11. *Aggarwal K.K., Yogesh Singh, Arvinder Kaur, Ruchika Malhotra.* Empirical Study of Object-Oriented Metrics // Journal of Object Technology. 2006. Vol. 5, no. 8.
12. *Briand L., Daly W., Wust J.* Exploring the Relationships Between Design Measures and Software Quality // Journal of Systems and Software. 2000.
13. *Chidamber S.R, Kemerer C.F.* A Metric Suite for OO Design // IEEE Transactions on Software Engineering, 1994.
14. ISO/IEC 25000:2014 Systems and Software Engineering – Systems and Software Quality Requirements and Evaluation (SQuaRE) – Guide to SquaRE: SO/IEC JTC 1 / SC 7 Software and Systems Engineering, 2014.
15. *Lorenz M., Kidd J.* Object-Oriented Software Metrics: A Practical Guide. Prentice-Hall, 1994.
16. *Mishra D.* New Inheritance Complexity Metrics for Object-Oriented Software Systems: An Evalution with Weyuker's Properties // Computing and Informatics. 2011. Vol. 30.
17. Object-Oriented Software Engineering:Measuring and Controlling the Development Process Fernando Brito e Abreu (INESC/ISEG) Rogério Carapuça (INESC/IST). URL: https://www.researchgate.net/publication/2253619 (date of the application: 11.09.2020).
18. *Ponisio María Laura.* Exploiting Client Usage to Manage Program Modularity: PhD thesis. University of Bern, 2006 (to the CPC metric algorithm).

DOI: 10.25586/RNU.V9187.20.04.P.065 УДК 004.4

С.Р. Набиев, Б.Р. Набиев

СИСТЕМА ВЕРИФИКАЦИИ УДОСТОВЕРЕНИЯ ЛИЧНОСТИ НА ОСНОВЕ ТЕХНОЛОГИИ BLOCKCHAIN

Посвящено вопросу обеспечения безопасности персональных данных с помощью системы верификации, основанной на технологии распределенного регистра. Актуальность соответствующей проблемы обусловлена в первую очередь ростом числа преступлений, связанных с подделкой документов и соответствующей задачей обеспечения безопасности персональных данных, регламентированной рядом основополагающих нормативных правовых актов. Уделяется значительное внимание техническим вопросам созданной системы верификации. Рассмотрен алгоритм, лежащий в основе разработанных приложений для проверки данных с применением технологии распределенного регистра.
Ключевые слова: блокчейн, верификация данных, кибербезопасность, QR-код, хеш-функция.

S.R. Nabiev, B.R. Nabiev

ID VERIFICATION SYSTEM BASED ON BLOCKCHAIN TECHNOLOGY

The purpose of this paper is to go into detail on how to ensure the security of personal data based on a verification system based on distributed registry technology. The relevance of the corresponding problem is primarily due to the increase in the number of crimes related to forgery of documents and the corresponding task of ensuring the security of personal data regulated by several fundamental regulatory legal acts. For example, GDPR provides residents of the European Union with the potential of complete

control over their data and increases the responsibility of companies for violation of security standards. When carrying out verification of identities by traditional methods, a number of problems are very likely to arise, including the illegal collection of personal data and their use in fraudulent transactions, the high quality and complexity of recognizing forged documents, as well as unauthorized changes to records in centralized databases. This paper pays considerable attention to the technical issues of creating an identity verification system following newly accepted privacy and identity regulations. The proposed identity verification system utilizes iOS and Android mobile apps that are connected to the decentralized DB which utilizes distributed registry technology. The created system also permits the ability of the keys pre-syncing which gives an opportunity to the verifier for offline validation of the provided data.
Keywords: blockchain, data verification, cybersecurity, QR code, hash function.

Введение

Распространение и развитие цифровых технологий привелок беспрецедентному росту массивов персональных данных; вместе с тем возросло и число случаев мошенничеств с персональными данными и документами, что наносит значительный вред государственным и общественным организациям, правам и интересам граждан. Получив паспортные или другие персональные данные, мошенники могут использовать данные жертвы для создания подменной личности в целях проведения мошеннических схем; создавать «зеркальные» удостоверения [2]; распоряжаться средствами банковских карт; совершать незаконные действия с недвижимостью; оформлять кредиты в банке и т.д.

Актуальность данной проблемы подчеркивается ростом усилий в области развития нормативных документов, регламентирующих процессы сбора, анализа и передачи персональных данных по всему миру. В данном контексте необходимо отметить, что с мая 2018 г. Европейский союз перешел на обновленные правила обработки персональных данных, представленные в Общем регламенте по защите данных (GDPR – General Data Protection Regulation). Регламент предоставляет резидентам Европейского союза возможность полного контроля над своими персональными данными и повышает ответственность компаний за нарушение норм безопасности. Более того, регламент имеет экстерриториальное действие, поэтому изложенные в данном документе правила применяются и к российским компаниям, обрабатывающим персональные данные резидентов и граждан ЕС. Что касается России, то действующее законодательство в сфере персональных данных в России и в ЕС подобны, требования отражают общие принципы обеспечения прав субъектов, однако степень детализации положений в регламенте ЕС более высокая, чем в законах Российской Федерации [1], что существенно повышает уровень защиты персональных данных.

Технологические основы системы верификации личности

Для демонстрации возможностей применения новых технологий для решения проблемы верификации документов и личности была разработана система верификации удостоверений с применением технологии blockchain (для iOS и Android). Система позволяет проверяемой стороне не предоставлять избыточную информацию, а проверяющей стороне, осуществив верификацию, быть полностью уверенной в подлинности информации; таким образом, снижаются риски для всех акторов данного процесса.

В созданной системе верификации личности для проверки целостности данных применяется SHA256 (используемая в Bitcoin) [11]. В будущем для предотвращения атак

с использованием квантовых компьютеров криптографическая хеш-функция может быть заменена другим алгоритмом (например, Lattice-based cryptography [8]). Для удобства передачи и обработки информации данные записываются в JSON-формате. Далее полный JSON-файл подписывается ключом эллиптической криптографии (стандарт NIST) [7]. Хеш от всего JSON-файла зашифровывается закрытым ключом, что является электронной подписью, которую можно верифицировать открытым ключом. Информация о цифровой подписи хранится в public blockchain с использованием технологии OpenIndex Protocol [10]. Таким образом, метаданные (хеш-подписи документа) хранятся в FLO blockchain [5] и надежно защищены от фальсификации уже внесенных и сохраненных данных.

Далее представлены два примера JSON-файла, которые передаются для подтверждения достоверности данных. В первом примере подтверждается совершеннолетие проверяемого.

Листинг 1. Верификация совершеннолетия

Listing 1. Age of majority verification

{
“Data”:
{
“Base64Image”: “/9jjifewjijflkmkiouhy82y2yg12g…”,
“passed_age_of_majority”: “true”
},
“SHA256SignedWithEC”: “MEUCIEVkdqXB5n7iFjETcb1l5baqpfu0aCvgx+Y5tvCxcP2f
AiEA6mtitlfHLUuzHHGFQOf84zV2okeZ+YNWWnvoygVk+vU=”}

Во втором примере JSON-файл содержит информацию о документе, который выдан государственным органом (паспорт, водительское удостоверение и др.).

Листинг 2. Верификация документа, удостоверяющего личность

Listing 2. Verification of ID

{
“Data”:
{
“Base64Image”: “/9jjifewjijflkmkiouhy82y2yg12g…”,
“DoB”: “01/01/1993”
“document_number”: “78632319484”
“expiary_date”: “01/01/2025”
},
“SHA256SignedWithEC”:
“MEYCIQDHEuct1U39f+TkKmtOi+7hcrcb6Cfb8mQUx76CdIJrMAIhAI0u7QqyjU9RJN91qKhaapsZG+KAUwMW/DEU45JxxXNV”
}

Как можно видеть из примеров, пользователю не нужно передавать избыточную информацию, как это часто происходит, когда для проверки возраста передают паспорт или водительское удостоверение. В примере пользователь передает лишь информацию о том, что он старше 18 лет, и свое верифицированное изображение (которое можно найти в действующих документах, удостоверяющих личность). Каждый пример имеет зна-

чение SHA 256 Signed With EC – хеш-значение объекта Data, зашифрованное закрытым ключом (пара ключей сгенерирована с Elliptic Curve Keygen). Для последующей верификации получатель данных должен синхронизировать открытые ключи, которые были использованы государственным органом или другой организацией, которая занимается созданием удостоверений личностей (данные об открытых ключах хранятся вместе с хешем подписи в открытом блокчейне). Зная открытый ключ (public key), можно расшифровать SHA 256 Signed With EC и получить хеш-значение. Далее, подсчитав хеш объекта Data, нужно сравнить получившийся хеш с хеш-значением из подписи. Если значения совпадают, можно сделать вывод, что данные не изменены, следовательно, полученной информации можно доверять.

При разработке системы верификации, поскольку информация (удостоверение личности) хранится на стороне пользователя, необходимо было решить задачу передачи верифицируемой информации от одного устройства к другому. При этом важно было выбрать метод передачи данных, который бы позволял использовать устройства с различными операционными системами.

В первую очередь была рассмотрена возможность передачи данных по Bluetooth [9] и Wi-Fi [4]. Данные технологии позволяют передавать большие объемы информации с высокой скоростью, но для осуществления передачи данных эти протоколы требуют создания точки доступа между двумя устройствами. Создание подключения между устройствами одной и той же операционной системы не составляет труда. Однако проблема возникает при использовании девайсов с различными операционными системами. На сегодняшний день наиболее распространенными операционными системами для мобильных устройств являются iOS и Android. При попытке передать файл между смартфонами различных операционных систем смартфон должен создать точку доступа и отобразить пароль для подключения к ней, что, в свою очередь, усложняет и замедляет передачу данных и последующую ее верификацию.

Решение задачи было найдено при наблюдении за работой системы сканирования авиабилетов при прохождении контроля при посадке. На сегодняшний день нет необходимости распечатывать билет на самолет, достаточно предоставить QR-код, который содержит всю нужную информацию о пассажире и его полете. Поскольку QR code Version 40 позволяет хранить только 4296 Char значений, изображение должно быть сохранено с минимальными потерями и занимать 2–3 kB. Так как изображение занимает на 30% больше места, когда оно закодировано в Base 64, более компактные методы кодировки могут быть использованы для передачи изображения в виде String. К примеру, одним из самых компактных методов кодировок считается yEnc [12] (что означает «зачем кодировать?»). Этот метод позволяет кодировать битовую информацию в String всего лишь с 4–7%-м увеличением размера памяти. Для дальнейшей компрессии изображения были применены JPEG Lossly Compression (60%) и перевод RGB Bitmap в grayscale Bitmap [3] перед компрессией, что позволило уменьшить размер изображения еще на 15%.

Алгоритм работы системы верификации личности

На рисунке 1 представлено графическое описание алгоритма работы системы верификации личности. На первом этапе уполномоченная организация проверяет информацию пользователя и выдает подписанный электронный документ. На втором этапе упол-

номоченный орган записывает персональные данные в защищенный центр обработки данных. Далее результат хеширования персональных данных пользователя, статуса документа и открытого ключа подписывается закрытым ключом и публикуется в блокчейне (децентрализованном цифровом регистре). На четвертом этапе пользователь получает проверенную фотографию с дополнительной информацией, подписанной уполномоченной организацией. После того, как данные подписаны, приложение генерирует QR-код, который содержит верифицированную информацию о пользователе. Личность, которая владеет этим верифицированным удостоверением, не нуждается в мобильном устройстве или подключении к интернету. Созданный QR-код может быть распечатан на бумаге или пластиковой карте. На пятом этапе для верификации данных по запросу от проверяющего пользователь предоставляет QR-код для проверки. На шестом этапе приложение проверяющего синхронизирует открытые ключи, а также может выполнить дополнительную проверку статуса документа (вызов облегченного клиента доступа, который проверяет статус документа в блокчейне).

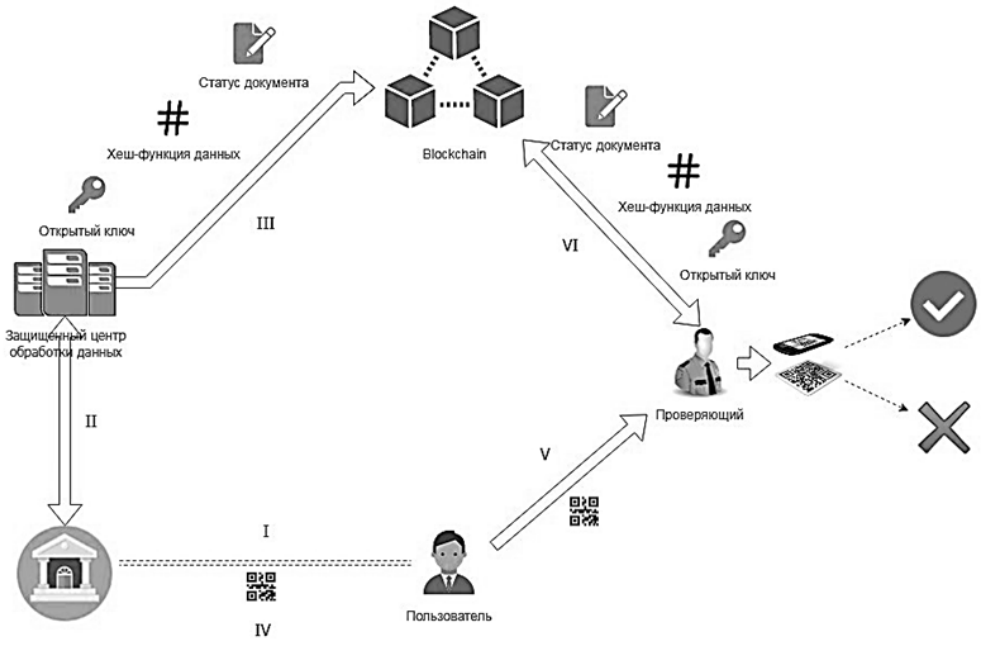

Рис. 1. Графическое представление алгоритма работы системы верификации

В результате работы рассмотренного выше алгоритма системой будет проведена верификация личности, позволяющая исключить возможности кражи данных на уровне «пользователь – проверяющий», несанкционированных изменений записей в централизованной базе данных и прохождения верификации личности с использованием поддельных документов. Интерфейс программы верификации личности на стороне «проверяющего» представлен на рисунке 2. Таким образом, пользователь заверяет свою личность и возраст (старше 19 лет), предоставив верифицированные данные и сохранив свою конфиденциальность.

Рис. 2. Результат верификации личности

Заключение

В статье предложена система верификации личности на базе технологии распределенного регистра, которая позволяет исключить незаконный сбор персональных данных и их использование в мошеннических операциях, а также несанкционированные изменения записей в базе данных. Блокчейн-технологии в разработанной системе играют важную роль в митигации и предотвращении фальсификаций удостоверений личности. В дальнейшем полученная система может быть улучшена путем добавления возможности сохранения хешей подписей в private block chain (к примеру, Hyper Ledger Fabric). Также возможна разработка нового способа передачи информации с улучшенными методами QR-кодировки [6; 13] или автоматического создания закрытой и безопасной точки для передачи информации посредством сканирования только идентификатора (секретного значения), а не всех данных сразу (что позволит хранить изображение лучшего качества).

Литература

1. Защита персональных данных пациентов. URL: http://www.remedium.ru/health/Zashchita_personalnykh_dannykh_patsientov/ (дата обращения: 21.01.2020).
2. «Липа» цветет: продажи поддельных документов выросли почти впятеро. URL: https://iz.ru/880437/vitalii-volovatov/lipa-tcvetet-prodazhi-poddelnykh-dokumentov-vyrosli-pochti-vpiatero (дата обращения: 21.01.2020).
3. *Black A., Amir B.* Choosing Binary or Greyscale Bitmaps: Some Consequences for Users // EP92: Proc. of Electronic Publishing. [S. l.], 1992. P. 247–260.
4. *Chan B.K.-T., Baril A.* System and Method of Ssecure File Sharing Using P2P. U.S. Patent No. 9,756,115. 5 Sep. 2017.
5. FLO Core Integration/Staging Tree. URL: https://github.com/floblockchain/flo (дата обращения: 21.01.2020).

6. *Kieseberg P.* QR Code Security. Proc. of the 8th International Conference on Advances in Mobile Computing and Multimedia. ACM, 2010, pp. 430–435.
7. *Lauter K.* The Advantages of Elliptic Curve Cryptography for Wireless Security. IEEE Wireless Communications 11.1, 2004, pp. 62–67.
8. *Micciancio D.* Lattice-Based Cryptography. Encyclopedia of Cryptography and Security, 2011, pp. 713–715.
9. *Mooring D.J., Pallakoff M.G.* File Sharing Between Devices. U.S. Patent No. 8,260,883. 4 Sep. 2012.
10. Open Index Protocol. URL: https://github.com/oipwg/wiki/wiki/Open-Index-Protocol (дата обращения: 21.01.2020).
11. *Taylor M.B.* The Evolution of Bitcoin Hardware. Computer 50.9, 2017, pp. 58–66. DOI: 10.1109/MC.2017.3571056.
12. *Tjin A., Giammarchi A., Rosenthal N.* Method and Apparatus for Providing Offline Binary Data in a Web Environment. U.S. Patent Application No. 13/281,041.
13. *Vongpradhip S.* Use Multiplexing to Increase Information in QR Code. 8th International Conference on Computer Science & Education. IEEE, 2013. DOI: 10.1109/ICCSE.2013.6553938.

Literatura

1. Zashchita personal'nyh dannyh pacientov. URL: http://www.remedium.ru/health/Zashchita_personalnykh_dannykh_patsientov/ (data obrashcheniya: 21.01.2020).
2. "Lipa" cvetet: prodazhi poddel'nyh dokumentov vyrosli pochti vpyatero. URL: https://iz.ru/880437/vitalii-volovatov/lipa-tcvetet-prodazhi-poddelnykh-dokumentov-vyrosli-pochti-vpiatero (data obrashcheniya: 21.01.2020).
3. *Black A., Amir B.* Choosing Binary or Greyscale Bitmaps: Some Consequences for Users // EP92: Proc. of Electronic Publishing. [S. l.], 1992. P. 247–260.
4. *Chan B.K.-T., Baril A.* System and Method of Ssecure File Sharing Using P2P. U.S. Patent No. 9,756,115. 5 Sep. 2017.
5. FLO Core Integration/Staging Tree. URL: https://github.com/floblockchain/flo (дата обращения: 21.01.2020).
6. *Kieseberg P.* QR Code Security. Proc. of the 8th International Conference on Advances in Mobile Computing and Multimedia. ACM, 2010, pp. 430–435.
7. *Lauter K.* The Advantages of Elliptic Curve Cryptography for Wireless Security. IEEE Wireless Communications 11.1, 2004, pp. 62–67.
8. *Micciancio D.* Lattice-Based Cryptography. Encyclopedia of Cryptography and Security, 2011, pp. 713–715.
9. *Mooring D.J., Pallakoff M.G.* File Sharing Between Devices. U.S. Patent No. 8,260,883. 4 Sep. 2012.
10. Open Index Protocol. URL: https://github.com/oipwg/wiki/wiki/Open-Index-Protocol (дата обращения: 21.01.2020).
11. *Taylor M.B.* The Evolution of Bitcoin Hardware. Computer 50.9, 2017, pp. 58–66. DOI: 10.1109/MC.2017.3571056.
12. *Tjin A., Giammarchi A., Rosenthal N.* Method and Apparatus for Providing Offline Binary Data in a Web Environment. U.S. Patent Application No. 13/281,041.
13. *Vongpradhip S.* Use Multiplexing to Increase Information in QR Code. 8th International Conference on Computer Science & Education. IEEE, 2013. DOI: 10.1109/ICCSE.2013.6553938.