ISSN 2311-8709 (Online)
ISSN 2071-4688 (Print)

Денежное обращение

ЦЕНТРАЛИЗОВАННЫЙ И ДЕЦЕНТРАЛИЗОВАННЫЙ ПОДХОДЫ К ОРГАНИЗАЦИИ СИСТЕМ ЭЛЕКТРОННЫХ ДЕНЕГ: НАСТОЯЩЕЕ И БУДУЩЕЕ

Наталия Юрьевна ТАНЮЩЕВА[a,•], Екатерина Ивановна ДЮДИКОВА[b]

[a] кандидат экономических наук, доцент факультета мировой экономики и управления кафедры мировой экономики и финансов, Астраханский государственный университет, Астрахань, Российская Федерация
n.tanyushcheva@rambler.ru

[b] аспирант факультета мировой экономики и управления кафедры мировой экономики и финансов, Астраханский государственный университет, Астрахань, Российская Федерация
dudikova.e@gmail.com

[•] Ответственный автор

История статьи:
Принята 28.06.2016
Принята в доработанном виде 12.07.2016
Одобрена 26.07.2016

УДК 336.74
JEL: E42

Ключевые слова:
электронные деньги, криптовалюта, электронная расчетно-платежная система, централизованные системы, децентрализованные системы

Аннотация

Предмет. В настоящее время внимание общества привлекает новое средство расчетов – «электронные деньги», особенностью которого является возможность существования как в централизованных, так и в децентрализованных системах. Применение децентрализованных технологий и криптовалютных систем позволяет устранить недостатки централизованных систем, касающихся вопросов информационной безопасности. Однако эксплуатация действующих криптовалют в неизменном виде несет высокие финансовые риски. В статье представлена сравнительная характеристика централизованного и децентрализованного подходов к организации систем электронных денег и предложены мероприятия по их усовершенствованию.

Цели. Рассмотреть особенности использования централизованных систем электронных денег и криптовалютных систем; предложить мероприятия, направленные на усовершенствование децентрализованных криптосистем, для их последующего практического применения на национальном уровне.

Методология. Применяются формальная логика, системный подход, метод сравнительного анализа, эмпирическое исследование (сравнение, сбор и изучение данных).

Результаты. Рассмотрены централизованный и децентрализованный подходы к организации электронных расчетно-платежных систем, а также выделены их достоинства и недостатки, представлен сравнительный анализ параметров популярных систем электронных денег и криптовалютных систем. Предложена авторская позиция в отношении возможности практического применения криптовалютных систем на государственном уровне, а также дополнена классификация электронных денег.

Выводы. Выделены преимущества и недостатки централизованных систем электронных денег и криптовалютных систем. Сделан акцент на том, что применение децентрализованных криптосистем в финансовой сфере для обращения электронных денег в существующем виде является небезопасным, и предложены мероприятия по их совершенствованию: запрет частных криптовалют; совместное применение централизованных и децентрализованных систем с усовершенствованным механизмом регулирования; создание новой инфраструктуры и др. Предложен дополнительный параметр классификации электронных денег в зависимости от подхода к организации системы: электронные деньги, обращающиеся в централизованной системе, и электронные деньги, обращающиеся в децентрализованной криптосистеме.

© Издательский дом ФИНАНСЫ и КРЕДИТ, 2016

Значение денег в современном мире сложно переоценить: они являются посредниками в осуществлении всех экономических и финансовых операций и связывают процессы в этих сферах между собой. Развитие денежного обращения неразрывно связано с совершенствованием вычислительных и информационных технологий.

Внедрение достижений научно-технического прогресса в финансовую сферу позволило отменить ряд ограничений, присущих материальной форме хранения финансовой информации, и способствовало появлению новых способов расчетов, ускорению процесса оборота денежных средств, снятию территориальных и временных ограничений совершения операций, снижению стоимости эмиссии, обслуживания и обращения. Так, сети передачи данных предоставили возможность дистанционного обмена финансовой информацией на больших расстояниях; вычислительные средства способствовали

появлению устройств для автоматизации финансовых процессов; с применением программного обеспечения стала возможной реализация алгоритмов обработки, хранения и передачи данных в финансовой сфере; применение криптографии позволило обеспечить безопасность и достоверность передаваемых данных, защиту обработки и передачи информации.

В последнее время внимание научного сообщества и государственных структур привлекают «электронные деньги» – новое средство расчетов, особенностью которого является возможность существования не только в централизованных, но и в децентрализованных криптографических системах.

Широкая практика применения новых технологий в финансах нашла отражение в работах следующих российских и зарубежных авторов: В.С. Аксенова [1], М. Беддели [2], А.А. Валинуровой[1], Л. Ван Хоува [3], А.В. Власова [4], А.С. Генкина [5], К. Гудхарда [6], В.Л. Достова [7], С.С. Квашнина [8], А.М. Косого [9], Д.А. Кочергина [10], Б. Коэна [11], М. Крюгера [12], В.А. Лопатина [13], С. Малиева [14], И.Г. Маликова [15], М.С. Марамыгина [16], Ю.В. Пашкуса [17], П.С. Пробина [18], П.В. Ревенкова [19], Накомото Сатоши[2], Е. Сейтим Айганым [20], С. Атей[3], Ч. Фридмана [21] и др.

Использование технологии блокчейн стало прорывом в области криптографии, которая уже оказала влияние на финансовую сферу, но еще не до конца реализовала свой потенциал. Данная технология применяется как для создания криптовалют[4] (Bitcoin – первая успешная криптовалюта), так и для предоставления распределенных сервисов (например, Ethereum). Блокчейн не просто обеспечивает защищенное хранение данных пользователя и финансовой информации, его преимуществом является предоставление гарантий достоверности этих сведений.

Для обращения электронных денег используются электронные расчетно-платежные системы (ЭРПС). При рассмотрении технологий организации ЭРПС можно говорить о двух применяемых подходах – централизованном и децентрализованном.

Реализация централизованной ЭРПС предполагает выполнение обработки информации на выделенном сервере (группе серверов, между которыми распределена обработка и/или хранение информации), имеющем единый «интерфейс» для взаимодействия с пользователем (рис. 1). Каждая операция выполняется на выделенном сервере и сохраняется в единую базу данных. Клиентское устройство не участвует в процессе обработки и хранения информации.

Децентрализованная организация ЭРПС не предусматривает единого интерфейса, и все серверы, входящие в такую сеть, являются равноправными (рис. 2). В процессе работы децентрализованной сети в качестве серверов принимают участие и клиентские устройства (компьютеры). Обработкой одной транзакции в подобных ЭРПС, как правило, занимается несколько вычислительных серверов одновременно, параллельно выполняя операцию, подтверждая или отклоняя ее.

Существенная территориальная распределенность децентрализованной сети делает ее невосприимчивой к потере отдельных серверов, например в связи с неблагоприятными последствиями катастроф, кратковременными неполадками в работе самих серверов и каналов связи, действиями злоумышленников и др.

Представлена сравнительная характеристика основных параметров централизованного и децентрализованного подходов к организации ЭРПС, функционирующих на начало 2016 г. (табл. 1).

Примерами популярных централизованных ЭРПС являются WebMoney Transfer, PayPal, Яндекс.Деньги, RBK Money (RUpay), E-gold, MoneyMail, CyberPlat, Google Wallet, Apple Pay,

[1] *Валинурова А.А.* Понятие и функции сетевых денег // Финансы и кредит. 2010. № 15. С. 61–67.

[2] *Nakamoto S.* Bitcoin: A Peer-to-Peer Electronic Cash System. URL: https://bitcoin.org/bitcoin.pdf

[3] *Атей С.* Может ли биткоин стоить 50 тысяч долларов? 2014. URL: http://coinspot.io/analysis/mozhet-li-bitkojn-stoit-50-tysyach-dollarov

[4] С нашей точки зрения, термин «криптовалюта» необходимо рассматривать как общее понятие в рамках децентрализованной криптосистемы, которое описывает способ представления информации о единице учета в системе, являющейся цепочкой записей, каждая из которых защищена криптографической подписью. При этом в процессе подписания учитывается предыдущая запись в цепочке.

QIWI Wallet. Рассмотрим каждую из них более подробно.

Технология международной системы расчетов WebMoney Transfer основана на предоставлении всем участникам системы единых интерфейсов управления денежными средствами, находящимися на хранении в специализированных компаниях (гарантах).

К достоинствам данной ЭРПС относятся следующие характеристики: значительное количество участников (более 30 млн); наличие обменных пунктов в 11 977 городах и поселениях 89 стран мира[5]; мультивалютность; возможность вывода денежных средств на банковскую карту; высокий уровень безопасности; оплата товаров и услуг реального мира (например, коммунальных услуг и штрафов). Недостатками WebMoney Transfer являются: необходимость установки специального программного обеспечения для работы с системой; наличие платной аттестации владельцев электронных кошельков; высокая комиссия.

PayPal работает в 203 странах[6], включает в себя более 179 миллионов зарегистрированных пользователей[7], является одной из крупнейших в мире ЭРПС. С октября 2002 г. входит в состав компании eBay.

Преимущества ЭРПС PayPal заключаются в ее мультивалютности и высоком уровне безопасности. К недостаткам относятся: отсутствие возможности оплаты услуг реального мира (например, коммунальных услуг и штрафов), а также вывода денег из системы наличными (только на расчетный счет); обязательная оплата регистрации; необходимость наличия карты Visa или MasterCard для использования системы.

QIWI Wallet – международная ЭРПС, созданная в 2007 г. и позволяющая производить расчеты с использованием различных устройств и каналов связи, как стационарных, так и мобильных.

В качестве достоинств данной ЭРПС следует рассматривать поддержку карт Visa и MasterCard; возможность оплаты товаров и услуг реального мира (например, коммунальных услуг и штрафов); проведение анонимных расчетов через анонимный электронный кошелек. Отрицательные моменты проявляются в отсутствии двухфакторной аутентификации и малом количестве стран охвата сервиса (8 стран-участниц[8]).

ЭРПС Яндекс.Деньги была запущена в 2002 г. При ее создании использовалась технология PayCash, предусматривающая хранение и передачу по открытым сетям конфиденциальной информации.

Плюс данной ЭРПС заключается в поддержке другими сервисами компании Яндекс. Недостатком представляется ее моновалютность (единственной валютой является рубль).

RBK Money – российская ЭРПС, созданная в 2008 г. на базе RUPay (2002 г.), которая входит в состав холдинга РБК.

К положительным моментам работы данной ЭРПС относятся: высокий уровень безопасности; отсутствие комиссии при расчетах между пользователями внутри системы; гарантия возврата денег. Среди минусов можно отметить низкую популярность системы и отсутствие двухфакторной аутентификации.

E-gold – международная ЭРПС, созданная в 1996 г. и прекратившая свое существование 20.01.2015 по причине обвинений властями США владельцев ЭРПС в организации бизнеса денежных переводов без соответствующей лицензии, а также в пособничестве отмыванию денег, добытых преступным путем. Отличительной особенностью данной ЭРПС являлось обеспечение единицы учета в системе драгоценными металлами (золотом, серебром, платиной, палладием).

Обеспечение в виде драгоценных металлов представлялось сильной стороной E-gold, так как изменение курсов официальных валют не отражалось на благосостоянии владельца электронного счета. Противовесом указанному преимуществу выступала комиссия за хранение

[5] Территория WebMoney сегодня – 11 977 населенных пунктов в 89 странах мира.
URL: http://geo.webmoney.ru/wmobjects/?lang=en)

[6] Весь мир как на ладони.
URL: https://www.paypal.com/ru/webapps/mpp/country-worldwide

[7] 179 млн. активных пользователей PayPal по всему миру.
URL: https://www.paypal.com/ru/signup/account

[8] QIWI в мире.
URL: https://corp.qiwi.com/company/world.action

и вывод законных денег из системы и высокая комиссия за переводы.

ЭРПС MoneyMail осуществляет работу с 2004 г. и функционирует исключительно на территории России.

Преимуществом данной ЭРПС является возможность переводов и выставления счетов тем, кто не зарегистрирован в системе, при этом слабым звеном представляются высокие комиссионные сборы за перевод и вывод денег из системы.

CyberPlat – первая российская ЭРПС (1998 г.). Необходимо отметить, что за все время существования CyberPlat не произошло ни одного случая взлома транзакции[9].

Широкая сеть приема расчетов (более 910 тыс. точек) в крупнейших городах всех стран мира; использование электронно-цифровой подписи (ЭЦП) с длиной ключа 2048 бит (что исключает риски мошенничества); проведение всех операций в ЭРПС с использованием ЭЦП выступают несомненными достоинствами данной системы. Очевидным минусом CyberPlat является необходимость наличия специализированного оборудования для работы в системе.

Google Wallet представляет собой систему онлайн-платежей компании Google. ЭРПС позволяет использовать бесконтактные платежи на устройствах, поддерживающих технологию NFC[10].

Ценность Google Wallet проявляется в высоком уровне защиты данных, гарантиях конфиденциальности и возврата денег; поддержке другими сервисами компании Google. Слабой стороной системы можно считать ориентированность мобильного приложения Google Wallet в основном на США и англоязычных пользователей.

Apple Pay представляет собой ЭРПС, запущенную в 2014 г. компанией Apple.

Совместимость с существующими бесконтактными считывателями Visa PayWave, MasterCard PayPass, American Express ExpressPay; поддержка другими сервисами компании Apple обеспечивают преимущества данной ЭРПС. Однако доступ к системе только с устройств компании Apple и низкая скорость расчетов ограничивают круг потенциальных пользователей.

В настоящем исследовании проведено детальное сравнение основных параметров популярных централизованных ЭРПС (табл. 2).

К ЭРПС, построенным на базе децентрализованных технологий, относятся Bitcoin, Ethereum, Litecoin, MaidSafeCoin, Dash, Factom, Syscoin.

Bitcoin является первой в мире цифровой криптовалютой, которая получила широкое распространение. В настоящее время существуют биржи по работе с криптовалютой Bitcoin.

Данная система выделяется среди прочих высоким уровнем признания. В качестве отрицательных моментов можно отметить волатильность курса криптовалюты, низкую скорость транзакций и фиксированный объем блока (2 МБ).

Ethereum – это децентрализованная криптоплатформа, позволяющая создавать децентрализованные приложения и «смарт-контракты» (автоматизированные финансовые контракты, которые не требуют участия третьей стороны, где разработчики могут реализовать собственные правила владения, форматы транзакций и условия выполнения контрактов). Единицей учета в данной системе является криптовалюта Ethereum.

Использование языка программирования Ethereum дает возможность реализовать любую вычислительную функцию, что положительно оценивается пользователями, тогда как угроза абсолютно всем данным пользователя при взломе учетной записи относится к негативной стороне системы.

Litecoin – цифровая криптовалюта (аналог Bitcoin), которая была создана в 2011 г., в настоящее время пользуется высоким спросом. Ее менее сложно майнить[11], поскольку на данный момент добыто небольшое количество учетных

[9] Преимущества системы электронных платежей CyberPlat («КиберПлат»). URL: http://www.cyberplat.ru/advantages

[10] Near field communication.

[11] Майнинг – способ добычи криптовалюты, базирующийся на решении компьютерами математических задач.

единиц. Однако алгоритм формирования ключа scrypt, используемого в системе, требует большего объема памяти, чем алгоритм SHA-256, используемый в Bitcoin.

MaidSafeCoin базируется на технологии блокчейн. Для поддержания функционирования децентрализованной системы применяется программа, которая использует ресурсы компьютера пользователя для хранения части общих данных всех пользователей системы. За предоставляемые пользователем вычислительные ресурсы распределяется вознаграждение в виде SafeCoin. Вознаграждение зависит от скорости процессора, пропускной способности памяти, дискового пространства и времени онлайн-подключения.

В системе действует низкая комиссия размещения коммерческих приложений, однако отсутствует цензура и ограничения для размещаемых приложений. К тому же при взломе учетной записи в системе под угрозой могут оказаться все данные пользователя.

Dash является криптовалютной системой со встроенным смесителем транзакций DarkSend, который позволяет выполнять анонимные расчеты. В системе пользователь имеет право выбора использовать DarkSend или не использовать (проводить транзакции напрямую).

Пользователи положительно относятся к анонимности, высокой скорости переводов и отсутствию комиссии. Тогда как платное использование смесителя транзакций и угроза данным при взломе учетной записи квалифицируются в качестве недостатков системы.

Криптовалютная система Factom использует технологию блокчейн для хранения реестра публичных записей и подтверждения авторства интеллектуальной собственности. За счет надстройки дополнительного информационного уровня к блокчейну возможно хранение большего объема информации.

Систему отличает отсутствие ограничений на размер блока, с одной стороны, с другой – низкая скорость и высокая стоимость транзакций.

Syscoin – это и криптовалюта, и инфраструктура, которые вместе предоставляют среду для финансовых расчетов на базе технологии блокчейн и обеспечивают децентрализованную инфраструктуру «все в одном», включающую торговую площадку, цифровые сертификаты, псевдонимы пользователей, зашифрованные сообщения, децентрализованное обслуживание и арбитраж.

Развитая финансовая инфраструктура, интегрированная с криптовалютой, дает несомненные преимущества при работе с Syscoin. Однако использование алгоритма формирования ключа scrypt, требующего большего объема памяти, чем алгоритм SHA-256 (Bitcoin), выступает отрицательным параметром данной системы.

Xaurum представляет собой функционирующую криптовалюту, которая имеет выражение в драгоценном металле (золото). Создатели данной системы предприняли попытку обеспечить криптовалюту золотом, при этом часть блоков уже сгенерирована в системе, а оставшаяся часть добывается пользователями. Каждый XAU соответствует одному грамму золота с гарантированным выкупом компанией Auresco Institute.

Обеспеченность единицы учета золотом (курс криптовалюты привязан к курсу драгоценного металла) и поддержка двухфакторной аутентификации для доступа к кошельку положительно характеризуют систему, тогда как низкий уровень доверия к гаранту Auresco Institute является серьезным негативным фактором.

Проведено подробное сравнение описанных децентрализованных криптовалютных систем (табл. 3).

На основании представленного анализа структурированной информации, продемонстрированной в таблицах, можно выделить общие достоинства и недостатки централизованных и децентрализованных ЭРПС, функционирующих на начало 2016 г.

К основным достоинствам централизованных ЭРПС относятся:

- защита персональных данных;
- обеспечение электронных денег законными деньгами либо драгоценными металлами;
- строгий курс соотношения электронных и законных денег;

- существование официального представителя, ответственного за функционирование и регулирование системы;
- наличие централизованного органа, ответственного за решение спорных вопросов и рассмотрение претензий;
- возможность блокировки счетов, отказ в проведении подозрительных переводов.

Типичными недостатками централизованных ЭРПС следует считать:

- централизованный характер управления системой и хранения информации, что является слабой стороной информационной системы, которая чаще всего используется для реализации разнородных атак (например, атака типа «отказ в обслуживании»[12] на конкретный адрес ЭРПС, «фишинг-атака» и др.);
- низкий уровень прозрачности деятельности ЭРПС (отсутствие доступа к статистическим данным, сложность проверки собственной (предоставляемой) информации).

В качестве преимуществ децентрализованных криптосистем можно выделить:

- явную независимость от атак или неисправностей отдельных серверов при территориальной распределенности сети;
- прозрачность всех финансовых операций;
- доступность исходного кода программного обеспечения для модификации системы ее пользователями;
- высокий уровень криптографической стойкости, достаточный для безопасного хранения персональных данных и финансовой информации;
- моментальность отражения на электронных кошельках отправителя и получателя суммы перевода, при этом для подтверждения транзакции необходимо некоторое время, после чего получатель будет иметь возможность распоряжаться суммой.

Слабыми сторонами децентрализованных криптосистем представляются:

- отсутствие централизованного органа, ответственного за контроль и функционирование системы;
- невозможность решения спорных вопросов и рассмотрения претензий по причине отсутствия официального представителя криптосистемы;
- отсутствие гарантированного обеспечения единицы учета в ЭРПС;
- высокая волатильность единицы учета криптосистемы, зависящая от уровня спроса на нее;
- возможность реализации атак «51%»[13], «пыль»[14];
- отсутствие возможности блокировки счетов и отказа в осуществлении подозрительных переводов, т.е. воздействия на статус счета и процесс перевода;
- невозможность восстановления закрытого ключа электронного кошелька и отмены операции перевода;
- низкая скорость подтверждения транзакции (около одного часа);
- отсутствие возможности смены закрытого ключа электронного кошелька (компрометация электронного кошелька делает его опасным для хранения криптовалюты).

С момента начала применения сетевых технологий для доступа к информационным системам финансовые организации постоянно находятся под угрозой атак злоумышленников. В настоящее время зафиксирован ряд удачных попыток взлома банковских систем, которые привели к многомиллионным убыткам и подорвали репутацию пострадавших организаций. Так, например, неоднократно

[12] Атака «отказ в обслуживании» – атака, при которой система становится перегруженной фиктивными запросами, в результате чего не может обработать запросы настоящих пользователей.

[13] Атака «51%» заключается в захвате большей мощности вычислительных устройств децентрализованной сети и, как следствие, возможности изменения порядка записи блоков цепи в нужную «злоумышленнику» сторону.

[14] Атака «пыль» проявляет себя в отправке большого числа микротранзакций размером до 0,0001 BTC в короткий промежуток времени в децентрализованную ЭРПС, что затрудняет ее работу, увеличивая время проведения переводов.

фиксировались успешные взломы межбанковской системы SWIFT[15]; нападения на платежную систему «Рапида»[16]; шантаж банковских организаций Англии[17] и др.

Существует актуальная информация о наличии угрозы атаки типа «отказ в обслуживании» для централизованных систем финансовых организаций по всему миру[18]. Успешная реализация атак на централизованные системы приводит не только к существенным финансовым убыткам и потери репутации пострадавших организаций, но и к дестабилизации экономики в целом.

В результате необходимые действия по устранению угроз в области технической и информационной безопасности должны быть направлены как на дальнейшее совершенствование централизованных ЭРПС и разработку для них новых способов защиты информации (в настоящее время этой сфере уделяется повышенное внимание), так и на применение децентрализованных технологий и криптовалютных систем, которые приведут к снижению, а в некоторых случаях устранению недостатков централизованных систем, касающихся вопросов информационной безопасности. Вместе с тем использование децентрализованных криптосистем в финансовой сфере для обращения электронных денег в существующем виде является небезопасным. Для дальнейшей эксплуатации таких систем, по нашему мнению, целесообразно проведение следующих мероприятий:

- запрет применения частных криптовалют, поскольку они не регулируются законом и, следовательно, могут быть использованы в незаконной деятельности;
- совместное использование централизованных и децентрализованных систем с усовершенствованным механизмом регулирования. В настоящее время применяется огромное количество разных способов и методов защиты централизованных систем от целенаправленных атак киберпреступного сообщества, однако обеспечить абсолютную безопасность таких систем весьма трудно и затратно[19]. Децентрализованные системы лишены многих этих недостатков. Несмотря на это, применение технологии децентрализованных систем к модернизации существующих централизованных систем без использования криптографических способов защиты информации не приведет к существенному увеличению информационной безопасности, поскольку не защитит от атак «двойного платежа», фальсификации процесса перевода и др.;
- применение приложений для доступа пользователей к электронному кошельку, размещенному на серверах децентрализованной сети, при этом на устройстве пользователя база блокчейн не размещается;
- открытие в ЭРПС только персонифицированных электронных кошельков;
- осуществление эмиссии криптовалюты не в момент обращения пользователя к системе, как в централизованных ЭРПС, а предварительно, до момента обмена законных денег на электронные. Электронные деньги (криптовалюта), являясь формой безналичного расчета, должны быть полностью обеспечены законными деньгами;
- создание новой инфраструктуры (децентрализованной), владельцем которой будет являться конкретная организация, ответственная за контроль и функционирование системы, что позволит при наличии спорных вопросов и претензий обращаться к официальному представителю. В качестве таких организаций могут быть две.

Первый вариант. Эмитент криптовалюты – центральный банк.

[15] *Попсулин С.* Хакеры взломали SWIFT «на бис». 2016. URL: http://www.cnews.ru/news/top/2016-05-13_na_sistemu_swift_sovershena_vtoraya_ataka_s_nachala

[16] *Попсулин С.* Полиция и ФСБ арестовали хакеров, похитивших сотни миллионов. 2016. URL: http://www.cnews.ru/news/top/2016-04-21_v_rossii_razoblachena_dve_gruppy_moshennikov_v

[17] Bitcoin cyberextortionists are blackmailing banks, corporations. URL: http://arstechnica.com/business/2015/09/uk-banks-corporations-are-being-blackmailed-by-bitcoin-cyberextortionists

[18] Anonymous Declares War on Banks, Starts with DDoS Attacks on Greece. 2016. URL: http://news.softpedia.com/news/anonymous-declares-war-on-banks-starts-with-ddos-attacks-on-greece-503683.shtml

[19] Anonymous объявили войну центробанкам мира, и начали с Греции. URL: https://geektimes.ru/post/275404

Функционал центрального банка при этом заключается в разработке собственной децентрализованной системы, в которой будет обращаться единый вид криптовалюты и осуществляться ее централизованный майнинг, выдача лицензии на осуществление деятельности в рамках функционирования единой криптовалюты в качестве средства расчетов, что позволит осуществлять государственный контроль, учет и регулирование.

Функционал финансовых организаций, получивших лицензию на осуществление операций с электронными деньгами, будет представлять собой участие в национальной децентрализованной системе путем присоединения к ней, размещение части серверов децентрализованной сети на собственных или арендуемых мощностях, полная регистрация конечных пользователей в офисе финансовой организации (агентов).

Второй вариант. Эмитент криптовалюты – финансовые организации.

Задачи центрального банка состоят в выдаче лицензии на осуществление деятельности с криптовалютой в качестве средства расчетов, что позволит осуществлять государственный контроль, учет и регулирование.

Задачи финансовых организаций, получивших лицензию на осуществление операций с электронными деньгами, заключаются в ценрализованном майнинге криптовалюты конкретным эмитентом – кредитной организацией, полной регистрации конечных пользователей в офисе финансовой организации (агентов).

В случае построения интегрированной (совместной) единой децентрализованной криптовалютной системы с возможностью присоединения к ней финансовых организаций разработку программного обеспечения должен обеспечить центральный банк.

В случае реализации автономных децентрализованных криптовалютных систем разработкой программного обеспечения занимаются финансовые организации.

В заключение отметим, что только при условии применения предложенных доработок к действующим криптосистемам криптовалюту можно будет считать разновидностью электронных денег и, как следствие, дополнить классификацию электронных денег, в которую предлагаем включить электронные деньги, обращающиеся в централизованной ЭРПС, и электронные деньги, обращающиеся в децентрализованной ЭРПС (криптовалюту).

Таблица 1

Основные параметры централизованного и децентрализованного подходов к организации ЭРПС

Table 1

Main parameters of centralized and decentralized approaches to electronic payment and settlement system (EPSS) organization

Параметры	Централизованный подход	Децентрализованный подход
Устройство обработки информации	Выделенный сервер или группа серверов	Распределенная сеть серверов
Хранение данных	База данных	Распределенные базы данных
Формат представления записей о единицах учета	Числовые записи на счетах пользователей	Записи о транзакциях в виде блоков*, подписанные закрытым ключом пользователя
Аналог открытого ключа	Номер счета	Номер кошелька
Аналог закрытого ключа	Пароль	Уникальный идентификатор пользователя
Возможность восстановления доступа к учетной записи пользователя	Да	Нет
Формат представления транзакции	Запись об операции перевода средств между счетами (проводка)	Скрипт на языке программирования криптосистемы (дополнительные условия)
Форма существования	Электронная	Электронная
Условия совершения операции	Бесперебойная работа минимум одного сервера, в том числе абонентских устройств, каналов связи и соответствующего программного обеспечения	Бесперебойная работа большей части серверов и каналов связи сети, а также абонентских устройств, программного обеспечения
Эмиссия единицы учета в ЭРПС	Централизованная	Децентрализованная
Делимость единицы учета	10^{-2}	10^{-8}
Данные о транзакциях находятся в общем доступе	Нет	Да
Анонимность	Да/нет (в зависимости от суммы перевода)	Не гарантируется
Курс обмена единицы учета ЭРПС на законные деньги	Четко установлен	Изменяется в зависимости от спроса
Наличие обеспечения единицы учета ЭРПС	Да (законные деньги)	Нет (социальное доверие)
Выражение (вид) единицы учета в ЭРПС	Национальная валюта/частная	Частная
Наличие государственного контроля и регулирования	Да/нет (в зависимости от суммы перевода)	Нет
Комиссия за проведение расчетов	Средняя	Низкая
Зависимость проведения операции от времени и места	Не существует	Не существует
Количество сторон, принимающих участие в проведении расчетов	3 (плательщик, получатель, оператор ЭРПС)	2 и более (плательщик, получатель, возможно привлечение посредников с целью проведения анонимных расчетов, т.е. для «размытия» суммы перевода)

* Блок – это группа транзакций, объединенная в массив данных определенного размера, который применяется для хранения последовательности транзакций при использовании блокчейн.
Источник: составлено авторами

* A block is a group of transactions combined in the data array of a certain size, which is used to store a sequence of transactions when using the blockchain.
Source: Authoring

Таблица 2

Основные параметры централизованных ЭРПС

Table 2

Main parameters of centralized EPSS

Параметры	WebMoney	PayPal	Яндекс.Деньги	RBK Money	E-gold
Общие характеристики					
Год создания ЭРПС	1998	1998	2002	2008	1996
Функционирование по состоянию на 01.06.2016	+	+	+	+	–
Мультивалютная	+	+	–	+	–
Анонимное использование	+	+	+	+	+
Статус пользователя ЭРПС (для Российских пользователей):					
физическое лицо	+	+	+	+	+
юридическое лицо (индивидуальный предприниматель)	+	+	–	+	–
Уровень сложности*					
Регистрация	3	2	1	1	–
Пополнение счета	2	1	1	1	–
Обмен валют в ЭРПС	1	1	–	1	–
Вывод законных денег из ЭРПС	2	1	1	1	–
Территория охвата для выполнения расчетных операций					
Транснациональная	+	+	–	–	+
США	–	+	–	–	+
СНГ	+	+	+	+	+
Россия	+	+	+	+	+
Число пользователей, млн	30	179	21	6,2	2
Взаимодействие пользователя с ЭРПС					
Браузер	+	+	+	+	+
Устройство с NFC	–	–	–	–	–
Платежный терминал	+	–	+	+	–
Карта	+	+	+	+	–
Устанавливаемое программное обеспечение на компьютер	+	–	–	–	–
Мобильное приложение	+	+	+	+	–
Защита данных, передаваемых между пользователем и ЭРПС					
ЭЦП	–	–	–	–	–
SSL шифрование	+	+	+	+	+
Сертификация агентов (посредников ЭРПС)	+	–	–	–	–
Защита личного кабинета пользователя					
Логин и пароль	+	+	+	+	+
Двухфакторная авторизация	+	+	+	–	–
Защита мобильного приложения PIN-кодом	+	+	+	+	–
Выражение единицы учета в ЭРПС					
Национальная валюта	–	+	+	+	–
Уникальная частная единица учета системы	+	–	–	–	–
Драгоценные металлы	+	–	–	–	+
Комиссия					
Расчеты между пользователями, %	0,8	0	0,5	0,3–0,5	–
Обмен единиц учета внутри ЭРПС, %	0	3,4	–	–	–
Страна регистрации головной организации	Гондурас	США	Нидерланды	Россия	Канада

Продолжение табл.

Параметры	MoneyMail	CyberPlat	Google Wallet	Apple Pay	QIWI
Общие характеристики					
Год создания ЭРПС	2004	1998	2011	2014	2007
Функционирование по состоянию на 01.06.2016	+	+	+	+	+
Мультивалютная	+	–	+	+	+
Анонимное использование	+	–	–	–	+
Статус пользователя ЭРПС (для Российских пользователей):					
физическое лицо	+	+	+	+	+
юридическое лицо (индивидуальный предприниматель)	+	+	+	+	+
Уровень сложности*					
Регистрация	1	2	1	1	1
Пополнение счета	1	1	1	1	1
Обмен валют в ЭРПС	–	–	–	–	1
Вывод законных денег из ЭРПС	1	2	1	1	1
Территория охвата для выполнения расчетных операций					
Транснациональная	–	+	+	+	–
США	–	+	+	+	–
СНГ	+	+	+	+	+
Россия	+	+	+	+	+
Число пользователей, млн	4	6	60	–	17
Взаимодействие пользователя с ЭРПС					
Браузер	+	+	+	+	+
Устройство с NFC	–	–	+	+	+
Платежный терминал	+	+	–	–	+
Карта	+	+	+	+	+
Устанавливаемое программное обеспечение на компьютер	–	+	–	–	–
Мобильное приложение	+	+	+	+	+
Защита данных, передаваемых между пользователем и ЭРПС					
ЭЦП	–	+	–	–	–
SSL шифрование	+	+	+	+	
Сертификация агентов (посредников ЭРПС)	–	+	+	+	–
Защита личного кабинета пользователя					
Логин и пароль	+	+	+	+	+
Двухфакторная авторизация	–	–	+	+	–
Защита мобильного приложения PIN-кодом	+	+	+	–**	+
Выражение единицы учета в ЭРПС					
Национальная валюта	+	+	+	+	+
Уникальная частная единица учета системы	–	–	–	–	–
Драгоценные металлы	–	–	–	–	–
Комиссия					
Расчеты между пользователями, %	1	1	0	0	0
Обмен единиц учета внутри ЭРПС, %	4	–	0	0,15	0
Страна регистрации головной организации	Россия	Россия	США	США	Кипр

* Уровень сложности выражается как 1 – простой, 2 – средний, 3 – сложный.
** Используется TouchID.
Источник: составлено авторами

* The level of complexity is expressed as 1 – easy, 2 – moderate, 3 — challenging.
** Use of TouchID.
Source: Authoring

Таблица 3

Основные параметры децентрализованных ЭРПС

Table 3

Main parameters of decentralized EPSS

Параметры	Bitcoin	Ethereum	Litecoin	MaidSafeCoin
Обозначение единицы учета	BTC	ETH	LTC	MAID
Дата начала функционирования	2009	2015	2011	2014
Криптографический алгоритм шифрования	SHA-256	Dagger-Hashimoto	Scrypt	Транзакционный сбор
Максимальное количество учетных единиц, млн	21	~ 90	84	4 300
Объем капитализации, Bitcoin (на 01.05.2016)	973890,1575	26919,2809	918,9455	676,7689
Объем капитализации, USD (на 01.05.2016)	518109661,2	14321060,13	488879,1	360041,1
Шаг добытых блоков до момента перерасчета сложности их майнинга	2016	–	2016	–
Количество выплачиваемых полных учетных единиц за один найденный блок	*[1]	–	–	*[2]
Используемые типы защиты сети*[4]	PoW*[5]	PoW	PoW	PoR*[6]
Возможность анонимизации транзакций	Нет	Нет	Нет	Нет
Разработчик (страна)	Сатоси Накамото (–)	Виталик Бутерин (Канада)	Чарльз Ли (–)	Дэвид Ирвин (Шотландия)

Продолжение табл.

Параметры	Dash	Factom	Syscoin	Xaurum
Обозначение единицы учета	DASH	FCT	SYS	XAU
Дата начала функционирования	2014	2015	2014	2015
Криптографический алгоритм шифрования	X11	Транзакционный сбор	Scrypt	Транзакционный сбор
Максимальное количество учетных единиц, млн	22	∞	2 000	10
Объем капитализации, Bitcoin (на 01.05.2016)	368,6577	351,6985	311,1213	0,6944
Объем капитализации, USD (на 01.05.2016)	196125,9	187103,6	165516,6	369,4209
Шаг добытых блоков до момента перерасчета сложности их майнинга	1	1	1	
Количество выплачиваемых полных учетных единиц за один найденный блок	*[3]	–	128	–
Используемые типы защиты сети*[4]	PoW	PoE*[7] / PoP*[8] / PoA*[9]	PoW	PoS*[10]
Возможность анонимизации транзакций	Да	Нет	Нет	Нет
Разработчик (страна)	Эван Даффилд (–)	Пол Сноу, Питер Кирби и Дэвид Джонстон (США)	Ден Василик (США)	– (Словения)

Примечание. «–» означает отсутствие данных.
*[1] Награда за блок составляла на начало добычи (2009 г.) 50 монет и уменьшается на 50% через каждые 210 000 блоков.
*[2] Вознаграждение зависит от скорости процессора, пропускной способности памяти, дискового пространства и времени он-лайн.
*[3] Формула расчета количества выплачиваемых полных единиц учета за один найденный блок –
2 222 222/(((difficulty + 2 600) / 9)2), где difficulty – актуальная сложность вычисления нового блока в сети.
*[4] Защита децентрализованной сети от пользователей, не имеющих доказательств наличия права на получение учетных единиц криптовалютной системы.
*[5] Proof of Work (PoW) – механизм защиты, основанный на доказательстве выполненной работы.
*[6] Proof of Resourses (PoR) – механизм защиты, основанный на обеспеченности вычислительными ресурсами.
*[7] Proof of Existence (PoE) – механизм защиты, основанный на доказательстве того, что документ существовал в таком виде в определенное время.
*[8] Proof of Process (PoP) – механизм защиты, основанный на доказательстве того, что документ был обновлен.
*[9] Proof of Audit (PoA) – механизм защиты, основанный на доказательстве аудита, т.е. проверка наличия изменений в обновленном документе.
*[10] Prof of Stake (PoS) – доказательство обеспечивается количеством монет на кошельке, умноженных на их «возраст» или время, которое они лежат нетронутыми.
Источник: составлено авторами

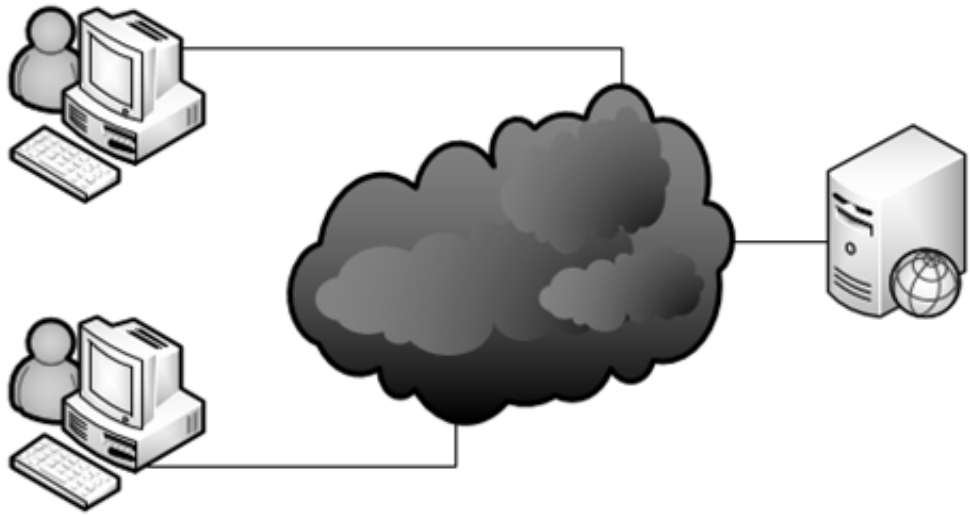
Note. "–" means no data.
*[1] A reward per block was 50 coins at the beginning of the production (2009); it is reduced by 50% every 210,000 blocks.
*[2] Remuneration depends on the processor speed, memory bandwidth, disk space, and time online.
*[3] Formula for calculating the number of fully paid accounting units per one found block –
2 222 222/(((difficulty + 2 600) / 9)2), where difficulty is the current difficulty of computing a new block in the network.
*[4] Protection of the local network from users who do not have evidence of rights to receive units of the cryptocurrency system.
*[5] Proof of Work (PoW) is a security mechanism based on proof of work performed.
*[6] Proof of Resources (PoR) – a security mechanism based on supply of computing resources.
*[7] Proof of Existence (PoE) is a security mechanism based on the proof that a document existed in this form at a certain time.
*[8] Proof of Process (PoP) – a security mechanism based on proof that the document has been updated.
*[9] Proof of Audit (OA) – a security mechanism based on the audit evidence, i.e. a check for changes in the updated document.
*[10] Prof of Stake (PoS) – proof is provided by the number of coins in the purse, multiplied by their "age" or time that they are intact.
Source: Authoring

Рисунок 1

Организация централизованной ЭРПС

Figure 1

Organization of centralized EPSS



Источник: составлено авторами

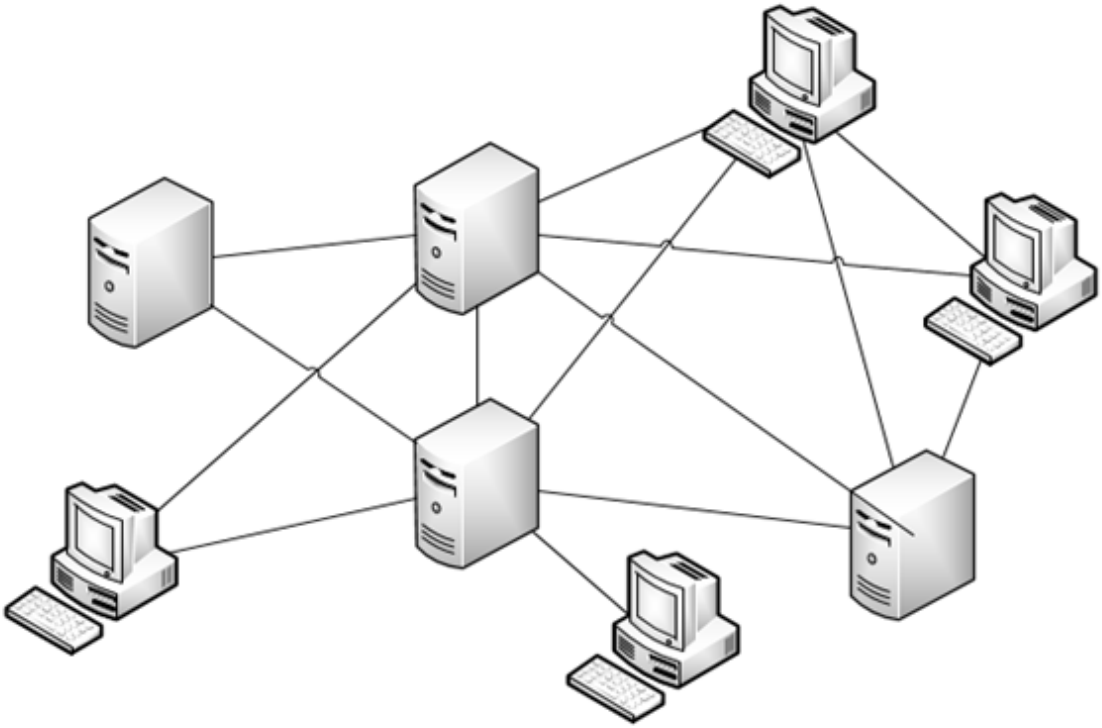
Source: Authoring

Рисунок 2

Организация децентрализованной ЭРПС

Figure 2

Organization of decentralized EPSS



Источник: составлено авторами

Source: Authoring

Список литературы

1. *Аксенов В.С., Захарова Н.В.* Государственное регулирование обращения электронных денег в зарубежных странах // Экономический журнал. 2010. № 20. С. 113–121.

2. *Baddeley M.* Using E-cash in the New Economy: An Economic Analysis of Micropayment Systems. *Journal of Electronic Commerce Research*, 2004, vol. 5, iss. 4, pp. 239–253.

3. *Van Hove L.* Electronic Purses and Currency: A Competition between Networks. *E-Money, The Journal of Electronic Commerce for the Financial Services Industry*, 1998, vol. 1, iss. 2, pp. 3–9.

4. *Власов А.В.* Электронные деньги и эволюционная теория происхождения денег // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. 2012. № 12. С. 13–23.

5. *Генкин А.С., Суворова Е.* Электронные платежи: Будущее наступает сегодня. М.: Альпина Паблишерз, 2011. 284 с.

6. *Goodhart C.* Can Central Banking Survive the IT Revolution? *International Finance*, 2000, vol. 3, pp. 189–209.

7. *Достов В.Л., Шуст П.М.* Электронные деньги: конкурент или новая возможность для розничного финансового сектора? // Банковское дело. 2012. № 12. С. 64–68.

8. *Квашнин С.С.* Электронные деньги как новое направление развития денежного обращения России // Вестник Нижнегородского университета им. Н.И. Лобачевского. 2004. № 1. С. 111–114.

9. *Косой А.М.* Современные деньги // Деньги и кредит. 2002. № 6. С. 42–52.

10. *Кочергин Д.А.* Электронные деньги: теория и анализ моделей эмиссии. СП.: Изд-во Санкт-Петербургского университета, 2006. 164 с.

11. *Cohen B.J.* Electronic Money: New Day or False Dawn. *Review of International Political Economy*, 2001, vol. 8, iss. 2, pp. 197–225.

12. *Krueger M.* Offshore e-money issuers and monetary policy. *First Monday*, 2001, vol. 6, iss. 10, pp. 13–19.

13. *Лопатин В.А.* Особенности оборота электронных денег // Ученые записки Российской академии предпринимательства. 2013. № 36. С. 184–190.

14. *Малиев С.* Электронные деньги: накопленный опыт и перспективные направления развития // Финансы и бизнес. 2008. № 3. С. 51–58.

15. *Маликов И.Г.* Криптовалюты как возможная альтернатива фиатным деньгам и новый эволюционный этап в развитии международных финансов // Проблемы экономики. 2014. № 6. С. 81.

16. *Марамыгин М.С., Прокофьева Е.Н., Маркова А.А.* Экономическая природа и проблемы использования виртуальных денег (криптовалют) // Известия УрГЭУ. 2015. № 2. С. 37–43.

17. *Пашкус Ю.В.* Деньги: прошлое и современность. Л.: ЛГУ, 1990. 184 с.

18. *Пробин П.С.* Проблемы формирования системы обращения криптовалют в России // Социальная политика и социология. 2013. Т. 2. № 4. С. 262–269.

19. *Ревенков П.В., Дудка А.Б.* Риски отмывания денег в условиях применения электронных денег // Вестник Омского университета. Серия «Экономика». 2015. № 4. С. 78–88.

20. *Сейтим Айганым Е.* Использование криптовалют как альтернативное решение проблем мировой валютной системы // Проблемы экономики. 2014. № 2. С. 50–55.

21. *Freedman C.* Monetary Policy Implementation: Past, Present and Future-Will Electronic Money Lead to the Eventual Demise of Central Banking? *International Finance*, 2000, vol. 3, iss. 2, pp. 211–227.

ISSN 2311-8709 (Online)
ISSN 2071-4688 (Print)

Currency Circulation

CENTRALIZED AND DECENTRALIZED APPROACHES TO THE ORGANIZATION OF ELECTRONIC MONEY SYSTEMS: THE PRESENT AND THE FUTURE

Nataliya Yu. TANYUSHCHEVA[a,•], Ekaterina I. DYUDIKOVA[b]

[a] Astrakhan State University, Astrakhan, Russian Federation
n.tanyushcheva@rambler.ru

[b] Astrakhan State University, Astrakhan, Russian Federation
dudikova.e@gmail.com

[•] Corresponding author

Article history:
Received 28 June 2016
Received in revised form
12 July 2016
Accepted 26 July 2016

JEL classification: E42

Keywords: electronic money, crypto-currency, electronic payment system, centralized system, decentralized system

Abstract

Subject The article presents a comparison of centralized and decentralized approaches to the organization of electronic money systems and actions for their improvement.

Objectives The study aims to consider the specifics of using the centralized systems of electronic payments and crypto-currency and to offer actions aimed at improving the decentralized cryptosystems for their practical application at the national level.

Methods We apply formal logic, systems approach, the comparative analysis method, and empirical research (comparison, data gathering and review).

Results We consider centralized and decentralized approaches to the organization of electronic payment systems, emphasize their advantages and shortcomings. The paper presents a comparative analysis of popular electronic payment systems and crypto-currency systems, and our own position to the possibility of practical use of crypto-currency systems at the State level. We provide an update of electronic money classification.

Conclusions The article emphasizes the fact that the use of decentralized cryptosystems in the financial sphere for electronic money circulation in its current form is unsafe. We offer actions for improvement, i.e. a ban on private crypto-currencies; joint use of centralized and decentralized systems with improved regulation mechanism; creation of a new infrastructure, etc. We propose an additional parameter of electronic money classification depending on approach to the system organization, namely, electronic money circulating in the centralized system, and electronic money circulating in the decentralized cryptosystem.

© Publishing house FINANCE and CREDIT, 2016

References

1. Aksenov V.S., Zakharova N.V. [State regulation of electronic money circulation in foreign countries]. *Ekonomicheskii zhurnal = Economic Journal*, 2010, no. 20, pp. 113–121. (In Russ.)

2. Baddeley M. Using E-cash in the New Economy: An Economic Analysis of Micropayment Systems. *Journal of Electronic Commerce Research*, 2004, vol. 5, iss. 4, pp. 239–253.

3. Van Hove L. Electronic Purses and Currency: A Competition between Networks. *E-Money* (The Journal of Electronic Commerce for the Financial Services Industry), 1998, vol. 1, iss. 2, pp. 3–9.

4. Vlasov A.V. [Electronic money and the evolutionary theory of money origin]. *Nauka i obrazovanie: khozyaistvo i ekonomika; predprinimatel'stvo; pravo i upravlenie = Science and Education: Economy and Economics; Business Undertakings; Law and Management*, 2012, no. 12, pp. 13–23. (In Russ.)

5. Genkin A.S., Suvorova E. *Elektronnye platezhi: Budushchee nastupaet segodnya* [Electronic payments: The future comes today]. Moscow, Al'pina Pablisher Publ., 2011, 284 p.

6. Goodhart C. Can Central Banking Survive the IT Revolution? *International Finance*, 2000, vol. 3, pp. 189–209.

7. Dostov V.L., Shust P.M. [Electronic money: a competitor or a new opportunity for retail financial sector?]. *Bankovskoe delo = Banking*, 2012, no. 12, pp. 64–68. (In Russ.)

8. Kvashnin S.S. [Electronic money as a new area of monetary circulation development in Russia]. *Vestnik Nizhnegorodskogo universiteta im. N.I. Lobachevskogo = Vestnik of Lobachevsky State University of Nizhny Novgorod*, 2004, no. 1, pp. 111–114. (In Russ.)

9. Kosoi A.M. [Modern money]. *Den'gi i kredit = Money and Credit*, 2002, no. 6, pp. 42–52. (In Russ.)

10. Kochergin D.A. *Elektronnye den'gi: teoriya i analiz modelei emissii* [Electronic money: theory and analysis of emission models]. St. Petersburg, Saint Petersburg State University Publ., 2006, 164 p. (In Russ.)

11. Cohen B.J. Electronic Money: New Day or False Dawn. *Review of International Political Economy*, 2001, vol. 8, no. 2, pp. 197–225.

12. Krueger M. Offshore E-Money Issuers and Monetary Policy. *First Monday*, 2001, vol. 6, iss. 10, pp. 13–19.

13. Lopatin V.A. [Features of electronic money circulation]. *Uchenye zapiski Rossiiskoi akademii predprinimatel'stva = Scholarly Notes of Russian Academy of Business*, 2013, no. 36, pp. 184–190. (In Russ.)

14. Maliev S. [Electronic money: the cumulative experience and prospects for development]. *Finansy i biznes = Finance and Business*, 2008, no. 3, pp. 51–58. (In Russ.)

15. Malikov I.G. [Crypto-currencies as a possible alternative to fiduciary money and a new evolutionary stage in the international finance development]. *Problemy ekonomiki = Problems of Economy*, 2014, no. 6, pp. 81. (In Russ.)

16. Maramygin M.S., Prokof'eva E.N., Markova A.A. [Economic nature and problems of using the virtual money (crypto-currencies)]. *Izvestiya UrGEU = Journal of Ural State University of Economics*, 2015, no. 2, pp. 37–43. (In Russ.)

17. Pashkus Yu.V. *Den'gi: proshloe i sovremennost'* [Money: The past and the present. Leningrad, Leningrad State University Publ., 1990, 184 p.

18. Probin P.S. [Problems of building the system of crypto-currencies circulation in Russia]. *Sotsial'naya politika i sotsiologiya = Social Policy and Sociology*, 2013, vol. 2, no. 4, pp. 262–269. (In Russ.)

19. Revenkov P.V., Dudka A.B. [Risks of money laundering in the conditions of electronic money use]. *Vestnik Omskogo universiteta. Seriya Ekonomika = Herald of Omsk University. Series Economics*, 2015, no. 4, pp. 78–88. (In Russ.)

20. Seitim Aiganym E. [Using the crypto-currencies as an alternative solution to the problems of the world currency system]. *Problemy ekonomiki = Problems of Economy*, 2014, no. 2, pp. 50–55. (In Russ.)

21. Freedman C. Monetary Policy Implementation: Past, Present and Future – Will Electronic Money Lead to the Eventual Demise of Central Banking? *International Finance*, 2000, vol. 3, no. 2, pp. 211–227.