КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ С ПОМОЩЬЮ ТЕХНОЛОГИИ БЛОКЧЕЙН

В.А. Абрамова, Н.И. Белодед

Академия управления при Президенте Республики Беларусь, Минск, Беларусь

В 21 веке, веке стремительного развития информационных технологий, обмен информацией играет важную роль. Однако этот процесс имеет как преимущества, так и ряд недостатков. И чем важнее информация, тем больше желающих ее «заполучить», воспользоваться в своих целях. Именно поэтому нужно знать, что такое криптография и как с ее помощью можно защитить важную для вас информацию.

Говоря простым языком, криптография – наука о методах шифрования информации. Для этого криптографы используют различные математические принципы, которые позволяют добиться высокой сохранности, целостности и подлинности информации.

Современная криптография включает в себя разные направления, самыми популярными являются системы электронной цифровой подписи (ЭЦП), хеш-функции, управление ключами, получение скрытой информации.

Используя цифровые подписи, каждый пользователь может потратить средства только со своего кошелька и только один раз. Этот принцип и лежит в основе самого принципа «электронных денег».

Механизм хэш-функций обеспечивает один из вариантов подтверждения алгоритма консенсуса – PoW (Proof of Work), а также – достоверность процесса майнинга, отвечающего как за генерацию новых монет в сети Биткоин, так и за проверку уже совершенных транзакций. В конкретной ситуации используется криптографическая функция SHA-256.

Именно криптографические методы защиты информации были положены в основу функционирования первой сети блокчейн – Биткоин.

Главной особенностью блокчейна является отсутствие централизованного управления. Это значит, что каждый узел распределенной системы делает записи в своей версии реестра независимо от других узлов и синхронизируется с ними в рамках одноранговой сети. Записи соединяются в инкрементальную цепочку блоков с использованием криптографических алгоритмов.

Блокчейн эффективно выполняет два из трех ключевых аспектов информационной безопасности – целостность и доступность информации. Благодаря децентрализованной топологии и криптографическим механизмам враждебные манипуляции данными становятся весьма дорогостоящими и затруднительными.

Но есть и недостаток традиционной технологии блокчейн. Он заключается в том, что технология не позволяет обеспечить третий аспект – конфиденциальность данных. Это приводит к редким, но все же взломам кошельков и «хищению» информации, электронных денег.

Существуют смарт-контракты, которые существенно расширяют возможности блокчейн-сетей, но в то же время приводят к немалому количеству новых атак.

Смарт-контракт - алгоритм, предназначенный для автоматизации процесса исполнения контрактов. Принцип его действия заключается в следующем: содержание договора записывается в виде кода в компьютерной программе, отслеживающей и обеспечивающей исполнение обязательств. Стороны сделки прописывают в таком контракте условия, а также санкции за их невыполнение. Смарт-контракты обладают такими преимуществами, как прозрачность сделки, защита от внесения изменений, не утвержденных сторонами, возможность совершения сделок анонимно. Умные контракты легли в основу множества блокчейн проектов и инициатив.

Таким образом, без понимания принципов работы криптографии, невозможно эффективное совершенствование сетей блокчейн в целом. Всестороннее изучение базовых криптографических методов защиты информации в технологии блокчейна необходимо для глубокого понимания безопасности и конфиденциальности систем, основанных на технологии блокчейн. Так, например, более поздние сети используют более эффективные протоколы кодирования, нежели SHA-256. С каждым днем это направление развивается, процесс не стоит на месте.

Список литературы

1. Балдов Д.В., Петрова С.Ю., Лебедев А.А. Использование технологии блокчейн для защиты данных // International Journal of Open Information Technologies. 2021. № 9.

2. Грошева Е.К., Невмержицкий П.И. Блокчейн – новая революция // Бизнес-образование в экономике знаний. 2018. №1 (9).

3. Сафарли Н.Э. Смарт-контракт: понятие, правовая природа, особенности заключения и исполнения // Legal Concept. 2019. № 4.