УДК 004.6

СОЗДАНИЕ НОВОЙ АНОНИМНОЙ КРИПТОВАЛЮТЫ

Алпатов А.В. (Самарский лицей информационных технологий (ГАОУ СО СамЛИТ, Базовая школа РАН))

Научный руководитель – Кудряшова Е.М.

(Самарский лицей информационных технологий (ГАОУ СО СамЛИТ, Базовая школа РАН))

Аннотация.

Как показали исследования специалистов добиться абсолютной анонимности первым криптовалютам не удалось. Отсутствие полной конфиденциальности стало одним из недостатков первой криптовалюты, и это подтолкнуло многих разработчиков к созданию новых анонимных альткоинов. Поэтому создание криптовалюты с повышенной анонимностью является актуальной задачей.

Введение. Цель работы: Создание новой криптовалюты (альткоина) способного обеспечить значительную конфиденциальность финансовых операций.

Задачи исследования:

1. Обзор существующих криптовалют и способов обеспечения конфиденциальности операций с ними.
2. Изучение составных частей криптовалюты и последовательности действий для ее создания.
3. Разработка идеологии новой криптовалюты.
4. Проектирование необходимых составных частей для создания новой криптовалюты.

Новизна работы заключается в:

1. Создании авторской hash-функции.
2. Создании Explorer, Miner и кошелька как обязательных составных частей новой криптовалюты.
3. Написании авторского программного кода «Бек-энд Explorer».
4. Написании авторского программного кода «Miner».
5. Написании авторского программного кода «Кошелека» под устройства, работающие на ОС Android.
6. Создании сайта эксплорера.

Настоящая работа носит прикладной характер и позволяет расширить возможности потенциальных клиентов в использовании новых финансовыхх инструментов с максимальной для них анонимностью.

Основная часть. Разработка идеологии новой криптовалюты

При работе над созданием новой криптовалюты мы исходили из следующих предположений:

Главной характеристикой валюты будет высокая степень анонимности работы с ней для клиентов.

Интерес пользователей к новой валюте будет обеспечиваться высокой степенью ее анонимности.

Новая валюта будет альтернативой известным криптовалютам, возможно в полной мере, повторяющей идеологию некоторых из них, но обладающей самостоятельными (уникальными) программными кодами и алгоритмами, например, алгоритмом хеширования.

Для обеспечения указанных принципов нами были выполнены работы по созданию составляющих элементов криптовалюты. Важнейший вопрос об алгоритме обеспечения анонимности операций решен нами на основании анализа существующей информации об эффективности применяемых для этих целей методов. В результате изучения вопроса принято решение об использовании протокола с нулевым разглашением (ZK-SNARK). Таким образом можно утверждать, что планируемая к реализации новая криптовалюта будет прямым конкурентом валюте Zcash.

Далее представлена информация об уже реализованных и планируемых к реализации составных элементов новой криптовалюты.

Протоколы доказательства блоков и транзакций.
На данный момент существует два протокола доказательства: PoW (Proof of Work) и PoS (Proof of Stake). Для работы первого необходимы майнеры, подтверждающие действительность транзакций в блоке и блока в целом. Во втором случае подтверждение блока осуществляется владельцами данных монет. PoW имеет преимущество в защищенности блокчейна, так как переписать уже созданный блок невозможно, а внести изменение в создаваемый блок крайне проблематично, потому что для такой атаки на монету необходимо иметь большую часть вычислительных мощностей, задействованных в майнинге этой монеты. По этой причине нами был выбран протокол PoW.
Реализация доступа к аккаунту посредством файла Keystore.
Keystore - файл, содержащий описание кошелька криптовалюты. В нашей криптовалюте должен содержать адрес кошелька, закрытый ключ, для подписи транзакций и открытый ключ, для проверки майнерами действительности этой транзакции. Кроме того, данный файл должен быть зашифрован для защиты аккаунта. Для создания пары ключей нами используется алгоритм RSA. Сам файл keystore шифруется с помощью алгоритма AES, ключом для которого является хеш от заданного пользователем пароля.
Создание структуры блоков и транзакций.
Описание транзакции состоит из адресов отправителя и получателя, отправляемой суммы. Затем создается хеш транзакции на основе предыдущих данных. после этого, транзакция должна быть подписана отправителем. Подпись состоит из зашифрованного закрытым ключом отправителя хеша транзакции и открытого ключа отправителя. Созданная транзакция отправляется в очередь транзакций, не записанных в блок.
Основой криптовалют является технология блокчейн. То есть, цепочка блоков, в которой каждый последующий блок хранит информацию о предыдущем, за счет чего осуществляется защита данных от изменения. В нашем случае, блок хранит информацию о транзакциях. После записи информации о транзакциях в блок добавляется хеш предыдущего блока. Затем для нового блока создается его хеш. После чего данный блок проверяется майнерами, и в случае, если все транзакции в блоке имеют правильную подпись и хеш блока соответствует хешу, созданному на основе хешей предыдущего блока и транзакций в данном блоке, он добавляется в блокчейн. Если что-либо из этого не соблюдается, то правильные транзакции снова добавляются в очередь, а данный блок и неправильные транзакции удаляются.
Разработка алгоритма хеширования.
Одной из индивидуальных особенностей новой криптовалюты является оригинальный алгоритм хеширования. Предлагается использовать сложный для взлома алгоритм, основанный на поиске точек пересечения двух классических кривых (синусоида и квадратная парабола), но не между собой, а с помощью вспомогательной линии, являющейся касательной к синусоиде в заданной точке. Сложность алгоритма наглядно представлена на рисунке. Устойчивость алгоритма к коллизиям была выполнена путем его тестирования. Установлены пределы его устойчивости. Численный анализ сложности алгоритма планируется выполнить в ближайшее время.
Выводы. Принята к реализации идеология новой анонимной криптовалюты.
Завершена часть работ по созданию новой анонимной криптовалюты – HAWKCOIN, а именно:
1. Создана авторская hash-функция.
2. Созданы Explorer, Miner и кошелек – обязательные составные части криптовалюты.
3. Написан авторский программный код «Бек-энд Explorer».
4. Написан авторский программный код «Miner».
5. Написан авторский программный код «Кошелека» под устройства, работающие на ОС Android.
6. Создан сайта эксплорера.
7. Определен путь обеспечения анонимности операций. Выбран для реализации алгоритм обеспечения анонимности – ZK-SNARK.

Алпатов А.В. (автор) 

Кудряшова Е.М. (научный руководитель)