электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель Общероссийская общественная организация "Академия инженерных наук им. А.М. Прохорова"
ISSN 2307-0609

 # 12, декабрь 2017

УДК 510

Перспективы использования легковесной криптографии в технологии блокчейн

***Бушуев В.В.**, студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»
vovabush94@mail.ru

***Иванников П.В.**, студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»
ivannikovpv@gmail.com

***Сосенко А.С.**, студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»
sosenkol995@gmail.com

***Чистяков Р.С.**, студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»
romchezz@gmail.com

Научный руководитель: Усанов А.Е., старший преподаватель
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана
кафедра «Информационная безопасность»

Аннотация: В данной статье дана оценка возможности применения легковесной криптографии при реализации криптовалюты на основе технологии блокчейн, с перспективой выполнения вычислений на мобильных и IoT-устройствах последних поколений.

Ключевые слова: криптография (cryptography), легковесная криптография (lightweight cryptography), блокчейн (blockchain), криптовалюта (cryptocurrency), смартфоны (smartphones).

Введение

С активным развитием сети Интернет появилась потребность в выполнении платежей безналичным расчетом. Ненадежность, разрозненность и централизованность банковской системы с конца 1990-х годов прошлого века вынуждали энтузиастов в области программирования и криптографии искать им подходящую замену. Итогом работы сообщества стала публикация в 2009 году документа с первым описанием принципа работы пиринговой сети биткоин [1], которая явилась первой успешной реализацией электронной валюты, соединившей принципы децентрализованности и надежности, которая достигалась за счет применения новой системы подтверждения валютных транзакций – блокчейн.

Множество экспертов сходятся во мнении, что криптовалюты продолжат свое развитие и, в конечном итоге, займут свою нишу в экономической отрасли. Это делает исследования в области создания и применения криптовалют и блокчейн технологий перспективными и ценными как для ученых, так и для промышленности.

1. Развитие Интернета вещей

По состоянию на октябрь 2017 года рыночная капитализация основных 20 криптовалют превысила 200 млрд. долларов. Около 50 процентов рынка занята биткоином, еще 30 процентов – сетью Ethereum (эфир).

Заметим, что большая часть криптовалют основа на концепции proof-of-work (доказательство через работу) и использовании криптографических хеш-преобразований. При этом для поддержания работы сети затрачиваются огромные мощности электроэнергии, а в вычислениях применяются дорогие ЭВМ или специализированные ASIC (СБИС).

С развитием микроэлектроники в нашу жизнь вошли сначала смартфоны, а затем «умные» вещи – розетки с поддержкой удаленного доступа, работающие по Wi-Fi, чайники, холодильники и т.д. Несмотря на то, что данные устройства не обладают достаточной мощностью для вычисления, например, SHA-1 хешей, их общее число велико и продолжает расти, что делает актуальным создание такого типа криптовалюты, для поддержания работоспособности которой можно применить данные IoT-устройства.

Согласно докладу компании, Huawei [2], являющейся одним из мировых лидеров в области разработки и производства электроники, к 2020 г. расходы на рынок Интернета вещей составят 1,7 трлн. долларов. Такое бурное развитие позволит в скором будущем перенести идеи блокчейн и криптовалют на новые «рельсы», и организовать действительно

распределенные системы. Это необходимо для обеспечения еще большей безопасности криптовалютных транзакций и обеспечения бесперебойной работы системы.

Основным препятствием на пути реализации идеи блокчейн в микроэлектронике стоит не вопрос взаимодействия, а отсутствие международных стандартов в области легковесной криптографии, что не позволяет производителям умных устройств встраивать аппаратную поддержку криптографических вычислений, необходимых для развития криптовалют на базе Интернета вещей.

2. Легковесная криптография

Агентство Национальной Безопасности США в 2013 году предложило два семейства шифров нового поколения [3], основанных на схеме ARX – Add (сложение), Rotate (циклический сдвиг), XOR (исключающее ИЛИ). Особенностью алгоритмов Simon и Speck явилось возможность применения в IoT-устройствах криптографии для защиты от злоумышленников за счет применения математических операций, не требующих большого места на кристалле микропроцессора, и одновременно обеспечивающих высокую скорость обработки защищаемой информации.

На рисунке 1 показана схема алгоритма Simon, предназначенного для аппаратной реализации. С небольшими изменения на базе данного алгоритма можно построить криптографическое хеш-преобразование, необходимое для применения в концепции proof-of-work технологии blockchain.

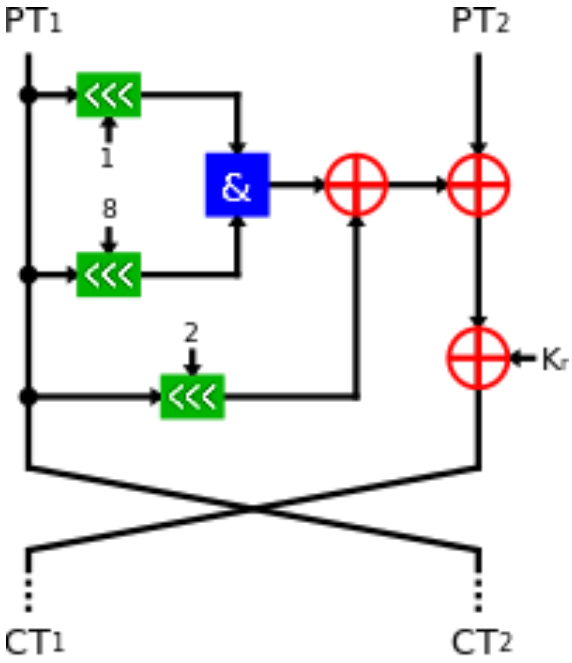

Рис. 1. Схема алгоритма шифрования Simon

К сожалению, в России проблема легковесной криптографии освещена недостаточно, что привело к полному отсутствию стандартов. На роль стандарта может быть предложен блочный шифр NASH [4], разработанный в МГТУ им. Н.Э. Баумана, проходящий испытания на стойкость.

Также одним из векторов создания отечественного стандарта для легковесной криптографии может выступить модифицированная версия отечественного шифрования, в котором S-блоки заменяются на операцию сложения в поле расширении.

Заключение

Активное развитие Интернета вещей и популяризация криптовалют, наблюдаемые в последние несколько лет, могут послужить толчком к появлению новых направлений – блокчейн технологий, реализованных не на базе мощных ЭВМ или специализированных микросхем, а при помощи применения в вычислениях повседневных устройств с реализованными аппаратно-криптографическими алгоритмами. Такой подход способен увеличить надежность системы, доверие к ней со стороны не только пользователей, но и кредитно-банковских учреждений. Высокая распределенность и наличие на рынке огромного числа умных устройств делает возможным запуск криптовалют нового поколения делом ближайшего будущего.

В качестве направления для дальнейших исследований могут быть выбраны как реализация легковесных криптографических преобразований на базе отечественных алгоритмов, так и проработка криптовалютной системы в целом, обеспечение ее надежности, реализация протокола для конкретных устройств и подготовка технологической базы для дальнейшего развития.

Список литературы

[1]. Nakamoto Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. Режим доступа: https://bitcoin.org/bitcoin.pdf (дата обращения: 10.11.2017).

[2]. Прохоров А. Рынок IoT. Оценок много, но нет консенсуса. 2016. Режим доступа: https://habr.com/company/huawei/blog/312888/ (дата обращения: 10.11.2017).

[3]. Beaulieu R., Shors D., Smith J., Treatman-Clark S., Weeks B., Wingers L. The Simon and Speck Families of Lightweight Block Ciphers. 2013. Режим доступа: https://eprint.iacr.org/2013/404.pdf (дата обращения: 10.11.2017).

[4]. Лебедев А.Н. Новый алгоритм шифрования NASH. 2017. Режим доступа: https://habr.com/post/337388/ (дата обращения: 10.11.2017).