УДК: 336.1, 336.7, 004.056

Принципы создания прототипа универсальной цифровой монеты

S.A. Borodulina, I.A. Selionov, A.A. Tyumentsev, P.A. Cherkashin, A.Yu. Shcherbakov

Principles for Creating a Prototype of a Universal Digital Coin

Abstract. *The article discusses the concept of digital coins as a means of achieving independence and mobility of the national financial system, reducing the cost of paper money circulation, strengthening the economic security of the state. The necessity of using symmetric cryptography mechanisms and rejection of certification centers is shown. The preliminary structure of a digital coin is given. A brief description of the system and technology of circulation of digital coins is presented.*

Keywords: *digital coin, zero processing, asymmetric cryptography, national credit institution, national central bank.*

С.А. Бородулина[1]
И.А. Селионов[2]
А.А. Тюменцев[3]
П.А.Черкашин[4]
А.Ю. Щербаков[5]
[1]Председатель правления Ассоциации «Евразийский деловой совет»
E-mail:info@eurasia.business
[2]Директор по стратегическому развитию управляющей компании "Технопарк Пушкино", вице-президент РАКИБ
E-mail: uk04@inbox.ru
[3]Генеральный директор ООО «Тюменцев и партнеры».
E-mail: tyumentsev@mail.ru
[4]Научный сотрудник Ассоциации РКЦФА
E-mail: pcherkashin@gmail.com
[5]Доктор технических наук, профессор, главный научный сотрудник РАН (ИТМиВТ им.С.А.Лебедева), начальник Центра развития криптовалют и цифровых финансовых активов (ЦРКЦФА) ВИНИТИ РАН.
E-mail: x509@ras.ru

Аннотация. *В статье рассматривается концепция цифровых монет в качестве средства достижения независимости и мобильности национальной финансовой системы, снижения издержек на бумажное денежное обращение, укрепления экономической безопасности государства. Показана необходимость использования механизмов симметричной криптографии и отказа от удостоверяющих центров. Приведена предварительная структура цифровой монеты. Представлено краткое описание системы и технологии обращения цифровых монет.*

Ключевые слова: *цифровая монета, нулевой процессинг, асимметричная криптография, национальная кредитная организация, национальный центральный банк.*

ВВЕДЕНИЕ. ПОСТАНОВКА ЗАДАЧИ

В современной экономической и геополитической ситуации намечаются тенденции центробежного характера, связанные со стремлением государств с их национальными денежными и финансовыми системами к выходу из общемировой системы денежного оборота, привязанного к доллару.

С другой стороны, развитие финансовой системы происходит в сторону снижения стоимости обслуживания наличного денежного оборота за счет внедрения безналичных платежных инструментов (например, пластиковых карт). При этом часто не учитывается ситуация, связанная с тем, что процессинг пластиковых карт выполняется теми же транснациональными финансовыми корпорациями, что существенно снижает независимость и мобильность национальной финансовой системы.

Учитывая описанные тенденции, можно констатировать, что для создания устойчивого к внешнему влиянию денежного обращения, свободного также и от сложностей и издержек бумажного денежного оборота, необходима разработка концепции и методологии цифровых монет.

Важно заметить, что движение цифровых монет решает задачу контроля денежного обращения с точки зрения борьбы с отмыванием доходов, полученных преступным путем, и ряд других вопросов, связанных с экономической безопасностью государства.

ИСХОДНЫЕ ПОЛОЖЕНИЯ ПРОЕКТА

Вполне очевидно, что для цифровой монеты, рассматриваемой как материальный объект определенной структуры, циркулирующий в общедоступных сетях передачи данных, в обязательном порядке необходимо использование криптографических механизмов при эмиссии (фиксация номинала и серии-номера монеты) и при движении (проверка валидности при переводах и торговых операциях).

При этом применение механизмов электронной подписи, особенно квалифицированной, использующей удостоверяющие центры для массового движения цифровых монет (ЦМ), попросту невозможно, поскольку утяжелит систему и, в частности, из-за проблемы отозванных сертификатов сделает невозможной ее эксплуатацию, вплоть до полной остановки системы. Кроме того, использование асимметричных алгоритмов также сделает систему неработоспособной. Это относится и к процедурам реализации «слепой подписи» для ЦМ [1].

Вполне очевидно, что хранилищами ЦМ и средствами их распоряжения могут стать массово используемые мобильные устройства (мобильные телефоны) клиентов. Однако реализация криптографических механизмов в рамках личного мобильного устройства сопряжена с рядом проблем как технического, так нормативного характера. В связи с этим наличие криптографических механизмов на кошельках клиентов требуется минимизировать, а в идеальном случае – исключить.

ОСНОВНАЯ ИДЕЯ ПРОЕКТА

Основной идеей проекта ЦМ является использование механизмов симметричной криптографии и качественных датчиков случайных чисел для генерации отдельных ЦМ с уникальным номером и последующее хранение эмитированных монет в национальном центральном банке, либо уполномоченной (аккредитованной) им службе процессинга.

При этом должна быть обеспечена невозможность компрометации системы при компрометации или утрате любого количества кошельков пользователей.

Кроме того, должно быть обеспечено неиспользование удостоверяющих центров.

Будем полагать, что система движения ЦМ состоит из нескольких национальных финансовых регуляторов (национальных центральных банков - НЦБ), подчиненных им национальных кредитных организаций (НКО) и клиентов. При этом данная иерархическая структура позволит заложить в систему ЦМ и трансграничные свойства – движение монет между НЦБ через общий «нулевой процессинг». По сравнению с базовой статьей [2], описывающей структуру универсального токена, предлагаемая концепция и методология движения ЦМ является принципиально новой, конструктивной и практически реализуемой.

УЧАСТНИКИ СИСТЕМЫ ОБРАЩЕНИЯ ЦИФРОВЫХ МОНЕТ. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Нулевой процессинг (НП) – уполномоченная (аккредитованная) национальным ЦБ служба процессинга, хранящая ключ НК0, обеспечивающий эмиссию монет и, при необходимости, учет всех транзакций участников.

Национальный центральный банк (НЦБ) – участник системы, владелец ключа КНЦБi, создаваемого либо на стороне НЦБ, либо на стороне НП. Ключ передается в виде защищенного контейнера и используется для проверки монет, циркулирующих между НЦБ и НП.

Национальная кредитная организация (НКО) – подчиненная НЦБ структура, владелец ключа КНКОj, используемого в тракте НКО-НЦБ.

Клиент – владелец мобильного приложения, содержащего монеты и дающий распоряжения по их использованию. Клиенту создается при регистрации в НКО ключ ККm, на котором вычисляется КА монет, переданных ему. Контейнер клиента может храниться на стороне НКО и открываться по каждой операции клиента, сопровождаемой распоряжением.

Распоряжение по операции с ЦМ – выраженное и зафиксированное в приложении клиента решение о перемещении монет (совершении операций). Для распоряжения необходима

сумма и имя клиента-получателя.

В системе рассматриваются следующие операции:

- перевод ЦМ,
- покупка при помощи ЦМ,
- размен ЦМ,
- обращение к справочнику клиентов.

Клиенты в системе имеют имя и соответствующий ему номер мобильного устройства. Один клиент может иметь несколько имен.

Код аутентификации (КА) – результат работы процедуры вычисления значения, зависящего от значения ключа и содержания информации. Эта процедура такова, что без знания ключа невозможно или вычислительно трудоемко рассчитать КА к заданной информации [3].

ПРЕДВАРИТЕЛЬНАЯ СТРУКТУРА ЦИФРОВОЙ МОНЕТЫ

Таблица 1

Предварительная структура цифровой монеты

№№	Назначение поля	Длина, байт	Примечание
1	Заголовок	8	
2	Идентификатор криптоалгоритма	2	
3	Номинал	4	
4	Номинал дробный	4	Зарезервировано, в данном проекте не используется
5	Серия, номер монеты	16	
6	Дата-время выпуска монеты	8	
7	Срок жизни монеты, до…	8	
8	Имя НЦБ	16	
9	Имя НКО	16	
10	Имя клиента	16	
11	Время последней транзакции	8	
12	Порядковый номер последней транзакции	8	Приращивается к предыдущему значению поля; обслуживание монеты с меньшим номером исключено
13	Статус монеты	2	Активна/неактивна
14	Резерв	8	Заполняется нулями
15	Код аутентификации (КА) НП на поля 1-13	8	Вычисляется на секретном ключе К0
16	Код аутентификации (КА) НЦБ на поля 1-13	8	Вычисляется на секретном ключе КНЦБi
17	Код аутентификации (КА) НКО на поля 1-13	8	Вычисляется на секретном ключе КНКОj
18	Код аутентификации (КА) клиента на поля 1-13	8	Вычисляется на секретном ключе ККm
19	Резервное поле	32	
	ИТОГО	186	

КРАТКОЕ ОПИСАНИЕ ТЕХНОЛОГИИ ДВИЖЕНИЯ ЦИФРОВОЙ МОНЕТЫ

1. НП эмитирует необходимое количество монет и фиксирует их КА на секретном ключе К0. НП регистрирует в системе НЦБ и формирует, либо получает от НЦБ ключ КНЦБi.

2. Передача НЦБ сформированного пула монет. НЦБ добавляет к каждой монете КА НЦБ.

3. НЦБ регистрирует ЦМ в системе НКО, формируя ключи КНКОj.

НЦБ инкассирует в НКО монеты и формирует в них КА НКО. НКО при получении проверяют КА НЦБ.

4. НКО подключает пользователей путем регистрации их приложений (кошельков) и формирования имен для них, и загружает в кошельки (или на карты) монеты с вычислением КА владельца на ККm.

5. При покупке или переводе файл монеты переходит к другому владельцу и в кошельке первичного владельца уничтожается. При этом увеличивается счетчик транзакций и меняется время последней транзакции. По всей цепочке передачи КА проверяются и при движении к новому владельцу пересчитываются на соответствующих ключах с изменением имен (НЦБ при трансграничной передаче, НКО при передаче в другую НКО, либо клиента - при передаче в рамках одной НКО, либо все необходимые поля).

6. При онлайн-платежах информация синхронно обновляется в базе НП и НЦБ, при офлайн-платежах информация остается в НКО или кассе и синхронизируется после завершения операционного дня, либо снятия кассы, либо периодически при большом числе транзакций. При этом поле статуса неактивно до подтверждения монеты в НП.

7. Если клиент не может подобрать сумму из имеющихся у него монет, он запрашивает процедуру размена монет – перечисляет монету в НЦБ и получает несколько монет, равных сумме отправленной (с вычислением всех КА при движении ЦМ).

8. Для перевода или покупки клиент или НКО может запросить имя абонента по номеру его телефона, используя справочники НКО и клиентов, размещенных в НЦБ.

9. Монеты могут быть выгружены в «холодные» кошельки (флеш-носитель), либо распечатаны в бумажном виде с визуализацией указанных выше полей в цифровом виде, либо в виде двумерного кода. При этом возможно предъявить «бумажную» ЦМ, которая будет загружена в систему. В дальнейшем она будет циркулировать цифровом виде.

Предложенная система может показаться излишне централизованной, поскольку требуется проверка или пересчет КА в каждом ее звене. Однако это увеличивает защищенность движения ЦМ и позволяет вести их полный учет. Кроме того, алгоритмы расчета КА в настоящее время являются весьма быстродействующими, а малый размер ЦМ не перегрузит современные каналы связи.

В ряде случаев возможна передача клиенту ЦМ в виде смс-сообщения.

Таким образом, при расчете КА для клиента в рамках национальной кредитной организации и последующей его проверке в той же или другой НКО, входящей в централизованную систему с нулевым процессингом, возможно использование цифровых монет в рамках других национальных центральных банков, подключенных к системе (трансграничные расчеты и оборот). При этом не требуется реализация криптографических механизмов в кошельке клиента.

ВЫВОДЫ

Предлагаемая концепция может стать основой для создания независимой системы цифрового денежного обращения для снижения влияния международного экономического санкционного фона, а при наличии нескольких связанных общим процессингом НЦБ – обеспечить доверенные и независимые трансграничные платежи и повысить устойчивость национальных экономик.

Подводя итоги, можно назвать следующие принципиальные преимущества цифровой монеты:

- высокая степень защиты от подделки и возможность автоматического восстановления при помощи вычисления КА;

- трекинг движения средств и возможность прослеживания нахождения каждой монеты;
- существенное снижение затрат на обслуживание бумажных денег;
- возможность перевода монеты в бумажную форму и обратно;
- оптимизация социальных выплат и выплат дивидендов;
- возможность оперативного регулирования денежной массы в рамках национальной экономики.

СПИСОК ЛИТЕРАТУРЫ

1. Слепая подпись. URL: https://ru.wikipedia.org/wiki/Слепая_подпись (дата обращения: 12.04.2021).
2. Гриняев С.Н., Злотин Р.А., Милушкин А.И., Правиков Д.И., Селионов И.А., Щербаков А.Ю., Щуко Ю.Н. К вопросу о создании универсального защищенного доверенного цифрового актива (токена) // Научно-технический сборник "Научно-техническая информация", сер. 2 Информационный процессы и системы. 2018. № 10. С. 20-28.
3. Код аутентификации. URL: https://dic.academic.ru/dic.nsf/fin_enc/23875 (дата обращения: 12.04.2021).