УДК 004 **DOI: 10.18413/2518-1092-2020-5-3-0-2**

Шевцов М.
Маслова М.А.

ИССЛЕДОВАНИЕ БЕЗОПАСНОСТИ СОВРЕМЕННЫХ СИСТЕМ ЦИФРОВОЙ НАЛИЧНОСТИ

Севастопольский государственный университет, ул. Университетская, д. 33, г. Севастополь, 299053, Россия

e-mail: maxim.sevtov@gmail.com, info@sevsu.ru, machechka-81@mail.ru

Аннотация
С развитием информационных технологий все большую популярность приобретают системы цифровой (электронной) наличности. Перед обычными денежными знаками цифровая наличность обладает рядом преимуществ, и количество преимуществ растет по мере того, как информационные технологии интегрируются в общественную жизнь.
Целью исследования является выделение преимуществ систем цифровой наличности перед обычными денежными знаками; провести классификацию различных видов цифровой наличности; сравнение существующих систем электронной валюты, и выявление уязвимостей современных систем цифровой наличности. Сравнение различных систем проводится по таким критериям, как возможность работы без связи с серверами, разновидности способов подтверждения подлинности, способам защиты от копирования, и т. д. По окончанию исследования, можно будет сделать выводы касаемо готовности мира к массовому переходу на системы цифровой наличности, о преимуществах и недостатках того или иного вида электронной наличности, выделить уязвимости в современных видах электронной наличности, а также сделать прогноз на развитие цифровой наличности в будущем.
Ключевые слова: цифровая наличность; криптовалюта; информационная безопасность; валюта; криптозащита; Bitcoin.

UDC 004

Shevtsov M.
Maslova M.A.

RESEARCH OF THE SECURITY OF MODERN DIGITAL CASH SYSTEMS

Sevastopol state University, 33 Universitetskaya St., Sevastopol, 299053, Russia

e-mail: maxim.sevtov@gmail.com, info@sevsu.ru, machechka-81@mail.ru

Abstract
With the development of information technology, digital (electronic) cash systems are becoming increasingly popular. Digital cash has a number of advantages over conventional currency, and the number of advantages grows as information technology is integrated into public life.
The aim of the study is to highlight the advantages of digital cash systems over conventional banknotes, provide a classification of various types of digital cash, compare existing electronic currency systems, and identify the vulnerabilities of modern digital cash systems. Comparison of various systems is carried out according to such criteria as the ability to work without communication with servers, a variety of authentication methods, copy protection methods, etc.
At the end of the research, it will be possible to draw conclusions regarding the world's readiness for a massive transition to digital cash systems, the advantages and disadvantages of this or that type of electronic cash, highlight vulnerabilities in modern types of electronic cash, and make a forecast for the development of digital cash in the future.
Keywords: digital cash; cryptocurrency; information security; currency; crypto protection, Bitcoin.

ВВЕДЕНИЕ

Несмотря на высокий уровень развития информационных технологий, их все более глубокое внедрение во все области человеческой деятельности, нельзя сделать вывод, что

цифровые деньги вот-вот вытеснят обычную валюту. Этому мешает и длительный опыт работы с привычными всем денежными знаками, так и недоверие к электронной валюте как со стороны обычных людей, так и со стороны государств. Во многих странах Центробанки все ещё очень настороженно относятся к наличию электронных денег. Также, нет определенного правового регулирования цифровой наличности, ибо многие государства все ещё не определились в своем отношении к цифровой валюте.

Немаловажным фактором торможения внедрения электронной наличности является слабые познания в безопасности таких систем. Исследование безопасности таких систем и является целью этого исследования. Дать ответ на вопрос, насколько безопасней использование цифровой наличности, сложней оттого, что история использования цифровой валюты достаточно коротка, и методы её реализации зачастую рознятся от типа рассматриваемой криптовалюты. Тот факт, что методы защиты валюты постоянно совершенствуются и меняются, также затрудняет изучение это вопроса.

Цель исследования: безопасность современных систем цифровой наличности.

Объект исследования: цифровая наличность.

Итогом исследования будет изучение уязвимостей различных систем цифровой наличности, что позволит дать ответ на то, какой из видов цифровой валюты на сегодняшний день наиболее перспективен, а также понять, готовы ли системы цифровой наличности прийти на смену привычным всем денежным знакам [7].

ОСНОВНАЯ ЧАСТЬ

В качестве входных материалов используются преимущества и недостатки обычных денежных знаков, что, в сравнении с цифровой наличностью, даст ответ на вопрос, стоит ли стремится к замене обычной наличности цифровыми деньгами [5].

Также, следует привести классификацию электронной наличности, выделить уязвимости каждой из них, и выполнить их сравнение, по таким вопросам, как: возможность работать в режиме off-line, способы подтверждения личности, способы защиты от копирования. Классификация электронных денег приведена на рисунке 1. [10]

Электронные деньги можно разделить на две категории: те, что построены на базе смарт-карт, и те, что на базе сетей. Так же, их можно разделить на фиатные и нефиатные. Фиатные деньги выражены в государственной валюте. Обращение таких денег происходит по всем тем правилам, что диктуют государства, Центробанки, и т.д. Нефиатные деньги используют свои платежные системы. Они могут быть привязаны к какой-либо валюте, однако, государство не гарантирует их ценность и надежность. Соответственно, и регулирование таких систем со стороны государства отлично от фиатных [7], [8].

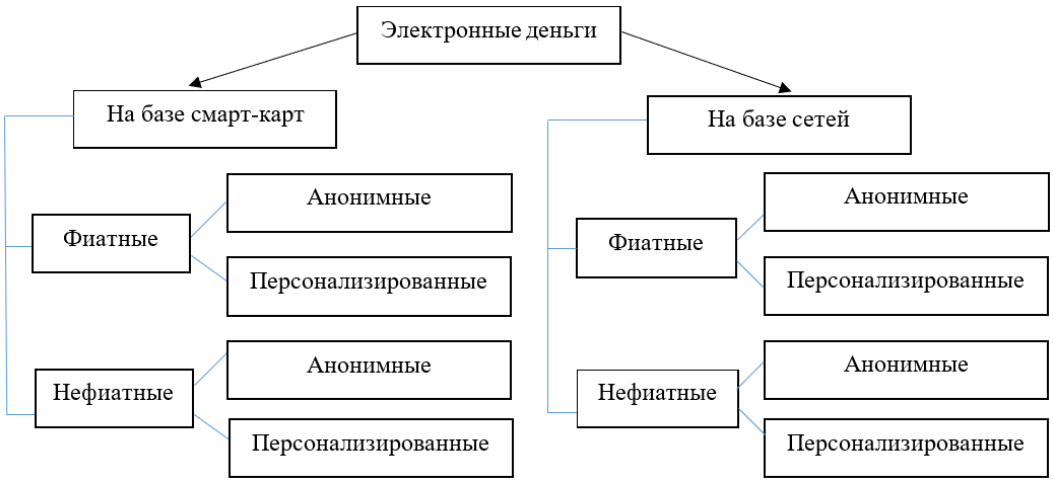

Рис.1. Классификация электронных денег
Fig.1. Classification of electronic money

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ И ИХ ОБСУЖДЕНИЕ

Выполнив сравнение обычных денежных знаков и цифровой наличности, можно сделать вывод, что обычная форма валюты проигрывает цифровой валюте. При использовании обычных денежных знаков отсутствует возможность провести идентификацию личности. Похищенные как материальный носитель, их будет почти невозможно отследить. При использовании персонализированных электронных систем, всегда можно будет узнать, кто произвел платеж. Наличные деньги, как предмет, является разносчиком инфекций, поскольку передается из рук в руки. Эпидемия COVID-19 показала, насколько опасно может быть использование таких носителей. Совершая же платежи по сети, или используя смарт карту, пользователь не контактирует с лишними предметами. Электронные деньги куда проще хранить, передавать на расстояния, а их номинал никак не связан с массой и габаритами хранителя.

Недостатки цифровой наличности во многом связанны с неприятием информационных технологий в мире. Статистика показывает, что в России значительная часть населения не пользуется банковской картой вообще, или же использует ее только для снятия наличных денег. Большинство людей старшего поколения имеют трудности с использованием компьютера, а соответственно, и с использованием цифровой наличности.

Исследование безопасности систем цифровой наличности заключается в выделении уязвимостей отдельных типов такой наличности.

Рассматривая электронные деньги на базе сетей, выделяются фиатные деньги (системы PayPal, M-Pesa), и нефиатные (системы WebMoney, Яндекс.Деньги, криптовалюты на базе Bitcoin). [9, 2] Для электронной наличности на базе сетей свойственны те уязвимости, которыми обладают все базы данных, расположенные в сети. Так, возможна кража данных, используемых для аутентификации – это логин и пароль для доступа к профилю, коды для восстановления профиля и т. д. Для предотвращения этой уязвимости можно использовать двухфакторную аутентификацию, включить уведомление о подтверждении операций, и т д. Но как правило, такие функции привязаны к одному устройству (чаще всего к телефону), и его похищение дает доступ злоумышленнику к кошельку. Имеют место быть и методы социальной инженерии, когда злоумышленник может получить доступ к данным, используя различные способы воздействия на хозяина кошелька [1].

Такие системы также подвержены хакерским атакам. К примеру, одна из последних уязвимостей системы PayPal была связанна с тем, как PayPal хранит токены CSRF и ID сессий в файле JavaScript, из-за чего они становились доступными для злоумышленников посредством XSSI-атак. Хотя для рандомизации имен при каждом запросе использовался обфускатор, все равно имелась возможность предсказать, где находятся токены и извлечь их.

Следует отдельно отметить уязвимости криптовалют, работающих на базе Bitcoin. Поскольку на сегодняшний день Bitcoin, а также работающие на его базе другие криптосистемы (Litecoin, Namecoin и др.) наиболее популярны, и внимание к таким системам более высокое. Bitcoin свойственны системные проблемы, к примеру взлом через бэкап кошелька. Восстановление старого кошелька с паролем восстанавливает текущий кошелек и текущий пароль. Существует Атака Сивиллы, что позволяет хакеру наполнить сеть подконтрольными ему узлами, и остальные пользователи смогут подключиться только к блокам, созданным для мошенничества [4].

Несмотря на анонимность системы, существует возможность проследить историю денежных транзакций. К тому же баланс кошелька находится в открытом доступе, и не каждый пользователь будет на это согласен [3].

Альтернативой электронной наличности на базе сетей будет использование смарт-карт. Это карта, содержащая микропроцессор и операционную систему, управляющую устройством и контролирующую доступ к объектам в его памяти. Кроме того, смарт-карты, как правило, обладают возможностью проводить криптографические вычисления. Не следует путать такое устройство с обычной банковской картой: банковские карты предоставляют доступ к банковскому счету, а на смарт-карте деньги хранятся в виде цифрового эквивалента. Это, в свою очередь,

позволяет проводить операции в режиме off-line. Примерами таких систем служат Visa Cash, Mondex, «Октопус» и другие.

Среди уязвимостей смарт карт, в первую очередь, следует выделить уязвимость криптоалгоритмов смарт-карт, так как они практически полностью доступны. Но, такие уязвимости быстро устраняют. Существует также вероятность дифференциального анализа питания. Оценка осциллограмм потребляемой смарт-картой электроэнергии в момент выполнения криптоалгоритма.

Следует отметить и тот факт, что смарт-карта – это физический носитель, который можно похитить. К примеру, можно получить доступ к электрическим цепям смарт-карты после химического снятия защитных слоев с кристалла. Это позволит провести анализ устройства смарт-карты и подключиться к ней с помощью микроэлектродов. Также, карта уязвима к необычным условиям окружающей среды, среди которых температура, магнитное воздействие и т.д.

В целом, по результатам исследования, делается вывод, что основную проблему перед внедрением электронной наличности играет не её уязвимость, а недоверие к таким системам со стороны общества и государства. Обращаясь к наиболее экономически развитым странам, можно отметить, что оборот наличных денег среди населения падает. Переход на электронную наличность также позволит снизить уровень преступности, и в особенности финансовых преступлений [6, с. 5-6]. В большинстве своем, мировая преступность всегда ведёт свои дела через наличные деньги. Конечно, имеет место использование криптовалют в мировой преступности, но её отследить проще, чем обычную наличность.

Для увеличения оборота цифровых денег, в первую очередь, следует бороться с недоверием к электронной наличности среди населения. Приобщение общества к цифровым технологиям, демонстрация преимуществ электронной наличности, значительно увеличит распространение цифровых денег.

ЗАКЛЮЧЕНИЕ

По результатам исследования, можно сделать вывод, что электронная наличность имеет больше преимуществ, чем недостатков, перед обычными денежными знаками.

Исходя из сравнений различных типов электронной наличности, нельзя сделать однозначный вывод, какой из систем следует отдать предпочтение. При выборе пользователь должен исходить из своих потребностей. Для обеспечения наибольшей безопасности своих средств, следует отдать предпочтение персонализированным фиатным системам, построенным на базе сетей, поскольку такие системы имеют наиболее совершенную систему подтверждения подлинности, надежную систему аутентификации пользователя, и обеспечение надежности курса валюты со стороны Центробанка.

При требовании высокого уровня анонимности следует обращаться к нефиатным анонимным системам криптовалют, особенно к системам, работающих на алгоритме круговой подписи (Bytecoin, Monero).

При требовании возможности работы off-line, предпочтение следует отдавать системам на смарт-картах.

Список литературы

1. Абдеева З.Р. Электронные новации платежных систем посредством банковских карт и электронных денег // Российское предпринимательство. – 2014. – № 24(270). – С. 109-114.
2. Ermakov N.S., Galkina E.A. Global approach to e-money protection and risk diversification // В сборнике: XXXIII International plekhanov readings. – 2020. – С. 19-25.
3. Какаев Д.В., Маслова М.А. Обзор вирусов удаленного доступа для мобильных устройств // Научный результат. Информационные технологии. – 2020. – Т. 5. – № 1. – С. 27-34.
4. Маслова М.А., Рыжая К.Ю. Интернет–мошенничество как угроза информационной безопасности личности // НБИ технологии. – 2019. – Т. 13. – № 2. – С. 25-28.
5. Минусы наличных денег [Электронный ресурс] – Режим доступа: https://benefit.by/page/show/articles/1651 (Дата обращения: 25.07.2020)

6. Миронкина А.Ю. Отказ от наличных денег: достоинства и недостатки // Синергия наук. – 2016. – № 5. − С. 54−60.
7. Строителева Е.В., Мигачев И.Б. Электронные деньги: виды, сущность и перспективы развития // Алтайский институт финансового управления, г. Барнаул, Россия – 2014.
8. Цифровые наличные [Электронный ресурс] – Режим доступа: http://kunegin.com/ref6/ecom/43.htm (Дата обращения: 24.07.2020)
9. Частные электронные деньги [Электронный ресурс] – Режим доступа: https://www.fd.ru/articles/62433-chastnye-elektronnye-dengi (Дата обращения: 25.07.2020)
10. Электронные денежные системы [Электронный ресурс] – Режим доступа: https://sites.google.com/site/elektronnyedeneznyesistemy/ (Дата обращения: 25.07.2020)

References

1. Abdeeva Z.R. Electronic innovations of payment systems via Bank cards and electronic money// Russian entrepreneurship. – 2014. – No. 24(270). – Pp. 109-114.
2. Ermakov N.S., Galkina E.A. Global approach to e-money protection and risk diversification // In: XXXIII International plekhanov readings. – 2020. – Pp. 19-25.
3. Kakaev D.V., Maslova M.A. Review of remote access viruses for mobile devices. // Research result. Information technology. – 2020. – Vol. 5. – No. 1. – Pp. 27-34.
4. Maslova M.A., Ryzhaya K.Yu. Internet-fraud as a threat to personal information security // NBI technologies. – 2019. – Vol. 13. – No. 2. – Pp. 25-28.
5. Cons of cash [Electronic resource] – access Mode: https://benefit.by/page/show/articles/1651 (accessed: 25.07.2020)
6. Mironkina A. Yu. Refusal of cash: advantages and disadvantages // Synergy of Sciences. – 2016. – No. 5. – P. 54-60.
7. Stroiteleva E. V., Migachev I. B. Electronic money: types, essence and prospects of development // Altai Institute of financial management, Barnaul, Russia-2014.
8. Digital cash [Electronic resource] – access Mode: http://kunegin.com/ref6/ecom/43.htm (accessed: 24.07.2020)
9. Private electronic money [Electronic resource] – access Mode: https://www.fd.ru/articles/62433-chastnye-elektronnye-dengi (accessed: 25.07.2020)
10. Electronic money systems [Electronic resource] – access Mode: https://sites.google.com/site/elektronnyedeneznyesistemy/ (accessed 25.07.2020)

Шевцов Максим, студент 4 курса кафедры «Информационная безопасность» Института радиоэлектроники и информационной безопасности
Маслова Мария Александровна, аспирант, старший преподаватель кафедры «Информационная безопасность» Института радиоэлектроники и информационной безопасности

Shevtsov Maxim, 4th year student of the Department «Information security»», Institute of Radioelectronics and Information security
Maslova Maria Alexandrovna, post-graduate student, senior lecturer of the Department «Information security», Institute of Radioelectronics and Information security