Communication Papers of the 18th Conference on Computer Science and Intelligence Systems pp. 323–327
DOI: 10.15439/2023F9620
ISSN 2300-5963 ACSIS, Vol. 37

Blockchain-based certification of research outputs and academic achievements: A case of scientific conference

Robert Susik
0000-0003-0653-433X
Lodz University of Technology, Institute of Applied Computer Science
Al. Politechniki 11, 90–924 Łódź, Poland
Email: rsusik@kis.p.lodz.pl
Robert Nowotniak
0000-0003-1104-4511
MetaSolid.tech, Al. Grunwaldzka 56/202, 80-241 Gdańsk, Poland
Email: rnowotniak@metasolid.tech
Emanuel Kulczycki
0000-0001-6530-3609
Adam Mickiewicz University in Poznań, Scholarly Communication Research Group
Poznań, Poland
Email: emek@amu.edu.pl

***Abstract*—We consider the problem of researcher output identification and its verification. Nowadays, researcher outputs verification is a challenging problem faced by institutions that want, for example, employ such a researcher. Usually, there is no verification, and the aforementioned institutions rely on trust that the received documents are authentic. Our solution is a based on blockchain technology, a public ledger with smart contracts, that is the root of emerging web3. We use the public wallet address as the researcher identification number and the wallet as the store of all researcher credentials. This paper presents ERC-721 standard-based solution and addresses the conference certification case. The solution proposed in this paper addresses two challenges that arise in collecting and verifying data on research output for managing, monitoring, and evaluating purposes. We show that the public wallet address can be successfully used as the researcher identification number, and the wallet can be used as a vault of all the researcher credentials.**

I. Introduction

A. Background

BLOCKCHAIN emerged as a distributed ledger used for cryptocurrency. The first successful cryptocurrency blockchain, Bitcoin, was introduced by [1]. Since that time, many alternative solutions and forks of Bitcoin have appeared. One of the recent milestones in blockchain development was the release of the Ethereum [2], the first implementation of Blockchain 2.0 concept [3]. Ethereum can be defined as a blockchain-based platform for decentralized application development. It is based on Ethereum Virtual Machine (EVM) that is Turing-complete, and which allows running any algorithms on the blockchain.

B. Areas of performance management where blockchain can be useful

The management of research institutions and research work is based on mechanisms that monitor and evaluate scientific achievements and research outputs. This includes evaluation conducted at the national level within performance-based research funding systems and evaluation of individual researchers or scholarly publication channels. One of the key elements of the whole system of monitoring are persistent identifiers. They are intended to uniquely identify a given object so that the products of scientific work can be monitored. Identifiers are commonly used to identify publications (e.g. DOI or ISBN) and recently also to identify researchers (e.g. ORCID or ScopusID) and organizations (e.g. Funder ID, Global Research Identifier Database (GRID) ID or Research Organization Registry (ROR) ID).

The solution proposed in this paper can address two challenges that arise in collecting and verifying data on research output for managing, monitoring, and evaluating purposes.

The first challenge concerns the legal aspect and relates to who owns the data or servers on which information about the output of researchers and institutions is collected. This challenge is crucial at the level of national policies, which is particularly evident in Europe with the General Data Protection Regulation. It is because it turns out that what is not problematic when identifying publications using DOIs, as it mainly contains publication metadata and possibly references, can pose significant legal problems when dealing with institutions and researchers. For example, Poland has one of the highest percentages of researchers with ORICDs [4]. It is a result of

©2023, PTI

Topical area: Information Technology for Business and Society

the announced changes in Polish science policy regarding the evaluation of research institutions. ORCID was supposed to be the primary source of information about publications and scientific activity of Polish researchers. However, it turned out that at the stage of implementation of this policy, there were doubts of legal nature as to in which country the servers containing information about the achievements of Polish researchers would be located and whether the Polish government could rely on its internal policy on such external information. Ultimately, ORCID became a recommended rather than an obligatory identifier.

The second challenge is related to the unambiguous legitimization of information by the authorized entity and verification of the validity of the presented information by the institution or researcher. When applying for a job at a scientific institution or promotion, researchers list their achievements and research outputs. In the case of scientific publications, there are no major problems with checking whether such a publication exists. However, there are publications published in the so-called hijacked journals [5], i.e., in journals pretending to be other journals. If a publication has a DOI, one can verify in which journal such a publication was actually published. However, this is no longer so easy in the case of scholarly book publications, as DOIs are rarely assigned to such publications. Moreover, many companies organize so-called questionable conferences [6] with confusingly similar names, which is done intentionally to resemble reputable events. Consequently, in the process of considering candidates for scientific positions or evaluating the output of an institution, it is not always clear whether such a conference was, in fact, organized by a reputable institution or a company organizing para-scientific events because certificates are mostly in the form of PDF files that can be produced by anyone.

C. Certification based on the blockchain

Certification based on the blockchain is known in the literature and was one of the interesting subjects during the last three years. Diverse approaches were proposed, but none of them was based on the ERC721 [7] tokenization standard, which supports multiple features (see Section II) and is compatible with the existing blockchain ecosystem (i.e. software and hardware wallets, such as MetaMask or Ledger). In [8] authors presented an outline of structure and functionality of certification system based on blockchain. They suggest a solution which is a combination of conventional database (off-chain transactions) of students and blockchain technology (on-chain transactions) where the front-end application combines information from both to present the data. This solution involves a third-party institution of Certificate Authority. [9] propose a blockchain-based solution that aims to share student results between Higher Education Institutions. [10] proposed a different approach that leverages a blockchain-based network composed of private and public blockchains to allow educational institutions, learning users, and talent markets exchange the information. An e-learning blockchain-based system was presented in [11]. Here the authors proposed an e-learning system that uses multi-chain architecture as a decentralized ledger that stores users' rewards (e-learning vouchers) and certificates. Another certification system was proposed in [12] where the platform incentives effort in grading via payments with crypto-tokens. In [13], authors proposed a blockchain-based academic certification solution for higher education institutions. They created an Ethereum-based Web3 DApp (a decentralized application [14]) with an application front-end implemented in React library using MetaMask connected to Infura node, and a back-end written in Solidity language using IPFS storage [15]. In [16] authors presented Student-Centered iLearning Blockchain framework which allows to certify, acknowledge and validate students' achievements, skills and competencies on Ethereum blockchain. Contrary to this and other previously presented solutions, in our approach an acknowledged ERC721 [7] standard is used. Thanks to this, digital certificates generated in our system are recognized and presented visually in popular cryptocurrency wallets like MetaMask or Ledger. A survey of over 30 other publications on Blockchain-based prototypes and use cases to transact digital certificates in public education was presented in [17].

D. Aim of the study

This paper aims to present an idea for certifying research outputs and academic achievements using blockchain. We show how such a certification can be designed and implemented in the example of a scientific conference. Moreover, we demonstrate how such a solution could, in the future, allow coping with specific challenges that face the collection of information about scientific activity and its verification in the research evaluation process.

Currently, mass adoption of this solution in the scientific community is difficult due to the high cost of implementation and certification of a single activity. However, the costs of using blockchain are steadily decreasing; therefore, our article may be an inspiration for discussion of whether blockchain can be used in the processes of managing scientific institutions and research evaluation, or whether it is instead a dead end.

II. Our approach

In this section, we present the design of a blockchain-based academic profile for conference attendance certification. The source codes of the solution are shared in the GitHub platform at github.com/rsusik/conference-certification. Our system consists of the following components:

1) Smart Contract (ERC721)
2) User Interface
3) Blockchain (Ethereum)
4) Certificate (Token)

The back-end of the solution is implemented as a smart contract written in Solidity language. The contract implements ERC721 interface and is deployed in the Ethereum blockchain but can also be deployed in any other compatible chain (e.g. Polygon, BSC).

We distinguish the following actors in our system: Participant, Organizer, and Others. A Participant is a person who

attends the conference and gains a credential, the Organizer is an entity (university, institute, organization, etc.) that organizes the conference, and the Others are all other blockchain users who want to check or validate the user's participation in the conference. The outline of the system is presented in Fig. 1. It consists of User Interface (UI), which is a web application (front-end) and a Smart Contract (back-end).

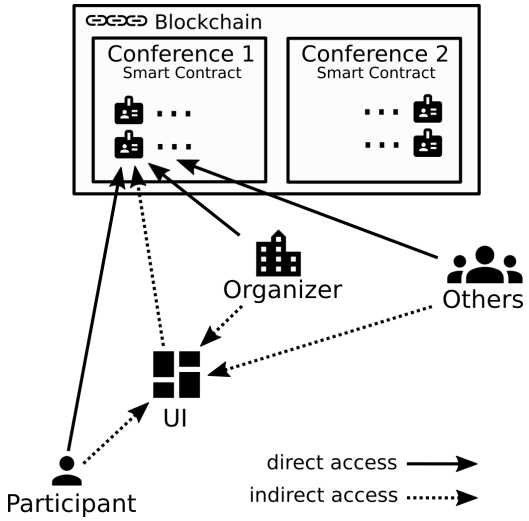

Fig. 1: System outline

The Smart Contract is created and deployed to Blockchain (Ethereum in our implementation) by the Organizer (or on his behalf) for a particular Conference Event. Once the contract is created the Organizer can mint tokens representing certifications for the Participants. The Participant can add the token to his wallet via the User Interface or any wallet manager such as MetaMask. The Others can check if the Participant attended the conference and read the metadata of his activity. The system allows to:

- issue certifications (mint the tokens),
- revoke certifications (burn the tokens),
- transfer certifications (transfer tokens),
- list Participant's certifications (list token owners),
- list the conference certifications (list tokens),
- validate the Participant's certificate.

The Organizer has permission for all of the listed activities. The Participant is the owner of the token that represents the credential. He has the same permissions as Others. The Others can list all participants and credentials of the conference.

The Participant is required to deliver his wallet public address, then the Organizer can issue a certificate for him (mint an NFT token). There are two types of participants: active (i.e. those who present their research results) and passive (listeners). According to [18] each certificate for active Participant contains such information as: Acronym, Event type (Conference, Workshop, Symposium), Year, Date (October 26-30), Location, Title (i.e. International Semantic Web Conference), Subject (what the conference is about, i.e. Semantic Web).

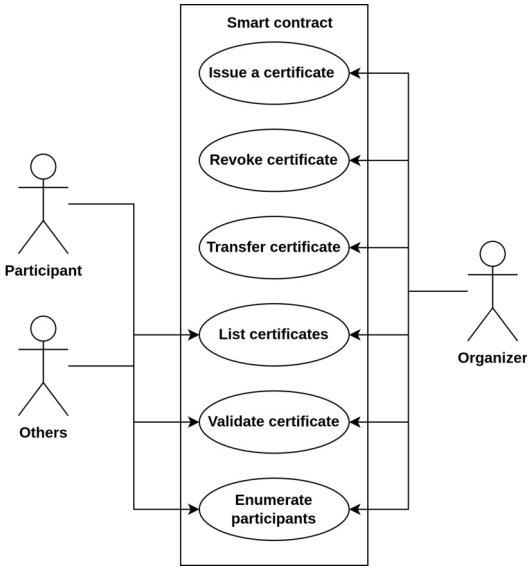

Fig. 2: Use case diagram

The Organizer delivers the conference Smart Contract address to Participants after the conference event. The Participants can then add the certifications to their wallets. Other users can read the conference participant list or validate credentials using either the User Interface or directly by executing a function in the Smart Contract on the blockchain.

The proposed approach is fully decentralized, there is no need to implement or use any specific API as the system is based on the public blockchain, so everyone who has access to the Internet and the blockchain nodes can read certifications and confirm their authenticity. Additionally, all the Internet users can write their applications and integrate with our solution without our permission as long as they use the same programming interfaces (the ERC721 standard and JSON Schema). Figure 3 shows a screenshot of MetaMask mobile crypto wallet containing an example conference certificate.

There are costs of smart contract deployment on blockchain and token minting. This may be perceived as a disadvantage of this system, but there are multiple options for cost optimizations (including the use of Layer2 chains or ERC115 contracts) [19], [20], [21]. On the other hand, there is no need to maintain any servers (i.e., databases, HTTP servers, DNS services, etc.) to store and share the data.

III. Conclusions and Future Work

In this paper, we address the problem of researcher output identification and its verification. We show that the public wallet address can be successfully used as the researcher identification number, and the wallet can be used as a vault of all the researcher credentials. Additionally, the proposed solution is based on the ERC721 standard, which makes it compatible with most existing crypto wallets and other software. Apart from the conference case, there are a number of interesting use cases for this solution. In fact, we believe that

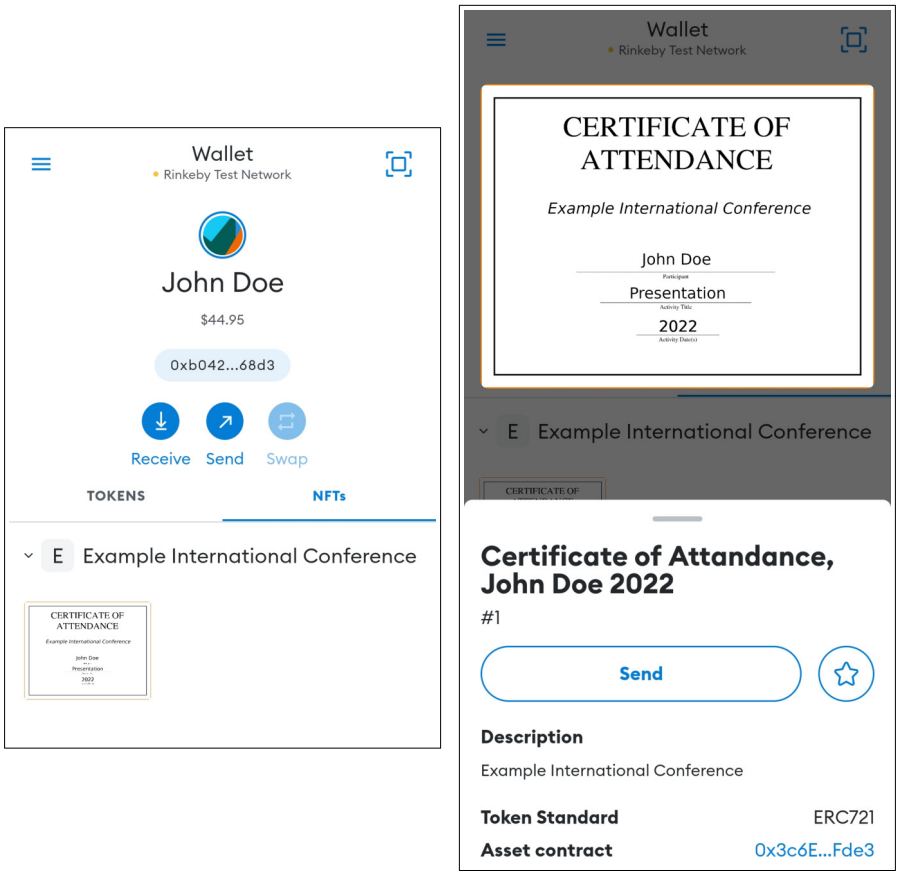

Fig. 3: Screenshot of a certificate of attendance displayed in MetaMask mobile crypto wallet

blockchain can be used to store complete researcher profile information and replace those commonly used nowadays.

The limitation we see in a blockchain–based certification system is the need to have smart contract addresses of legitimate conferences or journals. Questionable conferences or hijacked journals may mint tokens (representing credentials) in their smart contract (pretending to represent other journals) using any address. This situation is analogous to sharing credentials on a fake HTTP conference website. However, we do not consider it a significant disadvantage because, by knowing the smart contract address of a specific legitimate conference (for instance, obtained from its official website) or having a list of such respected conferences (with their smart contract addresses), we can easily verify if a particular certificate has been issued by mentioned conference (the token is minted on their smart contracts). Moreover, verifying such fake credentials is unnecessary, as the client application wouldn't display them. Another factor that may be considered a minor inconvenience in implementing this approach is when journals or conferences use diverse blockchains for credential certifications. In such a case, we need to query multiple blockchains to perform the verification, which is not an issue but may require additional work or a higher-level API.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, p. 21260, 2008.

[2] V. Buterin, "Ethereum white paper: A next generation smart contract & decentralized application platform," 2013.

[3] D. Efanov and P. Roschin, "The all-pervasiveness of the blockchain technology," *Procedia computer science*, vol. 123, pp. 116–121, 2018.

[4] S. J. Porter, "Measuring Research Information Citizenship Across ORCID Practice," *Frontiers in Research Metrics and Analytics*, vol. 7, p. 779097, Mar. 2022.

[5] M. Andoohgin Shahri, M. D. Jazi, G. Borchardt, and M. Dadkhah, "Detecting Hijacked Journals by Using Classification Algorithms," *Science and Engineering Ethics*, vol. 24, pp. 655–668, Apr. 2017.

[6] E. Kulczycki, M. Hołowiecki, Z. Taşkın, and G. Doğan, "Questionable conferences and presenters from top-ranked universities," *Journal of Information Science*, 2022.

[7] W. Entriken, D. Shirley, D. Evans, and N. Sachs, "ERC721." https://eips.ethereum.org/EIPS/eip-721, 2018. Accessed: 2022-04-20.

[8] M. Alshahrani, N. Beloff, and M. White, "Revolutionising higher education by adopting blockchain technology in the certification process," in *2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT)*, pp. 1–6, IEEE, 2020.

[9] S. Cardoso, H. São Mamede, and V. Santos, "Reference model for academic results certification in student mobility scenarios: Position paper," in *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)*, pp. 1–4, IEEE, 2020.

[10] L. Gao, "Management of online education based on blockchains," in *2020 International Conference on Modern Education and Information Management (ICMEIM)*, pp. 84–89, IEEE, 2020.

[11] C. Li, J. Guo, G. Zhang, Y. Wang, Y. Sun, and R. Bie, "A blockchain system for e-learning assessment and certification," in *2019 IEEE International Conference on Smart Internet of Things (SmartIoT)*, pp. 212–219, IEEE, 2019.

[12] J. Gupta and S. Nath, "Skillcheck: An incentive-based certification system using blockchains," in *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pp. 1–3, IEEE, 2020.

[13] M. P. Jaramillo and N. Piedra, "Use of blockchain technology for academic certification in higher education institutions," in *2020 XV Conferencia Latinoamericana de Tecnologias de Aprendizaje (LACLO)*, pp. 1–8, IEEE, 2020.

[14] W. Cai, Z. Wang, J. B. Ernst, Z. Hong, C. Feng, and V. C. Leung, "Decentralized applications: The blockchain-empowered software system," *IEEE Access*, vol. 6, pp. 53019–53033, 2018.

[15] J. Benet, "Ipfs-content addressed, versioned, p2p file system," *arXiv preprint arXiv:1407.3561*, 2014.

[16] A. S. Anwar, U. Rahardja, A. G. Prawiyogi, N. P. L. Santoso, *et al.*, "ilearning model approach in creating blockchain based higher education trust," *International Journal of Artificial Intelligence Research*, vol. 6, no. 1, 2022.

[17] A. Pfefferling and P. Kehling, "Design disclosure for blockchain-based application used in public education certificates with electronic hashes," in *Konferenzband zum Scientific Track der Blockchain Autumn School 2021*, no. 004, pp. 034–041, Hochschule Mittweida, 2021.

[18] J. Franken, A. Birukou, K. Eckert, W. Fahl, C. Hauschke, and C. Lange, "Persistent identification for conferences," *Data Science Journal*, vol. 21, no. 1, 2022.

[19] R. Susik and R. Nowotniak, "Pattern matching algorithms in blockchain for network fees reduction," *arXiv doi:10.48550/ARXIV.2207.14592*, 2022.

[20] A. Di Sorbo, S. Laudanna, A. Vacca, C. A. Visaggio, and G. Canfora, "Profiling gas consumption in solidity smart contracts," *Journal of Systems and Software*, vol. 186, p. 111193, 2022.

[21] G. A. Pierro, H. Rocha, S. Ducasse, M. Marchesi, and R. Tonelli, "A user-oriented model for oracles' gas price prediction," *Future Generation Computer Systems*, vol. 128, pp. 142–157, 2022.