Department: Head
Editor: Name, xxxx@email

Signing Blockchain Transactions using Qualified Certificates

Muhamed Turkanović
University of Maribor, Faculty of Electrical Engineering and Computer Science

Blaž Podgorelec
University of Maribor, Faculty of Electrical Engineering and Computer Science

***Abstract*—Blockchain technology is increasingly being considered among both private enterprises and public services. However, it poses a challenge with regard to aligning its identity management scheme with the Public Key Infrastructure and the Qualified Digital Certificates issued by Qualified Trust Service Providers. To solve this challenge, we will present a solution in the form of an architecture reference model, which enables enterprises and public services to leverage blockchain technology by integrating Qualified Electronic Signatures with blockchain transactions. The evaluation of the architecture reference model is provided through the design of a Blockchain-based Trusted Public Service and a use-case scenario example. The proposed architecture reference model is based on the CEF building blocks EBSI, eSignature, and eID compliant with eIDAS.**

BLOCKCHAIN TECHNOLOGY is becoming increasingly popular in the scientific and professional community outside the realm of cryptocurrencies. As a consequence, we are witnessing numerous new uses cases of blockchain within various domains, from finance and insurance to the public sector and elsewhere [1]. However, one significant problem has hampered it: the identity management layer. Regardless of the blockchain network type and blockchain platform, these typically apply Public-Key Cryptography (PKC) for the user identity management layer, which includes user representation and management of user-related blockchain operations. It is crucial to highlight that there are various blockchain platforms at the moment (e.g., Hyperledger Besu, Hyperledger Fabric), whereby each has its blockchain client implementation, and each utilizes different PKC methods for the identity management layer. Depending on the blockchain service requirements, a permissionless (i.e., public) or permissioned blockchain network can be formed [2]. In this work, we limit ourselves to permissioned blockchain net-

 Published by the IEEE Computer Society

works and related blockchain platforms. When considering enterprise use-cases expected to be implemented using permissioned blockchain networks, the Hyperledger Besu [3] and the Hyperledger Fabric [4] blockchain clients are currently one of the most utilized and recognized by enterprises. For instance, both platforms are specified in the first version of the European Blockchain Services Infrastructure (EBSI) specifications [5]. The aim of EBSI is to deliver the European Union (EU) cross-border public services deployed on the blockchain network with nodes distributed across the EU Members States running both Hyperledger Besu and Fabric clients. Considering the application of PKC methods, Hyperledger Besu utilizes the Elliptic Curve Cryptography (ECC), whereby Fabric utilizes ECC, as well as the Rivest-Shamir-Adleman (RSA) crypto-system [6]. Therefore, an issue of interoperability among different blockchain platforms on the identity management layer exists. Consequently, users have to use distinct identities for each blockchain platform they might be involved in. Furthermore, a significant but even more complex obstacle persists: How to associate a user's blockchain digital identity with a real-world entity (natural or legal), and consequently, enable all blockchain operations (i.e., blockchain transactions) performed by the user to have a legal effect? Such a requirement would be crucial in cases where blockchain-related services have to be involved with public services (e-government), where Qualified Digital Certificate are required. Typical examples are services (i.e., Notarisation, Diplomas, European Self-Sovereign Identity, and Trusted Data Sharing) implemented on EBSI. To the best of our knowledge, no such blockchain platform currently exists, which would utilize Qualified Digital Certificates for their user-related operations.

Due to the R&D activities of our laboratory, we came to a potential solution for the above-mentioned challenges, in the form of an architecture reference model, which enables Qualified Digital Certificates to be integrated with blockchain transactions regardless of the permissioned blockchain platform used. The proposed architecture reference model enables electronic public services to leverage blockchain technology and improve user experience. It supports the use of previously proven and implemented trust services within the blockchain, without the need for replacing the current user procedures, while also enabling the Once Only Principle (OOP) [7], which reduces the administrative burden for individuals and businesses when using blockchain technology.

BUILDING BLOCKS

We now present the concepts of the main building blocks of the architecture reference model and give examples for their existing implementations, including the Connecting Europe Facility (CEF) building blocks [8] such as EBSI, eID [9], and eSignature [10].

A high-level architecture of the reference model is depicted in Figure 1, using the C4 model for visualizing software architecture. The System Landscape view reveals the relations between individual reference model building blocks.

PERMISSIONED BLOCKCHAIN NETWORK - EBSI

Within permissioned blockchain networks, only defined and allowed nodes can participate in the process of reaching the consensus mechanism. In some cases, also writing to and reading from the blockchain ledger using the user's blockchain identity is limited only to a set of known members. Such network types are meaningful when implementing enterprise or public sector related use cases. Such use cases typically require some degree of trust between a set of members (e.g., organizations, companies, government entities). The reason for the utilization of blockchain technology in such use cases is to increase the level of trust to the highest possible degree. Furthermore, the permissioned blockchain networks are also enterprise-friendly due to their negligible energy consumption (i.e., it uses proof-of-authority rather than proof-of-work distributed consensus algorithms), zero transaction costs, efficiency in terms of scalability and speed, etc. Due to its properties, the permissioned blockchain network is also referred to as the consortium, or public-permissioned blockchain network [11].

The European Blockchain Services Infrastructure (EBSI) is materialized as a public permissioned blockchain network. Blockchain nodes

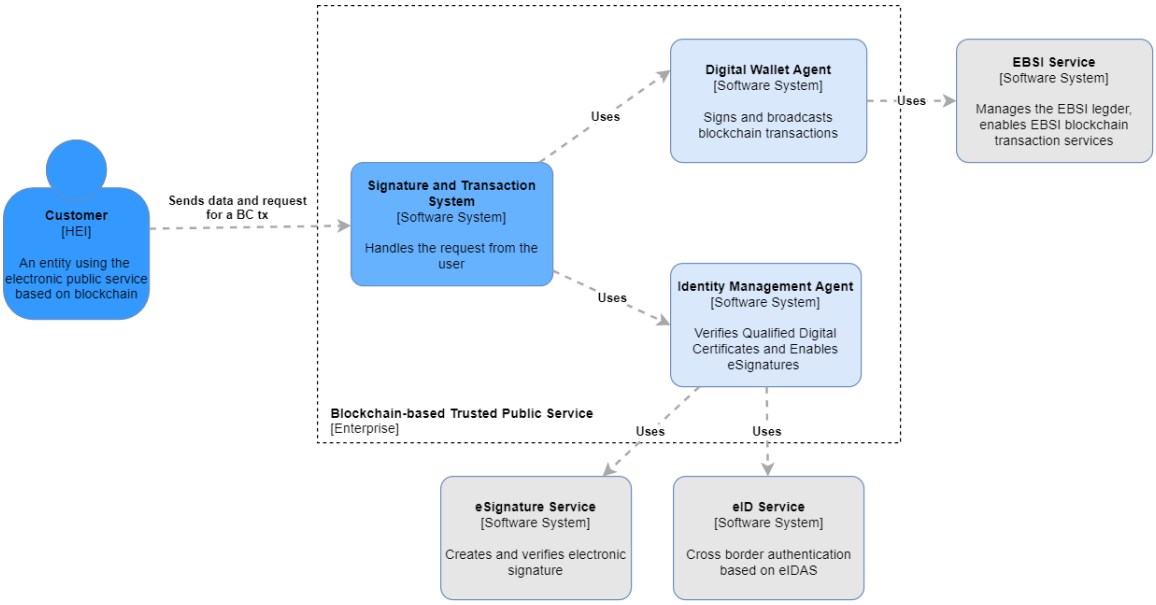

Figure 1. System Landscape Diagram of the Architecture Reference model.

involved in the process of achieving consensus are defined as a set of equal members, where each EU Member State is represented with at least one node running dedicated Hyperledger Besu and Fabric blockchain clients. Reading from the blockchain is expected to be available to the public. In contrast, writing to the blockchain is expected to be possible only for blockchain users with identities under certain conditions [5]. The idea of running multiple blockchain clients is probable in the sense that EBSI does not prioritize only one blockchain platform, hence leverage those, which are most technically advanced and used by enterprises by now. To the best of our knowledge, it is also not a de-facto last decision of EBSI to leverage only these two blockchain clients, meaning that others may join in the future.

IDENTITY MANAGEMENT - eID AND eSIGNATURE

According to the NIST Digital Identity Guidelines [12], a description of a digital identity is still widely internationally discussed without a specific definition. Generally, a digital identity is an online persona of an entity that can, in many ways, represent itself online. Furthermore, when considering digital identity as a legal identity, the definition is additionally complicated. A digital identity does not represent any real-world legal entity by default. To achieve the highest assurance level in electronic identification, there is a requirement to establish trust that the digital identity is, in fact, a real-world entity (natural/legal). The aforementioned trust can be achieved by implementing procedures and trust services as identity verification and authentication, which in technical terms are based on Qualified Digital Certificates.

A Qualified Digital Certificate (QDC) is a digital certificate issued by a Qualified Trust Service Provider (QTSP) that ensures the authenticity and data integrity of an Electronic Signature and its accompanying message. The QTSP can be a government authority or other identification-capable entity approved by the government. On a technical level, the features of QDC are enabled by the utilization of public-key infrastructure (PKI), which defines the usage of certificates (e.g., X.509) and cryptographic methods (e.g., RSA, ECC) [13]. Within the issuing process of a QDC, the QTSP is obligated to perform specified identity verification procedures, which bind a digital identity (i.e., QDC) with a real-world entity (natural or legal). A list of all QTSP is publicly available in order to enable the verification of Qualified Electronic Signatures (QES) created on the basis of a QDC [10], [14]. A QDC holds enough information to guarantee that a digital

signature (i.e., QES) created by QDC has an equivalent legal effect as a handwritten signature.

To enable a QDC issued by a QTSP from one EU Member State to be legally used in all other EU Member Countries, the CEF eID building block, including the eID schemes mandated by eIDAS regulation, was designed. Using this building block, public or private entities denoted as Service Providers can extend their online services to all EU citizens [9], [14]. This enables EU citizens or service providers (private or public) to validate every individual QDC, through the eIDAS network support, and the aforementioned CEF eID building block [9].

The term electronic signature usually also refers to its corresponding term: the digital signature. Based on the eIDAS regulation, three levels of electronic signature exist: (1) Simple Electronic Signature (SES), (2) Advanced Electronic Signature (AdES), and (3) Qualified Electronic Signature (QES). The latter is the most advanced electronic signature by the level of trust that can be achieved with its use. Such an electronic signature can be created by using a QDC, as described above. QES is used to enable businesses, citizens, and public authorities to perform secure and legally binding electronic transactions. Every QES can be cryptographically validated to determine whether the certificate, which was used to produce this QES is qualified or not and if the integrity of the accompanying message and/or attached data is intact [10], [14].

In the case of the EU, the utilization of the CEF eSignature building block provides users and service providers the ability to create and verify QES in line with EU laws and standards [9], [10].

The main difference between blockchain-based and conventional, non-blockchain-based ICT systems (e.g. online banking) is that all operations performed by users within the blockchain-based system must be digitally signed. This implies that every user owns a blockchain digital identity. If the users use various blockchain-based systems that operate on top of different blockchain platforms, they need to control and maintain multiple blockchain digital identities. Moreover, these digital identities are not designed to be interoperable. Blockchain digital identities are based on PKC and platform related PKI, where each digital identity is controlled by a private key known only to the user. Blockchain identities are often managed with a digital wallet, whose primary purpose is to facilitate users to control their blockchain-based digital identities in a user-friendly manner. Indeed, the main feature of a digital wallet is to support the process of the digital signing of blockchain transactions [15].

EBSI incorporates two distinct blockchain platforms. Hyperledger Besu is an enterprise design and implementation of the Ethereum blockchain platform, where blockchain identities are presented via a 42 long character address. This address is based on a 128 character long public key, acquired by the utilization of an ECC cryptosystem, specifically by the Elliptic Curve Digital Signature Algorithm (ECDSA) secp256k1 curve. A public key is generated from a 64 character long private key. Based on the protocol previously described, the address can be determined by a private key, while the private key cannot feasibly be determined from the address. An initial Hyperledger Besu node of the blockchain network is classified as the network owner. With its generated blockchain identity, it has the authority to define addresses that have permission to participate in a network consensus protocol and/or read and/or write from/into the blockchain [5], [15]. By contrast, the Hyperledger Fabric blockchain identity is presented with an X.509 certificate, primarily generated by an ECC PKC cryptosystem, specifically by an ECDSA prime256v1 curve – while other curves are also possible (i.e., secp384r1, secp521r1). The base of the Hyperleder Fabric identity management layer is a Fabric root CA X.509 certificate, controlled by the first node of the blockchain network. The Fabric root CA later serves as a ”Root of Trust”, and has the authority to specify the permissions (i.e., consensus, read, write) regarding other digital certificates used in the blockchain network. When considering the different identity management systems of Hyperledger Besu and Fabric, we can conclude that EBSI uses two distinct identity management systems, which are fundamentally not interoperable, as well as not aligned with the QDC [5], [15].

The aforementioned digital identity and trust service mechanisms are all part of the proposed architecture reference model, which enables the usage of QDC in a permissioned blockchain net-

work. Furthermore, the examples used in the descriptions are aligned with the policies described in Regulation (EU) No. 910/2014 (eIDAS) defined by the European Parliament of the Council [14].

REFERENCE MODEL ARCHITECTURE

The following section presents the architecture of the proposed reference model. We evaluate it by proposing a software architecture for a Blockchain-based Trusted Public Service (Figure 1), i.e., an electronic public service, which takes advantage of blockchain technology, regardless of the blockchain platform used. The core principle of the architecture reference model is its feature to enable blockchain transactions to be digitally signed using QDC. This implies that organizations can take advantage of blockchain technology, including the domain of public services, while not having to manage additional (blockchain) digital identities, as well as install and use dedicated software (e.g., a wallet) for managing these digital identities.

The architecture reference model consists of several identity trust building blocks, which allow blockchain-based services to achieve a high identity assurance level. In the case of the EU, the architecture reference model can take advantage of the EBSI service by incorporating the identity trust building blocks provided by CEF, including an eSignature and eID, capable of EU cross-border identification depending on the eIDAS network as the infrastructure consisted of all EU Member States QTSP. The implementation of the reference model empowers trust that a QES attached to an online transaction (i.e., blockchain transaction) can be verified and validated by a QTSP to guarantee a strong association between the user's digital identity with his real-world entity (natural/legal) [10], [14]. This furthermore implies that a digitally signed blockchain transaction by means of QDC has a legal effect similar to a handwritten signature.

For the sake of evaluating the architecture reference model, we analyzed it using the dynamic container diagram of the C4 software architecture model, which is depicted in Figure 2. The C4 dynamic diagram depicts, on a high-level shape, the communication and collaboration activities, and the responsibilities of the core elements of the proposed software architecture.

The Blockchain-based Trusted Public Service must set up three core Software Systems: (1) **Signature and Transaction System**, (2) **Identity Management Agent**, and (3) **Digital Wallet Agent**. These systems, in order to utilize the idea of the architecture reference model and enable high identity assurance level, must be connected with the CEF Building Blocks, i.e., EBSI, eID, and eSignature. The Signature and Transaction System is in charge of the graphical user interface (GUI) and handling the user interactions through the Service controller. It gathers the content from the user through the GUI, which will be processed as blockchain transaction into the permissioned blockchain network (i.e., EBSI), as well as mediate the processes of authentication and electronic signature for the user. The Identity Management Agent processes the authentication and electronic signature functionalities by communicating with the CEF identity trust building blocks (eID and eSignature). It includes the validation of the user's QDC, as well as the creation of a QES for a prepared blockchain transaction. The Digital Wallet Agent processes the blockchain transaction generation, its signing and broadcasting using the EBSI service.

QUALIFIED BLOCKCHAIN TRANSACTION AND THE EBSI DIPLOMA USE-CASE

In this section, the architecture reference model will be evaluated with the example of a diploma use-case defined by EBSI. An EBSI-permissioned blockchain service is used as a building block by the Blockchain-based Trusted Public Service. The overview of the use-case process can be followed via Figure 2.

As part of the diploma-use case, the issuance of a diploma with a blockchain-based service by a Higher Education Institution (HEI) from an EU Member State A to a Student from a Member State B is covered, as well as the verification of the blockchain issued diploma by an Employer from an EU Member State C. A prerequisite, that the diploma can be issued or verified, is that the HEI must at least own a QDC issued by a QTSP from the EU.

An HEI begins the process of diploma issuance by navigating towards the Blockchain-

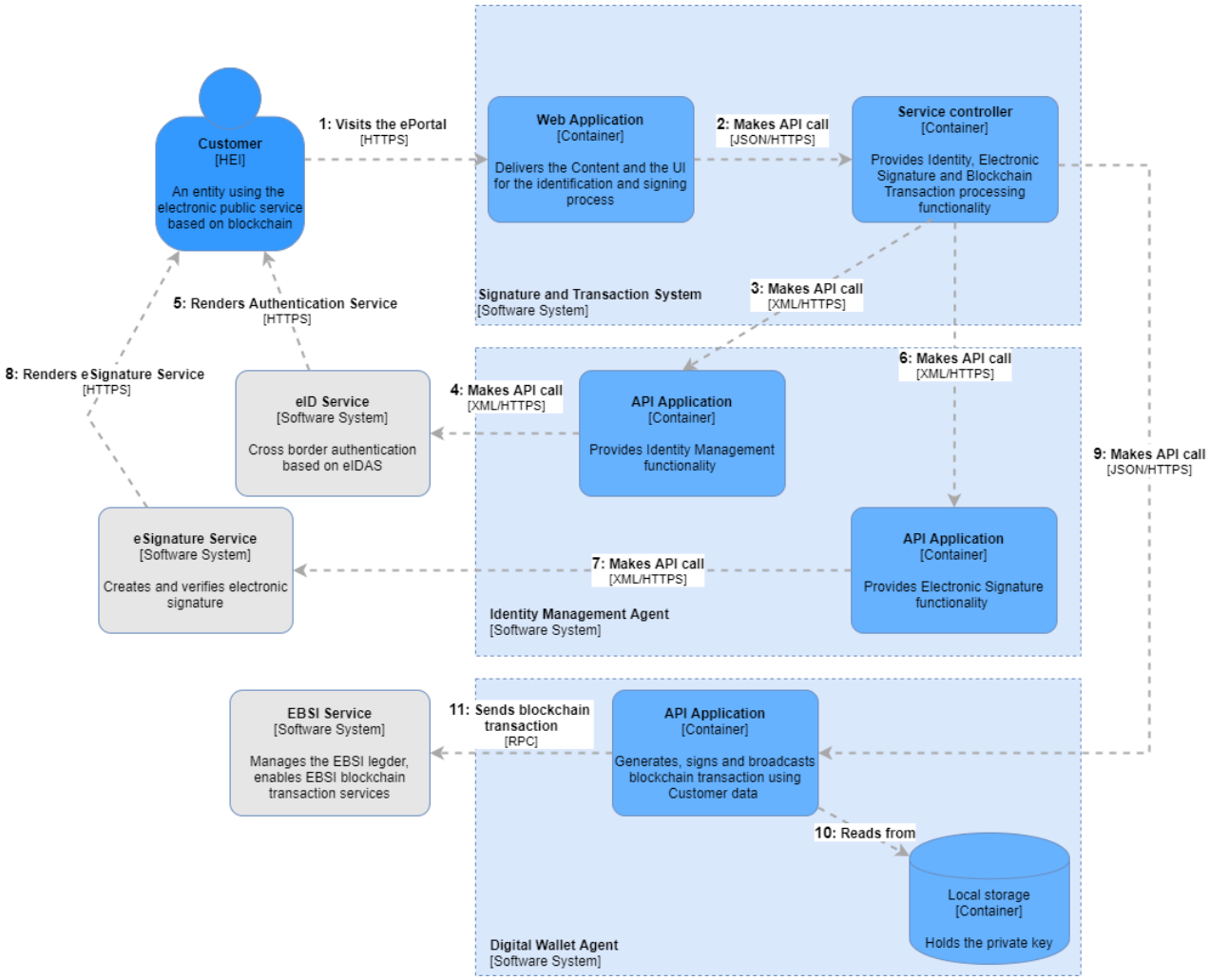

Figure 2. Dynamic Container Diagram of the proposed Architecture Reference Model.

based Trusted Public Service, more precisely its Web Application container (step 1 Figure 2). The Signature and Transaction System enables the HEI to upload and process the digital diploma document including the identifier of the student to which the diploma is issued. The whole process is controlled by the Service controller container, through the GUI of the Web Application (step 2, Figure 2). The Identity Management Agent validates both the HEI and the identifier of the student through the eID service and their QDC. As mentioned, this is controlled by the Service controller (step 3, Figure 2), which uses the Identity Management Agent's API Application to call the external eID Service (step 4-5, Figure 2). After that, the Identity Management Agent offers the prepared data to the HEI, which will be included in the blockchain transaction, to be digitally signed with the help of the eSignature service (step 6-8, Figure 2). After the HEI produces a QES with its QDC, this is passed to the Digital Wallet Agent (step 9, Figure 2), which generates a blockchain transaction with the digitally signed prepared data. The blockchain transaction, including the digitally signed student diploma with the QES of the HEI, is then signed by the private key of the Blockchain-based Trusted Public Service (securely held in the local storage of the Digital Wallet Agent; step 10, Figure 2) and broadcasted to the blockchain network through the EBSI service (step 11, Figure 2). It should be noted that the Blockchain-based Trusted Public Service enables the generation, signing and broadcasting of the blockchain transaction towards, and

in compliance with any of the EBSI supported blockchain clients (i.e. Hyperledger Fabric or Besu). The digitally signed blockchain transaction thus proves the authenticity and integrity of the diploma data on the eID highest trust level, as well as the fact that it was processed through the Blockchain-based Trusted Public Service. The HEI can now send the diploma document to the student in any digitally accessible manner. After the blockchain transaction initiated by the HEI is irreversibly executed and confirmed, the student can provide their diploma to an employer from an EU Member State C. With the usage of the Blockchain-based Trusted Public Service, an employer can validate the integrity and authenticity of the received digital diploma.

CONCLUSION

To remedy the gap between a blockchain-related ICT environment and those from classic ICT environments, which require Qualified Electronic Signatures, we propose an architecture reference model, which would facilitate their integration. We evaluate it through the proposed design of a Blockchain-based Trusted Public Service and a use case scenario related to the EBSI diploma. As future work, and as soon as the EBSI Service (v2) will be available in the production phase, the Blockchain-based Trusted Public Service will be validated in terms of efficiency, scalability and privacy. The architecture reference model will be proposed as part of the CEF building blocks.

ACKNOWLEDGMENT

This work was funded by the Slovenian Research Agency (research core funding No. P2-0057), and also in part by EC H2020 Project CONCORDIA G.A. No. 830927, and EC H2020 Project DE4A G.A. No. 870635.

REFERENCES

1. Casino, F., Dasaklis, T. K., and Patsakis, C. (2019). A systematic literature review of blockchain-based applications: current status, classification and open issues. Telematics and Informatics, 36, 55-81.
2. Helliar, C. V., Crawford, L., Rocca, L., Teodori, C., and Veneziani, M. (2020). Permissionless and permissioned blockchain diffusion. International Journal of Information Management, 54, 102136.
3. Hyperledger Besu. [Online]. Available: https://github.com/hyperledger/besu (URL)
4. Hyperledger Fabric. [Online]. Available: https://github.com/hyperledger/fabric (URL)
5. CEF Digital – European Blockchain Services Infrastructure (EBSI). [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI (URL)
6. Fernández-Caramès, Tiago M., and Paula Fraga-Lamas. "Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks." IEEE Access 8 (2020): 21091-21116.
7. CEF Digital – Once Only Principle. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Once+Only+Principle (URL)
8. CEF Building Blocks. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Building+Blocks (URL)
9. CEF Digital – eID. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eID (URL)
10. CEF Digital – eSignature. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eSignature (URL)
11. W. Wang et al., "A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks," in IEEE Access, vol. 7, pp. 22328-22370, 2019
12. Grassi, Paul A., M. Garcia, and J. Fenton. "DRAFT NIST Special Publication 800-63-3 Digital Identity Guidelines." National Institute of Standards and Technology, Los Altos, CA (2017).
13. P. Dunphy and F. A. P. Petitcolas, "A First Look at Identity Management Schemes on the Blockchain," in IEEE Security & Privacy, vol. 16, no. 4, pp. 20-29, July/August 2018, doi: 10.1109/MSP.2018.3111247.
14. European Union, "REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC". European Union, 2014.
15. Storublevtcev, N. (2019, July). Cryptography in Blockchain. In International Conference on Computational Science and Its Applications (pp. 495-508). Springer, Cham.

Muhamed Turkanović , PhD is the Head of Research and Development of the Blockchain Lab:UM, an Assistant Professor at the Institute of Informatics at the University of Maribor (UM), Faculty of Electrical

Engineering and Computer Science, Head of Operations at the Digital Innovation Hub UM, UM's coordinator of the H2020 project DE4A - Digital Europe for All.

Blaž Podgorelec is a member of the Blockchain Lab:UM and a PhD Student at the University of Maribor, Faculty of Electrical Engineering and Computer Science, with the primary research focus on blockchain technologies, UM's representative for the H2020 projects CONCORDIA and DE4A - Digital Europe for All.