ChorSSI: A Model-Driven Framework for Self-Sovereign Identity on Blockchain

(Oral Communication)

T. Cippitelli[1] A. Marcelletti[1] and A. Morichetta[1]

University of Camerino, Camerino, Italy
tommaso.cippitelli@studenti.unicam.it,{alessand.marcelletti, andrea.morichetta}@unicam.it

In the digital age, the continuous increment of connected services and technologies has led identity to become a critical aspect of online activities [1]. Indeed, we increasingly rely on digital platforms for communication, commerce, and other activities. Therefore the need for secure and reliable methods for identifying people has become more important than ever [13]. To address this challenge, different identity management systems were developed to manage digital identities and their interconnection [12]. However, those systems are often centralised [2] and require the involvement of third parties that must be trusted [6]. Unfortunately, such solutions can create security vulnerabilities like data breaches and identity fraud [3].

A promising alternative to traditional identity management systems is certainly Self-Sovereign Identity (SSI). SSI is a decentralised identity model that provides individuals control over their personal data and allows them to share this data securely and selectively with other parties, without having to rely on a single central authority [4]. This is possible thanks to blockchain, which is the underlying technology on which SSI systems are usually built on top of [5]. This integration provides a secure and tamper-proof distributed ledger to store and manage identity information [13]. To enable the information sharing, SSI relies on Verifiable Credentials (VCs), which are digital representations about an individual, organisation, or thing and they are issued by trusted parties and can be cryptographically verified [11].

Typical operations of SSI systems are related to the issuing and verification of VCs. These operations are done by the actors that interact with an SSI system and can play three roles: a **holder** who controls one or more VCs, an **issuer** who creates new VCs, and a **verifier** who receives the credentials to be verified [9]. Another key aspect of SSI is the confidentiality of interactions between actors, which is ensured by the Zero Knowledge Proof (ZKP) cryptographic protocol, allowing the holder to prove the validity of a statement to an issuer without sharing the underlying information [7]. ZKP enhances user privacy while maintaining the necessary institutional trust for the correctness of digital interactions and represents one of the key benefits of SSI.

While the concept of SSI is relatively new, there has been growing interest in the development of SSI systems and applications. Indeed, building SSI systems can be complex and challenging, particularly for non-expert users that have to learn different concepts and technologies, founding a barrier to its development [8]. For this reason, to simplify the development process, there is a need to integrate a low-code strategy that would make the development process more accessible to a wider range of developers, enabling the creation of SSI systems.

In this work, we propose ChorSSI, a model-driven framework supporting the creation and execution of an SSI system. To support the design, we use the BPMN choreography diagrams. These models enable the representation of the interactions between different and distributed parties that collaborate to reach a common goal from a high-level perspective, without the need of exposing their internal behaviours. Indeed, a choreography diagram only needs to define the

message exchange between the participants of a system, determining the overall execution flow [10].

In our proposal, each step defined in the choreography model is connected to an SSI-specific operation, directly matching the actors responsible for concluding a certain task. This approach enables users to design and develop typical scenarios using SSI operations in a black-box approach, allowing them to better focus on the complexity of the real-world use cases rather than the underlying technology.

The first phase of ChorSSI is the **Initialisation**, which creates the necessary infrastructure and components such as the public ledger, agents and the user application for interaction. During the **Modelling** phase, the choreography representing the SSI system and the communication among parties is designed. This model is then taken in input during the **Generation** phase to create the (i) connections among agents (through endpoints referral) and (ii) the templates for issuing and verification of credentials. Once the software infrastructure is generated, the last phase concerns the **Running** one in which the involved parties can execute the different operations according to the starting choreography which provides a graphic interface enforcing also the correct flow. During this phase, each user can perform each specific SSI action by interacting with the model that automatically invokes the previously generated code.

References

[1] D.S. Baars. Towards self-sovereign identity using blockchain technology, October 2016.

[2] Eranga Bandara, Xueping Liang, Peter Foytik, Sachin Shetty, and Kasun De Zoysa. A blockchain and self-sovereign identity empowered digital identity platform. In *2021 International Conference on Computer Communications and Networks (ICCCN)*, pages 1–7. IEEE, 2021.

[3] Rafael Belchior, Benedikt Putz, Guenther Pernul, Miguel Correia, André Vasconcelos, and Sérgio Guerreiro. Ssibac: self-sovereign identity based access control. In *International Conference on Trust, Security and Privacy in Computing and Communications*, pages 1935–1943. IEEE, 2020.

[4] Uwe Der, Stefan Jähnichen, and Jan Sürmeli. Self-sovereign identity − opportunities and challenges for the digital revolution. *arXiv preprint arXiv:1712.01767*, 2017.

[5] Md Sadek Ferdous, Farida Chowdhury, and Madini O Alassafi. In search of self-sovereign identity leveraging blockchain technology. *IEEE access*, 7:103059–103079, 2019.

[6] Andreas Grüner, Alexander Mühle, Tatiana Gayvoronskaya, and Christoph Meinel. A comparative analysis of trust requirements in decentralized identity management. In *International Conference on Advanced Information Networking and Applications*, pages 200–213. Springer, 2020.

[7] NV Kulabukhova. Zero-knowledge proof in self-sovereign identity. In *CEUR Workshop Proceedings*, volume 2507, pages 381–385, 2019.

[8] Sarah Manski. Distributed ledger technologies, value accounting, and the self sovereign identity. *Frontiers in Blockchain*, 3:29, 2020.

[9] Alexander Mühle, Andreas Grüner, Tatiana Gayvoronskaya, and Christoph Meinel. A survey on essential components of a self-sovereign identity. *Computer Science Review*, 30:80–86, 2018.

[10] OMG. Business process model and notation (bpmn). url=https://www.omg.org/spec/BPMN/2.0/PDF/, 2011.

[11] Johannes Sedlmeir, Reilly Smethurst, Alexander Rieger, and Gilbert Fridgen. Digital identities and verifiable credentials. *Business & Information Systems Engineering*, 63(5):603–613, 2021.

[12] Andrew Tobin and Drummond Reed. The inevitable rise of self-sovereign identity. *The Sovrin Foundation*, 29(2016):18, 2016.

[13] Dirk Van Bokkem, Rico Hageman, Gijs Koning, Luat Nguyen, and Naqib Zarin. Self-sovereign identity solutions: The necessity of blockchain technology. *arXiv preprint arXiv:1904.12816*, 2019.