УДК 004.01

ОБЗОР И АНАЛИЗ КРИПТОГРАФИЧЕСКИХ ПРИМИТИВОВ, ИСПОЛЬЗУЕМЫХ В ПРОТОКОЛЕ MIMBLEWIMBLE

Давыдов В.В. (Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)
Научный руководитель – д.т.н., доцент Беззатеев С.В.
(Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)

Данная работа посвящена обзору криптографических примитивов, используемых в протоколе MimbleWimble, который устраняет некоторые проблемы, существующие в реализациях блокчейн, и анализу важности и применимости таких примитивов.

На сегодняшний день криптовалюты становятся всё более популярными и актуальными – число пользователей постоянно увеличивается. Поскольку число криптовалют сегодня огромно и продолжает расти, разработчики ставят задачу привлечь как можно больше пользователей, совершенствуя механизмы и делая использование валюты максимально удобным и безопасным. Одним из важных свойств является приватность транзакций пользователей. В 2016 году было впервые опубликовано описание нового протокола MimbleWimble в IRC-канале #bitcoin-wizards пользователем под псевдонимом Tom Elvis Jedusor. Эндрю Поэлстра (Andrew Poelstra) из организации Blockstream, математик и специалист в области прикладной криптографии, внёс в описание ряд улучшений и опубликовал уточнённую версию в 2016 году. Такой протокол решает ряд проблем безопасности текущих реализаций блокчейн, однако, достаточно сложен.

В протоколе используются следующие криптографические примитивы: схема обязательств Педерсена, анонимные групповые подписи (однослойные и многослойные), погружаемая подпись, а также хэш-цепочки и деревья Меркла. На основе анализа данных примитивов было установлено, что такие механизмы используются для оптимизации хранения цепочек и значительного усовершенствования механизмов анонимности пользователей. К примеру, анонимные групповые подписи позволяют подписать блок одним из участников определённой группы, но не раскрывая личность этого участника; а деревья Меркла позволяют хранить не целую цепочку, а лишь её часть, что значительно оптимизирует пространство.

В работе проведён подробный анализ представленных в протоколе примитивов. В дальнейшем планируется усовершенствование и применение этих примитивов в разрабатываемых системах.

Давыдов В.В. (автор)

Беззатеев С.В. (научный руководитель)