Russian Journal of Economics and Law. 2021. Т. 15, № 4 / Russian Journal of Economics and Law, 2021, Vol. 15, No. 4
Переводные статьи / Translated articles

ISSN 2782-2923

ПЕРЕВОДНЫЕ СТАТЬИ / TRANSLATED ARTICLES

Ответственные за подбор: *А. В. Власов*, *П. А. Кабанов* /
Persons in charge of selection: *A. V. Vlasov, P. A. Kabanov*

Редактор рубрики *А. В. Власов* /
Rubric editor *A. V. Vlasov*

Научная статья **DOI: http://dx.doi.org/10.21202/2782-2923.2021.4.788-821**

УДК 004:336.74

ДЖ. ГУДЕЛЛ[1],
Х. Д. АЛЬ-НАКИБ[1],
П. ТАСКА[1]

[1] Центр блокчейн-технологий, Университетский колледж Лондона, Лондон, Великобритания

АРХИТЕКТУРА ЦИФРОВОЙ ВАЛЮТЫ, СИСТЕМНО ПОДДЕРЖИВАЮЩАЯ ПРИВАТНОСТЬ И КАСТОДИАЛЬНОЕ ХРАНЕНИЕ

Редактор переводной версии статьи: ***А. В. Власов***

Контактное лицо:
Джеффри Гуделл, Центр блокчейн-технологий, Университетский колледж Лондона
E-mail: g.goodell@ucl.ac.uk

Хазем Денни Аль-Накиб, Центр блокчейн-технологий, Университетский колледж Лондона
E-mail: h.nakib@cs.ucl.ac.uk

Паоло Таска, основатель и исполнительный директор, Центр блокчейн-технологий, Университетский колледж Лондона
E-mail: p.tasca@ucl.ac.uk
ORCID: http://orcid.org/0000-0002-5460-5940

Аннотация

Цель: представление нового подхода к совершению денежных транзакций с использованием цифровых валют.
Методы: абстрактно-логический, аналитический.

Цитирование оригинала статьи на английском: Goodell G., Al-Nakib H. D., Tasca P. A Digital Currency Architecture for Privacy and Owner-Custodianship, Future Internet, 2021, 13, 130. https://doi.org/10.3390/fi13050130
URL публикации: https://www.mdpi.com/1999-5903/13/5/130

ISSN 2782-2923

Результаты: в последние годы во многих развитых странах электронные розничные платежи все больше вытесняют оплату наличными деньгами. Особенно это заметно в секторе электронной коммерции и при выполнении оплаты картой в торговой точке. В результате общество утрачивает возможность использования оплаты розничных покупок, а розничные покупатели лишаются значимых прав, связанных с использованием ими наличных денег. Для решения этой проблемы мы предлагаем новый подход к использованию цифровых валют, который позволит людям совершать транзакции в электронной форме, а также приватно, без обращения к банкам, как в сфере электронной коммерции, так и в торговых точках, где требуется безналичная оплата.

В статье показаны преимущества наличных расчетов относительно безналичных платежей, а также определены возможности трансформации этих преимуществ в цифровые валюты центральных банков. Рассмотрены дискуссионные вопросы развития коммерческих банков в условиях распространения цифровых валют. Описана архитектура цифровых валют, в том числе технология распределенного реестра. Показано, что для более эффективной организации функционирования цифровой валюты необходимо заложить в ее архитектуру приватность операций розничных пользователей, а также определены необходимые для этого меры.

Научная новизна: предложенный в статье подход предлагается использовать для развития инфраструктуры цифровой валюты. Предполагается, что он управлялся бы частным образом, был обеспечен государством и поддерживал процесс регистрации каждой транзакции банком или оператором, опираясь на не связанные с депозитарием электронные кошельки на основе обеспечивающих анонимность технологий, например, слепых подписей или протоколов доказательств с нулевым разглашением (т. е. без раскрытия конфиденциальных сведений сторон сделки). Этот подход может также обеспечить более высокую эффективность и прозрачность взаиморасчетов, погашения задолженности и управления системными рисками. Мы утверждаем, что наша система может восстановить и сохранить важнейшие свойства наличности, включая приватность, подконтрольность владельцу, взаимозаменяемость и доступность, при этом поддерживая функцию частичного банковского резервирования и существующую двухуровневую банковскую систему.

Практическая значимость: предложенный подход может быть применен в практической организации системы денежных расчетов с использованием цифровых валют.

Ключевые слова: цифровая валюта, цифровая валюта центрального банка, ЦВЦБ, приватность, распределенные реестры, подконтрольность владельцу, не связанные с депозитарием электронные кошельки, защищенные транзакции, платежи, электронная коммерция

Благодарности: авторы благодарят Tomaso Aste за его неизменную поддержку нашего проекта, а также Larry Wall из Федерального резервного банка Атланты, Robleh Ali из Медиалаборатории Массачусетского технологического института и Erica Salinas из фонда Value Technology Foundation за их ценные замечания. Мы также высоко ценим поддержку Центра блокчейн-технологий Университетского колледжа Лондона, Центра технологии и мировой экономики Оксфордского университета и Центра системных рисков Лондонской школы экономики, а также выражаем особую благодарность Европейской комиссии за финансирование проекта ФинТех (H2020-ICT-2018-2 825215).

Финансирование: данное исследование финансировалось и было выполнено в рамках гранта Horizon 2020 № H2020-ICT-2018-2 825215.

Как цитировать русскоязычную версию статьи: Гуделл Дж., Аль-Накиб Х. Д., Таска П. Архитектура цифровой валюты, системно поддерживающая приватность и кастодиальное хранение // *Russian Journal of Economics and Law.* 2021. Т. 15, № 4. С. 788–821. DOI: http://dx.doi.org/10.21202/2782-2923.2021.4.788-821

Russian Journal of Economics and Law. 2021. T. 15, № 4 / Russian Journal of Economics and Law, 2021, Vol. 15, No. 4
Переводные статьи / Translated articles

ISSN 2782-2923

The scientific article

G. GOODELL[1],
H. D. AL-NAKIB[1],
P. TASCA[1]

[1] Centre for Blockchain Technologies, University College London, London, United Kingdom

A DIGITAL CURRENCY ARCHITECTURE FOR PRIVACY AND OWNER-CUSTODIANSHIP

Translated version editor of the article: *A. Vlasov*

Contact:
Geoffrey Goodell, Centre for Blockchain Technologies, University College London
E-mail: g.goodell@ucl.ac.uk
Hazem Danny Al-Nakib, Centre for Blockchain Technologies, University College London
E-mail: h.nakib@cs.ucl.ac.uk
Paolo Tasca, Centre for Blockchain Technologies, University College London
E-mail: p.tasca@ucl.ac.uk
https://orcid.org/0000-0002-5460-5940

Abstract

Objective: to present the new approach to perform monetary transactions with digital currency.
Methods: abstract-logical, analytical methods.
Results: in recent years, electronic retail payment mechanisms, especially e-commerce and card payments at the point of sale, have increasingly replaced cash in many developed countries. As a result, societies are losing a critical public retail payment option, and retail consumers are losing important rights associated with using cash. To address this concern, we propose an approach to digital currency that would allow people without banking relationships to transact electronically and privately, including both e-commerce purchases and point-of-sale purchases that are required to be cashless.
The article shows the advantages of cash payments compared to non-cash ones and defines the possibility to transform these advantages into the central bank digital currencies. The disputable issues of commercial banks development under the spread of digital currencies are discussed. The architecture of digital currencies is described, including distributed ledgers technology. It was shown that, for the digital currency to function effectively, it is necessary to include the privacy of end-users into its architecture; measures to achieve that are determined.
Scientific novelty: the approached proposed in the article should be used to develop the digital currencies infrastructure. It should be government-backed, privately-operated and ensure that every transaction is registered by a bank or money services business, relying upon non-custodial wallets backed by privacy-enhancing technology, such as blind signatures or zero-knowledge proofs, to ensure that transaction counterparties are not revealed. This approach can also facilitate more efficient and transparent clearing, settlement, and management of systemic risk. We argue that our system can restore and preserve the salient features of cash, including privacy, owner-custodianship, fungibility, and accessibility, while also preserving fractional reserve banking and the existing two-tiered banking system.
Practical significance: the proposed approach can be applied in the practical organization of perform monetary transactions using digital currencies.

Keywords: Digital currency, CBDC, Privacy, Distributed ledgers, Owner-custodianship, Non-custodial wallets, Shielded transactions, Payments, E-commerce

---

The article was first published in English language by Future Internet. For more information please contact the editorial office.
For original publication: Goodell G., Al-Nakib H. D., Tasca P. A Digital Currency Architecture for Privacy and Owner-Custodianship, Future Internet, 2021, 13, 130. https://doi.org/10.3390/fi13050130
Publication URL: https://www.mdpi.com/1999-5903/13/5/130

Russian Journal of Economics and Law. 2021. Т. 15, № 4 / Russian Journal of Economics and Law, 2021, Vol. 15, No. 4
Переводные статьи / Translated articles

ISSN 2782-2923

Acknowledgments: We thank Tomaso Aste for his continued support for our project, and we thank Larry Wall of the Federal Reserve Bank of Atlanta, Robleh Ali of the MIT Media Laboratory, and Erica Salinas of the Value Technology Foundation for their valuable feedback. We also acknowledge the support of the Center for Blockchain Technologies at University College London, the Center for Technology and Global Affairs at the University of Oxford, and the Systemic Risk Center at the London School of Economics, and we specifically acknowledge the European Commission for the FinTech project (H2020-ICT-2018-2 825215).

Financial Support: This research was funded by Horizon 2020 grant number H2020-ICT-2018-2 825215.

For citation of Russian version: Goodell, G., Al-Nakib, H. D., Tasca, P. (2021). A Digital Currency Architecture for Privacy and Owner-Custodianship. *Russian Journal of Economics and Law, 15 (4)*, 788–821. http://dx.doi.org/10.21202/2782-2923.2021.4.788-821

1. Введение

Такая форма денег, как наличные, предоставляет своему владельцу много преимуществ. Наличные деньги, принадлежащие непосредственно владельцам, позволяют последним совершать сделки приватно, не опасаясь раскрытия, дискриминации, блокировки, что может произойти, даже если сделка была законной. Наличные деньги представляют собой обязательство центробанка, никакой посредник не может помешать выполнить данное обязательство или злоупотребить доверием к центробанку. Напротив, банковские депозиты по своей сути тесно связаны с владельцем, который делится частью своих прав в обмен на возможность пользоваться наличными. В своем стремлении уничтожить наличные общество рискует не оставить нам свободы выбора. В данной статье авторы исследуют вопрос, могут ли цифровые валюты сохранить преимущества формы наличных денег в эпоху электронных платежей.

В работе Mancini-Griffoli и соавт. показано, что анонимность является значимым свойством наличных расчетов, что анонимность транзакций важна и что определенные черты дизайна цифровых валют центральных банков (далее – ЦВЦБ) могут оказывать существенное влияние на финансовую целостность [1].

Наше решение достаточно гибкое, чтобы соответствовать общепризнанным требованиям и целям ЦВЦБ, и имеет большое сходство с наличными. А именно оно обладает достаточной мерой контроля по ограничению сделок между отдельными лицами, при этом является тотальным контролем, который, кажется, считается обязательным, по мнению авторов предложенных ими архитектуроподобных систем [2]. Вместо этого мы предлагаем ограничить масштаб розничных сделок, что, однако, также можно изменить введением дополнительных мер контроля в определенных контекстах, функционально реализованных во внереестровой информационной системе (вне реестра).

Предлагаемый подход позволит регулирующим органам выбирать необходимые параметры в рамках компромисса в трилемме масштаба, контроля и приватности. Например, они могут установить, что определенные организации не могут принимать платежи выше некоторой суммы без сбора и предоставления дополнительной информации [о плательщике. – Прим. перев.], которая ограничивает приватность; или установить потолок перечислений на электронный кошелек для некоторых граждан или нефинансовых учреждений. Этот подход можно сравнить с конвейером, на котором находятся ключи, и если они подходят к замку, что определяется в целом [протоколом системы. – Прим. перев.] или в конкретном случае, то транзакция совершается автоматически. Чтобы избежать сомнений, такая автоматизация может включать так называемые встроенные транзакции, при которых платежи интегрируются напрямую в транзакцию без отдельных механизмов или согласований [для их выполнения. – Прим. перев.].

Структура данной статьи выглядит следующим образом. В следующем разделе (2) представлена общая информация о цифровых валютах, системах распределенного реестра и технологиях обеспечения приватности. В разделе 3 представлен авторский подход к построению архитектуры цифровых валют, обеспечивающий строгую приватность и подконтрольность владельцу, при этом дающий значительные возможности для контроля со стороны регулирующих органов. В разделе 4 сделан анализ существенных

ISSN 2782-2923

особенностей предложенного нами дизайна валюты. Последние два раздела содержат рекомендации и заключение.

2. Общая информация

Данный раздел представляет собой описание контекста и мотивации нашего предложения по архитектуре ЦВЦБ с четырех точек зрения: во-первых, выявлена потребность в публичном механизме для розничных электронных платежей, основанном на принципе оплаты в форме наличных денег; во-вторых, утверждается актуальность проблемы ЦВЦБ для центральных банков и институтов; в-третьих, установлено, что распределенные реестры и обеспечивающие приватность криптографические методы являются важнейшими технологиями, которые включены в наше предложение; наконец, показано, что требования к системе управления (согласно нашему предложению) имеют ряд общих характеристик с существующими системами надзора и контроля.

2.1. Наличные деньги в цифровую эпоху

В настоящее время розничные транзакции с цифровыми валютами воспринимаются как некая узко специфическая область, однако существуют основания того, что в ближайшие десятилетия возрастет как масштаб, так и охват таких транзакций. (Текст раздела 2.1, за исключением последних двух абзацев, также появился в ответ на недавнюю консультацию Агентства по борьбе с финансовыми преступлениями США [3].) Одна из важных причин этого состоит в массовом отказе от использования наличных в большей части развитых стран. Действительно, многие розничные торговцы пришли к выводу, что принимать наличные не обязательно, поэтому во многих юрисдикциях были приняты законы, обязывающие принимать наличные; такие законы действуют в Дании, Норвегии, Китае и нескольких штатах США [4, 5]. Однако этой законодательной защиты может оказаться недостаточно для сохранения наличных как формы оплаты. По мере распространения электронной формы оплаты в розничной торговле переменные расходы, связанные с инфраструктурой обработки наличных, падают по отношению к фиксированным затратам, а предельные затраты на работу с наличными растут. Это верно по отношению к любым розничным пользователям – как покупателям, так и продавцам, а также банкам и операторам сетей банкоматов. Так, в Великобритании сети банкоматов и отделения банков, работающих с наличностью, уже испытывают трудности, которые приводят к снижению объемов оказываемых услуг [6].

В отличие от современной инфраструктуры розничных платежей наличные деньги имеют ряд важных преимуществ, среди которых стоит выделить следующие:

– *Подконтрольность владельцу*. Отсутствие посредника означает, что он не может помешать владельцу осуществить перевод или установить различную стоимость перевода в зависимости от того, с кем совершается сделка. Возможность независимо принимать решение является существенной чертой владения, а важнейшей предпосылкой владения является возможность снимать и использовать наличные в неограниченном количестве сделок без какого-либо надзора.

– *Реальная взаимозаменяемость*. Поскольку использование наличных не требует какой-либо идентификации и не предполагает каких-либо отношений с финансовой организацией, пользователи наличных понимают, что ценность их денег такая же, как любых других. (В некоторых странах потертые банкноты могут стоить меньше, чем новые, и в таких случаях даже наличные не являются полностью взаимозаменяемыми.) Если бы этого свойства не было, участники сделки могли бы прибегать к дискриминации на основании личности владельца денег или посредника, и одинаковое количество денег имело бы разную ценность в руках у разных людей.

– *Приватность по умолчанию*. Не секрет, что розничные платежи оставляют за собой информационный след, который может быть использован для построения подробной картины личной жизни человека, включая его перемещения, финансовые обстоятельства, отношения и многое другое. Уже не одно десятилетие известен тот факт, что электронные платежи могут использоваться для слежения за населением [7, 8]. Ниже мы отмечаем, что защита данных, которая подразумевает доступ к собранной личной информации и ее использование, – это не то же самое, что приватность по умолчанию в том случае, когда пользователи вообще не раскрывают личную информацию о себе. Преимущества приватности по умолчанию, по сравнению со сбором личных данных, очевидны [9], неспособность государств и корпораций помешать несанкционированному доступу со стороны

ISSN 2782-2923

(других) государственных органов или недобросовестных соперников еще раз говорит о необходимости установления запрета на сбор личной информации [10]. Этот аргумент особенно тщательно прорабатывался в контексте систем обмена ценностями [11].

Не связанные с депозитарием электронные кошельки дают возможность сохранить свойства наличности в проведении цифровых сделок, и мы уже обсуждали, что популярность криптовалют во многом обусловлена желанием иметь цифровые наличные деньги в частном владении [12]. Мы считаем, что не связанные с депозитарием кошельки должны давать своим владельцам те же преимущества, что и наличные деньги. Тем самым они будут играть важнейшую роль в обеспечении личной приватности и прав человека. В этом случае широкое распространение онлайн-сделок и цифровых платежей не приведет к расширению контроля над отдельными гражданами через отслеживание денежных потоков и ограничение их обращения.

В контексте ЦВЦБ не связанные с депозитарием кошельки предлагают возможность организации прямых *экономических* отношений, но не прямых *технических* отношений между розничными пользователями ЦВЦБ и центральным банком. Под этим мы понимаем то, что ЦВЦБ представляют собой такие цифровые токены, по которым ответственность несет центробанк. Это соответствует нынешней двухуровневой банковской системе. Мы не имеем в виду, что розничные пользователи ЦВЦБ будут иметь счета в центральном банке или что они будут взаимодействовать с центральным банком напрямую.

2.2. ЦВЦБ и розничные банки

В мае 2020 г. Ив Мерш, вице-президент наблюдательного совета и член исполнительного совета Европейского центрального банка, подчеркнул важную роль частного сектора в управлении платежными сетями: «Дезинтермедиация стала бы экономически неэффективной и юридически несостоятельной. Согласно Договору ЕС, ЕЦБ должен функционировать в рамках принципов свободы рыночной экономики, в соответствии с политикой принятия децентрализованных рыночных решений при оптимальном размещении ресурсов. Исторические примеры размещения ресурсов центральными банками в масштабах всей экономики не являются примерами эффективности или качественного оказания услуг. Кроме того, ЦВЦБ на розничном рынке создаст непропорциональную концентрацию власти в центральном банке» [13].

За несколько месяцев до выступления Мерша заместитель генерального директора Международного валютного фонда (*IMF*) Тао Чжанг также высказал свое мнение об имеющихся предложениях по ЦВЦБ: «Они влекут за собой затраты и риски для центрального банка» [14]. Мы считаем, что эти выводы исходят из предложений, которые до настоящего момента разрабатывались центробанками и основаны на функционировании центрального реестра под управлением самого центробанка [15, 16]. По нашему мнению, такие предложения не отличались ни целостностью, ни соответствием существующим моделям для выполнения платежей, расчетов и клиринга. Напротив, наше предложение разработано специально с учетом затрат и рисков, о которых говорили Мерш и Чжанг, а также полностью соответствует существующей системе платежей. Об этом подробно говорится в разделе 2.3.1.

Чжанг также выдвинул идею «синтетической ЦВЦБ», состоящей из цифровых токенов, выпущенных банками частного сектора [14]. В нашей статье мы докажем, что те положительные качества, которыми, по мнению Чжанга, будет обладать синтетическая ЦВЦБ, будут также присущи и предлагаемой нами системе, за исключением того, что последняя не ставит препятствий существованию «реальной» ЦВЦБ, поскольку управление инфраструктурой будет осуществляться частными организациями по денежному обслуживанию (далее – ОДО) [*money services businesses*, *MSB*], включая, но не ограничиваясь банками. Такие организации охватывают для наших целей, как традиционные коммерческие банки и финансовые институты, так и новые организации, чьи активы будут состоять лишь из резервов центробанка и чьи обязательства будут, в свою очередь, представлять собой лишь депозиты. В этом состоит важное отличие от предложения г-на Чжанга. Хотя Чжанг не дает конкретного описания технической стороны синтетической ЦВЦБ, мы предполагаем, что она не включает распределенного реестра и не делает возможными частные сделки, поскольку частные банки смогут видеть все операции и владельцев цифровых токенов.

При этом эффективная розничная ЦВЦБ не обязательно приводит к дезинтермедиации банковского сектора. ЦВЦБ, которую мы предлагаем, имеет больше общего с физической наличностью, чем с бан-

ISSN 2782-2923

ковскими депозитами, и не заменяет последние. Она не будет использоваться для перезалога и не будет приносить проценты владельцам, по крайней мере в традиционном смысле. Мы рассматриваем розничную ЦВЦБ главным образом в качестве технологии, облегчающей выполнение платежей и транзакций потребителей. Это не просто более масштабируемая версия оптовой ЦВЦБ, отражающей различные требования розничных и оптовых пользователей денег. Розничные пользователи ЦВЦБ будут предпочитать банковские депозиты цифровой валюте центрального банка для своих долгосрочных инвестиций по тем же причинам, по каким они предпочитают банковские депозиты вместо наличности; этот аспект мы обсуждаем в разд. 4.3. Необходимо также отметить, что центробанк не может адекватно заменить все функции коммерческих банков, о чем будет сказано в разд. 4.6.

2.3. Аспекты архитектуры

Еще один важный вопрос – будет ли ЦВЦБ действовать «на основе счетов» [1], т. е. пользователи будут ли иметь дело только со *счетами*, представляющими собой долгосрочные взаимоотношения, или будут реализованы «на основе цифровых токенов», когда ЦВЦБ будет существовать независимо от каких-либо конкретных отношений, как это происходит с монетами или банкнотами. Счета могут представлять собой отношения с посредником или с самой системой-реестром, и цифровые валюты устроены по-разному. Например, токены биткоина существуют независимо [17], а токены эфириума – на счетах [18]. Эти архитектуры [протоколы сети. – Прим. перев.] не симметричны: хотя токены в системах «на основе токенов» могут находиться в распоряжении посредников, действующих от лица пользователей, такое устройство не обязательно, тогда как счета изначально создаются, чтобы представлять собой постоянные отношения.

ОДО не всегда выполняют все функции банков, например, по выдаче кредитов. Более того, наше предложение предусматривает полную конвертируемость альпари[2] для ЦВЦБ, банковских депозитов, банкнот и (для авторизированных ОДО) резервов; это облегчит как его внедрение, так и взаимозаменяемость и общий состав денежной массы. Насколько при этом возникнут какие-либо барьеры или ограничения, будет зависеть от политических решений. Однако по большому счету конвертируемость альпари для наличных и банковских депозитов по умолчанию необходима с точки зрения практического применения и реализацию данной структуры. Выпуск и внедрение ЦВЦБ представляет собой новый политический инструмент, регулирующий мотивацию для владения и использования ЦВЦБ через свои различные качества, а также уравновешивающий возможный отток средств из банковских депозитов [19]; мы не думаем, что ЦВЦБ может полностью заменить последние.

2.3.1. Технология распределенного реестра

Технология распределенного реестра (англ. *Distributed Ledger Technology*, сокр. *DLT*) дает возможность разделить ответственность за нормотворчество между пользователями. *Распределенный реестр* – это «реестр, разделенный между узлами *DLT* узлами сети[3] и синхронизированный между ними путем механизма консенсуса» [20]. Хотя с помощью централизованной технологии теоретически возможно построить публичную инфраструктуру цифровой валюты, и даже такую, которая будет сохранять приватность [21], мы считаем, что реализация характерных элементов распределенного реестра, включая без ограничений свойства *консенсуса* и *неизменности* внутри сообщества [20], необходима для успеха данной инфраструктуры на практике. Это не означает, что инфраструктура должна обеспечивать или позволять совершать сделки между пользователями напрямую, а указывает на то, что система должна управляться самим сообществом, без решений какого-либо привилегированного арбитра, и что единодушное мнение о том, какие транзакции были совершены, должно отражать соглашение, принятое в данном сообществе. В частности, *DLT*-технология должна реализовывать консенсус [правила. – Прим. перев.] среди независимых игроков таким образом, чтобы достичь практически полного единодушия[4] в сообществе пользователей перед вводом в реестр новой записи или перед изменением правил управления реестром.

[1] Или на основе принципа ведения счетов. – Прим. перев.

[2] Альпари (от итал. *al pari*) – точное соответствие между рыночной ценой и номинальной стоимостью цифрового актива. – Прим. перев.

[3] Пирами (*peers*), или нодами сети. – Прим. перев.

[4] Согласия, доверия между нодами (узлами сети) распределенного реестра. – Прим. ред.

ISSN 2782-2923

В контексте цифровой валюты *DLT*-технология обеспечивает прозрачность операций и правил в системе путем ограничения (на техническом уровне) каждого отдельного участника, включая центральный банк, а также правительственных регуляторов в тех действиях, что они могут выполнять в одностороннем порядке. Такая прозрачность дополняет, но не заменяет собой регулятивный надзор.

На рис. 1 показана таксономия цифровых денежных систем. ЦВЦБ является одной из таких систем. Прежде всего необходимо решить, будет ли наша система платежей основана на цифровых токенах или на счетах. Первый вариант имеет ряд преимуществ, в том числе существенное сокращение накладных расходов, связанных с попарной сверкой и регулятивной отчетностью. Однако еще важнее то, что любая система, основанная на счетах, не может обеспечить приватность, поскольку ее структура с необходимостью требует отображения идентификаторов счета, по которым можно определить обе стороны любой сделки. Таким образом, следует признать, что сохранение средств обмена на основе цифровых токенов отвечает интересам общества, повышает благосостояние и приводит к необходимости использования наличных, при этом обеспечивая центральные банки и правительства инструментами для предотвращения и оценки рисков, характерных для платформ цифровой платежной инфраструктуры.

2.3.2. Приватность по умолчанию

Мы предлагаем включить в дизайн системы требование того, чтобы розничные пользователи ЦВЦБ имели право на приватность, причем не только в отношении хранителей активов и других корпоративных игроков, но и в отношении государства. Правоохранительные органы могут попросить кастодиального хранителя[5] цифровых активов об исполнении предусмотренных законом действий. Однако легко представить, что вся информация о сделке может быть доступной правоохранительным органам (или иным лицам) по их запросу, что и стало широко распространенной практикой, с помощью которой государства оказывают влияние на отношения между гражданами и частными организациями.

К счастью, можно регулировать финансовые транзакции и без сбора данных, которые будут использоваться для квалификации действий отдельных граждан. Для этого в зависимости от конкретного случая

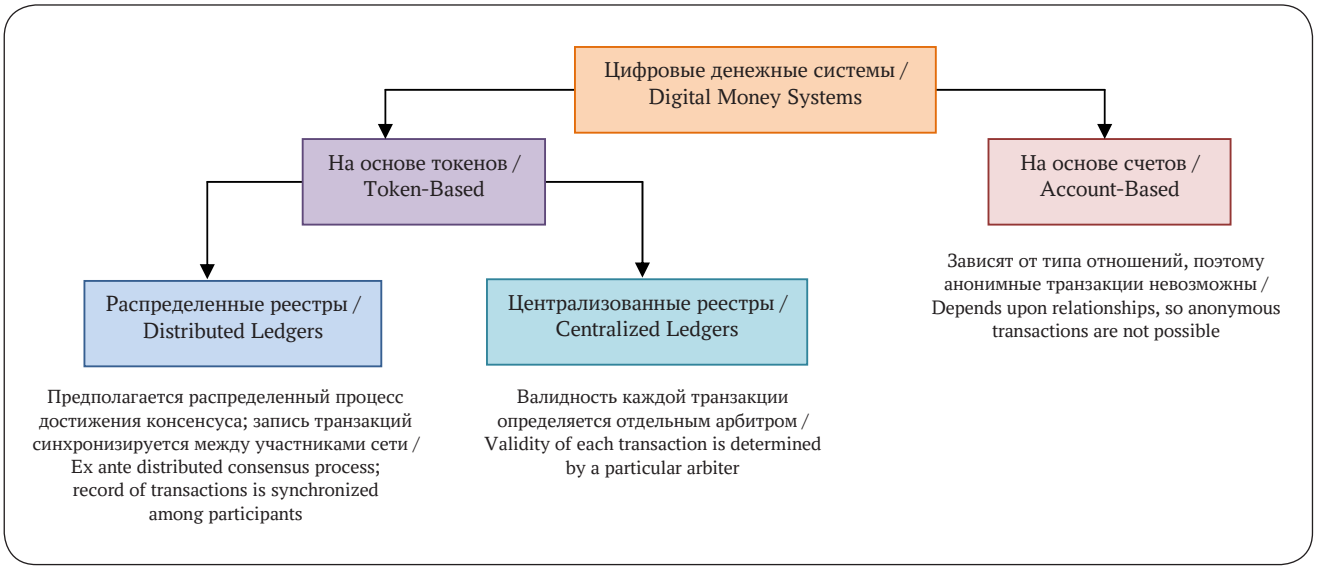

Рис. 1. Таксономия цифровых денежных систем
Fig. 1. Taxonomy of digital money systems

[5] Или кастодиальный депозитарий, кастодиан.

ISSN 2782-2923

применяются внешние средства базовой архитектуры, управляемые решениями руководства, среди которых можно назвать ограничение размера для перевода средств на анонимные адреса или ограничение размера перевода от частных лиц.

Мы не думаем, что приватность можно сочетать с полной прозрачностью системы (например, через «ваучеры анонимности» [22, 23]) или что она может определяться защитой, предлагаемой некоей третьей стороной. Если бы ЦВЦБ не обеспечивала определенную степень приватности, многие пользователи, включая тех, для кого важен риск быть учтенными или подвергнуться дискриминации, продолжили бы пользоваться менее зарегулированными способами для выполнения платежей, в том числе наличными деньгами [24]. Более того, существует потребность в частично анонимном средстве платежа [25], а также в разнообразных инструментах, которые могут быть использованы для выполнения платежей; соответственно, широкое разнообразие потребностей домохозяйств придает ЦВЦБ непосредственную социальную значимость [26].

В том же высказывании, которое уже упоминалось в разд. 2.2, Mersch также отмечает важность и значимость сохранения приватности, предположив, что любая попытка снизить степень приватности платежей «неизбежно повлечет за собой социальные, политические и юридические проблемы» [13].

Этот аспект важен по трем причинам. Во-первых, никакая цифровая валюта, будь то основанная на цифровых токенах или иная, на практике не гарантирует абсолютной анонимности: вспомним о возможностях атак по времени, ошибок в программном обеспечении, ограничений операционной безопасности. Даже использование банкнот не дает полной анонимности: их серийные номера позволяют отследить и пометить отдельные купюры, хотя, насколько нам известно, такие меры несовершенны и редко используются для слежения. Тем не менее следует рассмотреть области применения систем платежей, которые побуждают клиентов пользоваться различными свойствами обеспечения анонимности и в целом компромиссными решениями. Во-вторых, появляется возможность создать такую систему, в которой была бы достигнута и применена реальная приватность, в отличие от таких сомнительных предложений, как предоставление привилегированного доступа или защита приватности через предоставление полномочий, а не по умолчанию [27]. Подобная система, которую мы описываем в разд. 3, сочетает в себе усовершенствованный вариант применения различных систем цифровых валют при поддержке государства, которые предлагалось использовать до сих пор (поддерживаемых институционально, но не частных), и всевозможных «внешних» решений, включая *общедоступные* реестры, которые используются в таких [анонимных. – Прим. перев.] криптовалютах, как *Zcash* и *Monero*[6]. В-третьих, приватность достаточно важна для того, чтобы мы не спешили создавать или поддерживать инфраструктуру, которая могла бы ее подорвать. В отличие от *защиты данных*, которая предполагает предотвращение незаконного использования собранных данных, *приватность* главным образом не позволяет отдельным лицам (а иногда и организациям) раскрывать информацию о своих (законных) действиях. По сути, защита данных не заменяет приватности [9]. Следовательно, приватность является фундаментальным свойством архитектуры системы, которое не может быть «предоставлено» или «гарантировано» какими-либо полномочиями.

В принципе, приватность как свойство архитектуры должна совмещаться с регулятивным подходом, который неотчуждаемо защищает права розничных пользователей ЦВЦБ. (Остальная часть раздела 2.3.2 также служит ответом на недавнюю консультацию Агентства по борьбе с финансовыми преступлениями США [3].) Чтобы избежать нарушения важных аспектов приватности и прав человека, необходимо принять определенные регулятивные и технические меры, обеспечивающие следующее:

– не связанные с депозитарием кошельки не должны содержать постоянной идентифицирующей информации, такой как уникальный идентификатор или адрес, связанный с несколькими транзакциями;

– не связанные с депозитарием кошельки не должны раскрывать информацию, включая ключи или адреса, связанные с предыдущими или последующими транзакциями, которые могут быть использованы для идентификации их держателей, владельцев или источников средств;

– обязательство идентифицировать стороны сделки может действовать только во время транзакции;

[6] Частные криптовалюты (негосударственные. – Прим. ред.), не поддерживаемые институционально.

ISSN 2782-2923

– процесс предоставления информации по запросу банков или ОДО для целей бухгалтерского учета или отчетности не должен включать не связанные с депозитарием кошельки и может производиться только с согласия обеих сторон сделки.

Таким образом, обычные пользователи не связанных с депозитарием кошельков смогут быть уверены в том, что их рутинные действия не отслеживаются, за исключением случаев, когда пороговые суммы их транзакций не слишком высоки, и в некоторых других редких обстоятельствах, когда информация о сторонах сделки запрашивается для целей бухгалтерского учета или отчетности. Для каждого случая такого запроса должно быть обязательным получение отдельного явно выраженного согласия владельца или держателя цифровых токенов; такие запросы не должны быть постоянными для обычных граждан, совершающих простые действия, а также они не должны требовать от не связанных с депозитарием кошельков или иных персональных устройств раскрытия какой-либо информации, идентифицирующей их владельца или держателя.

2.3.3. Криптографические технологии, повышающие приватность

Для обеспечения приватности по умолчанию мы рассматриваем такую технологию, которая применяется в некоторых криптовалютах, например, таких как *Zcash* и *Monero*. Существует, по крайней мере, три возможных подхода:

1. ***Скрытый адрес, схема на основе обязательства Педерсена, кольцевая подпись***. Скрытые адреса, которые обеспечивают секретность публичных (открытых) ключей[7], генерируя их отдельно от приватных (закрытых) ключей[8] [28], передают функцию защиты приватности получателю ценности [29]. Применение обязательства Педерсена позволяет узнать размер транзакции только ее участникам [30, 31] и удаляет метаданные о транзакции из записей реестра [29]. Кольцевая подпись позволяет атрибутировать подписанные сообщения «определенному кругу возможных лиц без указания конкретного подписавшего» [32], тем самым передавая функцию защиты приватности отправителю ценности [29].

2. ***Доказательство с нулевым разглашением (Zero-knowledge proofs, ZKP)***. Реализация данной схемы «позволяет одной из сторон доказать другой стороне, что утверждение истинно, не раскрывая иной информации, кроме того факта, что утверждение истинно» [29]; потенциально эту схему можно использовать для защиты всех метаданных о транзакции [29]. Неинтерактивные методы доказательства с нулевым разглашением, такие как *ZK-STARK*, дают значительные преимущества в характеристиках по сравнению с интерактивными вариантами [33], и, судя по оценкам их эксплуатационных свойств [33–35], мы можем ожидать, что такие операции должны быть достаточно быстрыми, чтобы обслуживать транзакции непосредственно в точках продаж и в секторе электронной коммерции, хотя было бы полезно получить дополнительные доказательства этого предположения.

3. ***Слепые подписи или слепые кольцевые подписи***. Поскольку предлагаемая нами архитектура не является пиринговой в отношении к своим пользователям, мы считаем, что в ней можно использовать метод слепых подписей, подобный тому, который предложил Chaum [21]. При этом необходимо, чтобы получатели (потраченных) токенов немедленно возместили их эмитенту либо, аналогично, чтобы плательщик анонимно поручил эмитенту разместить средства на счете, предназначенном получателю. При использовании слепых подписей в качестве эмитента могут выступать несколько игроков, действующих независимо; при выпуске или возмещении токенов они, соответственно, либо размещают на общем счете, либо снимают средства с него, так же, как это делал бы один пользователь [36].

2.4. Управление системой

Поскольку технологии, способствующие повышению приватности, требуют постоянного внимания [37], ОДО и широкая общественность должны се-

[7] Публичный ключ (открытый ключ, англ. *public key*) – число, выведенное из приватного (закрытого) ключа с помощью однонаправленной функции. Доступен для публичного обмена и позволяет кому угодно удостовериться в том, что цифровая подпись сделана с использованием соответствующего закрытого ключа. – Антонопулос А. М. и Вуд Г. (2021). Осваиваем Ethereum: создание смарт-контрактов и децентрализованных приложений. Москва, ЭКСМО. 512 с. https://www.researchgate.net/project/Mastering-Ethereum-Book. – Прим. перев.

[8] Приватный (закрытый ключ, англ. *private key*, или *secret key*) – секретное число, с помощью которого пользователи Ethereum (в случае с блокчейн-платформой *Ethereum*, или пользователи другого блокчейн-протокола) могут доказать, что они владеют учетной записью или контрактами. Там же. – Прим. перев.

ISSN 2782-2923

рьезно заняться вопросами поддержания, проверки, изменения и улучшения технологии, обеспечивающей приватность средствами внутри самой системы [12]. Такой подход предполагает формирование процесса поддержания безопасности, а также непрерывных обновлений технологических решений и свойств по мере необходимости. Прозрачность, которую предоставляет технология *DLT*-технология, может сформировать базу, с помощью которой широкая общественность будет наблюдать и анализировать работу системы, включая любые изменения ее нормального функционирования; в результате стороны транзакции будут защищены от технологически продвинутых нарушителей, стремящихся раскрыть анонимность пользователей ЦВЦБ и отслеживать их.

В конечном итоге, кто контролирует код, на основе которого работает система, тот и контролирует работу системы. В качестве аналогии можно рассмотреть роль групп разработчиков в урегулировании споров по поводу реестра в криптосообществах [38]. По этой причине централизованное сообщество разработчиков может, разумеется, отрицать преимущества децентрализованного реестра. При этом предполагается, что каждый независимый участник системы должен установить свою собственную жесткую процедуру принятия изменений в коде, включающую, скорее всего, внутреннюю проверку кода и анализ безопасности, независимо от того, используют участники общую базу кода или нет; эта процедура, вероятно, должна также подлежать общественному надзору. Такие процедуры внутреннего и внешнего контроля должны охватывать широкий круг участников с различными интересами в области безопасности, и, в частности, следует обеспечить возможность своевременных изменений при решении возникающих проблем (включая, но не ограничиваясь полными и частичными отключениями сети от ее функционирования), при этом сохраняя защиту пользователей и операторов системы от программных лазеек и других уязвимостей, которые могут появиться при быстрых изменениях (кода). Это непростая задача, однако работа групп обеспечения безопасности в проектах с открытым кодом, например, Debian [39], показывает, что сочетание глубокого контроля и быстрых изменений вполне достижимо.

Кроме того, следует отметить, что регулятивные органы могут сотрудничать с частным сектором при выработке норм и установлении процедур проверок на соответствие. Примером могут служить установленные процедуры для управления торговыми сетями, такими как система национального рынка США [40]. В 2005 г. Комиссия по ценным бумагам и биржам США (*U. S. SEC*) ввела Правило 611, согласно которому все компании – агентства по регулированию деятельности финансовых институтов (FINRA) должны публиковать и быть подписанными на публикуемый в режиме реального времени список наилучших предложений для всех ценных бумаг из списка на всех биржах, входящих в данную систему, а также любая биржа, получившая рыночный ордер, должна перенаправить его на ту биржу, которая выполнит его по наилучшей цене. Таким образом, от компаний – членов *FINRA* требуется применять передовые технологии для обеспечения корректной передачи всех рыночных ордеров [41].

Эти примеры показывают, что регулятивные органы могут сформулировать нормы с учетом использования технологий, что частные игроки могут разработать технологии для поддержания таких норм и что изменения норм могут происходить в контексте совместного регулирования, хотя формально предложения будут инициироваться регулятивными органами. С нашей точки зрения, мнение о технической сложности вовлечения государственных игроков является предрассудком и не должно влиять на развитие общественных систем.

С точки зрения ЦВЦБ, управление и принятие решений в рамках платформы в основном сводится к аутентификации и последующему разрешению транзакций. Мы считаем, что частный сектор может самостоятельно контролировать инфраструктуру, лежащую в основе нашего предложения, при этом операционная деятельность должна осуществляться исключительно со стороны частного сектора. По нашему мнению, в пилотном проекте должно принять участие не менее пяти ОДО, а для надежной работы – не менее двадцати ОДО. Одобрение транзакций должно происходить путем консенсуса в масштабах операторов инфраструктуры всей платформы. При этом возможность формально стать оператором инфраструктуры и, соответственно, ОДО потребует одобрения местного регулятора. В этом контексте можно предположить, что центральный банк несет ответственность за контроль над расчетно-клиринговой деятельностью. (Например, в Великобритании

ISSN 2782-2923

этот контроль может быть организован с помощью совместного надзора со стороны Управления пруденциального регулирования (*Prudential Regulatory Authority*, сокр. *PRA*) и Управления по финансовому регулированию (*Financial Conduct Authority*, сокр. *FCA*) в отношении данного вида деятельности).

3. Предложение авторов

Суть нашего предложения изложена в статье Goodell и Aste [12], где описаны два подхода к усилению институциональной поддержки цифровой валюты. Мы опираемся на второй из этих подходов, а именно перемещение частных средств при посредничестве организаций; при этом функционирование системы полностью осуществляется регулируемыми институтами, и она имеет следующие черты:

1. Используется *электронный токен, выпускаемый правительством,* с помощью которого средства перемещаются без необходимости попарной сверки счетов.

2. Позволяет управлять инфраструктурой транзакций (платежей, взаиморасчетов и клиринга) *независимым частным игрокам* (предполагается, что независимые частные игроки будут участвовать в деятельности совместно с регулирующим органом, таким как *FINRA* в США, или полуавтономных комитетов, таких как *FCA* в Великобритании), при этом позволяя центральным банкам контролировать денежную политику и выпуск ЦВЦБ, а именно создание и уничтожение ЦВЦБ, но не ее распределение.

3. Защищает *метаданные о транзакциях,* по умолчанию связывая отдельных пользователей ЦВЦБ с историей их транзакций, без посредничества доверенных третьих сторон.

4. Обеспечивает *прозрачность* каждой транзакции для регуляторов (исключая информацию о сторонах сделки), давая возможность анализировать системные риски.

В данном разделе мы описываем, как предлагаемый нами механизм цифровой валюты функционирует на системном уровне, идентифицируя интерфейсы между институциональным и техническим аспектами архитектуры.

3.1. Основные положения

По нашему мнению, цифровая валюта может быть выпущена центральным банком в качестве «истинной» *цифровой валюты центрального банка*, хотя она может быть выпущена и правительством, представляя собой обязательство по обеспеченным залогом государственным средствам, таким как суверенный фонд благосостояния или казначейские обязательства. В любом случае следует отметить, что во многих странах (включая Великобританию) никакая отдельная сторона (включая центральный банк) не обязана разрабатывать, поддерживать и обновлять нормы записи финансовых переводов и улаживать споры относительно их истинности. Заметим также, что обязанность управлять инфраструктурой транзакций и контролировать платежные системы отличается от обязанности создавать цифровые токены и поддерживать стоимость государственной валюты. Во многих странах системы платежей, клиринга и расчетов управляются совместными усилиями [42, 43]. Структура, предусматривающая внешнее управление инфраструктурой транзакций с цифровой валютой, вполне может совмещаться с управляющей функцией центрального банка по использованию цифровой валюты для эмиссии денег и осуществления денежной политики.

В частности, мы оспариваем аргумент о том, что, поскольку у центрального банка нет очевидных мотивов для злоупотребления данными, то все пользователи должны доверять ему информацию о своих платежах. Идея о наделении властей правом исключительного доступа к частной информации, и в частности, идея о разделении доступа к частной информации между множеством полномочных органов, была уже опровергнута [44]. Так, явно незаинтересованный пользователь может очень быстро превратиться в заинтересованного, если будет обладать чем-то, что интересует его влиятельных партнеров. Поэтому можно проявлять разумное доверие к денежной политике центрального банка, но не в вопросе информации о транзакциях.

Наш подход к цифровой валюте существенно отличается от вариантов, предложенных несколькими центральными банками [15, 16]. Мы утверждаем, что назначение цифровой валюты – обеспечивать, в контексте розничных продаж, механизм электронных платежей, не опирающийся на счета, а в контексте оптовых продаж – являться средством расчетов, более надежным и менее затратным с операционной точки зрения, чем ныне существующие. Цифровая валюта не должна заменять банковские депозиты, которые по-прежнему будут необходимы для осуществления

ISSN 2782-2923

экономически важных функций, таких как частичное банковское резервирование, создание кредита, страхование вкладов. Не заменяет она и наличные средства, которые дают множество преимуществ, включая широкий доступ к финансовым услугам, операционную надежность, а также уверенность в том, что транзакция будет завершена без участия третьих сторон. По нашему мнению, на практике цифровую валюту будут использовать, прежде всего, для облегчения переводов средств, которые нельзя выполнить с помощью физических наличных, и люди будут пользоваться ею лишь в тех случаях, в которых пользуются наличными.

Тем не менее наше предложение предусматривает наличие у цифровой валюты некоторых свойств наличных денег. А именно мы считаем необходимым сохранить следующие свойства:

1. Устойчивость к массовому отслеживанию. Наличные позволяют владельцам совершать транзакции без опасения, что их действия будут отслеживаться кем-либо. В разделе 4.5 мы сравниваем наше предложение с наличными и наглядно показываем, что наша система не повышает риск мошенничества или нарушения политики *AML/KYC* [законодательство о противодействии легализации (отмывании) доходов, полученных преступным путем, и о проверках благонадежности клиентов. – Прим. переводчика] по сравнению с существующей системой. Фактически мы думаем, что эффект будет обратным, учитывая возможности использования инструментов цифрового мониторинга и анализа данных в случае регулируемых видов деятельности, которые требуют соблюдения определенных норм, и к которым можно применить анализ деятельности регулируемых институтов.

2. Гарантия совершения сделки. Наличные позволяют владельцам быть уверенными, что потенциальная транзакция успешно завершится независимо от отношений с держателем или третьей стороной, которые могут заблокировать, отложить сделку, или потребовать ее верификации.

3. Отсутствие дискриминации. Наличные позволяют владельцам быть уверенными, что их деньги будут приняты так же, как любые другие, и в частности, что их стоимость не будет зависеть от характеристик владельца.

Для выполнения этих требований наша система должна быть основана на токенах, что мы понимаем как возможность для розничных пользователей держать цифровые токены, представляющие ценность вне отношений с кастодианом[9], а также как отсутствие обязательной привязки данных токенов к какому-либо адресу или идентификатору, который можно использовать для идентификации пользователя или его других цифровых токенов. Счета могут использоваться в связке с инфраструктурой, в которой будут реализованы цифровые токены, хотя мы категорически не согласны с аргументом, представленным Bordo и Levin, о том, что процент может начисляться только на счет, а значит, любые ЦВЦБ должны содержаться на счетах [45]. В частности, система ЦВЦБ не обязательно должна выплачивать проценты своим держателям; заметим, что с наличными этого не происходит (см. разд. 2.1 и 4.1). (Отдельно отметим, что мы допускаем возможность выплаты реестром некоей компенсации наподобие процентов непосредственно на цифровые токены, с некоторыми существенными ограничениями.) Говоря более конкретно, свойство доверия, к которому мы стремимся, внутренне присуще нашему цифровому токену, поскольку мы хотим, чтобы розничные пользователи доверяли самому цифровому токену, а не какому-то числу предоставляющих счета институтов или операторов данной системы. Кроме того, мы прямо заявляем: доверие не может быть произведено, а может быть только заслужено. Еще важнее то, что доверие не создается, если о нем просят; оно возникает, когда показывают, что оно не нужно. Это положение лежит в основе подхода, который мы описываем в разд. 3.

В предлагаемой нами системе многие – не обязательно все – граждане и организации будут иметь банковские счета, на которые они будут принимать платежи. На эти счета могут начисляться проценты путем кредитной деятельности банка. Банки смогут обменивать цифровую валюту на наличные или на резервы центрального банка на условиях альпари и, как правило, не будут являться держателями электронных кошельков с количеством цифровой валюты, равным размеру их депозитов. В случае ЦВЦБ банки смогут также напрямую обменивать цифровую валюту на резервы центрального банка. Если частное

[9] Кастодиан – учреждение (обычно банк), осуществляющее хранение ценных бумаг и иных финансовых активов клиентов, а также управление этими ценными бумагами. – Прим. ред.

ISSN 2782-2923

лицо (или организация) просит вывести цифровую валюту, банк сможет ее предоставить так же, как сейчас он предоставляет наличные. Как и с наличными, в распоряжении банка может быть ограниченное количество цифровой валюты, поэтому на объем и частоту таких снятий будет установлен лимит, как это происходит и в настоящее время при снятии наличных. Получив цифровую валюту, граждане и организации смогут использовать ее для покупок или иных платежей, в качестве альтернативы платежным системам на основе счетов или банковским переводам, и цифровая валюта будет, как правило, приниматься на кошельки регулируемых ОДО так же, как и наличные.

3.2. Описание дизайна системы

Наше предложение по дизайну ЦВЦБ основывается на подходе, описанном в работе Goodell и Aste [12] как перемещение частных средств при посредничестве организаций, который разрабатывается в данной статье и служит основой дальнейших исследований. В нем используется технология *DLT*-технология для осуществления платежей, что мотивировано причинами, описанными в разд. 2.3.1.

Мы предлагаем использовать архитектуру контролируемого распределенного реестра, участниками которого должны стать регулируемые ОДО. Предприятия по денежному обслуживанию включают банки, другие финансовые организации, например, службы по обмену иностранной валюты и безналичным банковским переводам, а также некоторые нефинансовые организации, такие как почта [42]. В отличие от общедоступных *DLT*-систем, требующих ресурсоемких и вычислительно-затратных механизмов, например, доказательства выполнения работы для противодействия «атаке Сибиллы» [10] (англ. *Sybil attack*), контролируемые *DLT*-системы поддерживают эффективные механизмы консенсуса, такие как протокол консенсуса, устойчивого к Византийским сбоям[11] (*Practical Byzantine Fault Tolerance, PBFT*) [46], и работают аналогично популярным платежным сетям. В частности, опыт платформы *Ripple* показал, что ее сеть способна надежно обрабатывать 1 500 транзакций в секунду [47]. Хотя оператор популярной платежной сети *Visa* утверждает, что его система может обрабатывать более 65 000 транзакций в секунду [48], ее реальная пропускная способность составляет не более 1 700 транзакций в секунду [49]. По этой причине мы ожидаем, что система цифровой валюты сможет достичь необходимой пропускной способности без дополнительных инноваций. Кроме того, хотя распределенный реестр основан на одноранговых коммуникациях между участниками, мы считаем, что потребление ресурсов будет сравнимо с таковыми у центров обработки данных, которые поддерживают фондовые биржи или расчетные сети, в отличие от тех центров обработки данных, которые поддерживают так называемые майнинговые пулы для публичных *DLT*-сетей.

В нашей схеме только стороны, совершающие транзакции в рамках реестра и участвующие в достижении консенсуса[12], могут быть ОДО, т. е. регулируемыми организациями[13]. Записи в реестре должны быть доступны всем участникам; кроме того, мы считаем, что некоторые лица, не входящие в число участников, например, сотрудники регулятивных и правоохранительных органов, должны получать от ОДО актуальную информацию, которая позволит им напрямую обращаться к реестру, без необходимости запрашивать информацию в каком-либо ОДО. Хотя записи в реестре сами по себе не будут, как правило, содержать метаданные о сторонах транзакции, однако ОДО, проводившее каждую транзакцию, будет известно властям, и предполагается, что ОДО будут вести учет своих транзакций, включая их размер и любую имеющуюся информацию о сторонах сделки, даже если она быда ограничена (изначально), а также что власти будут иметь доступ к этим записям. Далее рассмотрим вопросы доступа к реестру:

– *Записи в реестре*. Мы предполагаем, что операторами реестра могут быть только организации, авторизованные для внесения в него записей, а именно регулируемые ОДО (включая, но не ограничиваясь бан-

[10] Вид атаки в одноранговой сети, в результате которой жертва подключается только к узлам, контролируемым злоумышленником. – Прим. ред.

[11] Или Византийской ошибке, или отказоустойчивость к византийским сбоям – это способность системы продолжать функционировать, в ряде случаев в сокращенном объеме, не выходя полностью из строя, когда часть ее компонентов работает неправильно. – Прим. ред.

[12] То есть участвующие в работе сети. – Прим. ред.

[13] Согласно местному законодательству и требованиям регулятора (например, Банка России в РФ). – Прим. ред.

ISSN 2782-2923

ками) и центральный банк. Последний вносит записи, создающие или уничтожающие ЦВЦБ, а ОДО вносят записи, «перемещающие» цифровые токены внутри системы путем переписывания их от одного владельца ключа (со счета. – Прим. ред.) на другого. Все записи должны быть одобрены через механизм консенсуса, а именно квалифицированным большинством (возможно, практически всеми, в зависимости от конкретных настроек консенсуса внутри системы) частных пользователей (участников системы платежей).

– *Чтение реестра*. В дизайне нашей системы, набор организаций-пользователей, имеющих право читать записи реестра, должен включать тех, кто имеет право делать в нем записи, а также расширительно должен быть представлен для регулирующих организаций, которые будут контролировать стороны, имеющие право делать записи в реестр. По нашему мнению, нет необходимости в общедоступном программном интерфейсе для чтения реестра, хотя правительство может счесть такой механизм полезным, например, для выполнения функции общественного контроля за функционированием системы или для мониторинга подозрительной активности (в сети). Для обеспечения приватности по умолчанию необходимо, чтобы запись о транзакции в реестре в целом не раскрывала историю транзакций отдельных пользователей, поэтому предполагается, что объем информации, раскрываемой в записях реестра, должен быть ограничен.

3.3. Не связанные с депозитарием электронные кошельки

Еще одна важная черта предлагаемой архитектуры – это *приватность по умолчанию*. Мы считаем, что защита данных не заменяет приватность (см. разд. 2.3.2), однако Ulrich Bindseil отмечает: «Существует мнение, что более сбалансированное решение должно включать адекватную защиту данных об электронных платежах» [50]. В рамках предлагаемого нами решения можно предположить, что вся сеть управляется регулируемыми ОДО, поэтому будет предложено создать «мастер-ключ» или другой механизм исключительного доступа [51], чтобы уполномоченный на данную процедуру орган мог нарушить анонимность розничных пользователей ЦВЦБ. Это искушение следует преодолеть, помня о долгой истории такой аргументации [27, 44, 52] и последующих признаний политиков Европы и Америки [53, 54], которые неоднократно говорили о потенциальной возможности злоупотреблений, как и о внутренних уязвимостях безопасности таких систем. В конечном счете замена защиты данных приватностью может обернуться созданием ограничений для законопослушных розничных пользователей ЦВЦБ, совершающих свои действия в рамках закона, которые не смогут доказать, что осуществляли сбор данных не с целью дальнейшего анализа. Заставить людей пользоваться системой, опирающейся на защиту их данных, означает производить доверие, что невозможно – так как доверие нужно заслужить. Более того, преступники и лица (организации), имеющие привилегированный доступ, будут иметь целый спектр возможностей, включая, но не ограничиваясь доверенностями, криптовалютами и кражами идентичности, которые окажутся в их распоряжении в качестве «внешних решений», если законодатели попытаются принудить их к прозрачности.

В отличие от схем, содержащих механизмы исключительного доступа, которые позволяют уполномоченным органам отследить стороны каждой транзакции, а значит, не обеспечивают анонимности, наша система нацелена на достижение истинной, хотя и частичной анонимности[14], когда стороны транзакции могут оставаться анонимными, но все транзакции подлежат контролю на уровне интерфейса со стороны ОДО. Мы считаем, что уникальность дизайна нашей системы состоит в достижении анонимности и контроля одновременно; это достигается тем, что все транзакции происходят с участием регулируемого игрока, но при этом власти (а также инсайдеры, взломщики и т. д.) не имеют возможности раскрыть анонимность сторон транзакции, будь то напрямую или через корреляционные атаки.

Для выполнения требования приватности по умолчанию мы вводим концепцию *не связанного с депозитарием электронного кошелька*, под которым понимается программное обеспечение, взаимодействующее с реестром через ОДО и позволяющее розничному пользователю ЦВЦБ отделять свои токены ЦВЦБ от любой значимой информации[15] о своей личности

[14] Квазианонимности. – Прим. ред.

[15] Имеется в виду персональная информация (данные), информация, необходимая для идентификации плательщика (или получателя). – Прим. ред.

ISSN 2782-2923

или личностей прежних владельцев этих токенов. Пользователь выводит (переводит) токены из ОДО в собственный не связанный с депозитарием кошелек, а через некоторое время возвращает их в ОДО через последующую транзакцию, как показано на рис. 2. Система реестра работает как публично контролируемая DLT-система, участниками которой являются регулируемые ОДО. Алиса выводит цифровые токены из ОДО на свой не связанный с депозитарием кошелек в рамках транзакции T_{out}, а затем возвращает их в ОДО через транзакцию T_{in}. ОДО, из которого выведены токены, может быть тем же, что ОДО, на которую их возвратили, или иным. В частности, транзакция, в которой взаимозаменяемый токен переходит из не связанного с депозитарием кошелька к ОДО, не раскрывает никакой значимой информации об истории этого токена или его владельца.

Для обеспечения описываемых свойств приватности у не связанных с депозитарием кошельков система ЦВЦБ должна обладать встроенной технологией обеспечения приватности, подобной той, о которой мы говорили в разд. 2.3.3. Если используются протоколы доказательств с нулевым разглашением конфиденциальных сведений или сочетанием скрытых адресов, обязательства Педерсена и кольцевых подписей, то становится возможным избежать необходимости требовать от принимающих ОДО немедленного возврата эмитенту (потраченных) токенов, которые они получили. Однако использование метода слепых подписей, возможно, дает некоторое преимущество в виде эффективности вычислений; этот метод подходит в качестве примера, так как в нашей системе ОДО участвует в выполнении любой транзакции. А именно поскольку мы устанавливаем, что цифровой

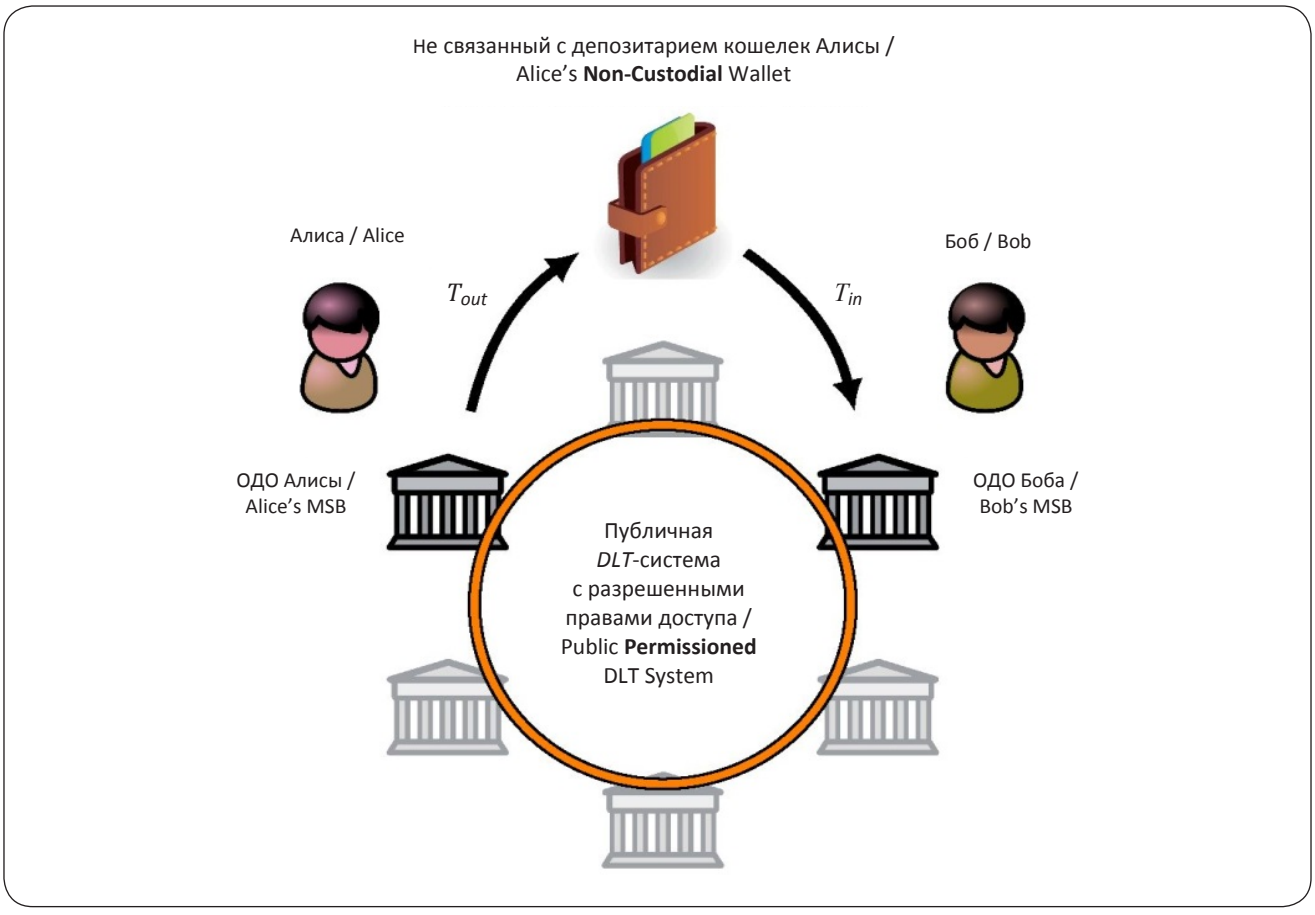

Рис. 2. Схематическое изображение предлагаемого дизайна системы
Fig. 2. Schematic representation of the system design

ISSN 2782-2923

токен, изъятый из регулируемого ОДО, будет возвращен в регулируемый ОДО без обращения к другим не связанным с депозитарием кошелькам, то можно установить, что пользователь сначала получит анонимный токен от ОДО, а затем пошлет неанонимную версию этого токена в ОДО получателя. При условиях, сформулированных Chaum, это можно сделать без раскрытия информации, связывающей транзакцию, в которой токен выводился, с транзакцией, в которой он был возвращен.

Часто утверждают, что современные криптографические технологии, такие как доказательства с нулевым разлашением, слишком сложны для понимания или эффективного применения в инфраструктуре с публичным реестром; однако в реальности они широко применяются. Кроме того, во множестве случаев регулирование осуществляется без уточнения деталей конкретных технологий, с помощью которых достигается соответствие установленным нормам. Примером может служить принцип совместного регулирования, применяемый регулирующими органами в контексте систем исполнения на наилучших условиях, как описано в разд. 2.4.

3.4. Цикл активности пользователей

На рис. 3 показан типичный цикл активности пользователей ЦВЦБ, иллюстрирующий предлагаемый нами дизайн системы. Пользователь (физическое лицо *B*) имеет счет в банке и получает обычный платеж банковским переводом на свой счет (в банке *B*). Затем пользователь поручает своему банку (банку *B*) вывести ЦВЦБ. При этом некое количество цифровых токенов переводятся на не связанный с депозитарием электронный кошелек собственника через несоедини-

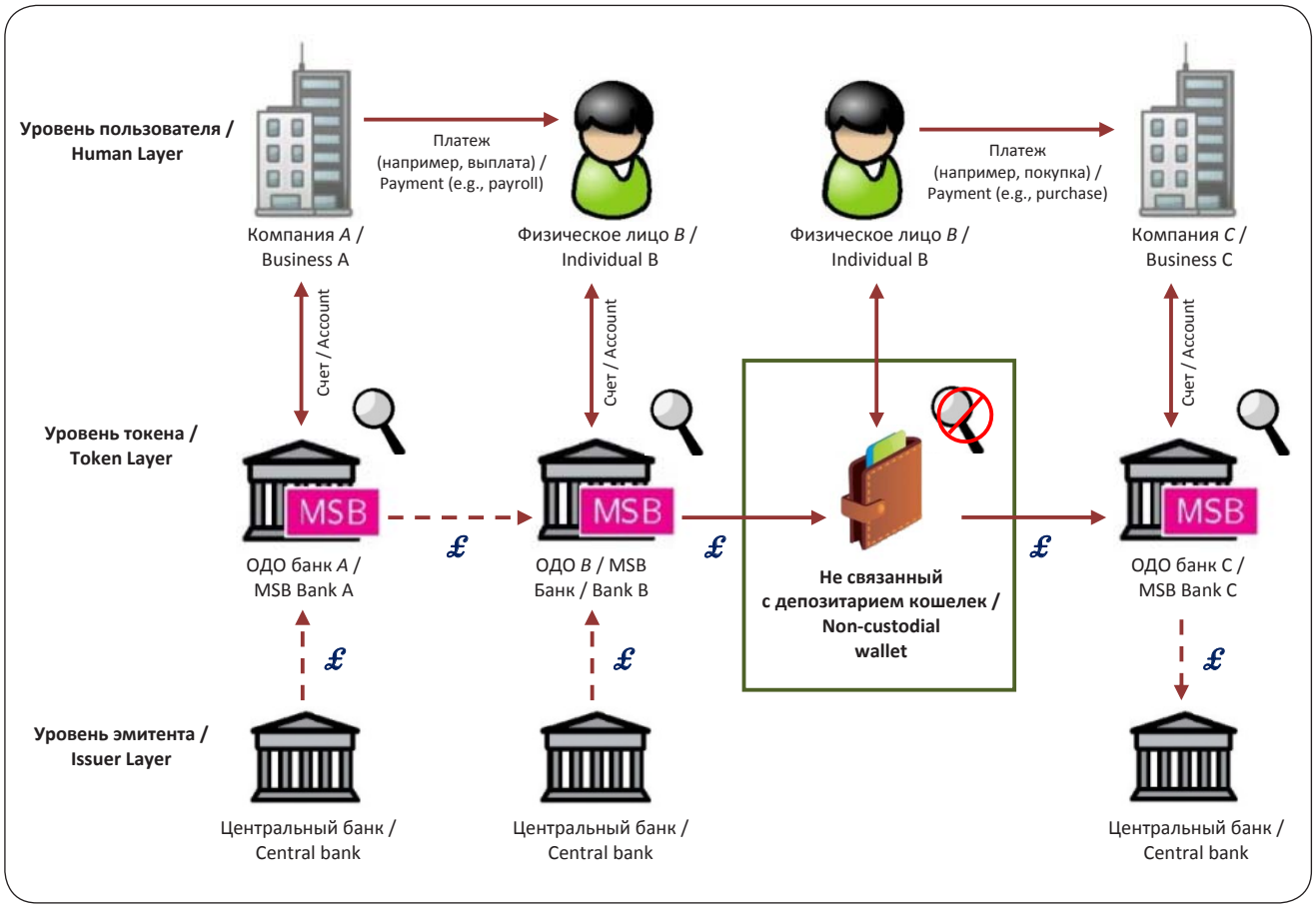

Рис. 3. Схематическое изображение типичного цикла активности пользователей

Fig. 3. Schematic representation of a typical user engagement lifecycle

ISSN 2782-2923

мые транзакции. Транзакции ЦВЦБ в реестре представлены на рисунке в виде символа фунта стерлинга (£). (Если банк *B* не получил ЦВЦБ напрямую из банка *A* вместе с платежом, то он может предоставить ЦВЦБ из своих собственных средств или получить ЦВЦБ из центрального банка в обмен на наличные или резервы.) Затем пользователь обращается к продавцу или другому поставщику услуг (компания *C*), лично или онлайн, который имеет счет в банке (банк *C*), настроенный на получение ЦВЦБ. С помощью своего не связанного с депозитарием электронного кошелька собственник взаимодействует с программным обеспечением, которое создает взаимодействие этого кошелька с банком продавца; этот банк записывает несколько транзакций в реестр, оформляя перевод ЦВЦБ из кошелька в банк продавца, кредитуя счет продавца и информируя продавца об успешном проведении транзакции. Затем банк продавца может вернуть ЦВЦБ в центральный банк в обмен на наличные или резервы. Свойства приватности, заложенные в программное обеспечение реестра и не связанного с депозитарием электронного кошелька, не позволяют пользователю раскрыть информацию о себе или об истории (перемещения и владения) токенов, которая могла бы служить для обнаружения или отслеживания идентичности. В более общем виде выделим четыре механизма, с помощью которых розничный пользователь сможет получить цифровую валюту:

1. Через обмен денежных средств на счете ОДО на цифровую валюту. В нашей системе частное лицо или компания, имея счет в ОДО, сможет *вывести* цифровую валюту с этого счета на не связанный с депозитарием электронный кошелек. Цифровая валюта розничного пользователя на его не связанном с депозитарием электронном кошельке является аналогом наличных. Поскольку ОДО не является ее держателем, она не инвестируется и не приносит процентов; это равносильно хранению денег в физическом кошельке. Возможно, государство сможет выплачивать поощрения или налагать взыскания на сам актив, но это не будет «истинным» процентом и не будет выполнять его функций. Аналогично, частное лицо или компания со счетом в ОДО сможет *депонировать* цифровую валюту с не связанного с депозитарием электронного кошелька на счет, как показано на рис. 4. Розничные пользователи смогут помещать средства на свои собственные счета, возможно, с определенными ограничениями или дополнительными проверками, в случае если это происходит часто или ими размещаются крупные суммы средств.

2. Как получатель цифровой валюты из внешнего источника на счет в ОДО. В этом случае пользователь будет получателем платежа в цифровой валюте. Отправитель этого платежа может быть известен, например, если это счет в ОДО, или неизвестен, например, если это не связанный с депозитарием электронный кошелек.

3. Как получатель цифровой валюты из внешнего источника на *не связанный с депозитарием электронный кошелек*. Любая транзакция, в ходе которой на не связанный с депозитарием электронный кошелек поступает цифровая валюта из внешнего источника, должна проходить через ОДО. Таким образом, ключевое отличие между этим режимом получения цифровой валюты и снятия с собственного счета пользователя состоит в том, что в данном случае получатель не имеет (или не использует) счет в ОДО. Эта форма транзакций показана на рис. 5. Розничные пользователи ЦВЦБ, желающие осуществить транзакцию между собой с помощью не связанного с депозитарием кошелька, должны делать это через регулируемый институт либо через регулируемую компанию со счетом в регулируемом институте. Этот институт создает транзакции в реестре между не связанным с депозитарием и кошельками двух розничных пользователей ЦВЦБ, при этом не создавая для них счетов. Мы предполагаем, что для этого нужно будет установить некие законные требования, определяющие роль ОДО в таких транзакциях, например, лимит на размер транзакции или требование получателю представить идентифицирующие документы сотруднику-человеку. Мы также считаем, что этот процесс был бы очень полезен при осуществлении государственных выплат (в качестве экономического стимулирования или по другим причинам) розничным пользователям без участия банковских счетов, как показано на рис. 6. На этом примере видно, как розничный пользователь может запросить причитающуюся ему ЦВЦБ либо напрямую у центробанка, либо через институт, такой как государственная казна или частный банк. Пользователь идентифицирует себя в регулируемом ОДО, который выполняет необходимые проверки на соответствие.

4. Через обмен физических наличных денег на цифровую валюту. Транзакции, в которых физические

ISSN 2782-2923

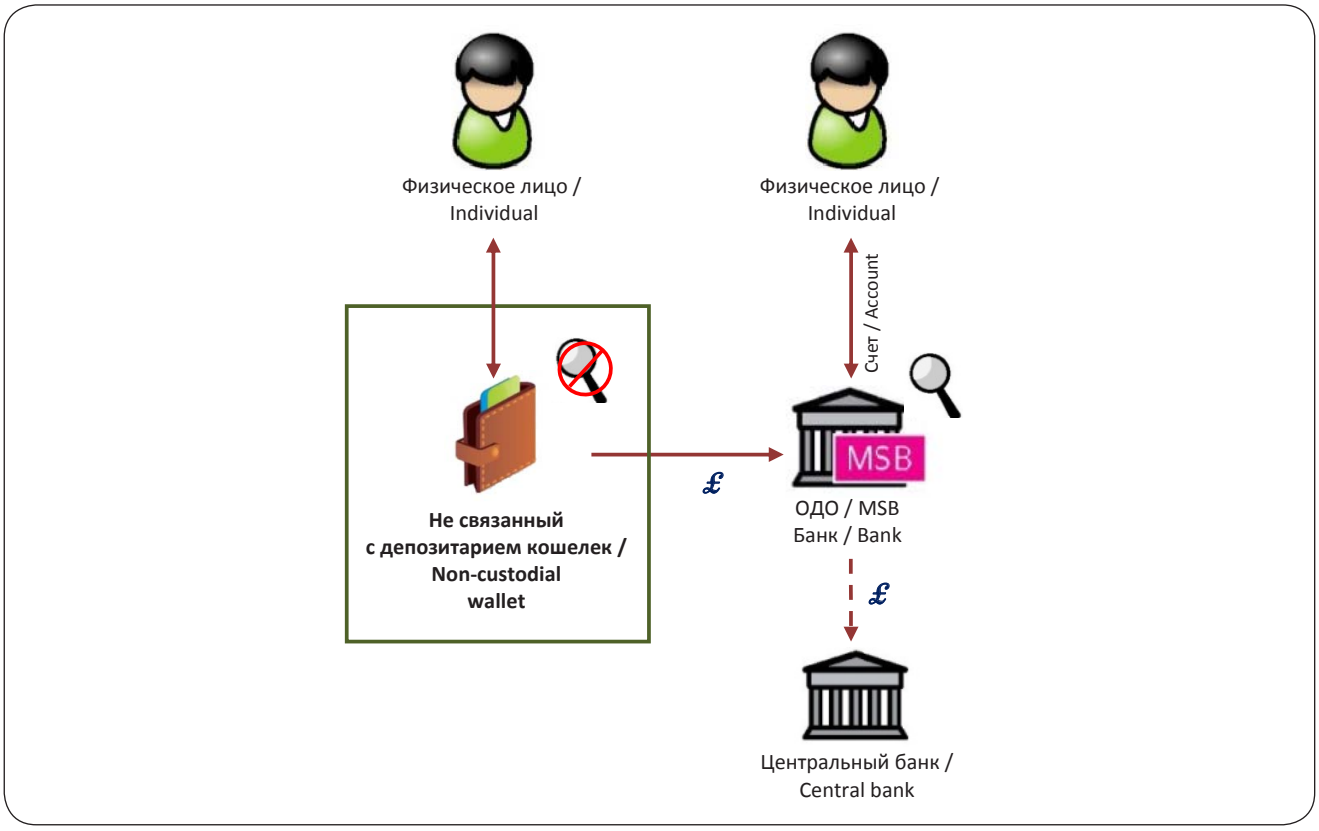

Рис. 4. Схематическое изображение размещения (перевода) ЦВЦБ пользователем на банковский счет
Fig. 4. Schematic representation of a user depositing CBDC into a bank account

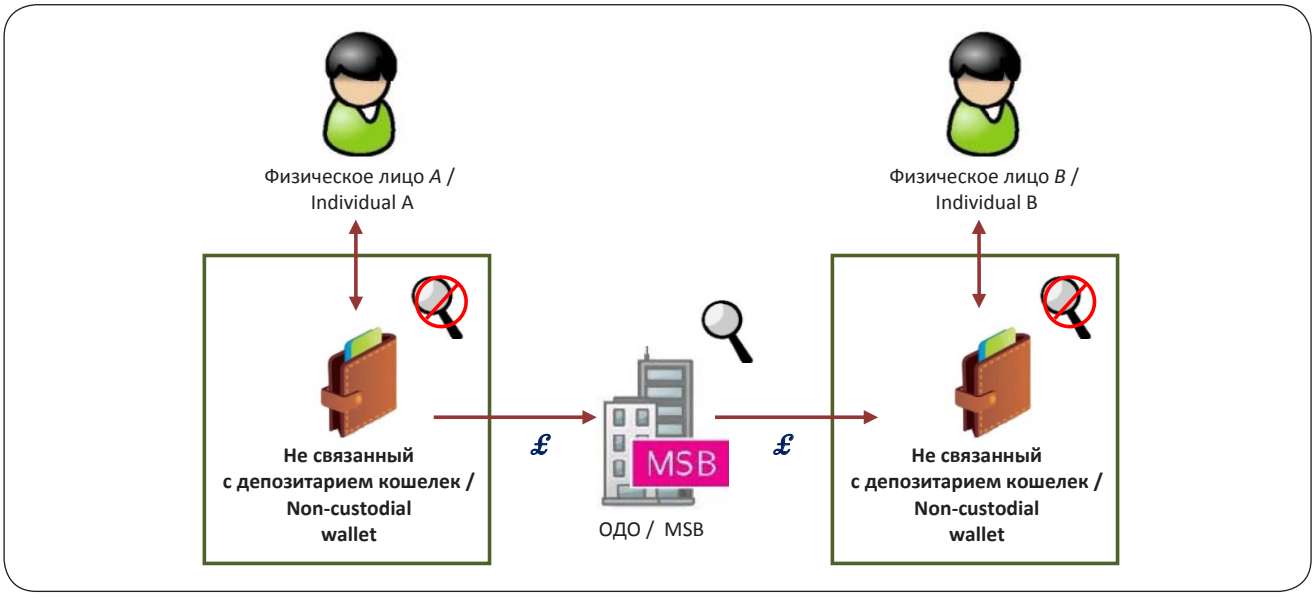

Рис. 5. Схематическое изображение опосредованной транзакции между пользователями
Fig. 5. Schematic representation of a mediated transaction between consumers

ISSN 2782-2923

наличные конвертируются в цифровую валюту, будут осуществляться через ОДО согласно соответствующим правилам, так же как цифровая валюта, получаемая напрямую из внешнего источника. Например, можно установить, что ОДО должно запрашивать информацию о происхождении денег, если объем превышает определенное пороговое значение.

Отметим, что обычно на розничных банковских счетах нельзя держать ЦВЦБ от имени отдельного пользователя, так же как и наличные. Время от времени банк обменивает ЦВЦБ на резервы центрального банка, и наоборот, поскольку ожидается, что банк будет выдавать ЦВЦБ своим розничным клиентам в соответствии с объемом и частотой расходования средств.

Отметим также, что сообщения в реестре публикуются регулируемыми финансовыми институтами. Это важное свойство предлагаемой системы: все транзакции в реестре должны быть опубликованы регулируемыми ОДО, а поскольку реестр полностью управляется регулируемыми ОДО, частные игроки не могут обменивать ценности напрямую между своими не связанными с депозитарием кошельками. Не связанные с депозитарием кошельки представляют собой уровень перенаправления, в результате чего ОДО не могут идентифицировать *стороны* сделок с их участием. Нельзя проследить связь любой транзакции с не связанным с депозитарием кошельком с другой такой транзакцией, вплоть до уровня косвенных доказательств, таких как время транзакции. К банкам может предъявляться требование «знай своих клиентов» (*KYC*), но к продавцам такого требования обычно не предъявляют. Более того, банку продавца не нужно знать клиентов этого продавца, а банку клиентов продавца не нужно знать ничего о продавце или его банке. В тех случаях, когда продавцу все-таки нужно знать своих покупателей, речь идет обычно о сущности взаимоотношений между ними, нежели о механизме оплаты, и идентификация такого рода должна происходить вне платежной системы.

Если сформирован механизм, с помощью которого никакая отдельная организация или группа не сможет построить профиль какой-либо отдельной транзакции в системе, то при использовании распределенного реестра выполняется важнейшее структурное требование. В дополнение к вышеуказанному требованию о наличии механизмов, защищающих транзакции с не связанным с депозитарием кошельками, таких как скрытые адреса или доказателяьства с нулевым раскрытием, служащих для разделения приходных и расходных операций, предполагается, что частные лица будут использовать свои не связанные с депозитарием кошельки для транзакций с самыми разными сторонами; при этом они будут взаимодействовать с ОДО, выбранными другой стороной, а не с теми, в которых были открыты их не связанные с депозитарием кошельки.

На рис. 5 показан механизм, с помощью которого частные лица смогут совершать операции между не связанными с депозитарием кошельками. Сначала они должны выбрать регулируемое ОДО, которое будет заносить транзакцию в реестр, возможно, за небольшую плату. Это ОДО должно будет обработать ряд транзакций с (условно) первого не связанного с депозитарием кошелька в ОДО и из ОДО на второй не связанный с депозитарием кошелек. ОДО может предоставлять аналогичную услугу частным лицам при обмене ЦВЦБ на наличные и наоборот. Вероятно, ОДО будут собирать информацию о своих клиентах, необходимую для выполнения требований соответствия, однако мы считаем, что для личных и относительно небольших транзакций можно отменить такую серьезную идентификацию клиента, как, например, рекомендованная FATF [55]. В случае небольших онлайн-транзакций между двумя частными лицами мы считаем достаточной учетную идентификацию на основе атрибутов, показывающих, что отправитель или получатель имеет право совершать сделки [56]. Наконец, некоторые ОДО могли бы оказывать розничным пользователям ЦВЦБ услуги по обмену цифровых токенов, метаданные о которых были случайно раскрыты.

Рассматривая возможные варианты стимулирования, представленные на рис. 6, следует отметить следующее. Если государство хочет сделать стимулирующие выплаты определенной группе граждан либо всем гражданам или жителям страны, то каждого из них можно будет найти по уникальному номеру налогоплательщика. (Подобную процедуру возможно реализовать для организаций.) Затем государство просит указать банковский счет, текущий счет или электронный кошелек, на который будут перечислены средства. Если у гражданина или организации нет банковского счета, они могут обратиться к уполномоченному ОДО (например, почтовое отделение) для верификации их прав на выплату; ОДО выполняет необходимые процедуры идентификации, чтобы определить, дей-

ISSN 2782-2923

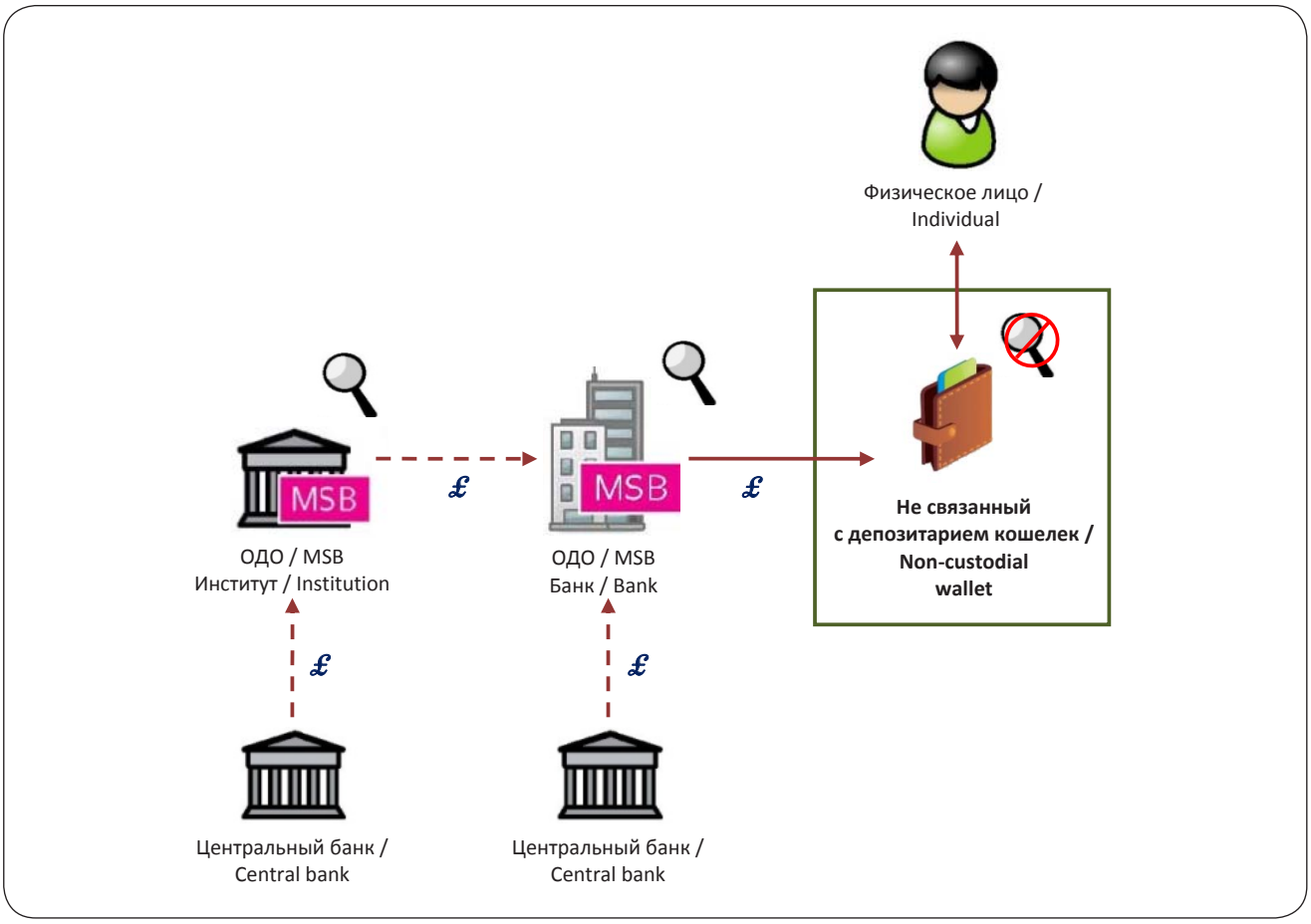

Рис. 6. Схематическое изображение выплаты (перевода) розничному **пользователю на не связанный с депозитарием кошелек**

Fig. 6. Schematic representation of a disbursement to a retail user with a non-custodial wallet

ствительно ли обратившийся с данным уникальным номером налогоплательщика имеет право на выплаты. Если это так, то ОДО может совершить транзакцию по переводу цифровой валюты непосредственно на его не связанный с депозитарием кошелек (без использования банковского счета). Мы предлагаем сделать такой вариант получения выплат доступным как для частных лиц, так и для организаций.

3.5. Вопросы безопасности

В целом функционирование цифровых валют опирается на использование и управление секретной криптографической информацией, такой как ключи; поэтому мы признаем, что использование цифровой валюты, позволяющей самостоятельно владеть цифровыми токенами вне политик безопасности со стороны какой-либо финансовой организации, потребует от пользователей управления безопасностью данными цифровыми активами[16]. Для этого существует целый ряд инструментов, включая идентификацию с применением с однофакторной или двухфакторной аутентификации, кастодиальные услуги, оказываемые третьей стороной, использование однопользовательских физических токенов в качестве альтернативы программному обеспечению электронного кошелька для устройств общего назначения или просто вы-

[16] Имеется в виду то, что пользователям необходимо будет выбрать собственный набор инструментов для управления цифровыми токенами и их безопасного хранения. – Прим. ред.

ISSN 2782-2923

бор лимита цифровой валюты, которую они держат в определенный момент времени у себя на счете. Мы считаем, что все эти инструменты могут быть полезны и, как и использование вместе со многими финансовыми решениями, наилучший выбор будет зависеть от структуры предпочтений и рисков каждого отдельного пользователя.

Разумеется, технология обеспечения приватности сама по себе не предполагает абсолютной анонимности. Хотя описываемый подход намеренно направлен на избегание связей транзакций друг с другом или с любыми идентификаторами владельцев не связанных с депозитарием кошельков, с помощью косвенных доказательств потенциально можно установить связь между множеством транзакций, а информацию о связи отдельного пользователя с конкретной транзакцией можно связать с другими данными и вывести паттерны использования. Например, при совершении анонимных транзакций через Интернет пользователи могут стремиться скрыть информацию о своем операторе мобильной связи или иную информацию, способную нарушить их анонимность. Кроме того, атаки с помощью временного анализа всегда представляют риск для любых действий с низким значением задержки, и мы настоятельно рекомендуем пользователям выдержать определенный период времени, возможно, несколько часов или дней, между снятием денег на электронный кошелек и использованием этих денег. Если бы большинство пользователей немедленно тратили ЦВЦБ после ее поступления на электронный кошелек, то было бы потеряно преимущество их смешения с другими пользователями, которые держат деньги на электронном кошельке некоторое время.

По нашему мнению, в ряде случаев частное лицо может сознательно поделиться личной криптографической информацией о цифровой валюте (например, ключом для совершения транзакции) с другим лицом, тем самым разрешая этому другому лицу совершать транзакции от своего имени. Такие действия сходны с тем, как коллеги или члены семьи пользуются одной дебетовой картой. Мы не рассматриваем этот обмен информацией как платеж, поскольку система не предусматривает запрета для первого лица потратить цифровую валюту до того, как это сделает вторая сторона. Такой обмен правильнее характеризовать как «общий кошелек» или «обещанный платеж», а не как платеж как таковой, так же как выдача чека, датированного будущим числом. Нельзя запретить людям давать обещания. Если частное лицо или организация владеют цифровой валютой, то методы распоряжения ею будут противоположны методам ее получения.

4. Анализ

Следует отметить, что предлагаемый нами дизайн системы цифровой валюты, хотя и может включать в себя ЦВЦБ, но обобщается в качестве «хранилища ценности» [57], которое потенциально может представлять множество различных активов и их инфраструктуру, включая, но не ограничиваясь центральным банком и государственными активами. Для целей нашего анализа мы сосредоточимся на использовании предложенного дизайна ЦВЦБ, и в особенности розничной ЦВЦБ, в качестве инструмента, предоставляющего широкий доступ для общественности к публичной цифровой форме наличных денег.

4.1. ЦВЦБ как система розничных платежей

По нашему мнению, главное преимущество ЦВЦБ состоит в том, что розничные пользователи могут держать ее на своих не связанных с депозитарием электронных кошельках. Аргумент, что ЦВЦБ следует держать только на попечительских счетах, основан на двух допущениях: во-первых, что цифровые активы в токенах невозможно возмещать напрямую; и, во-вторых, что ЦВЦБ предназначена, главным образом, для решения проблемы эффективности, к примеру, транзакционных издержек или распространения эффективной кредитно-денежной политики, и ни для чего больше. Однако существуют вполне приемлемые механизмы, позволяющие напрямую возмещать цифровые активы в токенах, а неизбежное снижение роли наличных в качестве средства платежа является, очевидно, гораздо более глубокой проблемой, чем распространение кредитно-денежной политики. Благодаря наличным люди всегда имели возможность совершать финансовые транзакции с активами, полностью находящиеся под их контролем, которые нельзя было отследить, и которые в целом не были подвержены дискриминации или влиянию третьей стороны. Однако снижение использования наличных показывает, что связанная с ними инфраструктура может в скором будущем стать экономически несостоятельной; в этом случае указанные фундаментальные

ISSN 2782-2923

права могут исчезнуть. Следовательно, ЦВЦБ можно рассматривать, в первую очередь, как возможность для розничных пользователей сохранять преимущества неподотчетных денег в цифровую эпоху.

Возникает вопрос, является ли ЦВЦБ скорее современной формой банковских депозитов или цифровой формой наличных. Если будет предложена система ЦВЦБ, основанная на счетах (прим. ред. см. выше) и подлежащая перезалогу, то она может стать в общем случае жизнеспособным заменителем банковских депозитов; однако если будет использоваться система ЦВЦБ с дизайном, как мы предлагаем, основанным на токенах, которая не будет подлежать перезалогу, тогда она будет больше похожа на реализацию формы наличных денег. В последнем случае у пользователей по-прежнему остаются причины для использования банковских депозитов в качестве средств накопления (среди таких причин – начисление процентов и инфляционные риски) и использовать ЦВЦБ преимущественно в качестве средства платежа, даже если обе формы денег подходят для обеих целей.

Важно отметить, что архитектура предлагаемой системы обеспечивает ее приватность как *по структуре,* так и *по умолчанию*. Наше предложение показывает, как можно поддерживать уровень истинной анонимности даже на платформах, управляемых институционально; тем самым мы опровергаем мнение, что электронные средства розничных платежей, управляемые институционально, должны обязательно собирать все возможные данные о сторонах транзакции.

4.2. Децентрализация

Необходимо прояснить несколько важных вопросов о структуре, основанной на токенах, например, должны ли токены выпускаться напрямую центральным банком или другими институтами (в виде «стейблкоинов») или они могут функционировать полностью вне институциональной среды (в виде «криптовалюты»). Нужно отметить, что стейблкоины несут в себе системный риск. Они связаны с каким-либо другим [обычно физическим. – Прим. перев.] активом, который может рухнуть. Таким образом, пользователи стейблкоинов несут партнерские риски по отношению к тем, кто должен поддерживать указанную связь. Эти риски состоят в том, что либо стейблкоины должны торговаться со скидкой по отношению к активу, с которым они связаны, либо эта связь должна гарантироваться государственной организацией, например, центральным банком. В первом случае стейблкоины не будут стабильными; во втором они не будут отличаться от фиатной валюты.

Системы на основе токенов, в том числе системы с ярко выраженным свойством приватности, могут быть централизованными, т. е. опираться на конкретного арбитра при разрешении споров о валидности каждой транзакции (возможно, с разными арбитрами для разных транзакций), или они могут быть децентрализованными, т. е. использовать для валидации транзакций технологию распределенного реестра, использующую процедуру достижения консенсуса. В случае использования децентрализованной структуры следует рассмотреть вопрос о том, кто будет управлять системой. Например, в случае ЦВЦБ, хотя мы считаем, что за разработку и выпуск токенов ЦВЦБ отвечает центробанк, это не означает, что он же будет отвечать и за управление инфраструктурой транзакций или платежной системой; до сих пор за эти аспекты отвечали, как правило, частные организации. Как отмечалось выше, системы платежей, клиринга и расчетов часто управляются совместными усилиями [42, 43]. Действительно, современная инфраструктура цифровых платежей, основанная на банковских депозитах, зависит от множества игроков, и мы считаем, что такой будет и инфраструктура цифровых платежей, основанная на ЦВЦБ. Ответственность за управление и поддержание стоимости валюты – это не то же самое, что ответственность за управление и контроль над транзакциями, а ответственность за контроль над платежными системами – это не то же самое, что ответственность за управление ими. Структура, которая обеспечивает внешнюю ответственность за управление инфраструктурой транзакций, поддерживающей ЦВЦБ, вполне совместима с операционной ролью центрального банка при использовании ЦВЦБ для создания денег и реализации денежной политики.

Предлагаемая нами модель ЦВЦБ опирается на инфраструктуру распределенного реестра по нескольким причинам. По нашему мнению, в настоящее время это наиболее жизнеспособный метод реализации сотрудничества центрального банка с частными компаниями в сфере создания общенациональной платежной инфраструктуры под управлением частных компаний; это может быть реализовано как через государственно-частное партнерство, так и в рамках иных

ISSN 2782-2923

моделей сотрудничества или надзора. Использование технологии распределенного реестра не предполагает, что домохозяйства или отдельные граждане должны иметь счет в центральном банке или непосредственные отношения с ним, как ошибочно утверждают некоторые авторы. Напротив, в нашем предложении велика роль ОДО, особенно при идентификации, регистрации и сопровождении новых клиентов, соблюдении требований соответствия и управлении их счетами.

По нашему мнению, преимущества технологии распределенного реестра можно распределить по трем категориям, причем каждая из них будет относиться к диапазону ошибок, возможности взлома системы и ответственности, возникающей в результате внутренних и внешних рисков. Мы считаем, что каждое из этих преимуществ обязательно должно присутствовать в системе, чтобы она была успешной. Мы отмечаем следующие преимущества:

1. *Ликвидация прямых затрат и рисков, связанных с управлением системой в реальном времени в роли мастера или арбитра*. Поскольку база данных системы управляется централизованно, централизованный реестр будет с неизбежностью опираться на некоего центрального оператора, играющего операционную роль в транзакциях. Эта роль предполагает следующее. Во-первых, центральный оператор несет административные обязанности, включая обязанность гарантировать надежность системы на техническом уровне и улаживать любые проблемы и споры на техническом и человеческом уровне. Во-вторых, поскольку центральный оператор имеет возможность влиять на транзакции, он будет нести издержки на обеспечение ожидаемого осуществления транзакций, а также риски обвинений в халатности или злоупотреблениях, если транзакции не были осуществлены, как ожидалось. В-третьих, поскольку центральный оператор в одностороннем порядке определяет границы допустимых действий, он может быть обвинен в невыполнении установленных правил.

2. *Предотвращение односторонних действий отдельных пользователей или групп*. Как было показано в исследовании Michael Siliski [58], администратор централизованного реестра может наложить запрет на отдельных пользователей или давать им преференции; явно или неявно взимать плату с пользователей системы; искажать официальные записи о транзакциях; в любой момент менять правила; остановить действие системы без предупреждения.

3. *Обеспечение прозрачности и подотчетности процесса для операторов системы*. Поскольку администратор централизованного реестра может принимать односторонние решения, внешние наблюдатели не могут определить, корректно ли он исполняет свои обязанности. В частности, управление реестром и средства доступа других сторон к реестру находятся под исключительным контролем администратора, который не обязан раскрывать факт своей заинтересованности при изменении протокола или просить другие стороны одобрить изменения. В случае же распределенного реестра можно использовать «обратное наблюдение», когда любые изменения правил должны быть в явном виде одобрены частными операторами.

4. *Повышение эффективности и качества услуг через конкуренцию и инновации*. Если операторы системы подотчетны и заинтересованы в своей деятельности, становится возможным достичь важных целей при предоставлении услуг, включая скорость принятия решений, отсутствие дискриминации в сфере финансов, а также развитие частной инициативы (например, поддержка местных банков) в отличие от насаждения директив сверху.

Каждое из перечисленных преимуществ относится к аспектам диапазона ошибок, возможности взлома системы, а также ответственности центрального органа управления, возникающей в результате внутренних и внешних рисков. Центральный регулирующий орган может наблюдать за функционированием всей сети транзакций и решать, какое из частных ОДО получит право стать ее участником; однако распределенный реестр позволяет передать ответственность за транзакции непосредственно в ОДО. А именно ОДО будет нести ответственность за каждую транзакцию, а распределенный реестр можно использовать для создание (потенциально) неизменяемых записей, связывающих каждую транзакцию с соответствующим ОДО, при этом центральный игрок не будет нести ответственности за отдельную транзакцию.

4.3. Влияние на ликвидность

Выпуск и использование ЦВЦБ может стать для центробанков полезным инструментом управления совокупной ликвидностью. Например, если цифровая валюта центрального банка станет широко распро-

ISSN 2782-2923

страненной, это может привести к изменению совокупной ликвидности; последнее относится к активам, которые используются, обмениваются и обладают премией за ликвидность [19]. В некоторых моделях ЦВЦБ повышает эффективность обмена, учитывая ее низкую затратность и стабильность единицы учета, особенно в тех случаях, когда цифровая валюта (как в нашем предложении) используется для широкого круга децентрализованных транзакций; это позволяет укрепить каналы распространения денежной политики в торговле. В распоряжении центробанка будут определенные возможности для контроля выпуска и стоимости ЦВЦБ, включая целенаправленное использование положительных и отрицательных стимулов для создания более высокой ликвидности или более низкую премию за ликвидность в ЦВЦБ или в банковских депозитах, ориентируясь на наличие трудностей с инвестированием [19]. Кроме того, держатели ЦВЦБ могут использовать ее в качестве внутридневной ликвидности, когда инструменты поглощения ликвидности не достигают аналогичного эффекта. В настоящее время ощущается недостаток краткосрочных инструментов денежного рынка, которые совмещали бы надежность и ликвидность, которые может потенциально обеспечить ЦВЦБ. Следовательно, ЦВЦБ может играть важную сдерживающую роль против шоков ликвидности.

Одно из опасений относительно ЦВЦБ состоит в том, что во время финансового кризиса клиенты могут отказаться от банковских депозитов в пользу ЦВЦБ. Это вполне возможно, однако мы утверждаем, что с нашей системой отказ в пользу ЦВЦБ не более вероятен, чем в пользу наличных. Действительно, ЦВЦБ может способствовать замене активов частного сектора на безрисковые активы с целью обезопасить свои средства, особенно учитывая, что банковские депозиты подвержены рискам непогашения кредита и остаточной ликвидности, несмотря на широкое использование страхования до определенной суммы. В то же время существуют лимиты на вывод ЦВЦБ из финансовых институтов; мы также считаем, что для физических лиц будут установлены лимиты снятия ЦВЦБ с их банковских счетов, так же как такие лимиты установлены для снятия наличных. Если начнется массовое снятие средств, то оно будет сдерживаться такими лимитами и, в принципе, правительство может даже попросить банки установить более жесткие лимиты или вовсе приостановить вывод средств в случае чрезвычайной ситуации. Более того, если правительство гарантирует возврат средств до определенной суммы, то в сочетании с другими выгодами депозитов это может остановить массовое снятие средств. В других случаях соотношения «затраты – выгода» и «риск – выгода» потребуют более тщательного анализа на основе полномочий. Кроме того, мотивация к накоплению средств будет снижаться благодаря наличию «срока годности» на цифровые активы и отсутствию выплаты процентов. Мы признаем, что банковские депозиты останутся привлекательными даже при наличии ЦВЦБ, поэтому считаем, что ЦВЦБ должны быть дополнительным инструментом наряду с депозитами и что банки должны играть определяющую роль в выпуске и хранении токенов ЦВЦБ.

4.4. Влияние на финансовый сектор

В предлагаемой нами системе ЦВЦБ представляет собой самостоятельный финансовый инструмент, который тем не менее имеет с наличностью много общих свойств, включая полное обеспечение и невозможность займов и перезалогов. В сущности, цифровая валюта остается деньгами, относящимися к типу M0[17]. Более того, мы не предлагаем снизить роль банкнот или банковских депозитов. Напротив, мы понимаем, что все три указанных инструмента имеют преимущества и ценность для домохозяйств и компаний, они могут дополнять друг друга и увеличивать совокупное благосостояние частных лиц и организаций и после выпуска ЦВЦБ [26]. Существенным недостатком предложений об отмене наличных является то, что наличные играют относительно большую роль в социально-экономических областях более низкого уровня, а значит, введение ЦВЦБ с целью их отмены негативно отразится на таких домохозяйствах и компаниях. Стоит задаться вопросом, перевесят ли затраты на поддержание инфраструктуры наличных затраты на предоставление широкого доступа к технологической инфраструктуре, которая должна заменить наличные.

Самое непосредственное влияние, которое предлагаемая нами система окажет на финансовый сектор, относится к различным уровням управления рисками.

[17] Денежный агрегат M0 – денежная масса. – Прим. ред.

ISSN 2782-2923

Увеличивая скорость взаиморасчетов, цифровая валюта может улучшить управление рисками ликвидности в сфере финансовых институтов. Кроме того, цифровая валюта может помочь в борьбе с системными рисками как непосредственно, позволяя регулирующим органам отследить практически любую транзакцию, так и косвенно, давая государству инструмент стимулирования при сохранении контроля над всеми рычагами влияния в системе.

Таким образом, в целом технология распределенного реестра обеспечивает создание перспективного инструмента для снижения рисков [59]; поэтому наша архитектура основана на *DLT*-сети под управлением ОДО и других частных институтов, а не на централизованном реестре под управлением единственной государственной (или частной, как в случае стейблкоинов) организации. Вследствие этого наша система снижает целый ряд рисков, связанных с зависимостью от центрального арбитра: (1) технические риски, связанные с доступностью, надежностью и техническим обслуживанием; (2) риски, связанные с вопросами доверия и операционной прозрачности; (3) финансовые и юридические риски. Кроме того, наша система позволяет передать под управление частного сектора инфраструктуру розничных платежей и расчетно-кассовых операций, при этом сохраняя за государственными регулирующими органами контроль над системой на организационном уровне. Поскольку в нашей системе цифровая валюта не заменяет, а дополняет банковские депозиты, роль коммерческих банков оптимизируется без снижения объемов их активов. В частности, мы считаем, что активы центральных банков не будут существенно увеличены после введения нашей системы цифровой валюты, так как, согласно нашему предложению, основное назначение токенов ЦВЦБ состоит не в создании долгосрочного средства накопления, а в повышении эффективности электронных платежей.

4.5. Влияние на уровень мошенничества и ухода от налогов

Мы считаем, что работа ОДО и их взаимоотношения с клиентами должны проходить в режиме строгого соответствия требованиям. В частности, банки должны выполнять требования по надежной идентификации клиентов, а другие ОДО, такие как организации по переводу безналичных средств, пункты обмена валют, почтовые отделения, должны иметь как процедуры идентификации и авторизации, так и ограничения транзакций. Предполагается, что уполномоченные органы смогут отслеживать любую транзакцию и определять конкретное ОДО, выполняющее ее, а также что они будут иметь доступ к записям о транзакциях, которые должны вести ОДО.

Однако, поскольку наша система предполагает истинную анонимность, она не позволяет властям узнать конкретные стороны транзакции. В частности, даже если уполномоченные органы имеют все записи, некоторые транзакции будут совершаться через не связанные с депозитарием электронные кошельки, так же как в операциях с наличными стороны часто остаются анонимными. Хотя уполномоченные органы будут иметь информацию обо всех розничных пользователях и истории снятий ими цифровой валюты, они не смогут связать не связанный с депозитарием электронный кошелек с конкретным пользователем. Вспомним, что отдельные пользователи будут иметь возможность выводить цифровую валюту из ОДО так же, как они получают наличные из банка или банкомата, с такими же ограничениями. Розничные пользователи смогут тратить цифровую валюту так же, как они тратят наличные, делая покупки у продавцов, для которых существуют свои ограничения и которые находятся под контролем финансовых институтов и знают, что получение ими токенов будет отслеживаться уполномоченными органами. Последние будут знать, кто недавно переводил цифровую валюту на не связанный с депозитарием электронный кошелек, так же, как они могут узнать, кто недавно снимал наличные, а также они будут знать, кто недавно получал цифровую валюту с не связанного с депозитарием электронного кошелька. При этом нельзя будет с помощью цифровой валюты связать конкретного получателя денег с тем, кто снимал деньги. Мы утверждаем, что это свойство наличных необходимо и обязательно для защиты индивидуальных пользователей от отслеживания и манипулирования со стороны злоумышленников и других заинтересованных лиц, включая игроков из частного сектора. Более того, раскрытие информации о сторонах каждой сделки налагает ответственность за выявление мошенничества на правоохранительные органы, значительно увеличивая нагрузку на них, тогда как при наличии мотивации преступники все равно смогут использовать промежуточные серверы или

ISSN 2782-2923

взломанные учетные записи для достижения своих целей, даже если каждая транзакция будет полностью прозрачной.

Для борьбы с мошенничеством в нашей системе применен другой подход, ориентированный скорее на механизмы контроля и аналитику данных о транзакциях, чем на отслеживание сторон сделки. Поскольку в каждой транзакции участвует регулируемый финансовый посредник, который должен соблюдать процедуры *AML/KYC*, возникает возможность эффективно рассматривать каждую транзакцию. Уполномоченные органы смогут обеспечить выполнение определенных правил и ограничений держателями счетов, которые получают переводы с не связанных с депозитарием электронных кошельков, включая, но не ограничиваясь налоговым контролем. Записи с таких счетов, а также подлежащие аудиту записи в реестре, генерируемые *DLT*-системой, могут обеспечить сбор данных в режиме реального времени для сферы налогообложения, согласования и соответствия. Поскольку все розничные платежи с участием цифровой валюты будут использовать в конечном итоге один и тот же реестр, станет возможным более непосредственное (по сравнению с текущей ситуацией) распознавание ненормативных действий, таких как намеренное предоставление заведомо неверного адреса для перечисления с не связанного с депозитарием электронного кошелька; в то же время автоматическое подтверждение его соответствия в режиме реального времени станет более доступным. Эти действия смогут производить не только власти, но даже пользователи, тем самым снижая вероятность их совершения.

Рассмотрим также, будет ли безопасное хранение крупных сумм в физических наличных более или менее затратным, чем хранение крупных сумм в цифровой валюте. В принципе, цифровую валюту можно экономно хранить онлайн, однако в защите онлайн-систем могут быть серьезные дефекты, а сроки службы цифровых офлайн-устройств ограничены. Отметим, что обеспечение безопасности обычно оценивается в зависимости от объема ценности, а не от стоимости хранения. Кроме того, использование группировки цифровых токенов, например, по годам выпуска, может предотвратить накопление крупных запасов цифровой валюты, чего не происходит с физическими наличными. (Токены из одной группы подлежат обмену друг на друга, но не на токены из других групп.)

Стоит также рассмотреть вопрос, смогут ли преступные организации, с целью избежать взаимодействия с ОДО, применять обмен частных ключей, вместо того чтобы вступать в транзакции. Мы считаем, что совместное использование приватного ключа – это эквивалент возможности совместно использовать деньги, которые можно использовать только один раз, тем самым создавая договорную обязанность; противоположное действие состоит в передаче права собственности, как при использовании не связанного с депозитарием электронного кошелька. (Заметим, что каждый токен будет иметь свой собственный приватный ключ.) Преступники могут совершать обмен договорными обязанностями с помощью различных частных и офлайн-методов даже при отсутствии обеспечивающей приватность платежной системы. С одной стороны, такие обмены невозможно отследить или ограничить; с другой – для них изначально требуется высокий уровень доверия, а мы утверждаем, что отношения транзитивного доверия должны быстро сойти на нет после успешных транзакций. В то же время будет легко отследить попытки дважды использовать один и тот же цифровой токен; можно организовать систему, оповещающую уполномоченные органы о таких попытках непосредственно в момент их совершения. Мы считаем, что выгоды от применения обеспечивающей приватность системы платежей превосходят ее возможные недостатки; этих недостатков практически нет, учитывая дополнительные возможности, которые получают правоохранительные органы, а также механизмы, которые можно ввести в будущем. Не стоит забывать, что злоумышленники действуют во многих областях и множеством различных способов, а предлагаемая нами система не способствует распространению незаконных проявлений.

4.6. Сравнение с альтернативным и подходами

В табл. 1 представлено сравнение основных свойств предлагаемого нами дизайна с несколькими популярными системами ЦВЦБ. Среди таких свойств отметим следующие:

1. *Розничные пользователи могут хранить цифровые активы вне своих счетов*. В большинстве систем предполагается, что цифровые активы всегда находятся у посредников. Напротив, наша система

ISSN 2782-2923

Таблица 1

Сравнение свойств некоторых предлагаемых систем розничных цифровых валют
Table 1. Comparison of features among proposed retail digital currency architectures

	Goodell, Al-Nakib, Tasca R3 [22]	R3 [22]	Sveriges Riksbank [61]	Bank of England [16]	Adrian and Mancini-Griffoli (МВФ) [62]	Bordo and Levin [45]	ConsenSys [63]	Zhang «Синтетическая ЦВЦБ» (МВФ) [14]	Auer and Bohme (БМР) [64]
Ценности можно хранить без счетов / Ine Can hold value outside an account	●	○	○	○	○	○	○	○	○
Система распределенного реестра / DLT system	●	●	○	●	○	○	●	○	○
Нет центрального контроллера транзакций / No central gatekeeper for transactions	●	●	○	●	●	○	●	●	○
Может управляться исключительно частными, независимыми игроками / Can be operated exclusively by private, independent actors	●	●	○	●	●	○	●	●	○
Государство осуществляет выпуск и уничтожение цифровой валюты / State manages issuance and destruction	●	●	●	●	●	○	●	○	●
Розничные пользователи не имеют счетов в центральном банке / Retail users do not hold accounts with the central bank	●	●	●	○	●	○	○	●	●
Истинная приватность (в отличие от защиты данных) / True privacy (in contrast to data protection)	●	○	○	○	○	○	○	○	○
Все транзакции записываются в реестр / All transactions are on-ledger	●	●	●	●	○	●	○	○	●
Все транзакции требуют наличия регулируемого посредника / All transactions require a regulated intermediary	●	●	●	○	●	●	○	●	●
В числе посредников могут быть нефинансовые институты / Intermediaries can include non-financial institutions	●	○	○	○	○	○	●	○	○

наделяет отдельных пользователей возможностью реально контролировать активы, которыми они владеют, и выбирать распорядителя на своих условиях, если это необходимо.

2. *Отсутствие у частных лиц и нефинансовых организаций счетов в центральном банке*. По нашему мнению, требование иметь счет в центральном банке приводит к увеличению затрат и рисков безопасности. Такая структура может привести к тому, что центральный банк будет брать на себя сделки, во многих странах обычно проводимые частными банками, что сведет на нет преимущества от использования цифровых токенов по сравнению со счетами. Группа исследователей под управлением Jesus Fernandez-Villaverde отмечает, что многие разработчики ЦВЦБ, например Bordo и Levin [45], предусматривают передачу посреднических функций от коммерческих банков центральным банкам, позиционируя эту возможность как преимущество ЦВЦБ [60]. Однако в их анализе описывается компромисс между возможностью избежать массовых изъятий средств из банков и оптимальным размещением капитала [60]; при этом

ISSN 2782-2923

недооценивается ключевая роль коммерческих банков по несению рисков. На наш взгляд, эту роль нельзя недооценивать.

3. *Специализированная внутренняя система розничных платежей*. Мы преднамеренно не включили в нашу систему требование поддерживать международные или оптовые платежи. Наша система разработана целенаправленно по требованиям розничных платежей внутри страны, которые, как мы считаем, кардинально отличаются от требований к международным или оптовым платежным системам.

4. *Истинная, проверяемая приватность для розничных пользователей*. Защита данных – не то же самое, что приватность, поэтому наша структура не опирается на доверие к третьим сторонам или на защиту метаданных в их транзакциях. В некоторых системах цифровых валют на основе счетов предлагается использовать «ваучеры анонимности», действующие в течение ограниченного времени [22, 23]. Мы не думаем, что такие подходы будут эффективными – не только из-за рисков, связанных с обеспечением анонимности в течение конкретных временны*х* промежутков, но и из-за атак, которые всегда возможны при передаче средств напрямую с одного регулируемого счета на другой.

5. *Отсутствие новых систем цифровой идентификации*. Наша система не требует никаких специальных систем идентификации, кроме тех, которыми уже пользуются ОДО и частные банки. В частности, она не требует какой-либо инфраструктуры идентификации в масштабах всей системы, а также позволяет отдельным пользователям совершать платежи со своих электронных кошельков, не раскрывая своей личности.

6. *Отсутствие новой операционной инфраструктуры режима реального времени, управляемой центральными уполномоченными органами.* В нашей системе управление может осуществляться исключительно частными, независимыми игроками; никакая отдельная часть инфраструктуры не нуждается в опоре на центрального игрока для своего функционирования. Распределенный реестр позволяет передать ответственность за большинство транзакций в ОДО без участия центрального банка. ОДО несет ответственность за каждую транзакцию, которую записывает в реестр, а технологию распределенного реестра (*DLT*) можно использовать для создания (потенциально) неизменяемой записи, связывающей каждую транзакцию с соответствующим ОДО, которое ее провело. Центральный банк в данном случае не несет ответственность за проведение отдельной транзакции.

5. Рекомендации

Мы считаем, что все ранее предложенные модели ЦВЦБ не отвечают важным критериям, указанным в табл. 1. В частности, мы показали, что у них отсутствует ряд свойств, влияющих на критические характеристики в области создания ценности, а также в управленческой и финансовой сферах. Наше предложение полностью отвечает всем важнейшим требованиям.

Уникальность нашей модели обусловлена следующими свойствами. Во-первых, в ней использована система взаиморасчетов на основе технологии распределенного реестра, которая контролируется государственными органами, но управляется исключительно частными, независимыми игроками. Во-вторых, она направлена на повышение благосостояния и безопасности пользователей через использование *приватности по умолчанию,* при этом не исключая возможности анализа основных рисков, что ценно для государственных органов.

В любом случае очень важно отделять требования регулирования для идентификации («политика») от внутренних протоколов и технологий, обеспечивающих проведение платежей («механизм»). Такое разделение должно быть обязательным требованием для не связанных с депозитарием кошельков. Механизм осуществления розничных электронных платежей через банк-кастодиан делает возможным отслеживание как побочный результат отношений ответственного хранения. Чтобы владельцы денег могли по-настоящему свободно пользоваться ими, они должны иметь средства для использования денег вне отношений ответственного хранения и без риска отслеживания. Если на не связанные с депозитарием кошельки будут наложены требования, существенно ограничивающие такие операции, то это будет означать, что нельзя в полной мере владеть цифровыми деньгами, так как их пользователи будут вынуждены принять ограниченный набор прав. (Данный абзац является также ответом на недавнюю консультацию Агентства по борьбе с финансовыми преступлениями США [3].)

ISSN 2782-2923

6. Выводы

При создании нашей системы мы руководствовались основополагающим принципом: нельзя доверять тому, что нельзя проверить. Мы показали, что возможно создать цифровую платежную систему, сочетающую наиболее характерные свойства наличных денег и контроля регулятивных органов. Мы также показали, как обеспечивающая приватность технология может защитить пользователей от слежения, позволяя сторонам транзакции сохранять анонимность, даже если транзакции не являются пиринговыми и регулирующие органы могут видеть каждую из них. Мы утверждаем, что технология распределенного реестра помогает избежать затрат и рисков, присущих централизованной инфраструктуре под управлением правительства или его контрагентов, при этом позволяя государству удостоверяться, что система функционирует так, как заявлено. Мы пришли к выводу, что возможно и необходимо позволить пользователям хранить свои средства вне системы ответственным хранением («на стороне»), и показали, как внедрить эффективную систему ЦВЦБ, не разрушая существующие отношения пользователей ЦВЦБ с банками и не вводя обязательных централизованных счетов или систем управления идентификацией.

Мы надеемся, что государственные служащие и руководители бизнеса согласятся с нами в том, что обеспечение прав отдельных граждан в контексте электронной коммерции и электронных розничных платежей является чрезвычайно важным, особенно учитывая постоянный рост доли таких систем в розничном секторе экономики. Существующая инфраструктура электронных розничных платежей подвергает пользователей рискам, среди которых можно назвать слежение, дискриминацию и недостаточную автономию. Наше исследование показывает, что можно обеспечить эффективное функционирование специализированной децентрализованной системы розничных платежей внутри страны, что отвечает также и государственных интересам.

Список литературы / References

1. Mancini-Griffoli, T., Peria, M., Agur, I., Ari, A., Kiff, J., Popescu, A., Rochon, C. (November 2018). Casting Light on Central Bank Digital Currency. *IMF Staff Discusion*, *Note SDN/18/08*. https://www.imf.org/~7media/Files/Publications/SDN/2018/SDN1808.ashx (access date: 10.05.2020).

2. Auer, R., Cornelli, G., Frost, J. (3 April 2020). Covid-19, cash, and the future of payments. *BIS Bulletin, 3*. https://www.bis.org/publ/bisbull03.pdf (access date: 04.04.2020).

3. Goodell, G. (7 January 2020). Comment on FR Doc #2020-28437. *Public Submission to the US Financial Crimes Enforcement Network*. https://downloads.regulations.gov/FINCEN-2020-0020-4720/attachment_1.pdf (access date: 08.01.2021).

4. *Access to Cash Review (UK) (*March 2019*)*. Final Report. https://www.accesstocash.org.uk/media/1087/final-report-final-web.pdf (access date: 07.01.2021).

5. Sadeghi, M. Fact Check: No US Law Requires Businesses to Take Cash, But Local Laws May Mandate It (16 September 2020). *USA Today*. https://eu.usatoday.com/story/news/factcheck/2020/09/16/fact-check-cashless-businesses-banned-only-some-local-state-laws/3330804001/ (access date: 07.01.2021).

6. Tisher, D., Evans J., Cross K., Scott R., Oxley I. (2020). *Where to Withdraw? Mapping Access to Cash across the UK*, University of Bristol, Bristol, UK. http://www.bristol.ac.uk/media-library/sites/geography/pfrc/Where%20to%20withdraw%20-%20mapping%20access%20to%20cash%20across%20the%20UK.pdf (access date: 07.01.2021).

7. Armer, P. (1968). Privacy Aspects of the Cashless and Checkless Society. In *Testimony before the US Senate Subcommittee on Administrative Practice and Procedure*, RAND Corporation*: Santa Monica, CA, USA.

8. Armer, P. (1975). Computer Technology and Surveillance. *Comput. People, 24*, 8–11, https://archive.org/stream/bitsavers_computersA_3986915/197509#page/n7/mode/2up (access date: 07.01.2021).

9. Nissenbaum, H. (May 2017). *Deregulating Collection: Must Privacy Give Way to Use Regulation?*. https://doi.org/10.2139/ssrn.3092282 (access date: 29.09.2020).

10. Rychwalska, A., Goodell, G., Roszczynska-Kurasinska, M. (2021). Data management for platform-mediated public services: Challenges and best practices. *Surveill. Soc., 19*, 22–36. https://doi.org/10.24908/ss.v19i1.13986

11. Goodell, G. (2020). Privacy by Design in Value-Exchange Systems. *Discussion Paper*. https://arxiv.org/abs/2006.05892 (access date: 10.06.2020).

12. Goodell, G., Aste, T. (2019). Can Cryptocurrencies Preserve Privacy and Comply with Regulations?. *Front. Blockchain*.

ISSN 2782-2923

https://doi.org/10.3389/fbloc.2019.00004

13. Mersch, Y. (11 May 2020). *Speech at the Consensus 2020 Virtual Conference*. https://www.ecb.europa.eu/press/key/date/2020/html/ecb.sp200511~01209cb324.en.html (access date: 11.05.2020).

14. Zhang, T. (2020). *Keynote Address on Central Bank Digital Currency*. London School of Economics. London. UK. https://www.imf.org/en/News/Articles/2020/03/19/sp031920-deputy-managing-director-tao-zhangs-keynote-address-on-central-bank-digital-currency (access date: 22.04.2020).

15. *Monetary Authority of Singapore, Bank of Canada, and Bank of England. Cross-Border Interbank Payments and Settlements: Emerging Opportunities for Digital Transformation* (November 2018). https://www.mas.gov.sg/-/media/MAS/ProjectUbin/Cross-Border-Interbank-Payments-and-Settlements.pdf (access date: 30.04.2020).

16. Bank of England. Central Bank Digital Currency: Opportunities, Challenges and Design (12 March 2020). *Discussion Paper*. https://www.bankofengland.co.uk/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design-discussion-paper (access date: 16.03.2020).

17. Nakamoto, S. (3 January 2009). *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf (access date: 04.10.2018).

18. Buterin, V. (2013). *Ethereum Whitepaper*. https://ethereum.org/en/whitepaper/ (access date: 08.01.2021).

19. Keister, T., Sanches, D. (2019). Should Central Banks Issue Digital Currency?. *Federal Reserve Bank of Philadelphia Working Papers WP,* 19–26. Philadelphia, PA, USA, pp. 26–28. https://ideas.repec.org/p/fip/fedpwp/19-26.html (access date: 08.01.2021).

20. International Organization for Standardization (ISO) (2020). *Blockchain and Distributed Ledger Technologies – Vocabulary*, 1st ed.; ISO/22739:2020; ISO: Geneva, Switzerland. https://www.iso.org/obp/ui/#iso:std:iso:22739:ed-1:v1:en (access date: 01.12.2020).

21. Chaum, D., Grothoff, C., Moser, T. (January 2021). How to Issue a Central Bank Digital Currency. *Swiss National Bank Working Paper*. https://www.snb.ch/n/mmr/reference/working_paper_2021_03/source/working_paper_2021_03.n.pdf (access date: 25.02.2021).

22. Calle, G., Eidan, D. (April 2020). Central Bank Digital Currency: An Innovation in Payments. *R3 White Paper*. https://www.r3.com/reports/central-bank-digital-currency-an-innovation-in-payments/ (access date: 05.05.2020).

23. dGen. *CBDC: Considerations for the Digital Euro*. https://www.dgen.org/cbdc (access date: 05.05.2020).

24. Agur, I., Ari, A., Dell'Ariccia, G. (2019). How Could Central Bank Digital Currencies be Designed?. *SUERF Policy Note, 129*. https://www.suerf.org/policynotes/9763/how-could-central-bank-digital-currencies-be-designed (access date: 05.05.2020).

25. Lagarde, C. (14 November 2018). *Winds of Change: The Case for New Digital Currency*. Speech to Singapore Fintech Festival as Prepared for Delivery. https://www.imf.org/en/News/Articles/2018/11/13/sp111418-winds-of-change-the-case-for-new-digital-currency (access date: 26.02.2020).

26. Agur, I., Ari, A., Dell'Ariccia, G. (2018). Designing Central Bank Digital Currencies. *IMF Working Paper*. https://www.imf.org/-/media/Files/Publications/WP/2019/wpiea2019252-print-pdf.ashx (access date: 27.04.2020).

27. Benaloh, J. (29 November 2018). What if Responsible Encryption Back-Doors Were Possible?. *Lawfare Blog*. https://www.lawfareblog.com/what-if-responsible-encryption-back-doors-were-possible (access date: 11.12.2020).

28. Courtois, N., Mercer, R. Stealth Address and Key Management Techniques in Blockchain Systems. In *Proceedings of the 3rd International Conference on Information Systems Security and Privacy (ICISSP 2017)*, Porto, Portugal, 19–21 February 2017, pp. 559–566. http://www.scitepress.org/Papers/2017/62700 /62700.pdf (access date: 10.10.2018).

29. International Organization for Standardization (ISO) (2020). *Blockchain and Distributed Ledger Technologies – Privacy and Personally Identifiable Information Protection Considerations* (1st ed.; ISO/TR 23244:2020; ISO). Geneva, Switzerland.

30. Pedersen, T. Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing. In *Proceedings of the Advances in Cryptology (CRYPTO '91)*, Santa Barbara, CA, USA, 11–15 August 1991 (pp. 129–140). https://link.springer.com/content/pdf/10.1007%2F3-540-46766-1_9.pdf (access date: 10.10.2018).

31. van Wirdum, A. (2 June 2016). Confidential Transactions: How Hiding Transaction Amounts Increases Bitcoin Privacy. *Bitcoin Magazine*. https://bitcoinmagazine.com/articles/confidential-transactions-how-hiding-transaction-amounts-increases-bitcoin-privacy-1464892525/ (access date: 10.10. 2018).

32. Rivest, R., Shamir, A., Tauman, Y. (2018). *How to Leak a Secret*. Lecture Notes in Computer Science 2248. Springer, Berlin/Heidelberg, Germany (pp. 552–565). https://link.springer.com/content/pdf/10.1007%2F3-540-45682-1_32.pdf (access date: 10.10.2018).

33. Ben-Sasson, E., Bentov, I., Horesh, Y., Riabzev, M. (2018). *Scalable, Transparent, and Post-Quantum Secure Computational Integrity*, International Association for Cryptologic Research (IACR), Lyon, France. https://eprint.iacr.org/2018/046.pdf (access date: 03.03.2020).

34. Guan, Z., Wan, Z., Yang, Y., Zhou, Y., Huang, B. (2019). *BlockMaze: An Efficient Privacy-Preserving Account-Model*

ISSN 2782-2923

Blockchain Based on zk-SNARKs. Report 2019/1354; International Association for Cryptologic Research (IACR): Lyon, France. https://eprint.iacr.org/2019/1354 (access date: 30.03.2020).

35. Sapling. *Zcash*. https://z.cash/upgrade/sapling/ (access date: 15.04.2020).

36. Ghadafi, E. (2013). Sub-linear Blind Ring Signatures without Random Oracles. In M. Stam (ed.), *Cryptography and Coding, 8308*. IMACC 2013. Lecture Notes in Computer Science. Springer. Berlin/Heidelberg. Germany. https://doi.org/10.1007/978-3-642-45239-0_18 (access date: 25.02.2021).

37. Zimmermann, P. (1991). Why I Wrote PGP. In *PGP User's Guide*. Massachusetts Institute of Technology: Cambridge, MA. USA. https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html (access date: 11.10.2018).

38. Wong, J., Kar, I. (18 July 2016). Everything You Need to Know about the Ethereum 'Hard Fork', *Quartz*. https://qz.com/730004/everything-you-need-to-know-about-the-ethereum-hard-fork/ (access date: 16.07.2020).

39. *Software in the Public Interest*, Inc. Debian Security FAQ. https://www.debian.org/security/faq (access date: 16.07.2020).

40. *U. S. Securities and Exchange Commission. SEC Proposes Improvements to Governance of Market Data Plans*, Press Release (8 January 2020). https://www.sec.gov/news/press-release/2020-5 (access date: 16.07.2020).

41. *United States Securities and Exchange Commission Division of Trading and Markets*. Memorandum to SEC Market Structure Advisory Committee (30 April 2015). http://sec.gov/spotlight/emsac/memo-rule-611-regulation-nms.pdf (access date: 03.11.2020).

42. *Bank for International Settlements. Payment, Clearing and Settlement Systems in the CPSS Countries, 2* (November 2012). Committee on Payment and Settlement Systems "Red Book". https://www.bis.org/cpmi/publ/d105.pdf (access date: 31.05.2020).

43. *Bank for International Settlements. Payment, Clearing and Settlement Systems in the United Kingdom, 2* (November 2012), Committee on Payment and Settlement Systems "Red Book" (pp. 445–446). https://www.bis.org/cpmi/publ/d105_uk.pdf (access date: 16.04.2020).

44. Abelson, H., Anderson, R., Bellovin, S., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., Green, M., Landau, S., Neumann, P. et al. (2015). Keys under doormats: Mandating insecurity by requiring government access to all data and communications. *J. Cybersecur, 1*, 69–79. https://academiccommons.columbia.edu/doi/10.7916/D82N5D59/download (access date: 11.03.2019).

45. Bordo, M. D., Levin, A. T. (2017). *Central Bank Digital Currency and the Future of Monetary Policy*. National Bureau of Economic Research. Cambridge. MA. USA.

46. Castro, M., Liskov, B. (1999). Practical Byzantine Fault Tolerance. In *Proceedings of the Third Symposium on Operating Systems Design and Implementation*, New Orleans, LA, USA, 22–25 February 1999. http://pmg.csail.mit.edu/papers/osdi99.pdf (access date: 12.10.2018).

47. *Ripple. XRP*. https://ripple.com/xrp/ (access date: 03.03.2020).

48. *Visa. Fact Sheet*. https://usa.visa.com/dam/VCOM/download/corporate/media/visanet-technology/aboutvisafactsheet.pdf (access date: 03.03.2020).

49. *Visa. Visa Acceptance for Retailers*. https://web.archive.org/web/20200103093557/https://usa.visa.com/run-your-business/small-business-tools/retail.html (access date: 03.03.2020).

50. Bindseil, U. (January 2020). Tiered CBDC and the Financial System, *European Central Bank Working Paper Series 2351*. https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2351~c8c18bbd60.en.pdf (access date: 21.05.2020).

51. Li, Y., Yang, G., Susilo, W., Yu, Y., Au, M. H., Liu, D. (2021). Traceable Monero: Anonymous Cryptocurrency with Enhanced Accountability, *IEEE Trans. Dependable Secur. Comput, 18*, 679–691.

52. Abelson, H., Anderson, R., Bellovin, S., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., Neumann, P., Rivest, R., Schiller, J. et al. (27 May 1997). *The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption*. https://academiccommons.columbia.edu/doi/10.7916/D8R2176H/download (access date: 11.03.2019).

53. *115th Congress of the United States. H.R. 5823, "Secure Data Act of 2018"*. (15 May 2018). Introduced by Representative Zoe Lofgren [D-CA-19]. https://www.congress.gov/bill/115th-congress/house-bill/5823 (access date: 11.03.2019).

54. Thomson, I. (15 January 2016). French say 'Non, merci' to Encryption Backdoors. *The Register*. https://www.theregister.co.uk/2016/01/15/france_backdoor_law/ (access date: 11.03.2019).

55. Financial Action Task Force (FATF) (2018). *The FATF Recommendations*. Updated February. http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf (access date: 16.09.2018).

56. Goodell, G., Aste, T. (2019). A Decentralised Digital Identity Architecture. *Front. Blockchain, 2*. https://doi.org/10.3389/fbloc.2019.00017

57. Pilkington, M. (2016). Blockchain Technology: Principles and Applications. *Working Paper*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2662660 (access date: 11.05.2020).

58. Siliski, M., Pott, A. (10 April 2018). Blockchain Alternatives: The Right Tool for the Job. Medium. https://medium.com/

ISSN 2782-2923

swlh/blockchain-alternatives-b21184ccc345 (access date: 24.10.2019).

59. Tasca, P., Morini, M. (24–27 February 2017). Managing Risk Under the Blockchain Paradigm, Harvard Business Review China.

60. Fernandez-Villaverde, J., Sanches, D., Schilling, L., Uhlig, H. (June 2020). Central Bank Digital Currency: Central Banking for All?. *Working Paper WP 20–19*. Federal Reserve Bank of Philadelphia. Philadelphia, PA, USA. https://doi.org/10.21799/frbp.wp.2020.19

61. *Technical Solution for the e-Krona Pilot*. (20 February 2020). Sveriges Riksbank. https://www.riksbank.se/en-gb/payments--cash/e-krona/technical-solution-for-the-e-krona-pilot/ (access date: 25.05.2020).

62. Adrian, T., Mancini-Griffoli, T. (July 2019). The Rise of Digital Money. *International Monetary Fund FinTech Note 19/01*. https://www.imf.org/~/media/Files/Publications/FTN063/2019/English/FTNEA2019001.ashx (access date: 21.05.2020).

63. Bouchaud, M., Lyons, T., Olive, M. S., Timsit, K. *Central Banks and the Future of Digital Money***.** https://pages.consensys.net/central-banks-and-the-future-of-digital-money (access date: 26.07.2020).

64. Auer, R., Bohme, R. (2020). The technology of retail central bank digital currency. *BIS Q. Rev.*, 85–100. https://www.bis.org/publ/qtrpdf/r_qt2003j.pdf (access date: 19.05.2020).

65. Goodell, G., Al-Nakib, H. D., Tasca, P. (2021). A Digital Currency Architecture for Privacy and Owner-Custodianship. *Future Internet*, *13*, 130. https://doi.org/10.3390/fi13050130

* Признана нежелательной организацией в РФ с 06.12.2023 / Recognized as an undesirable organization in the Russian Federation as of 06.12.2023.

Краткие биографии авторов

Джеффри Гуделл работает исследователем в Университетском колледже Лондона, специализируясь на социально-технических системах, в частности, цифровых валютах, децентрализованных финансах, электронных рынках. Он является руководителем двух рабочих групп технического комитета ISO в области технологий распределенного реестра и блокчейн, а также консультирует финансовые регулирующие органы, центральные банки и международные промышленные группы. Ранее был партнером и главным специалистом по инвестициям в специализированной компании по управлению активами в Бостоне и партнером в компании Голдман Сакс в Нью-Йорке.

Хазем Денни Аль-Накиб является специалистом по финансовым технологиям и регулированию, генеральный партнер венчурной компании 7BC Venture Capital, старший советник юридической фирмы Farrer & Co, отраслевой партнер Центра блокчейн-технологий Университетского колледжа Лондона. Ранее занимал различные должности в Королевском банке Канады и Бостонской консалтинговой группе.

Паоло Таска – специалист в сфере цифровой экономики, в частности, одноранговых (пиринговых) финансовых систем. Выступал консультантом в области блокчейн-технологий для различных международных организаций, в том числе для Европейского парламента и ООН. Является основателем и исполнительным директором Центра блокчейн-технологий Университетского колледжа Лондона. Ранее работал ведущим экономистом по цифровым валютам и пиринговым финансовым системам в центральном банке Германии во Франкфурте. Является главой нескольких компаний и обладателем патента в области взаимодействия с использованием блокчейн.

Short Biography of Authors

Geoffrey Goodell Geoff Goodell is a researcher at University College London specializing in sociotechnical systems, with a focus on digital currency, decentralised finance, and electronic marketplaces. He is the convenor of two ISO working groups on blockchain and distributed ledger technology, and he advises financial regulators, central banks, and international industry groups. Previously, he was Partner and Chief Investment Officer of a boutique asset management firm in Boston and an associate at Goldman Sachs in New York.

Hazem Danny Al-Nakib Hazem Nakib is a fintech and regulatory technology expert, General Partner at the venture capital firm 7BC Venture Capital, senior advisor at the law firm Farrer & Co and industry associate at the UCL Center for Blockchain Technologies. Previously, Hazem had various roles at the Royal Bank of Canada and Boston Consulting Group.

ISSN 2782-2923

Paolo Tasca is a Digital Economist specialised in P2P financial systems. He has advised different international organizations on blockchain technologies including the EU Parliament and the United Nations. He is the founder and Executive Director of the Center for Blockchain Technologies at University College London (UCL CBT). Previously, he was Lead Economist on digital currencies and P2P financial systems at the German Central Bank, Deutsche Bundesbank in Frankfurt. Paolo Tasca is also a serial entrepreneur and a patent holder on blockchain interoperability.

Вклад авторов

Дж. Гуделл – концепция, методология, написание текста – первоначальный вариант, написание текста – исправление и редактура.

Х. Д. Аль-Накиб – методология, написание текста – первоначальный вариант, написание текста – исправление и редактура.

П. Таска – методология, написание текста – исправление и редактура.

Все авторы прочли и согласились с публикуемым вариантом статьи.

The author's contribution

G. Goodell – conceptualization, methodology, writing – original draft, writing – review & editing.
H. D. Al-Nakib – methodology, writing – original draft, writing – review & editing.
P. Tasca – methodology, writing – review & editing.
All authors have read and agreed to the published version of the manuscript.

Конфликт интересов: авторами не заявлен.

Conflict of Interest: No conflict of interest is declared by the authors.

Дата поступления / Received 09.06.2021
Дата принятия в печать / Accepted 12.07.2021