

Privacy-preserving and reward-based mechanisms of proof of engagement

Matteo Marco Montanari and Alessandro Aldini

University of Urbino Carlo Bo, Italy

`m.montanari41@campus.uniurb.it, alessandro.aldini@uniurb.it`

Abstract. Proof-of-Attendance (PoA) mechanisms are typically employed to demonstrate a specific user’s participation in an event, whether virtual or in-person. The goal of this study is to extend such mechanisms to broader contexts where the user wishes to digitally demonstrate her involvement in a specific activity (Proof-of-Engagement, PoE). This work explores different solutions, including DLTs as well as established technologies based on centralized systems. The main aspects we consider include the level of privacy guaranteed to users, the scope of PoA/PoE (both temporal and spatial), the transferability of the proof, and the integration with incentive mechanisms.

Keywords: Proof of attendance · Engagement · Incentive mechanisms · Privacy-preserving identification

1 Introduction

The increasing interest in digitizing human processes and interactions has led to the development of new ways to certify the involvement of users in events, in both virtual and physical contexts [15,12,14,26,13]. Digital certificates of attendance are commonly provided in academic conferences, cultural events, and business training courses. These digital proofs of attendance (PoA) serve as verifiable, reliable, and potentially tamper-resistant evidence that a user has participated in the event. They can be used to grant access to exclusive content or improve traceability and efficiency in human resource management.

The implementation of these mechanisms can be based on innovative technologies, such as Distributed Ledger Technologies (DLT) [7,2,8] and Non-Fungible Tokens (NFT) [28], or traditional centralized architectures. In any case, key features to consider include the level of privacy offered to users, the possible transferability of the evidence, its spatial and temporal validity, and the integration with rewarding and incentive mechanisms.

Extending the concept of PoA, in this paper, we introduce the Proof of Engagement (PoE), the purpose of which is to digitally certify a user’s involvement in any activity. PoA and, more in general, PoE find application in a variety of scenarios, from educational systems to gamification platforms, from social inclusion initiatives to more complex contexts related to the digital economy [22,17,23,14].

Example 1. As motivating examples, consider the two following scenarios. Firstly, user Alice enrolls in a Master’s course in Digital Innovation for Cultural Heritage at the Alan Smithee Institute of Higher Education. In addition to issuing a paper certificate, the Institute generates a digital badge detailing the skills Alice has acquired, which she attaches to her CV to increase her chances of accessing job opportunities. At the same time, the tourism board in Alice’s country decides to offer all graduates of any higher education institute a one-time voucher, which can be used for privileged admission to exhibitions and events. Secondly, during a vacation in Smallville, user Bob is invited by the local tourism office to evaluate the tourism services being offered and point out any gaps and areas for improvement. At the end of the vacation, for this service, Bob receives an NFT certifying him as *friend of Smallville*, which Bob collects along with similar NFTs from other places. At the same time, he receives an anonymous voucher that grants him a hotel discount for the next visit to Smallville.

The first contribution of this paper is the design of a privacy-aware system enabling PoE generation and management. As an additional contribution, we integrate the PoE with an incentive-based anonymized mechanism providing rewards, thus offering a general-purpose framework for various scenarios, like those described in Example 1. The proposed, integrated framework decouples the PoE generation and the reward management in order to ensure a high degree of flexibility from the perspective of usability and privacy. From the technical standpoint, we show how to deploy the proposed system with both centralized and distributed solutions.

The rest of the paper is organized as follows. In Section 2, we briefly discuss the state of the art about Proof of Attendance and incentive mechanisms. In Section 3, we describe the proposed PoE architecture by proposing both a centralized and a distributed architecture. In Section 4, we focus on the applicability of our framework to real-world case studies and we comment on a prototype implementation of the PoE management system. In Section 5, some conclusions terminate the paper.

2 Background and related work

The state of the art in PoA relies on technologies such as NFTs created and distributed through smart contracts on a blockchain. One example is given by the Proof of Attendance Protocol (POAP) [24], which is a proprietary technology providing a distributed application that leverages an Ethereum sidechain called Gnosis. POAP NFTs are managed via web/mobile interfaces and are represented by ERC-721 tokens, including metadata (event, date, time, and location) and an image associated with the event. The claiming process employs a QR code or a direct link. Each NFT is uniquely identified, transferable, and managed through the POAP wallet. NFT POAPs have various real-world use cases in the setting of PoA, and they are often used as passes for events, proofs of membership or ownership, event souvenirs and collectibles, digital trophies for achieving milestones [10] (sometimes they are even the subject of real trades).

With a similar purpose, Vitalik Buterin, founder of Ethereum, introduced the concept of soulbound token (SBT) [20], which is a non-transferable NFT associated with a digital identity and representing self-generated certificates.

The Worth One Minute (WOM) platform [6] is a centralized system that recognizes social value through the awarding of anonymous digital vouchers with no monetary value, which can be obtained by participating in specific activities considered of social value. Merchants, institutions, and retailers can decide to apply discounts and promotions to holders of these vouchers, thus contributing to the recognition and enhancement of citizens' social contributions.

The Open Badges technology [1] is an open standard defined by Mozilla Foundation and, nowadays, maintained by the international e-learning consortium 1EdTech. The objective of the project is to facilitate the digital certification of competencies, skills, knowledge, and experience within academic and professional domains. Open Badges aim to have the same legal value as any paper certificate issued by the organizations participating in the consortium. Formally, an open badge is a digital image including JSON metadata and is uniquely linked to information about the recipient, the badge purpose, and details about its acquisition and temporal validity. More recently, Blockcerts [3] has been proposed as an open standard based on Open Badge 2.0 for the certificate format and on the blockchain technology for storage and management.

3 System Architecture

Our PoE framework can be deployed on two different architectures, depending on whether the PoE is managed by a central authority or via a distributed ledger technology. In the following, we describe these two different architectures.

3.1 Centralized PoE

The centralized solution to the PoE problem is based on a lightweight handshake that allows a possibly uncertified client to interact with a certified server to transfer data whose ownership can be proven by the client at any time in the future and to any interested third party. Such a data transfer can be either server-client (as in the case of buying a ticket) or client-server (as in cases where the client is motivated to share information with the server, like in crowdsourcing scenarios). The client must always initiate the handshake, while the server must provide its own certificate (as in a one-way Authenticated Key Exchange - AKE [21]). Depending on the context, mutual authentication could be necessary (as in the case of a certification issue to a legitimate client). At the end of the handshake, the client possesses an ephemeral key pair, which is used later on to show the PoE to third parties (e.g., through zero-knowledge sigma protocols [16]). At the same time, the server, in turn, associates the public key with the data exchanged during the handshake.

The centralized solution to the PoE management is presented in Figure 1. The Client (C) initiates a connection with the Engagement System – ES (phase

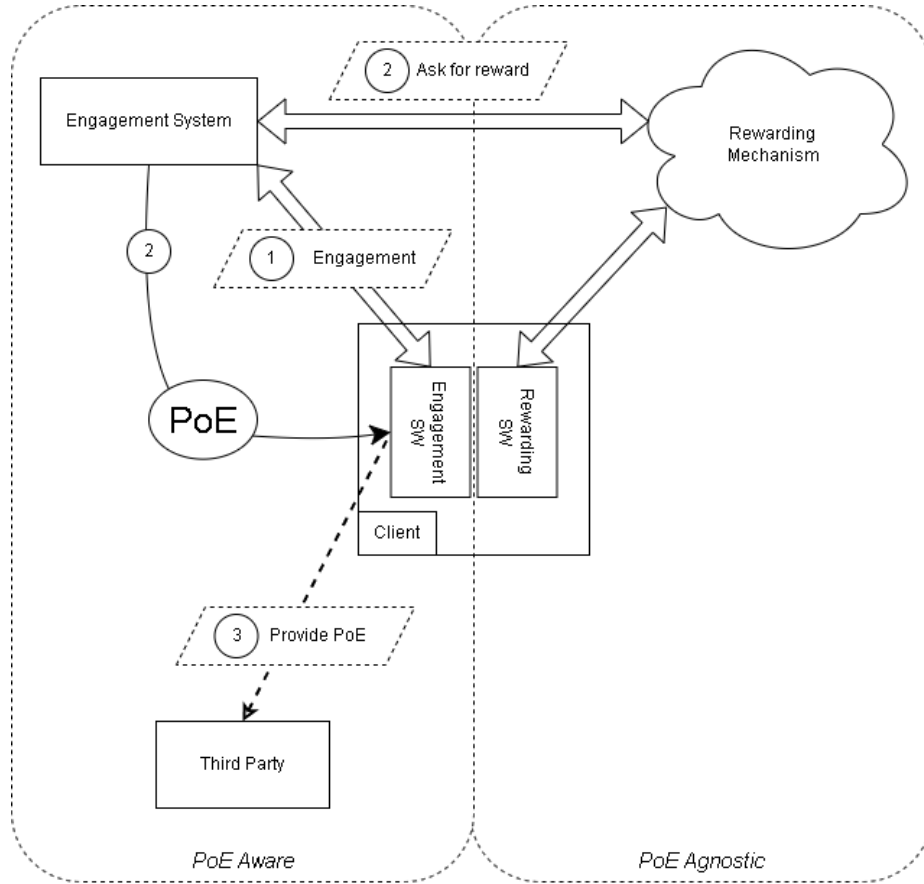


Fig. 1. Centralized PoE architecture

1) by using the Engagement Software – ESW. Then, ES generates and signs the PoE (phase 2), which is stored locally by the client. If applicable, ES notifies the Rewarding Mechanism – RM to enable the association of incentives with the engagement. Afterwards, the client can exhibit the PoE to any Third Party – TP an arbitrary number of times (phase 3), and redeem the incentives from the RM in the form of one-time vouchers, by using the Rewarding Software – RSW. To ensure the confidentiality of the exchanged data and, wherever necessary, the authentication of the involved parties, all the handshakes are based on virtual private networks (VPNs) established via AKE protocols, like, e.g., TLS [21].

Generating the PoE The protocol at the base of the phases 1 and 2 discussed above is defined in Figure 2. The session starts with the client sending data to the ES to prove her engagement, see step (2). At this time, C and ES negotiate the degree of data anonymization before building the PoE to balance C’s privacy and

the accuracy and detail level of the PoE. The result of such a trade-off strictly depends on the application domain and type of PoE (we recall that the PoE may represent a ticket, a badge, a certificate, a proof of ownership, or simply a proof of the engagement of C in some kind of activity). We claim that, in general, the PoE should contain as little information about C as possible, as the PoE will be exposed to third parties (as we will see, the PoE is exposed publicly in the case of a distributed architecture). In many practical scenarios, the PoE may include only essential data together with the integrity proof (e.g., in the form of a hash value) of a detailed data record, which is maintained locally by C and shared with selected third parties on demand. After the negotiation, C generates a pair of ephemeral keys, see step (3), a fresh one-time password (which, as we will see, will be used to claim the reward, if any), see step (4), and then sends to ES the public key of the ephemeral pair and the password, see step (5). At step (6), ES builds and stores locally the PoE, which includes the information agreed with C and the public key chosen by C. At step (7), ES signs the PoE with her secret key sk_{ES} , and at step (8), ES sends the PoE and the signature to C.

- (1) VPN setup : $C \longleftrightarrow ES$
- (2) $C \xrightarrow{\text{VPN}} ES : (\text{engagement_data})$
- (3) $C : (\text{secret_key}, \text{public_key}) \leftarrow \text{Gen}()$
- (4) $C : Pwd := \triangleleft \text{randomly chosen by client} \triangleright$
- (5) $C \xrightarrow{\text{VPN}} ES : (\text{public_key}, Pwd)$
- (6) $ES : DB_{PoE} \leftarrow DB_{PoE} \cup \{PoE\}$
- (7) $ES : PoE_sign \leftarrow \text{Sig}(sk_{ES}, PoE)$
- (8) $ES \xrightarrow{\text{VPN}} C : (PoE_sign, PoE)$

Fig. 2. PoE generation protocol

Exhibiting the PoE In this phase, Client C uses the PoE through the ESW to prove the engagement, an arbitrary number of times, to any Third Party – TP. A Challenge-Response ID protocol with digital signature [21] is used for the realization of this phase, see Figure 3.

At step (1), C sends the ES-signed PoE to TP. At step (2), TP verifies the validity of the PoE signature by using the ES public key pk_{ES} and, if accepted, responds to C by sending a random challenge chosen by the challenge domain \mathcal{C} , see step (3). At step (4), C uses the secret key corresponding to the PoE to sign the challenge, and then sends it to TP. At step (5), TP uses the public key stored in the PoE to verify the signature provided by C. The PoE is accepted if such a verification succeeds.

- (1) $C \xrightarrow{\text{VPN}} TP : (PoE_sign, PoE)$
- (2) $TP : Ver(pk_{ES}, PoE_sign, PoE) \stackrel{?}{=} \mathbf{accept}$
- (3) $TP \xrightarrow{\text{VPN}} C : ch \xleftarrow{R} \mathcal{C}$
- (4) $C \xrightarrow{\text{VPN}} TP : z \leftarrow Sig(secret_key, ch)$
- (5) $TP : Ver(public_key, z, ch) \stackrel{?}{=} \mathbf{accept}$

Fig. 3. PoE exhibition protocol

3.2 Distributed PoE

The solution discussed above modulates the information exchanged between the parties, thereby ensuring compliance with the privacy requirements dictated by the context or by the client's preferences. Nevertheless, certain constraints may be encountered by the client/server in storing and/or managing the PoE.¹ Therefore, we propose an alternative, distributed solution that integrates established methodologies with DLT-based tools.

In a distributed context, DLT-based solutions to the PoE problem can be realized through NFT technologies and blockchain. Here, we propose two alternatives: in one case, the PoE is stored directly on the blockchain, while in the other case, the PoE is inserted within the metadata of an NFT, which is managed on the blockchain by means of a smart contract.

The general architecture of the distributed solution to the PoE management is presented in Figure 5. Unlike the centralized case, the interaction between C, ES, and TP involves the mediation of a blockchain (BC). Indeed, basically, while the engagement is not different with respect to the centralized scenario (phase 1), the remaining phases related to the PoE management (registration of the PoE by the ES and its sharing with C, exhibition of the PoE by C to any TP, and potential transferability of the PoE) require access to the blockchain, as detailed in the following.

The solution that does not involve the use of NFTs consists of having the server sign a blockchain transaction containing the PoE, once the handshake initiated with the client at the time of engagement is finished. In this way, the server can publish the PoE on the blockchain, which includes the ephemeral public key chosen by the client. Hence, the PoE generation protocol is a slight variant of the handshake illustrated in Figure 2, where the last three steps are replaced as follows:

- (6) $ES : BC_{PoE} \leftarrow BC_{PoE} \cup \{PoE\};$
- (7) $ES \xrightarrow{\text{VPN}} C : (Ref_{PoE})$

¹ For instance, after issuing the PoE, the ES might not be interested in ensuring its maintenance, including long-term storage or additional services, like transferability, which is a case we have not considered in the centralized scenario.

Step (6) involves the registration of the transaction on the blockchain that contains the PoE signed by the ES. Finally, at step (7), the ES sends to C the reference to such a transaction.

- (1) $C \xrightarrow{\text{VPN}} TP : \text{Ref}_{PoE}$
- (2) $TP : PoE \xleftarrow{\text{Ref}} BC$
- (3) $TP \xrightarrow{\text{VPN}} C : ch \xleftarrow{R} C$
- (4) $C \xrightarrow{\text{VPN}} TP : z \leftarrow \text{Sig}(\text{secret_key}, ch)$
- (5) $TP : \text{Ver}(\text{public_key}, z, ch) \stackrel{?}{=} \mathbf{accept}$

Fig. 4. Blockchain-based PoE exhibition protocol

The Challenge-Response ID protocol used to exhibit the PoE is a variant of the protocol of Figure 3 – see Figure 4. The main difference is that in the distributed scenario, the PoE is recovered from the blockchain (see, e.g., [27]).

The NFT-based solution is inspired by the buying and selling system of NFTs of POAP. Once the blockchain technology to be used is chosen and users are equipped with the digital wallets associated with their blockchain account, a smart contract is employed to manage the creation, transfer, and/or ownership verification of the NFT associated with the PoE. The engagement data are exchanged during a client-server handshake and are stored outside the blockchain, but can be retrieved via the associated NFT. The data integrity is guaranteed by the immutability of the NFT via a cryptographic hashing mechanism. After the engagement, the ES proceeds to register the proof thus generated within the BC and to return to the Client (via the ESW) the reference to the BC where to retrieve the PoE (which is no longer stored by the Client as in the centralized case). The secret key associated with a specific user’s digital wallet is used to claim ownership of the proof to anyone with read access to the blockchain. The association of the public key (related to a user’s wallet) with the engagement data is ensured by the corresponding NFT, by using the smart contract that manages the NFTs. To this aim, it is sufficient for the Client to send to the TP the reference to the proof that must be shown.

PoE transferability As in the classical NFT marketplace, we assume that, depending on the application domain, the ownership of certain PoEs could be transferred, along with the ability to subsequently claim the ownership.

The solution without NFTs is a general-purpose one inspired by the Bitcoin protocol [18] and can be adapted to any blockchain. The protocol is shown in Figure 6, where C is the current owner of the PoE, R is the recipient to whom the ownership of the PoE is transferred, and T is the transaction establishing the current ownership of the PoE. At step (1), R chooses the pair of ephemeral

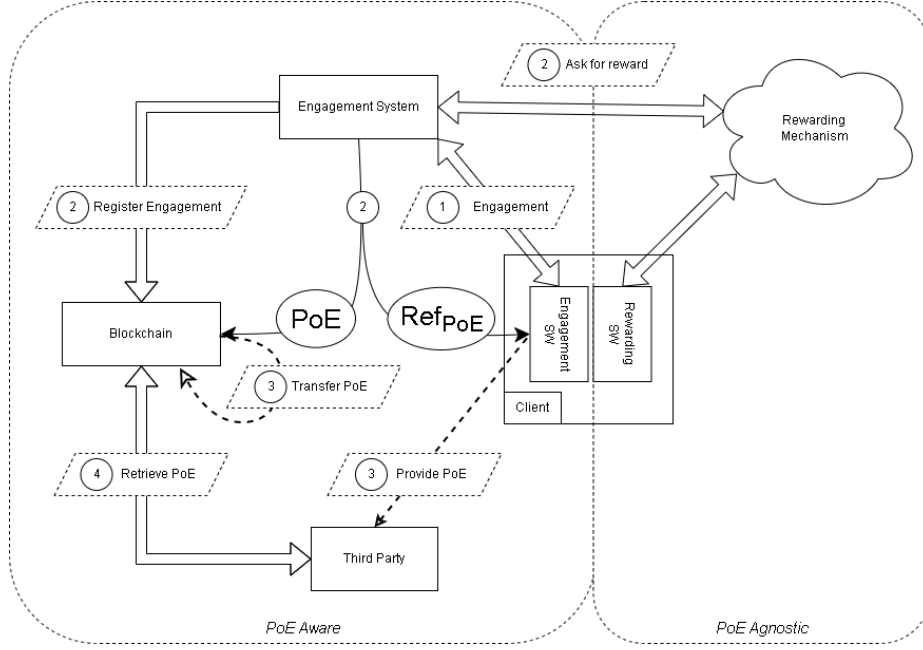


Fig. 5. Distributed PoE architecture.

keys associated with the transfer, while at step (2), the public key of such a pair is sent to *C*. Then, at step (3), *C* builds the transfer transaction stating that the PoE is now associated with a new public key. Such a transaction is signed by *C* with the ephemeral secret key associated with *T*, and then written to the blockchain, see step (4).

- (1) *R* : $(pk_{rec}, sk_{rec}) \leftarrow Gen()$
- (2) $R \xrightarrow{VPN} C : (pk_{rec})$
- (3) *C* : $T' := \{pk_{rec} \text{ is the new owner of the } PoE \text{ at transaction } T\}$
- (4) *C* : $BC \leftarrow Sig(secret_key, T')$

Fig. 6. PoE transfer protocol without NFT

Whenever the PoE is stored as an NFT, the machinery managing the transfer is left to a smart contract. Starting from the interface of the ERC-721 standard [9,11], it is possible to implement a smart contract that manages the NFT associated with a PoE. In this solution, the paternity of the PoE can be made transferable by exchanging the corresponding NFT between the wallets of any two users (see, e.g., [19]).

3.3 PoE with rewards

The system we propose envisages the possibility of creating a PoE associated with incentives in the form of rewards. The Rewarding Mechanism – RM used in both PoE architectures (centralised and distributed) is shown in Figure 7.

In this system, after the handshake between C and ES certifying some kind of engagement (phase 1), another handshake is activated between ES and the Rewarding System – RS (phase 2). In response, RS generates the reward corresponding to the ES request. The client then proceeds to redeem the reward through a Reward Claim (phase 3) by using the Rewarding Software – RSW. The reward is then delivered (phase 4) and subsequently spent (phase 5) by the client in any interaction with merchants accepting the corresponding type of incentive. The RS guarantees that a reward cannot be used more than once and that no more than one reward can be generated for the same PoE.

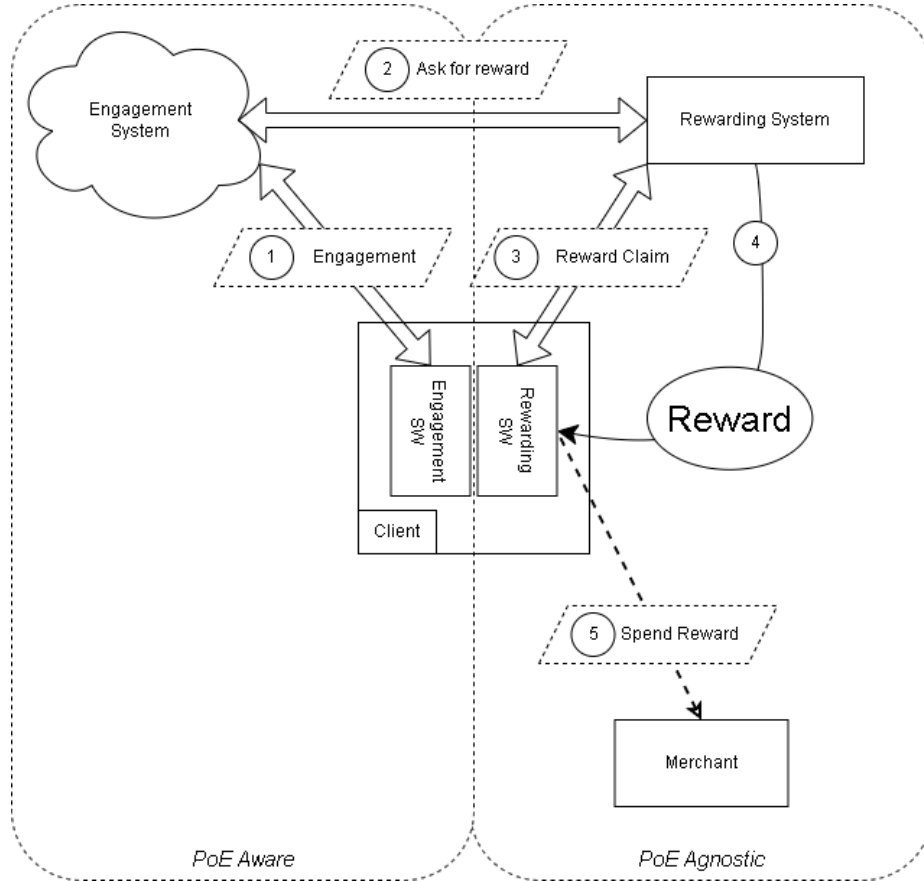


Fig. 7. Reward mechanism architecture.

Independent of the specific use case and the PoE architecture, it is worth observing that RS and reward are designed to be agnostic of the PoE, meaning that they do not manage or include any information about the client or the details of the PoE. During phase 2, ES guarantees that a given PoE, which is not shown to the RS, is eligible to issue a certain type of reward. Hence, the reward is completely anonymous.

Generating and Redeeming the Reward The protocol at the base of the phases 2-4 discussed above is defined in Figure 8.

- (1) $ES : filtered_data \leftarrow \mathbf{Anonymize}(engagement_data)$
- (2) $ES \xrightarrow{VPN} RS : (filtered_data, H(Pwd))$
- (3) $RS \xrightarrow{VPN} ES : (OTC, H(Pwd))$
- (4) $ES \xrightarrow{VPN} C : (OTC, H(Pwd))$
- (5) $C \xrightarrow{VPN} RS : (OTC, Pwd)$
- (6) $RS \xrightarrow{VPN} C : (Reward)$

Fig. 8. Reward generation protocol

At step (1), ES extracts from the PoE engagement data the minimum amount of information needed to issue a reward request to the RS (e.g., the type of eligible request, which allows the RS to specify in which context a reward can be spent). Then, the handshake between ES and RS is based on an AKE protocol with mutual authentication. At step (2), the ES transmits the digest $H(Pwd)$ (computed using the hash function H) of the one-time password Pwd associated with the PoE by the client (see Figure 2), together with the filtered data. This will allow the client to redeem the reward later on. Then, the RS issues the reward and sends to the ES the One Time Code (OTC) for accessing it, see step (3). At step (4), the ES forwards such information to the client within the same handshake session related to the PoE generation, e.g., in step (8) of Figure 2 (together with the signed PoE). In steps (3) and (4), the hashed password acts as a nonce associated with the OTC. Afterwards (and by the expiration time associated with the reward), the client employs the OTC to access the reward and redeem it by exhibiting the corresponding Pwd as proof of claim, as in classical password-based identification protocols [21], see steps (5) and (6). Note that to transmit the reward, the digest of the received password must correspond to the locally stored value associated with the related OTC.

The protocol presented above is inspired by the WOM platform, to which our system can be integrated. For the presentation of the details of the one-time spending process of the WOM vouchers, the interested reader can refer to [14].

4 Case studies

In this section, we describe a prototype of the proposed system that has been implemented for a specific case study, and we discuss potential integration with other platforms and in several real-world application domains.

4.1 Simulation

To simulate the behavior of the proposed system, we have implemented a prototype system managing the PoE in the case of attendance at seminars, which is a case study already under development at the University of Urbino for the assignment of WOM vouchers.

The software was developed using the programming language Dart and the Google Flutter framework. It includes three modules implementing the centralized solution to the PoE and deployed as three web applications representing Client², Engagement System³ and Third Party⁴. The Client module allows the user to collect and manage PoEs resulting from the interaction with the Engagement System. At the same time, the module allows the user to exhibit the PoE to the Third Party, which verifies its validity. The three web apps interact in a virtual LAN through a server⁵ that follows the WebSocket protocol. The PoE includes student ID, name, surname, email, GPS data, and timestamp. Once approved by the Engagement System web app, the PoE is generated, signed, and sent to the Client. By following the corresponding protocol, the Client can choose a PoE from the wallet managed by the web app and exhibit it to the Third Party, which performs the validation check.

The PoE format is based on JSON (JavaScript Object Notation) [5] and the standard ECMA-404 – chosen for its flexibility and interoperability – and includes the following information (see the example illustrated in Figure 9):

- The public key of the ephemeral key pair associated with the PoE generation, which is implemented using the RSA scheme;
- Spatial (e.g., GPS coordinates) and temporal (e.g., timestamp of the engagement) information (if eligible);
- Engagement data as negotiated between the Client and the Engagement System;
- Any other structured data (e.g., images) following the JSON standard;
- The integrity proof (expressed as the digest deriving from the application of a one-way hash function, like, e.g., SHA-256) of additional data that are not stored directly within the PoE but are maintained locally by the Client web app;
- The *transferability* flag stating whether the PoE can be transferred to another client;
- The expiration date of the proof (if eligible).

² https://github.com/MatteoMarcoM/poe_client

³ https://github.com/MatteoMarcoM/poe_es

⁴ https://github.com/MatteoMarcoM/poe_tp

⁵ https://github.com/MatteoMarcoM/web_socket_dart

```

JSON = {
  "proof_type" : "PoE",
  "transferable" : true,
  "public_key" : {
    "algorithm" : "SHA-256/RSA",
    "verification_key" : "AAAAB3NzaClyc2EAAAABJQAAAQBA/
                          OWmcKS0A8 ... x836Sj/6LcjQ8n"
  },
  "timestamp" : {
    "time_format" : "UTC",
    "time" : "2005-10-30 T 10:45"
  },
  "gps" : { "lat" : -34, "lng" : 151, "alt" : 1200 },
  "engagement_data" : {
    "encoding" : "base64",
    "data" : "TG9yZW0gaXBzdW0gZG9sb3Igc2l0IGFtZX
              QsIGNvbnNlY3RldHVyIGFkaXBpc2NpIGVs
              BpbmNpZHVudCB1d ... YWJvcmlUgZSQgZG"
  },
  "sensitive_data" : {
    "data_1" : "<HASH(value_1)>",
    "data_2" : "<HASH(value_2)>",
    ...
    "data_n" : "<HASH(value_n)>"
  },
  "other_data" : {
    "expiration_date" : {
      "date_format" : "UTC",
      "date" : "2035-10-30 T 10:45"
    }
  }
}

```

Fig. 9. Example of a PoE in JSON format.

4.2 Application domains

The context that provided us with the motivational basis for proposing a general-purpose framework for PoE management is the project *Casa delle Tecnologie Emergenti di Pesaro* (CTE Square) [4], which was conceived as an advanced center for technological innovation and skills transfer, where the application of emerging technologies in the areas of Culture, Tourism and Engagement can be tested. In this setting, the PoE is conceived as a framework serving to cover the temporal and spatial distance between the action to be recognized, the recognition of the corresponding validity, and the application of incentives, by achieving an adequate trade-off between fairness, usability, and privacy protection. The technology identified for realizing the reward-based incentive mechanism is the WOM Platform [14,25,6]. Two case studies that emerged in the CTE Square project are illustrated as follows.

University exams certification In a way inspired by the Open Badge solution, a PoE is provided to the student upon passing an exam. In this case, the ES is implemented within the University platform that manages the students' careers. The PoE is flexible enough to include customized information detailing

competences acquired or projects developed to pass the exam, which represents very specific data that is usually not maintained by the University. Such a PoE can be integrated into the student’s CV and diploma supplement. In addition, as a social incentive, for each exam that is passed, a reward is assigned in the form of anonymous education vouchers that can be spent to obtain discounts in partner shops and stores, such as bookstores and cafes. The same approach is applied to certify and incentivize participation in other extracurricular events and activities (seminars, soft skills courses, job placement workshops, and many more). In this case study, the proposed solution is centralized, where the ES acts as the central certifying authority, and the PoE is not transferable.

Tourism office initiatives In a way inspired by the POAP NFT solution, a PoE is provided to the users contributing actively to improving the quality of the local tourist and cultural receptivity (e.g., by visiting tourist sites, providing feedback, and supporting events). The specificity of the PoE is that it is anonymous and may include exclusive and individual contents representing collectibles whose ownership could be transferred. In addition, anonymous vouchers are emitted that entitle the holder to discounted access to exhibitions and other events. In this case study, the proposed solution is distributed and blockchain-based, and the PoE is transferable.

5 Conclusions

In this work, we analyzed and designed flexible, general-purpose, and privacy-aware solutions to the Proof-of-Engagement problem, integrating also incentive aspects and combining advanced technologies, ranging from Distributed Ledger Technologies to Non-Fungible Tokens. The main strengths of adopting our proposed PoE solutions can be summarized as follows:

- Flexibility: PoE solutions allow a wide range of data types to be stored within the proof, making the system adaptable to multiple use cases and application scenarios.
- Ease of integration: the implementation of such solutions is facilitated by standardized and well-established technologies that allow minimizing implementation time, even in contexts that involve integration with other platforms, like, e.g., WOM.
- Efficiency and privacy protection: PoE technologies ensure high operational efficiency, while still maintaining an adequate level of privacy guaranteed to users, thanks to the use of tools designed specifically for this purpose.

The centralized architecture offers simplicity and rapid deployment in different scenarios, which is ideal in controlled enterprise and corporate environments. The distributed architecture, on the other hand, provides transparency, data immutability, and scalability, which are features particularly required in public and collaborative settings. The integration of the PoE with incentive mechanisms has

also shown considerable potential in scenarios requiring interaction and enhancement of human behaviors (like, e.g., in crowdsourcing), with positive implications for large-scale applications.

The proposed framework is currently under development for the deployment of digital services supported by the municipality of the city of Pesaro and by the University of Urbino, Italy. These services aim to promote tourism, culture, and engagement in activities recognised for their high social value. As future work, it is worth completing the deployment of the framework and its full integration with the WOM platform, in order to test its efficacy and efficiency in large-scale scenarios and various application domains, including environmental sustainability initiatives, social awareness campaigns, and global educational programs.

Acknowledgements

This work is partially funded by MIMIT, under FSC project “Pesaro CTE SQUARE”, CUP D74J22000930008.

References

1. 1EdTech: Open Badges FAQ: Frequently asked questions & glossary. Online, <https://openbadges.org/about/faq>
2. Chowdhury, M.J.M., Ferdous, M.S., Biswas, K., Chowdhury, N., Kayes, A.S.M., Alazab, M., Watters, P.: A comparative analysis of distributed ledger technology platforms. *IEEE Access* **7**, 167930–167943 (2019). <https://doi.org/10.1109/ACCESS.2019.2953729>
3. CINECA: Bestr website. Online, <https://bestr.it/>
4. Comune di Pesaro: Project Pesaro CTE SQUARE: Culture, tourism, and engagement. Online (2023), <https://ctesquare.it/>
5. Crockford, D.: Json project website. Online, <https://www.json.org/json-en.html>
6. Digit srl: Worth one minute website. Online, <https://wom.social/home/>
7. Dongre, P., Verma, P.: An IOT based private blockchain framework for attendance management using QR code. In: *Proceedings of the 1st Conference on Advanced Scientific Innovation in Science, Engineering and Technology, ICASISSET. EAI* (2021). <https://doi.org/10.4108/eai.16-5-2020.2303960>
8. El Ioini, N., Pahl, C.: A review of distributed ledger technologies. In: Panetto, H., Debruyne, C., Proper, H.A., Ardagna, C.A., Roman, D., Meersman, R. (eds.) *On the Move to Meaningful Internet Systems. OTM 2018 Conferences. LNCS*, vol. 11230, pp. 277–288. Springer (2018). https://doi.org/10.1007/978-3-030-02671-4_16
9. Entriken, W., Shirley, D., Evans, J., Sachs, N.: Eip-721: Erc-721 nonfungible token standard. *Ethereum Improvement Proposals*, no. 721 (2018)
10. Hallila, J.J.: Improving a live streamer’s community’s engagement with use of blockchain applications: Development project for Juffu streaming. Bachelor’s Thesis, Metropolia University of Applied Sciences (2021)
11. Hong, S., Noh, Y., Park, C.: Design of extensible non-fungible token model in hyperledger fabric. In: *Proceedings of the 3rd Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers*. p. 1–2. Association for Computing Machinery (2019). <https://doi.org/10.1145/3366611.3368142>

12. Joseph, M.A., Natarajan, J., Buckingham, J., Al Noumani, M.: Using digital badges to enhance nursing students' attendance and motivation. *Nurse Education in Practice* **52**, 103033 (2021). <https://doi.org/10.1016/j.nepr.2021.103033>
13. Jovanovic, J., Devedzic, V.: Open badges: Novel means to motivate, scaffold and recognize learning. *Technology, Knowledge and Learning* **20** (04 2014). <https://doi.org/10.1007/s10758-014-9232-6>
14. Klopfenstein, L.C., Delpriori, S., Aldini, A., Bogliolo, A.: "Worth one minute": An anonymous rewarding platform for crowd-sensing systems. *Journal of Communications and Networks* **21**(5), 509–520 (2019). <https://doi.org/10.1109/JCN.2019.000051>
15. Marinescu, A.M., Popescu, E.: A gamified approach for monitoring student attendance and fostering learner engagement: AttendanceManager platform. In: Bădică, C., Gușev, M., Iftene, A., Ivanović, M., Manolopoulos, Y., Xinogalos, S. (eds.) *Advances in ICT Research in the Balkans*. pp. 135–145. Springer (2025). https://doi.org/10.1007/978-3-031-84093-7_10
16. Morais, E., Koens, T., van Wijk, C., Koren, A.: A survey on zero knowledge range proofs and applications. *SN Applied Sciences* **1**(8), no. 946 (2019). <https://doi.org/10.1007/s42452-019-0989-z>
17. Nah, F.F.H., Zeng, Q., Telaprolu, V.R., Ayyappa, A.P., Eschenbrenner, B.: Gamification of education: A review of literature. In: Nah, F.F.H. (ed.) *HCI in Business*. LNCS, vol. 8527, pp. 401–409. Springer (2014). https://doi.org/10.1007/978-3-319-07293-7_39
18. Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S.: *Bitcoin and Cryptocurrency Technologies*. Princeton University Press (2016)
19. Niu, X., Kong, L., Jin, F., Song, X., Min, X., Li, Q.: NFT cross-chain transfer method under the notary group scheme. In: 2023 26th International Conference on Computer Supported Cooperative Work in Design (CSCWD). pp. 996–1001 (2023). <https://doi.org/10.1109/CSCWD57460.2023.10152551>
20. Ohlhaver, P., Weyl, E.G., Buterin, V.: Decentralized society: Finding web3's soul (2022). <https://doi.org/10.2139/ssrn.4105763>
21. Paar, C., Pelzl, J.: *Understanding Cryptography*. Springer (2010). <https://doi.org/10.1007/978-3-642-04101-3>
22. Paspallis, N., Andreou, P., Bullo, A.: Design and evaluation of a gamification-based information system for improving student attendance. In: Andersson, B., Johansson, B., Barry, C., Lang, M., Linger, H., Schneider, C. (eds.) *Information Systems Development: Designing Digitalization, ISD 2018*. Lund University and Association for Information Systems (2018), <https://aisel.aisnet.org/isd2014/proceedings2018/General/5>
23. Pinter, R., Čisar, S., Balogh, Z., Manojlovic, H.: Enhancing higher education student class attendance through gamification. *Acta Polytechnica Hungarica* **17**, 13–33 (2020). <https://doi.org/10.12700/APH.17.2.2020.2.2>
24. POAP Inc.: Poap project website. Online, <https://poap.xyz/>
25. Remedi, G., Aldini, A., Bogliolo, A., Delpriori, S., Klopfenstein, L.: Modeling and verification of the worth-one-minute security protocols. In: *Italian Conference on Cyber Security - Proceedings (ITASEC)*. vol. 2597. CEUR (2020), <https://ceur-ws.org/Vol-2597/paper-03.pdf>
26. Shields, R., Chugh, R.: Digital badges – rewards for learning? *Education and Information Technologies* **22**(4), 1817–1824 (Jul 2017). <https://doi.org/10.1007/s10639-016-9521-x>

27. Sun, X., Yu, F.R., Zhang, P., Sun, Z., Xie, W., Peng, X.: A survey on zero-knowledge proof in blockchain. *IEEE Network* **35**(4), 198–205 (2021). <https://doi.org/10.1109/MNET.011.2000473>
28. Wang, Q., Li, R., Wang, Q., Chen, S.: Non-fungible token (NFT): overview, evaluation, opportunities and challenges. *CoRR* **abs/2105.07447** (2021). <https://doi.org/10.48550/arXiv.2105.07447>