БЕЗОПАСНОЕ ХРАНЕНИЕ ЦЕЛЕВЫХ ДАННЫХ В BITCOIN С ПРИМЕНЕНИЕМ ДЕЦЕНТРАЛИЗОВАННОЙ СЕТИ ОБМЕНА ФАЙЛОВ INTERPLANETARY FILE SYSTEM

Гриненко Т.А., Скичко Д.В.
Научный руководитель – д.т.н., проф. Олейников Р.В.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, просп. Науки, 14, каф. БИТ, тел. +38 (057) 702-14-25)
e-mail: meksvinz@gmail.com

In this work discusses the method of ensuring the properties of information security, which is based on the joint use of the Bitcoin decentralized accounting system and the decentralized IPFS data exchange network.

Существует множество способов обеспечения свойств информационной безопасности. В работе рассмотрен способ, который базируется на совместном применении децентрализованной учётной системы Bitcoin и децентрализованной сети обмена данных IPFS (InterPlanetary File System). Совместное применение этих двух систем может дать довольно мощный инструмент по обмену файлами.

База данных децентрализированной учётной системы Bitcoin состоит преимущественно из транзакций [1]. У каждой транзакции может быть один или несколько входов, каждый из которых содержит поле scriptSig (доказательство владения монетами) и один или несколько выходов, каждый из которых содержит поле scriptPubKey (условие траты монет). Эти поля представляют собой набор операций, написанных на языке описания сценариев для траты монет Bitcoin Script. Под выполнением сценария подразумевается последовательное выполнение операций (OP-кодов) над некоторыми данными, которые содержатся в том же скрипте, а при выполнении помещаются в стек.

Рассмотрим OP-код OP_RETURN. Код OP_RETURN позволяет поместить в выход транзакции до 80 байт произвольных данных. Это может быть хэш-значение, данные в открытом или зашифрованном виде и т.д. Плюсы в помещении какой-либо произвольной информации в выход транзакции в том, что после распространения такой транзакции по сети и при условии, что она попадает в блок, который будет добавлен к самой длинной цепочке блоков, эти данные фактически будут храниться на всех узлах децентрализированной учётной системы Bitcoin, а это около 10115 узлов. Информация, которая была добавлена в цепочку блоков таким способом, будет храниться там до тех пор, пока владельцы большей части вычислительной мощности не решат переписать историю (предложат альтернативную цепочку блоков, что очень маловероятно). Поэтому наиболее вероятно, что произвольно записанные данные останутся доступными любому желающему навсегда. Это обеспечивает целостность и доступность информации, даже при условии, что субъект, который

отправил транзакцию, потерял доступ к целевым данным. Стоит заметить, что одна транзакция может включать более чем один выход с кодом OP_RETURN (возможное количество выходов зависит от размера данных, записываемых в транзакцию. В Bitcoin максимальный размер транзакции ограничен размером ¼ от максимального размера блока) [1]. С помощью такой транзакции можно сохранить, к примеру, доказательство совершения какого-либо действия (оплаты, сделки) и получить к нему доступ в любой момент времени, просто просмотрев транзакцию, в которой оно записано. Но есть определенные недостатки хранения информации в базе учётной системы Bitcoin таким способом, так как любой субъект может просмотреть информацию, записанную в OP_RETURN-выходе. Чем больше данных записывается в выходы с OP-кодом OP_RETURN, тем большую комиссию придется заплатить за отправку транзакции (если вообще не установить комиссию, то вероятность попадания транзакции в блок стремится к нулю, а если установить слишком маленькую комиссию, то возможна ситуация, когда узлы-валидаторы просто не станут включать транзакцию в блок из-за маленькой комиссии). Для обеспечения конфиденциальности информации, записанной в OP_RETURN-выходе транзакции, можно применять асимметричную криптографию.

В транзакцию невозможно поместить информацию большого объёма (документ, видеофайл и т.д.). Но при этом в транзакцию можно поместить hash значение файла, который необходимо отправить. Например, hash значение любого файла, который хранится в децентрализированной сети обмена данных IPFS.

Рассмотрим пример типичного обмена файлами в связке Bitcoin и IPFS: Алиса выбирает файл, который хочет отправить Бобу, и загружает его в сеть IPFS, получая в ответ хэш-значение (hash), по которому другой пользователь сети IPFS может скачать данный файл. Далее Алиса берёт публичный ключ Боба и шифрует на нём hash целевого файла, после чего записывает уже зашифрованный hash в выход bitcoin-транзакции (при помощи OP_RETURN). После чего сообщает идентификатор транзакции (txid) Бобу, по нему Боб находит транзакцию с зашифрованным hash и успешно расшифровывает его при помощи своего личного ключа, тем самым получая расшифрованный hash файла в сети IPFS, по которому может скачать файл, который Алиса ему адресовала. При таком обмене, третьей стороне будет трудно сказать, был ли обмен вообще, так как однозначно определить кому адресованы данные в OP_RETURN-выходе невозможно. А также, невозможно будет определить содержится ли именно hash в OP_RETURN-выходе, а не любые другие данные.

Список источников:

1. Блокчейн и децентрализованные системы: учеб. пособие для студ. Ч.1 /П. Кравченко, Б. Скрябин, О. Дубинина.– Харьков: ПРОМАРТ, 2018. – 440 с.