АДАПТАЦИЯ МЕТОДОВ КРИПТОГРАФИИ К ПРИМЕНЕНИЮ В СИСТЕМАХ РАСПРЕДЕЛЕННОГО РЕЕСТРА В СОЦИАЛЬНО-ЭКОНОМИЧЕСКОЙ СФЕРЕ

А.М. Макаров, Б.М. Гаджимурадов, Е.А. Писаренко, А.С. Ермаков

ФГБОУ ВО «Пятигорский государственный университет», Пятигорск, Россия

Появление сведений о внедрении технологии блокчейн в финансовую сферу деятельности и последовавшее практическое применение трансакций криптовалют вызвало бурную реакцию в научном и технологическом сообществе. Появилось множество публикаций по майнингу и транзакциям криповалют. Применение криптографии (асимметричного шифрования, двухключевой системы с открытым ключом), криптостойкого хэширования и цифровой электронной подписи на основе двухключевой схемы привело к пониманию сложности технологии блокчейн [1].

Обеспечение безопасности данных в сети блокчейн, наличие всей текущей базы данных и транзакций каждого абонента у каждого участника сети привело к возникновению эффекта доверительных отношений в цифровой среде. Однако, реализация доверительности автоматической обработки информации в системе «цифровая вычислительная система – цифровая вычислительная система» достигается за счет применения дорогостоящих технологий современных криптографических методов и средств. Поэтому весьма актуальной является задача адаптации теории и приложений криптографии для ее использования на объектах социально-экономической сферы.

В данной работе сделана попытка решения задачи адаптации двухключевой системы шифрования к объектам таких социально-значимых сфер, как жилищно-коммунальное хозяйство, фармацевтика, ведение и хранение медицинских карт, работа следственных органов. Как показал анализ поставленной задачи, основную трудность представляет адаптация технологий обмена ключами между участниками сети, назначение майнера и его роль в функционировании системы с распределенным реестром. Важным является и тот факт, что подавляющее большинство участников блокчейн-сети не только не являются профессиональными криптографами, но и ничего не знают о методах шифрования. То есть, большая часть пользователей сервисных услуг на основе криптографических методов подвергается цифровыми трансформациями своего привычного уклада деятельности в сфере получения услуг.

Список литературы

1. Materials the 3rd International Conference on Blockchain Technology and Information Security (ICBCTIS 2022), Xi'an, May 26–28, 2023.