентифицирующая система уязвима для атаки. Хеш-функции, благодаря своей максимальной надежности, сглаживают этот риск.

Заключение. В настоящей статье были рассмотрены принципы работы смарт-контрактов и теоретически доказана зависимость процессов исполнения смарт-контрактов от математических, в частности криптографических, методов и алгоритмов шифрования.

Были теоретически рассмотрены и изучены различные методы шифрования и хеширования, которые тесно связаны с математическими алгоритмами.

Список литературы

1. *BitcoinWiki, [Электронный ресурс]. Режим доступа: https://ru.bitcoinwiki.org/wiki. Дата доступа : 29.03.2022.*
2. *Фролов, А.В. Создание смарт-контрактов Solidity для блокчейна Ethereum / А. В. Фролов — «ЛитРес», 2019. – 240 с.*
3. *Darren Lau, Sze Jin The, Kristian Kho, Erina Azmi, Benjamin Hor, Lucius Fang, Win Win Khor. How to DeFi / "Coin Gecko", 2021. – 239 с.*

UDC 004.056.55

MATHEMATICAL FOUNDATIONS OF SMART CONTRACTS

Danilchenko D.I. and Khralovich Y.A.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus (style T-institution)

Tynkovich V.V., teacher of the highest category disciplines of the natural-mathematical cycle

Annotation. The subordination of smart contract technology to mathematical sciences has been studied. Encryption methods in smart contracts that are implemented using cryptography are described, and their advantages are analyzed. It has been established that the use of encryption guarantees the maximum reliability of the execution of smart contracts. The basic principles of the operation of smart contracts technology are also considered.

Keywords. smart contracts, cryptography, encryption.