[1.]R–V. BRĂCĂCESCU, [2.]Carmen BRĂCĂCESCU, [2.]Oana–Diana CRISTEA

ASPECTS REGARDING IDENTITY MANAGEMENT USING BLOCKCHAIN

[1.]Politechnica University Bucharest, Bucuresti, ROMANIA
[2.]INMA Bucharest, ROMANIA

Abstract: In order to develop technologies that capitalize on the concept of digital identity, it is necessary to increase the security of the systems, their decentralized character, the immutability and the control of the user to his private data. A digital identity management model is traditionally interpreted as a tripartite model consisting of an end–user, an identity provider and a service official. The latest and most modern model is the Self–Sovereign Identity (SSI) model, which no longer uses the identity and service providers and aims the users to regain control over their identities, gives them the opportunity to share only the data they want to share and facilitates access to various services and applications. The article presents the major models of identity management, focusing on the recent approach, namely SSI, which operates blockchain technology and its advantages.

Keywords: identity management, models, blockchain, self–sovereign identity, decentralized

INTRODUCTION

Digital identity is the representation of an entity (a person, an organization, a device) in the digital environment and consists of a unique identifier and other associated attributes. The evolution of digital identity and identity management models over time has been based on meeting three main requirements: security (data of user identities must be protected), control (the holder of digital identity must maintain control over his private data, he decides who can see them, access and for what purpose) and portability (users must be able to use their digital identity any time and not be depend on a specific provider) *(Laurent et al., 2015; White et al., 2019).*

With the advance of information technology more and more applications, services, smart devices appered that require users in one way or another to create an account. This generated to many credentials for users to be able to manage.

It is also important to note that all information about a user associated with an account must be well kept and secured by service providers or products, respecting certains rules of protection and maintaining their privacy. In this regard, the General Data Protection Regulation (GDPR), which includes all aspects of the handling of personal data, for which consent is absolutely necessary, has already been implemented in the European Union since 2018, including very high sanctions for individuals, organizations, companies that do not comply with these provisions.

Globally, identity theft has become one of the most common cybercrimes in the digital world and has led to numerous frauds, causing huge financial losses and, in some cases, escalating to the point where it could endangers people's lives *(Cameron, 2015).*

Taking into consideration all the above, the article presents a new approach to digital identity management, namely, state–of–the–art technology, blockchain.

MATERIALS AND METHODS

A digital identity management model can traditionally be interpreted as a tripartite model consisting of an end user, an identity provider and a service provider.

The end user is the entity that has a digital identity and wants to take different actions using it. The Identity Provider (IdP) is the entity that registers new users, manages digital identities and performs the authentication process. In some cases, it is also possible that the IdP verifies the veracity of the identity provided by the user with the help of an identity card, proof of residence or even with a simple proof of the receipt of an e–mail. The Service Provider (SP) is the entity that provides users with a service, usually a web service, and relies on the IdP to verify their identities.

In the literature *(L'Amrani et al., 2016); Dunphy and Petitcolas, 2018; Goodell and Aste, 2019)* there are mentioned five main identity management models: Isolated Identity Model (Silo), Centralized Identity Model, Federated Identity Model, User–Centric Identity Model and Self–Sovereign Identity Model (SSI).

— **Isolated Identity Model**, illustrated in Figure 1, is a standard identity management model.

It is based on the user's memory in the sense that he needs to know his identity data for each service provider. The user must remember all the identifiers (IDs) and all the credentials (passwords) generated for all the services he wants to benefit from. The attributes associated with identifiers are managed separately by each service provider. The control over the identities belongs entirely to the service providers, they assume the responsibility for each user. Currently, there are a lot of Web services that use the Isolated Identity Model. The disadvantage of this type of model is related to the large number of authentication data, passwords, which a user must store. For this reason, some users prefer to use the same password for multiple accounts, which can lead to security issues.

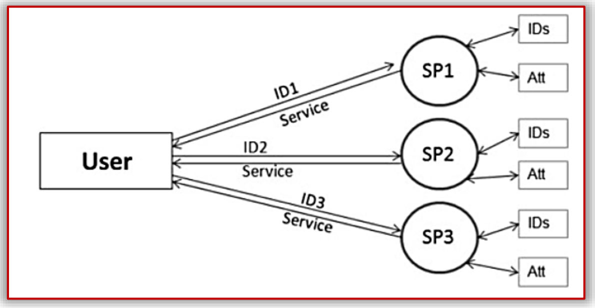

Figure 1 – Isolated Identity Model

- **The Centralized Identity Model** introduces an Identity Provider (IdP) that centralizes the digital identity management process (Figure 2).

The user can authenticate to service providers (SP) using a single identity, with the same credentials, without having to repeat the authentication for each new service provider requested.

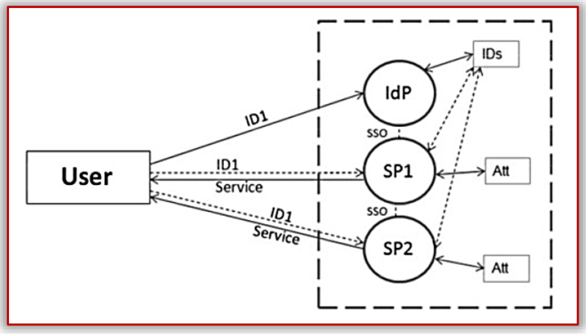

Figure 2 – Centralized Identity Model

This results in the Single–Sign On (SSO) mechanism through which a single authentication instance provides access to all SPs that belong to the same Identity Provider. The ease of use is undeniable compared to the Isolated Identity Model, but the centralized model still has some inconvinients. Disclosing an identifier along with the associated credentials is sufficient to provide unauthorized access to all services. In addition, the centralized layout of this model does not make it suitable for a large number of users or SPs.

- **Federated Identity Model**, illustrated in Figure 3, assumes that IdPs and SPs group together to form a federation of identities and are linked by relationships of trust due to trade agreements and a common technology platforms.

This federation is called the Circle of Trust (CoT). As with the centralized model, SSO mechanisms can be implemented, the user can authenticate once with the IdP to access the services of SPs that are members of the CoT. The user accessing an SP is referred to by the SP under a pseudonym. In fact, all data exchanges between SP and IdP related to a user are based on pseudonyms. The Federated Identity Model is suitable for a large number of uses and SPs, being interesting in the context of distributed and collaborative services. As in the previous model, the user sends the attributes and identifiers of the IdPs, the service providers are obliged to trust them.

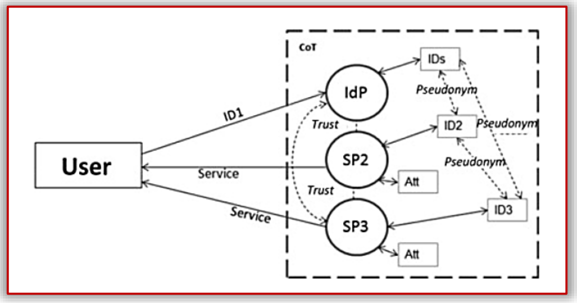

Figure 3 – Federated Identity Model

- **The User–Centric Identity Model** gives the user complete control over his personal attributes.

It has, using an IdP of its choice, an electronic identity portfolio and sometimes an identity selector. Upon request to access the services, the user can select an identity and decide whether to provide certain attributes. Service providers act individually in this model and may, although with some difficulties, provide collaborative services. They are increasingly inclined to propose user authentication, leaving them to decide on the choice of IdP. An example is the case of Yahoo, which offers the possibility to authenticate users using their Facebook or Google account. However, the User–Centric Identity Model still depends on the IdP, is not a complete user–based model, and requires very good integration of all components of the assembly.

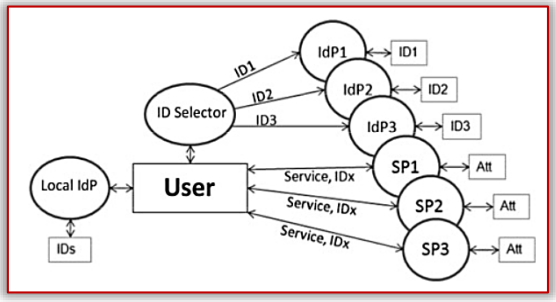

Figure 4 – User–Centric Identity Model [17]

The latest model and the most modern one is the Self–Sovereign Identity (SSI) model. It goes a step further than the user–centric model and eliminates the need for an external identity provider. The end–user gains full control over his identity, being his own identity provider, and because of this, the danger of identity theft is diminished *(Hileman and Rauchs, 2017; Der et al., 2018; Vadapalli, 2020)*.

Regardless of the model, identity management solutions should follow the laws of identity, described by Cameron (2005), an evaluation framework used to identify the pros and cons of digital identity solutions.

This laws suggest that identity information should be disclosed only to legitimate parties, who have this right and only with the user's consent. Moreover, the information collected and stored should be minimal, according to the needs of the service. End–users should be wise to interact with the funds and be aware of the implications of the actions taken. They should be able to share identity information either in private or in public.

From a legal point of view, identity management solutions must respect the data confidentiality and security in accordance with the regulations in force. For example, the solutions that are implemented in European Union countries must comply with the GDPR, a set of data protection policies that appeared in May 2018. Similar principles exist outside Europe, for example, the Digital ID & Authentication Council of Canada (DIACC) has introduced ten principles that a digital identity ecosystem should follow.

Blockchain is essentially a distributed database of records or public information of all transactions or digital events that have been executed and shared between the participating parties. Blockchain can be interpreted as a public distributed ledger, containing information about transactions, in a verifiable and permanent manner, managed by a peer–to–peer network. Each transaction made in the public register is validated by the consensus mechanism. Once entered, the information cannot be deleted or altered *(Allen, 2016)*. It is important to note that the technology called Distributed Ledger Technology and Blockchain technology are not synonymous, the last oane mentioned being a distributed registry implementation that in addittion uses cryptography *(Yaga et al., 2018)*.

From an architectural point of view, Blockchain is a growing list of records called blocks, which communicate with each other through encrypted messages *(Zheng et al., 2017)*. As a data structure, a blockchain is a simple linked list, in which the connections between the blocks are made by a hash. Each block contains its own cryptographic hash and the one of the previous block, a timestamp and transaction data.

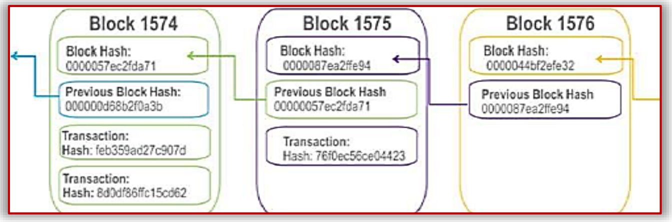

Figure 5 – Blockchain sequence example [23]

Every participant in a Blockchain network, every connected device, server, mobile phone, computer, is called a node. There are several types of nodes, the most important are Full Nodes, Light Nodes or SPV (Simple Payment Verification) and Mining Nodes.

Full Nodes contain a copy of the entire blockchain, information about all transactions made, and all blocks created. They require sufficient resources and a amount large memory, hundreds of gigabytes. With their help, any new entered transaction, any modification and any added block are validated. Full Nodes provide the consensus mechanism by which all changes required require the agreement of some or all of the nodes in order to be accepted *(Mühle et al., 2018)*.

Light Nodes have the same purpose as Full Nodes, but do not store the entire history of the blockchain, they usually contain a block header used to further query a Full Node in the process of verifying a transaction. Light Nodes do not require as many resources as Full Nodes, on which they are dependent. Light Nodes were designed to increase the network capacity and the level of decentralization *(Mühle et al., 2018)*.

Mining Nodes are the nodes that create other blocks for the network. To add a new block it is necessary to calculate its hash, practically to solve a problem of cryptography by brute force. The first node that solves this problem and receives approval from a Full Node can add the new block.

RESULTS

Decentralization is one of the most important features of the Blockchain. In contrast to centralization, within the blockchain the central authority is no longer required. Consensus algorithms are used to maintain the consistency of the data in the distributed network. Persistence is another feature of a Blockchain system. Transactions can be validated quickly and it is almost impossible for transactions to be deleted or withdrawn once they are included in the blockchain *(Hilleman & Rauchs, 2017)*.

The blockchain has an accelerated dynamic of changing its status, new transactions can continuously occur. Therefore, its large publicly shared registers need an efficient, real–time, functional, reliable and secure mechanism to ensure that all transactions that take place on the network are authentic and that all participants agree with changes made to the status of the register. This important task is accomplished by the consensus mechanism, which is a set of rules that decides on the contributions of different blockchain participants *(Yaga et al., 2018)*. There are different types of consensus mechanism algorithms that work on different principles: PoW (Proof of Work), PoS (Proof of Stake), PBFT (Practical Byzantine Fault Tolerance), DpoS (Delegated Proof of Work).

Blockchains can be classified into permissionless or public and permissioned or private. In a Permissionless blockchain, any entity can become a node and can participate in the consensus mechanism. The Permissioned blockchain increases control over the system by limiting participation in the consensus mechanism. Usually, in a Permissioned blockchain only the nodes in a specific organization provide the consensus mechanism. Depending on the application and needs, one type or another can be used. For example, cryptocurrencies such as Bitcoin are Permissionless.

A Smart Contract is an agreement or set of rules that governs a transaction. It is a computer program code stored in the blockchain and which is executed automatically as part of the transactions performed. Smart contracts are entirely digital, being written in various programming languages. This code defines the rules and consequences in the same way as a traditional legal contract, indicating the obligations, benefits and sanctions that could be due to each party in different circumstances. The purpose of using smart contracts is to reduce delays, costs and bottlenecks generated by traditional legal documents, while ensuring a higher level of security.

Digital signatures, based on asymmetric cryptography, are used in the Blockchain to complete the consensus process and to sign Smart contracts. Each user has a key pair, a private key and a public key. The private key is confidential and will be used to sign transactions. The signed digital transactions will be distributed throughout the blockchain network. The digital signature involves two phases of signing and verification (*Yildirim and Mackie, 2019*). The typical digital signature algorithms used in the blockchain is the ECDSA algorithm, Elliptic Curve Digital Signature Algorithm.

Identity management solutions built using blockchain technology benefit from its intrinsic advantages. It eliminates the need for a central authority to control and manage the system and gives the responsibility back to the user. Some of the problems that occur in centralized systems, such as identity theft and data loss, can be largely solved by using the blockchain. By construction, the blockchain brings transparency in the changes made and the data history cannot be altered otherwise (unless most nodes agree on a change). On the other hand, there are challenges in terms of implementation efficiency and even security.

A blockchain–based identity management solution should allow for the selective storage of identities in the blockchain. Identities must be certified by authorities or other entities in the blockchain. Usually things work as follows. An entity claims an identity through a verifiable claim. This is attested after checking user attributes (eg phone number, e–mail, biometrics). In blockchain identity management, there is a clear distinction between the digital identifier (a value that uniquely identifies an entity) and the attributes associated with it *(Lesavre et al., 2019)*. As unauthorized disclosure of attributes leads to security and confidentiality breaches, their storage (if any) should be carried out in accordance with well–defined principles.

CONCLUSIONS

Identity management is a field that is attracting more and more attention. There is a clear need for platforms to address this growing number of user accounts. Throught the paper, the five major models of identity management were presented: Isolated Identity Model, Centralized Identity Model, Federated Identity.

Model, User–Centered Identity Model and Self–Sovereignty Identity Model. From these, the Self–Sovereign Indentity Model is the one that will be used more and more in the future, due to the increasing in popularity technology on which it is based, blockchain, and due to the principles of data security, control and persistence that is following. Blockchain is one of the top technologies nowadays, which continues to develop and is capable to reform the information technology domain.

Note: This paper was presented at ISB–INMA TEH' 2021 – International Symposium, organized by University "POLITEHNICA" of Bucuresti, Faculty of Biotechnical Systems Engineering, National Institute for Research–Development of Machines and Installations designed for Agriculture and Food Industry (INMA Bucuresti), National Research & Development Institute for Food Bioresources (IBA Bucuresti), University of Agronomic Sciences and Veterinary Medicine of Bucuresti (UASVMB), Research–Development Institute for Plant Protection – (ICDPP Bucuresti), Research and Development Institute for Processing and Marketing of the Horticultural Products (HORTING), Hydraulics and Pneumatics Research Institute (INOE 2000 IHP) and Romanian Agricultural Mechanical Engineers Society (SIMAR), in Bucuresti, ROMANIA, in 29 October, 2021

References

[1] Allen C. (2016). The path to Self–Sovereign Identity, http://www.lifewithalacrity.com
[2] Cameron K. (2005), The Laws of Identity, Microsoft Corporation, http://www.identityblog.com
[3] Der U., Jähnichen S., Sürmeli J. (2018). Self–sovereign Identity – Opportunities and Challenges for the Digital Revolution.
[4] Dunphy P., Petitcolas F. (2018). A First Look at Identity Management Schemes on the Blockchain, IEEE Security & Privacy, 16 (4), 20–29.
[5] Goodell G., Aste T. (2019). A Decentralised Digital Identity Architecture. SSRN Electronic 1447 Journal.
[6] Hileman G., Rauchs M. (2017). Global blockchain benchmarking study.
[7] L'Amrani H., Berroukech B.E., EL Bouzekri EL Idrissi Y., Ajhoun R. (2016). Identity management systems: Laws of identity for models 7 evaluation, 4th IEEE International Colloquium on Information Science and Technology (CIST)
[8] Laurent M., Denouël J., Levallois–Barth C., Waelbroeck P. (2015). Digital Identity management, 1 – Digital Identity, 1–45
[9] Lesavre L., Varin P., Mell P., Davidson M., Shook J. (2019). A Taxonomic Approach to Understanding Emerging, Blockchain Identity Management Systems.
[10] Mühle A., Grüner A., Gayvoronskaya T., Meinel C. (2018). A Survey on Essential Components of a Self–Sovereign Identity, Computer Science Review, 30, 80–86
[11] White O., Madgavkar A, Manyika J., Mahajan D., Bughin J., McCarthy M., Sperling O. (2019). Digital identification: A key to inclusive growth, McKinsey Global Institute Journal.
[12] Vadapalli, R. (2020). Fundamentals of Blockchain, Edition 1.1, Publisher Blockchainprep, Editor Blockchainprep UAE, ISBN 301.345.908.
[13] Yaga D., Mell P., Roby N., Scarfone K., (2018). Blockchain Technology Overview, National Institute of Standards and Technology Internal Report 8202
[14] Yildirim M., Mackie I. (2019). Encouraging users to improve password security and memorability, International Journal of Information Security, 8, 741–759
[15] Zheng Z., Xie S., Dai H., Chen X., Wang H. (2017). An Overview of Blockchain Technology: Architecture, Consensus and Future Trends, Proceedings of 6th International Congress on Big Data IEE, 557–564
[16] *** EU Regulation (2016) General Data Protection Regulation (GDPR). https://gdpr–info.eu/art–5–gdpr

ACTA TECHNICA CORVINIENSIS
Bulletin of Engineering

ISSN: 2067–3809
copyright © University POLITEHNICA Timisoara,
Faculty of Engineering Hunedoara,
5, Revolutiei, 331128, Hunedoara, ROMANIA
http://acta.fih.upt.ro