OLYMPUS: A distributed privacy-preserving identity management system

Rafael Torres Moreno*, Jesús García Rodríguez*, Cristina Timón López*, Jorge Bernal Bernabe*, Antonio Skarmeta*
*Department of Information and Communications Engineering
University of Murcia, Spain
{rtorres, jesus.garcia15, mariacristina.timon, jorgebernal, skarmeta}@um.es

***Abstract*—Despite the latest initiatives and research efforts to increase user privacy in digital scenarios, identity-related cybercrimes such as identity theft, wrong identity or user transactions surveillance are growing. In particular, blanket surveillance that might be potentially accomplished by Identity Providers (IdPs) contradicts the data minimization principle laid out in GDPR. Hence, user movements across Service Providers (SPs) might be tracked by malicious IdPs that become a central dominant entity, as well as a single point of failure in terms of privacy and security, putting users at risk when compromised. To cope with this issue, the OLYMPUS H2020 EU project is devising a truly privacy-preserving, yet user-friendly, and distributed identity management system that addresses the data minimization challenge in both online and offline scenarios. Thus, OLYMPUS divides the role of the IdP among various authorities by relying on threshold cryptography, thereby preventing user impersonation and surveillance from malicious or nosy IdPs. This paper overviews the OLYMPUS framework, including requirements considered, the proposed architecture, a series of use cases as well as the privacy analysis from the legal point of view.**

***Keywords*-Privacy; Security; Identity management; Privacy-preserving; Privacy enhancing technologies; Digital identities; IoT**

I. Introduction

Current Identity Management (IdM) systems are struggling to ensure holistic protection for user's rights and freedoms, and in particular satisfy fully the recently in force General Data Protection Regulation in terms of privacy and data minimization. In this sense, privacy concerns have motivated the necessity of revising and improving traditional IdM systems in order to achieve a more privacy-enhanced mechanism for users' identification online. European projects such as H2020 ARIES[1], has recently addressed these privacy issues by endowing users with privacy-preserving tools based on Anonymous Credentials Systems [2][3], increasing user sovereignty, through data minimization and selective disclosure. However, these systems are not distributed enough to prevent surveillance from malicious IdPs.

The solution proposed by OLYMPUS is born in the context of generalized use of delegated IdM services and Single-Sing On Solutions, with the purpose of addressing the principal drawbacks of these mechanisms which suffer from excessive data collection and deficient security measures to ensure data privacy. To this aim, OLYMPUS novel cryptographic approach allows to distribute, from a technical point of view, the task of a single Identity Provider (IdP) among several IdPs, increasing security while, at the same time, guaranteeing user-friendliness and interoperability with existing IdM technologies. In this sense, OLYMPUS distributed architecture hampers multiple forms of identity-related crime, which combined with proactive security mechanisms, offers a good solution to avoid the disastrous effects consequence of the common late detection of security breaches compromising users' identity.

Furthermore, delegated IdM favours surveillance practices positioning the IdP as an intermediary of those movements which take place online. Nevertheless, this position cannot justify these practices, as there exist technical and legal remedies to prevent the same. Indeed, OLYMPUS constitutes a great example of these technical solutions foreseeing the IdP "obliviousness", whereby IdP will be incapable of tracking user behaviour, limiting the data disclosure within an authentication process to a subject that had not been considered until the moment and restraining surveillance practices by design. This is essential in an era characterized by phenomena such as the Big Data merged with techniques of data analysis and search of patterns which even allow as to talk about a phenomenon of "data capitalization".

IdM systems are in constant evolution, so it cannot be claimed that we are in presence of a definitive model or system. This is particularly important because even if self-sovereign identity presents promising prospects, it also presents some drawbacks, hence the possibility of introducing innovations to delegated IdM systems, increasing their security as well as their privacy must be considered. This is the idea we pretend to present in the following sections by describing, in a summarized way, the technical architecture of a new approach to delegated IdM services, its impact in terms of privacy, as well as its possible deployment in two use cases. Thus, this paper aims to offer a multidisciplinary approach with some technical and legal ground to the technology proposed by OLYMPUS project in the framework of EU Horizon 2020 Program for the purpose of constructing a strong and privacy-preserving digital identity.

The rest of this paper is structured as follows. Section II introduces the approach provided by OLYMPUS and the proposed architecture as well as its main components and two proposed use cases. Section III evaluates the impact in terms of privacy. Finally, Section IV concludes the paper with obtained conclusions.

II. The OLYMPUS approach

The approach provided by OLYMPUS evolves from federated identity systems, eliminating the IdP as the single point of failure. The idea behind this is to prevent IdP from being able to track their users through his access to Service Providers (SPs).

To achieve this, advanced cryptographic methods are used to distribute work among different IdPs where none of them need to be totally reliable while maintaining the system's integrity guarantees. Only by compromising all the IdPs can an attacker put the system at risk.

The set of IdPs that work collaboratively is called a Virtual Identity Provider (vIdP). This vIdP addresses all the tasks that were previously performed by a single IdP.

A. *Privacy-preserving Requirements*

With the above vision, OLYMPUS addresses different requirements for a truly oblivious and privacy-preserving identity management solution.

Distributing the role of the IdP enables stronger security requirements. In OLYMPUS, any group of IdPs, whether they are malicious or corrupted, which does not include all IdPs that conform the vIdP cannot issue a token. That is, unless all OLYMPUS IdPs are controlled it is impossible to impersonate a user. What is more, it is required that the compromise of fewer than all IdPs and the data stored for user authentication is not enough to perform offline attacks on user's passwords.

In terms of privacy, three main requirements are defined, which contrast with currently used federated systems. Firstly, OLYMPUS solution must enable data minimization, where tokens presented to service providers contain only the strictly necessary information to access a resource or utility. Secondly, tokens generated with OLYMPUS must be *unlinkable* in the sense that it is not possible to determine if two different tokens were issued for the same user or not (unless the user chose to reveal that in the content of the token). This means that coalitions of service providers cannot successfully track user's activity nor construct detailed profiles of specific users by sharing information about them. Lastly, OLYMPUS must avoid *traceability* from the IdPs. That is, the IdPs will know that a user is performing an authentication process, but they will not learn which service provider the user is contacting.

There are also requirements that involve the ease of implementation and use of the OLYMPUS solution. It must minimize trust requirements in user devices, and it should not require any specific software or hardware environments at the client side. This could lead to a somewhat insecure use of authentication tokens, so they should be short lived to minimize risks. In addition, convenience for the verifier (usually a service provider) is also considered, so OLYMPUS solution must be easily integrated with existing IdM technologies, so it can be adopted with no or minimal changes.
In that sense, the solution will be required to be integrable with existing standards. OLYMPUS will support issuance of distributed tokens that will have to conform to the format defined in OpenID Connect [4], an instantiation of the standard OAuth [5]. On another note, attribute based credentials will also be supported. In this case, the generated tokens will adhere to the recently developed W3C Verifiable Credentials [6] specification.

B. *Olympus Architecture*

To address the requirements presented in II-A, OLYMPUS proposes an architecture (Figure 1) that divides the way of operating into two main processes. Firstly, authenticating the user and secondly, issuing tokens or credentials in a distributed manner depending on the scenario.

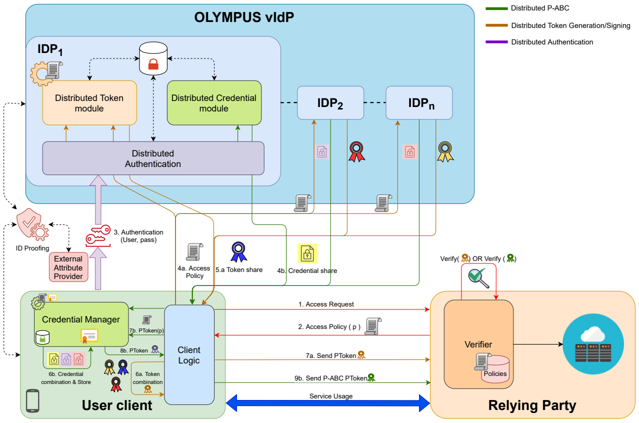

Figure 1. OLYMPUS architecture

For user authentication, OLYMPUS proposes a modular design that allows the use of different methods. However, the development of the project is focused on the authentication through user and password.

Since one of the objectives is to reduce the trust requirements in the users' devices, the classic user and password method is desirable because it does not need any kind of secure storage or other kind of trust systems. In addition, this also increases the usability for the users since they only need to remember a single password that is protected with distributed cryptography techniques.

OLYMPUS architecture supports two different approaches to deal with the service access requests. On the one hand, in the *distributed token approach* where the user client sends the specific access policy to the IdPs. Each IdP performs a distributed threshold-based signature using PESTO[7] cryptography which, in turn, is based on PASTA[8]. Once the client receives the set of signed token fragments from the

IdPs, a composition step takes place and, as result, a one-time access token is generated. Then, the client automatically presents this standardized access signed token to the Relying Party who is the Service Provider (SP). This provider is asking for some kind of authentication from the user to grant access to his service and deposits its trust in the OLYMPUS infrastructure.

On the other hand, OLYMPUS adds a *distributed P-ABC credential approach*. These approach provides support for privacy attributed based credentials (p-ABC) in a distributed way based on PS signatures [9]. The client receives from each IdP a credential fragment. With these fragments, the client will be able to recombine them into a complete p-ACB credential and store it locally in a secure way (e.g. mobile wallet).The credential enables the user to generate privacy-preserving crypto-tokens to be presented to the relying party and in this case, the credential can be used several times to derive unlinkable tokens reducing the need of being online to interact with the IdP to get a new token (as in the first approach). This approach allows working with OLYMPUS in face-to-face scenarios where the verifier relying party can be accessible by the user through short-range wireless communications (e.g. Bluetooth, NFC, 802.11p).

The architecture describes a series of roles and modules.

Virtual Identity Provider (vIdP). This is the main role of the proposed architecture. It is composed of multiple IdPs that do not need to be totally trusted. In addition, each of the IdPs implement a set of modules that supports different functionalities (1) *distributed authentication* and (2) *issuance*. The issuance process, in particular, can be performed by two different methods (1) *distributed tokens* and (2) *distributed credentials*.

Distributed authentication: In a nutshell, it is responsible for checking the username and password provided by the user using cryptographic methods based on secret distribution protocols [10].

Issuance process: It is the process by which you obtain tokens or ABC credentials to work with. There are two modules that support each case.

1) *Distributed token module*. It is in charge of the generation of fragments (token shares). Each IdP that forms the vIdP generates a token share based on a given access policy. When all these fragments are received by the client, he is able to combine them into an access token that can be used to access a service offered by a relying party.
2) *Distributed credential module*. This module supports the generation of ABC credentials in a distributed way. As it happens in the generation of distributed tokens, each IdP generates a fragment (credential share), that the client is able to recompose. Unlike the previous case, this approach results in a full ABC credential with all user attributes and is not tied to a particular access policy. Furthermore, it can be reused by the client.

User client defines another core part in the OLYMPUS architecture. Its first function is to send username and password to the vIdP to start the distributed authentication process. Then, it supports distributed token management directly included in the client logic module or distributed p-ABC mechanisms with the credential manager module.

Client logic: works with distributed token technology, taking care of token recomposition and presentation to the corresponding service. This module delegates the management of credentials to the credential manager module.

Credential manager module: . It supports distributed p-ABC credential management. This module is able to recompose the credential received from the vIdP and then store it locally for later use. When the client wants to use the stored credential, the access policy is communicated to the credential management module, generating an access token that can be presented to the relying party service.

1) Relying party (RP): It is an entity that relies on the OLYMPUS infrastructure and generates access policies that must be enforced by the clients in order to access its services. Moreover, users must give their consent to disclose the corresponding attributes. The RP plays the role of **Verifier**, so that it needs to validate the signed access tokens presented by the user. Thus, two main components are involved.

Verifier module: . It is in charge of validating and verifying the access tokens submitted. This verification process includes checking that the requirements of the access policies are met. The verifier can incorporate any of the methods introduced by OLYMPUS, i.e. verify distributed tokens or verify tokens derived from p-ABC credentials.

Policy DB: It contains a set of policies defined by a service provider that define the specific attributes required to make use of a given service as well as the format or predicates to be met.

Finally, OLYMPUS foresees that users can obtain attributes from external sources by using *external attribute providers*. This attribute provision can also be preceded by a *proof of identity* (e.g. for bank details). In this sense, the user would be able to add these external attributes to his profile in OLYMPUS with the specific cryptographic signatures that enables the validation of the identity if needed.

C. Olympus validation through Use cases

To test and validate the viability of the proposed architecture, as well as the technical deployment of the OLYMPUS solution, two specific use cases have been considered. Both of them illustrate how OLYMPUS solution can be applied to enhance user's privacy and his control over his data in situations where a digital verification of his identity or his attributes is needed.

Credit File scenario: The first use case introduces OLYMPUS in the process of establishing a relationship with a financial entity. Currently, the financial entity would use the information contained in a financial report of the user obtained from an external provider (in this case, Credit File). However, this kind of financial report contains more information than what is actually needed to evaluate a proposal, for example the user's identity. This is where the OLYMPUS solution can help. Instead of using the financial report directly, it becomes a source of information that can be used to generate tokens that ensure minimal disclosure and are the target for evaluation of the proposition. That way, the financial entity only has to manage the minimum user data necessary to accept or reject a proposal. This enhances user privacy and makes it easier for the financial entity to adhere to GDPR, as the amount of sensitive data treated is greatly reduced. If the offer is accepted, the user can then reveal his identity (and other financial information if necessary) to start the contractual relationship.

Mobile Driving License: The second use case focuses on improving the process of user verification using an electronic identifier, the Mobile Driving License (mDL), which is being finalized as standard ISO 18013 (Driver's License) part 5 [11]. In particular, it considers verification of some user attributes to access a restricted good, most commonly that the user's age is greater than some value (e.g. 18). Here, the mDL would have the same role as a physical ID card in a usual face to face verification. However, this would lead to the disclosure of more information than necessary, such as full name or exact date of birth. Again, OLYMPUS solution can help to preserve user privacy providing the tools to perform user verification consisting exclusively of the relevant attributes. In addition, using distributed credentials as presented in the previous section allows the possibility of doing the verification *offline*, where user and relying party communicate using some short range technology (like Bluetooth or NFC) and do not need Internet connection.

III. OLYMPUS IMPACT IN TERMS OF PRIVACY BY DESIGN

In the context of widespread use of delegated IdM services and the emergence of social awareness about the importance of data protection in the guarantee of the basis of a democratic society and individual's Fundamental Rights and Freedoms, OLYMPUS has introduced some major innovations which have a significant impact in terms of privacy. Indeed, increasing surveillance practices poorly challenged until the moment has arisen some of the problems consequence of the privileged position acquired by the IdPs controlling user's movements online. In addition, centralized (or at least, non-distributed) architectures have shown serious drawbacks preventing user impersonation in the fight against identity theft. OLYMPUS circumvents these drawbacks by using the architecture explained above, offering the user a more privacy-enhanced solution for his authentication processes.

A. Towards oblivious identity management in the context of the surveillance society

One of the central innovations introduced by OLYMPUS is its ability to "hide" user's activity before the IdP, which has important consequences regarding generalised practices of surveillance by the part of public and private actors. In this sense, individual's intellectual privacy is substantially curtailed affecting the basis of a democratic and free society as recent examples of microtargeting for political purposes have made visible. Moreover, a situation of power imbalance is created between the subject who "watches" and the one who "is watched", resulting in unlawful practices such as extortion or discrimination[12], or at least of questionable ethic as is the case of consumers persuasion in AdTech. OLYMPUS stands as a technology able to put end to these surveillance practices thanks to its ability to "hide" user's activity before the IdP, hence removing it from its privileged controlling position. Besides avoiding the effects aforementioned, an "oblivious IdP" will also enable GDPR compliance, whose data minimization principle results contrary itself to the concept of surveillance, and it will be in line with European recent rulings rejecting all forms of mass and blanket surveillance (e.g. Digital Rights)[13].Furthermore, it will ensure the content of the right to data protection in European Law, which means more than the possibility of the individual to avoid or prevent external menaces, but it also involves a faculty of the individual to control his own information[14]; control which is lost after countless data transfers which take place within these practices.

Although we can distinguish different types of surveillance by the part of public and private actors, they are not easy to separate in practice as they tend to use the same technologies or agree on some forms of partnerships[15]. This highlights the importance of privacy by design, and the development of a technology respectful itself with data protection regulation requirements. Hence, if we apply data minimization principle to IdM services, the data disclosed to the SPs must be strictly limited to the necessary to provide the services. This also stands out the lack of need that the IdP has knowledge of the destination thereof, restraining by design surveillance practices that usually take place in these IdPs who act like a window for online movements.

B. Improving security, increasing privacy

OLYMPUS other major innovation relates to its distributed architecture designed for the prevention of attacks aimed to impersonate the user. Identity related cybercrime represents one of the most common forms of cybercrime and it involves a substantial infringement of individual's right to privacy apart from additional criminal matters[16]. In this sense, attackers take advantage of centralized architectures to impersonate users in those services connected with the IdP.

Olympus hampers those cyberattacks aiming to steal individual's identity thanks to its distributed architecture described in the previous sections and mechanisms such as key-resharing, requiring the intruder a control over the whole architecture (i.e. all the IdPs) in a limited time to succeed in his attack. In this sense, regarding token identity theft, OLYMPUS requires for the token issuance the collaboration of all the IdPs which conform the vIdP, demanding the attacker to have the control over all the structure, as user's password (necessary for the token issuance) appears disaggregated through thereof. In addition, against traditional identity theft attacks (i.e. those relating to discovery of passwords), OLYMPUS also includes important safeguards. Indeed, safeguards such as key-resharing mechanism allowing password redistribution pose different scenarios before the attacker, thus in the event he successfully compromise one of the IdPs, the "segment" of password obtained will just remain valid for a short period of time before redistributing and becoming all the IdPs honest again.

Consequently, OLYMPUS offers notorious improvements before attacks against the IdP architecture, minimising risks and preventing the ability of the attacker to impersonate users in those services connected with the IdP. This innovative architecture, combined with the rest of the components of OLYMPUS, prevents in a successfully way many of the attacks against software architecture (e.g. a man-in-the-middle-attack).Therefore, although the user remains the critical point of attack, through practices such as phishing, we can conclude that OLYMPUS offers significant improvements in terms of privacy by design

C. OLYMPUS use cases: a user's centric approach in delegated IdM

OLYMPUS use cases described above also present consequences in terms of privacy. It is particularly interesting the new approach given to a delegated IdM system, in which even if the role of the IdP is maintained, user's power of decision, and therefore of control over his data is increased. This is particularly clear in mDL use case which allows the user to prove any of the data contained in his mDL without the necessity of storing separated previous credentials for thereof or to disclose all the data contained in the same.

On the other hand, data minimisation principle is enhanced in a different way regarding Credit File scenario by the possibility of creating an anonymized credit file to present before the financial entities in order to request any of its services. Although it could seem artificial,in many cases it is not necessary to know the real identity of an individual for a service provision, or at least, not in a first moment where the analysis is just limited to confirm suitability.

Consequently, both use cases empower the user in the decision of using his data, at the same time this prevents profiling activities which normally result in discriminatory practices. Nevertheless, the essence of these use cases could be applied to different scenarios, offering delegated identity management systems a new possibility to rebuild themselves in a more privacy-respectful way as an alternative to the self-sovereign identity approach.

IV. Conclusions

This paper has presented OLYMPUS as an approach towards a decentralised and privacy-preserving digital identity management system. Introducing the proposed architecture with features and key capabilities needed to achieve truly privacy-preserving Identity Management solutions, including unlikability across services provides and identity providers, user impersonation protection, selective and minimal disclosure of private personal information. Along with the presented architecture, two use cases have been also introduced that will be used to evaluate the capabilities of the framework.

Furthermore, as we previously stated in the introduction, IdM services are dynamic and they evolve according to two main factors: user-friendliness and privacy. During the last years the purpose of achieving a user-friendly solution in the context of Internet of Things (IoT), has overshadowed in some way the privacy requirement. That development is not too surprising if we bear in mind that technology is always a step forward of law. Nevertheless, this tendency has definitely change worldwide but especially in Europe. From the legal perspective, the entry into force of the GDPR and the emerging regulation in the area have been a step forward. In addition, from a technical point of view, the irruption of technologies such as Blockchain (DLT scenarios), where privacy protection takes on other dimensions, has made privacy-based solutions necessary. In this sense, OLYMPUS represents an example of IdM systems evolution according to this tendency, focused on a privacy enhancement, at the time it keeps necessary concerns in terms of ease of use and interoperability.

Current legal and technical scenarios open the possibility that technologies developed in OLYMPUS have application in DLT scenarios [17]. For example, adapting the p-ABC approach to generate non-interactive crypto-proofs for blockchain achieving privacy-preserving data provenance in distributed ledgers.

In any case, this dynamic scenario requires multiple approaches analysing IdM systems main advantages as well as principal deficiencies, testing their suitability in different contexts and counting on the collaborative work of professionals of different areas. Indeed, that is the idea proposed in OLYMPUS as an attempt of redevelopment of delegated authentication models, which result consistent with the current model of online service provision. In short, IdM services have encountered the necessity of readapting to social and human values because, as François Rabelais once said: “science without conscience is but the ruin of the soul”.

Acknowledgment

The project leading to this application has received funding from the European Union’s Horizon 2020 research and innovation program under grant agreement No 786725 (OLYMPUS project).

References

[1] J. B. Bernabe, M. David, R. T. Moreno, J. P. Cordero, S. Bahloul, and A. Skarmeta, “Aries: Evaluation of a reliable and privacy-preserving european identity management framework,” *Future Generation Computer Systems*, vol. 102, pp. 409–425, 2020.

[2] J. Camenisch and E. Van Herreweghen, “Design and implementation of the idemix anonymous credential system,” in *Proceedings of the 9th ACM conference on Computer and communications security*, pp. 21–30, ACM, 2002.

[3] K. Rannenberg, J. Camenisch, and A. Sabouri, “Attribute-based credentials for trust,” *Identity in the Information Society, Springer*, 2015.

[4] D. Recordon and D. Reed, “Openid 2.0: a platform for user-centric identity management,” in *Proceedings of the second ACM workshop on Digital identity management*, pp. 11–16, ACM, 2006.

[5] D. Hardt, “The oauth 2.0 authorization framework,” tech. rep., 2012.

[6] D. Longley, M. Sporny, B. Zundel, D. Burnett, and G. Noble, “Verifiable credentials data model 1.0,” W3C recommendation, W3C, Nov. 2019. https://www.w3.org/TR/2019/REC-vc-data-model-20191119/.

[7] C. Baum, T. K. Frederiksen, J. Hesse, A. Lehmann, and A. Yanai, “Pesto: Proactively secure distributed single sign-on, or how to trust a hacked server.” Cryptology ePrint Archive, Report 2019/1470, 2019. https://eprint.iacr.org/2019/1470.

[8] S. Agrawal, P. Miao, P. Mohassel, and P. Mukherjee, “PASTA: password-based threshold authentication,” in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS 2018, Toronto, ON, Canada, October 15-19, 2018*, pp. 2042–2059, 2018.

[9] J. Camenisch, M. Drijvers, A. Lehmann, G. Neven, and P. Towa, “Short threshold dynamic group signatures.” Cryptology ePrint Archive, Report 2020/016, 2020. https://eprint.iacr.org/2020/016.

[10] M. Stadler, “Publicly verifiable secret sharing,” in *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 190–199, Springer, 1996.

[11] ISO/IEC CD 18013-5:2019(E), “Personal Identification – ISO Compliant Driving Licence – Part 5: Mobile Driving Licence (mDL) application,” Committee Draft Standard, International Organization for Standardization, oct 2019.

[12] N. M. Richards, “The dangers of surveillance,” *Harv. L. Rev.*, vol. 126, p. 1934, 2012.

[13] V. Mitsilegas, “Surveillance and digital privacy in the transatlantic war on terror: the case for a global privacy regime,” *Colum. Hum. Rts. L. Rev.*, vol. 47, p. 1, 2015.

[14] J. Martínez de Pisón, “Vida privada sin intimidad. una aproximación a los efectos de las intromisiones tecnológicas en el ámbito íntimo,” 2017.

[15] M. Tzanou, “The eu as an emerging surveillance society: the function creep case study and challenges to privacy and data protection,” *Vienna Online J. on Int’l Const. L.*, vol. 4, p. 407, 2010.

[16] C. Sullivan, “Is identity theft really theft?,” *International Review of Law, Computers & Technology*, vol. 23, no. 1-2, pp. 77–87, 2009.

[17] J. B. Bernabe, J. L. Canovas, J. L. Hernandez-Ramos, R. T. Moreno, and A. Skarmeta, “Privacy-preserving solutions for blockchain: review and challenges,” *IEEE Access*, vol. 7, pp. 164908–164940, 2019.