

Identity Management on (Arweave) Blockchain

Andreea-Elena Drăgnoiu

andreea-elena.panait@drd.unibuc.ro

Department of Computer Science, University of Bucharest

Bucharest, Romania

The Research Institute of the University of Bucharest (ICUB)

Bucharest, Romania

Abstract

In today's world, efficient and secure digital identification is a must. Traditional identity management (IdM) systems, often centralized, face challenges around privacy, data security, and user control, leaving users vulnerable to data breaches and misuse. This paper explores the potential of using blockchain technology for identity management, focusing on the Arweave network.

ACM Reference Format:

Andreea-Elena Drăgnoiu. 2025. Identity Management on (Arweave) Blockchain. In . ACM, New York, NY, USA, 2 pages. <https://doi.org/10.1145/nnnnnnn.nnnnnnn>

1 Introduction

With the adoption of digitization at a large scale, the demand to digitally identify entities in a correct, efficient, secure, and interoperable way became paramount. This holds for individuals, but also organizations, services, applications, and devices. A *digital identity* is a representation of an actual entity in the digital world [8]. In this context, privacy and security are fundamental. To give some examples, *authentication*, *authorization* and *access control* should restrict entities from accessing services they are allowed to (e.g., they pay for), *anonymity* of entities accessing some online services should sometimes be maintained (e.g., the real identity of a buyer of an art piece at an auction), *confidentiality* and *minimal disclosure* should be enforced (e.g., to vote, one needs to prove that a person is major of age, but not necessarily disclose the exact age).

In Europe, Electronic IDentification, Authentication, and trust Services (eIDAS) regulates electronic identification (eID), to allow and secure access to online services within the EU and EEA countries [3–5]. For a natural person, the mandatory identity attributes are the *Current Family Name*, *Current First Names*, *Date of Birth*, and *Unique Identifier*, while optional attributes include *FirstNames at Birth*, *Family Name at Birth*, *Place of Birth*, *Current Address*, *Gender*, *Phone no.*, *E-mail Address*, etc. [2, 3]. Digital identification benefits of high attention in Europe nowadays also because of the EU Digital Identity Wallet, which is planned for full adoption across EU member states by 2026 [4].

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
Conference'17, Washington, DC, USA

© 2025 Copyright held by the owner/author(s). Publication rights licensed to ACM.
ACM ISBN 978-x-xxxx-xxxx-x/YYYY/MM
<https://doi.org/10.1145/nnnnnnn.nnnnnnn>

Digital identity management is normally defined as a three-party model: (1) the *end-user* or the *holder*, which possesses a digital identity and wants to perform an action, (2) the *identity provider* or the *issuer*, which enrolls new users, manages digital entities and performs authentication, and (3) the *service provider* or the *verifier*, which provides services to the end-user, and relies on the identity provider to verify the identity of the end-user [8].

A blockchain is a type of *Distributed Ledger Technology (DLT)* with cryptographic enhancements, which is *distributed* (it is spread between multiple nodes, each node stores a copy of the blockchain) and *decentralized* by design (it is not a single point of decision, but the decision is a result of a consensus of the nodes) [8]. Identity management solutions on blockchain benefit from the transparency, security, and immutability of the underlying blockchain technology [2]. By construction, blockchains eliminate the necessity of a single point of trust or a centralized authority. However, blockchain-based solutions must be treated with care. In particular, sensitive information should not be stored on-chain, not even in encrypted form.

2 Previous work

Our previous research looks at the security of digital identities using blockchain technology. The goal is to offer users a more secure digital identity experience, allow users to exclusively control their digital identities (enforce *self-sovereignty*), and guarantee the connection between the user's physical identity and their digital identity. Our main contributions are as follows.

- (1) Present the state-of-the-art for identity management (IdM) on blockchain, analyze and compare the existing solutions in terms of security and privacy [7, 8];
- (2) Leverage the digital identity domain by practical usage of privacy-preserving techniques like Zero-Knowledge (ZK) proofs along with the blockchain technology [6];
- (3) Look into an identity management solution on Arweave, a solution specialized in permanent storage [2].

3 Ongoing research - IdM on Arweave

Arweave [1] emerged as a decentralized platform designed for permanent storage of digital information, ensuring long-term data availability. We explore the possibilities of building an IdM solution on Arweave, and we consider the regulations and standards related to digital identities in the European Union (EU) [3, 4, 9]. We consider three phases: **Phase 1 - Setup and registration**, **Phase 2 - VCs and zk-proofs generation**, and **Phase 3 - Identity verification** [2].

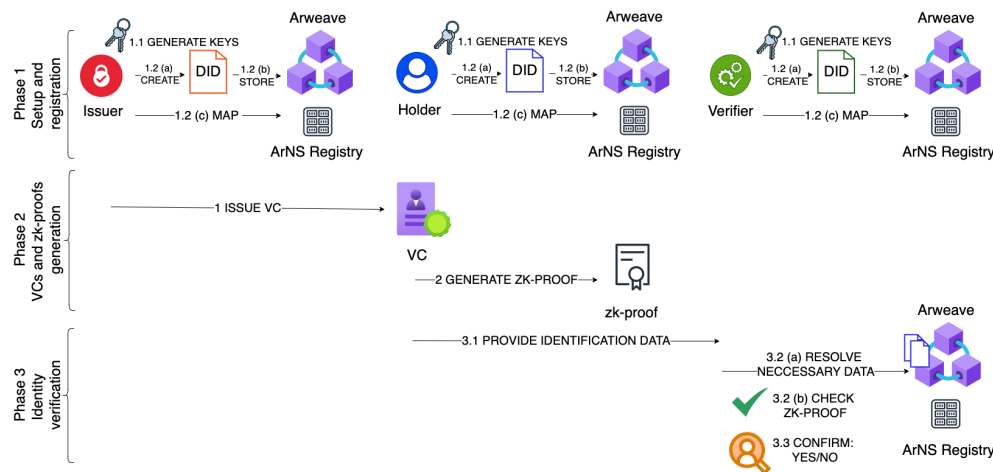


Figure 1: Overview of IdM framework on Arweave [2]

Phase 1 deals with the setup and registration of the parties. Each entity generates a public-private key pair, creates a DID document [2] containing the corresponding public key, and stores the DID document on Arweave [2]. Each entity can register a name within the ArNS Registry [2] and map the ArNS name to the Arweave transaction ID that corresponds to the DID document.

Phase 2 is responsible for generating the verifiable credentials (VCs) and the zk-proofs that attest identity claims. The issuer uses the BBS(+) signature scheme [10] to sign the holder’s credentials and generates the holder’s credentials, which contain one or more attributes and their certification. The VC also contains the public key of the holder. The issuer signs the credential using the BBS(+) signature scheme. The signature will be embedded in the proof field of the VC, which is transmitted securely to the holder. The VC holder generates a zk-proof for a specific claim [2].

Phase 3 deals with the verification of identity claims. First, the holder provides the verifier with the ArNS name and the zk-proof computed on the VC data. Second, the verifier checks the validity of the claims provided [2]. The verifier retrieves the holder’s DID document from Arweave through the ArNS, which resolves to the transaction ID corresponding to the DID Document. The verifier further checks the zk-proof to validate the claim. The verifier confirms whether the user’s identity claim is valid or not based on previous verifications [2].

4 Future work and Conclusion

A detailed analysis of the security and privacy aspects of this solution, along with detailed implementation insights and an experimental evaluation of a fully operational system, is subject to future work. Beyond the specific use case of IdM, one can explore the potential of Arweave for other applications, assessing its limitations, and gaining a deeper understanding of its strengths. Another possible line of work relates to the anonymity of identity or service providers. Although most of the solutions implement minimal disclosure on the user side, there is currently only minimal work on enforcing privacy at the other end. For example, hiding the national

authority that issued the credentials might be necessary to hide the exact nationality of a European citizen.

Acknowledgments. This work was supported by a private scholarship offered by EntityC Consulting SRL to the first author. This work was supported by a grant of the Ministry of Research, Innovation and Digitalization, CNCS/CCCDI - UEFISCDI, project number ERANET-CHISTERA-IV-PATTERN, within PNCDI IV.

References

- [1] Arweave. [n. d.]. Meet Arweave: Permanent information storage. <https://arweave.org>. Last Accessed: August 2024.
- [2] Andreea Elena Drăgnoiu and Ruxandra F Olimid. 2024. Towards an identity management solution on Arweave. *arXiv preprint arXiv:2412.13865* (2024).
- [3] eIDAS Technical Sub-group. 2023. eIDAS Cryptographic Requirements for the Interoperability Framework. <https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/eIDAS+eID+Profile>. Last Accessed: August 2024.
- [4] European Commission. 2024. The EU Digital Identity Framework Regulation Enters into Force. <https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/The+Digital+Identity+Regulation+Enters+into+Force>. Last Accessed: November 2024.
- [5] European Union. 2023. Regulations of the European Parliament and of the Council amending Regulation (EU) No.910/2014 as regards establishing the European Digital Identity Framework. <https://data.consilium.europa.eu/doc/document/PE-68-2023-REV-1/en/pdf>. Last Accessed: September 2024.
- [6] Andreea-Elena Panait and Ruxandra F. Olimid. 2021. On Using zk-SNARKs and zk-STARKs in Blockchain-Based Identity Management. In *Innovative Security Solutions for Information Technology and Communications*, Diana Maimut, Andrei-George Oprina, and Damien Sauveron (Eds.). Springer International Publishing, Cham, 130–145.
- [7] Andreea-Elena Panait, Ruxandra F. Olimid, and Alin Stefanescu. 2020. Analysis of uPort Open, an Identity Management Blockchain-Based Solution. In *Trust, Privacy and Security in Digital Business*, Stefanos Gritzalis, Edgar R. Weippl, Gabriele Kotsis, A. Min Tjoa, and Ismail Khalil (Eds.). Springer International Publishing, Cham, 3–13.
- [8] Andreea-Elena Panait, Ruxandra F. Olimid, and Alin Stefanescu. 2020. Identity Management on Blockchain – Privacy and Security Aspects. In *PROCEEDINGS OF THE ROMANIAN ACADEMY, Series A*, Vol. 21. 45–52. <https://acad.ro/sectii2002/proceedings/doc2020-1/06-Panait.pdf>
- [9] Regulation (EU) 2016/679. [n. d.]. General Data Protection Regulation GDPR. <https://gdpr-info.eu/>. Last Accessed: October 2024.
- [10] Stefano Tessaro and Chenzhi Zhu. 2023. Revisiting BBS signatures. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 691–721.