Current Trends in Blockchain Implementations on the Paradigm of Public Key Infrastructure: A Survey

Daniel Maldonado-Ruiz, Jenny Torres, Nour El Madhoun, Mohamad Badra

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

Current Trends in Blockchain Implementations on the Paradigm of Public Key Infrastructure: A Survey

DANIEL MALDONADO-RUIZ[1], JENNY TORRES[1], NOUR EL MADHOUN[2] , AND MOHAMAD BADRA [3]

[1]Departamento de Informática y Ciencias de la Computación, Facultad de Ingeniería en Sistemas
Informáticos y Computación, Escuela Politécnica Nacional, Ecuador (e-mail: {daniel.maldonado02, jenny.torres}@epn.edu.ec)
[2]Security and System Laboratory, EPITA, 14-16 Rue Voltaire 94270 Le Kremlin-Bicêtre, France (e-mail: nour.el-madhoun@epita.fr)
[3]College of Technological Innovation, Zayed University, P.O. Box 19282 Dubai, U.A.E (e-mail: mohamad.badra@zu.ac.ae)

Corresponding author: NOUR EL MADHOUN (e-mail: nour.el-madhoun@epita.fr).

ABSTRACT Since the emergence of the Bitcoin cryptocurrency, the blockchain technology has become the new Internet tool with which researchers claim to be able to solve any existing online problem. From immutable log ledger applications to authorisation systems applications, the current technological consensus implies that most of Internet problems could be effectively solved by deploying some form of blockchain environment. Regardless this 'consensus', there are decentralised Internet-based applications on which blockchain technology can actually solve several problems and improve the functionality of these applications. The development of these new blockchain-based solutions is grouped into a new paradigm called Blockchain 3.0 and its concepts go far beyond the well-known cryptocurrencies. In this paper, we study the current trends in the application of blockchain on the paradigm of Public Key Infrastructures (PKI). In particular, we focus on how these current trends can guide the exploration of a fully Decentralised Identity System, with blockchain as be part of the core technology.

INDEX TERMS BKI, Blockchain, Decentralised, Identity Management, PKI, Smart-Contracts.

I. INTRODUCTION

The need to establish unique identities for the Internet has existed for a very long time insofar as users need to interact with different products and services, and to validate the users' identities with an authority, a server or a government entity. This means that, whoever the user is, he always needs to have a virtual identifier that is not only reliable for that user, but also for all users on the network [1]. Indeed, the most common and easiest way to have an identity is to receive it from a centralised entity. The latter is not only able to certify the user's identity, but also to certify that the identities of other users are trustworthy [2]. However, there are several security conditions that make this centralised approach insecure and untrustworthy. Beyond the fact that each centralized entity can be a single point of failure for all of its dependents, the distrust of any Trusted Third Party (TTP) is due to the fact that users do not have the freedom they need to promote or preserve on the Internet. In the context of PKI, the compromise of a CA will break the trust in all certificates issued by that CA and its descendants. The Certificate Transparency project [3] makes it more difficult for a compromised CA to issue false but valid certificates without being detected. Nevertheless, it cannot detect whether a certificate has been issued to fraudulent but not impersonating websites.

The development of the blockchain technology has become a very promising option for decentralising online services. One of the particularly important considerations is the creation of a new way to have time-immutable information on the network. The ability to store immutable information is a powerful property that enables new ways of understanding not only an identity management as a concept but also most of the features of the Internet, such as data tampering that remains one of the main security threats on the Internet. Several reviews and surveys on blockchain [4] [5] [6] [7] [8] [9] [10] have been performed, with a focus on: a) how the ledger is implemented, b) what type of blockchain technology is implemented, c) what types of security features and technologies are used, and d) what the possible flaws found in existing implementations

are. However, none of these surveys described the way the blockchain could be used as a management tool in the so-called Blockchain 3.0 technologies, which are being used to solve current problems beyond cryptocurrencies and financial affairs [11].

The main contributions of this survey are to a) analyse the implementations of blockchain as a Public Key Infrastructure (PKI) or PKI-added system, and b) to provide insight into how blockchain is used from the perspective of decentralised identity creation and management without the need of using TTPs. The survey also presents a review of the blockchain and PKI backgrounds and an overview of their security flaws Furthermore, it is presented an analysis of the current trends over the mentioned technologies. The aforementioned works analyse the implementations, theoretical and practical, and with that information we analyse the existing flaws in decentralised identity implementations, like pseudo decentralisation or some dependency on centralised entities. Finally, we present developments to be considered as missing in order to achieve a full decentralised identity service on the Internet.

The remaining of this paper is organised as follows. Section II explains why the current identity technologies are merging to find a new way to understand and implement identity management systems. This implies the study of decentralised identity concepts and how they are reflected in different systems where users have most of the control of the process of creating and storing their certificates. Section III presents an analysis on how existing works use blockchain to solve identity problems on the Internet. Finally, section IV concludes the survey and outlines future work.

II. BLOCKCHAIN WITH PKI

One of the main achievements of Bitcoin's development [12] was the creation of a ledger capable of storing all transactions via peer-to-peer methods, making them public and transparent to every user on the network. This was the best way to avoid having a centralized management system to review and validate transactions: [13] [14] [15]. Since then, two branches of this new technology called blockchain have been developed: the first is based on the transactions represented by bitcoin and other cryptocurrencies, and is known as Blockchain 1.0 [11]. The second is based on the storage of several types of information and programmable features, also known as the smart contract paradigm or Blockchain 2.0 [16], of which Ethereum is the main representative. These two developments are applications of the same principle: an interconnected succession of information storage blocks linked to the previous one by cryptographic tools that make the chain an immutable ledger.

With the evolution of Blockchain 2.0, called Blockchain 3.0 (based on advanced smart contracts) [11], several new implementations of blockchain have emerged that aim to diversify the application of the decentralized ledger. However, all Blockchain 3.0 applications retain the main characteristics of the ledger, in which the transparency of the stored data remains. This makes the information safe and trustworthy, but it is not private by default. This can be considered a security flaw from the perspective of the information owners. Therefore, owners can implement some existing solutions to maintain the security of the information in an off-chain storage system, as shown in [4] [17] [18] [19], or they can keep the information encrypted inside the blockchain, as shown in [20], and use the blockchain to ensure the digest of this information in order to preserve the improvements of Blockchain 3.0 and its applications.

At the same time, users should have a system that allows them to share and use their credentials in a simple and secure way, as has been proposed, for example, in [21]. Any communication must guarantee the reliability of each party, especially between unknown and untrustworthy parties. It is therefore necessary to have entities that guarantee this reliability throughout the communication process. This requires the development of a system that can be easily used by any user. It is in this spirit that electronic certificates were created. The basic function of a certificate is to bind a public key generated by a Certification Authority (CA) to a specific and unique user. The certificates are public and widely distributed by CAs, which makes each CA a primary element in the certificate creation and distribution processes. Each CA must validate each issued certificate, not only between users (by validating the identity of each user) but also between the user and the issuer of his certificate, which means the availability of a storage server where the certificate associated with the public key of each user is stored. It is therefore impossible to have a single issuer capable of securing all the certificates generated. Furthermore, it is almost impossible to have one entity capable of managing the issuance of all the certificates in the world. It is also important to have a standard for certificates to create the smoothest possible communication. This is how the Public Key Infrastructure (PKI) and the X.509 certificate standard were created. [22] [23] [24].

The PKI is the hierarchical infrastructure that supports the distribution of certificates on the Internet [25]. It is essentially a hierarchically structured and layered set of CAs, where the issuing CA (the one that creates the user's certificate) is certified by a higher CA. The highest CA is known as the Root CA. This pyramid structure, known as the "Certificate Chain of trust", allows each user's certificate to be considered valid on the Internet. It is impossible to have a single root CA, so there are trust links between the Root CAs, known as Trust Anchors, through which users can be validated among the Root CAs without needing to be registered in each Root CA. In addition, the chain of trust must not only validate active certificates but also distribute invalid or expired certificates to each CA in the hierarchy. To facilitate this task, there are structures called Certificate Revocation Lists (CRLs) [26]. The CRLs are stored in the same pyramid structure of the CA, and users must not only purchase a valid certificate but also a CRL, which checks whether other certificates are still valid. PKIs are the

fundamental structures that enable secure communications on the Internet.

The main security threat of a PKI is that the entire structure is a centralized and pyramidal core, making the certificate validation system dependent on a hierarchical structure. This is because the higher the failure in the pyramid, the more certificates and identities could be compromised. But this is not the only possible security flaw; the PKI is susceptible to compromise by any of its major components [27]. Any failure of a PKI component can cause chains of trust or trust anchors to fail, leaving final certificates unable to be validated. Any identity that cannot be validated is considered fraudulent, making it impossible to create a secure communication channel or establish trust between unknown and distrustful Internet parties.

A. OVERVIEW

The classical design of PKI presents several security flaws [27]. Thus, there are several works that aim to improve its design. The properties of blockchain technology and its derivatives present a solution to some of the problems of PKI, in particular the transparency of certificates and the elimination of a single point of failure. As described in [13] and [28], blockchain has many features used in Blockchain 3.0 to implement decentralised applications for many Internet uses. As for the identity management, the main idea is to generate a system that can store and manage identities with all the advantages of a decentralised ledger. To achieve this goal, blockchain-related identity management implementations and WoT share one very important feature: the consensus protocol [29]. Miners or validators (depending on the type of blockchain used) and older users on WoT, while creating the blocks, validate and secure the identity storage of each user accessing the ledger. However, there is one important difference: in WoT, the so-called consensus is performed by the older users, not by the network itself. For this reason, a group of malicious users can hijack the network by acting as a pseudo-CA and corrupt the whole validity of the network [30] [31]. Contrarily, in a blockchain network, if the transaction (the creation or modification of a user's certificate) is valid (it meets the parameters defined for creating a block, such as the hash or Merkle tree specifications), miners or validators add the block to the ledger without modifying the internal information of the transaction or interacting with the new block outside the defined consensus algorithm. This means that the blockchain acts not only as a decentralised ledger but also as a neutral ledger, where users do not depend on the validation of others to create or use their certificates.

In addition, the security features of the blockchain have some additional considerations compared to PKI implementations, [13] [28] [32]. The transparency property, for example, makes it possible to know and verify every transaction made by the user and stored in the blockchain. In other words, each certificate (which is a "human" way of representing an identity based on a public key paradigm) is public and can be searched and viewed without any special access or authorisation. Moreover, the immutability property of the blockchain, which makes it impossible to alter or modify any certificate already stored, makes a blockchain-based PKI not only extremely public (fully transparent by design), but also completely immutable, even for the certificate owner. Indeed, this property can also pose a problem for a traditional PKI; the need to revoke certificates. In a blockchain-based PKI, each stored certificate is immutable, which means that each stored certificate cannot be unloaded, discarded, or the owner cannot lose access to it. Although certificates cannot be modified or deleted from the blockchain, the functionality of a smart-contract allows users to "replace" their own certificates or stored information without affecting previously stored data [33]. This means that when a certificate becomes obsolete or rogue, it can be declared invalid by the owner himself by creating a new certificate with the same information of the original one, which will be stored in a new block and the only one considered valid since the moment of its creation. The previous certificate will never be deleted or changed, but the new one will explain that it is the only valid one for current and future transactions. For a decentralised PKI, this feature eliminates the need for a CRL or the need for another related system that could be hijacked or become rogue for malicious users [27]. In fact, the immutability of blockchain also provides a transparent and always-available way to keep a record of every transaction made in the PKI. Auditability and accountability are important considerations for any PKI, and blockchain technology offers a natural solution that allows the migration of all features from a centralised and insecure environment to a new decentralised environment where the reliability of the entire system does not rely on one authority or group of users, but on the network itself and all of its capabilities.

B. EXISTING PROPOSALS/SOLUTIONS

All the considerations presented in the previous section leads to different solutions related not only to the concepts of a blockchain-based or blockchain-related PKI, but also to identity and certificate management. This means that it is important to understand the overall representation of PKI and blockchain in various studies, proposals and prototypes. To gather the information needed to conduct this analysis, the research was structured as follows:

- It was delimited between 2016 (according to [11], the concept of identity management blockchain-based systems appears in 2016, and that date was reflected in the paper search) and 2021 (the last search was conducted on June 11, 2021).
- The search string used was "PKI and Blockchain", to know all existing works published on both technologies.
- The works related to the Internet of Things (IoT) were excluded, as identity-related IoT has a different treatment of people's certificates.

- The surveys found in the search process [4] [5] [6] [7] [8] [9] [10] [11] were excluded for the implementation analysis because they did not explain new developments on the subject, but analyses of the state-of-the-art. Those surveys were instead used as a theoretical basis for this survey.

All analysed proposals are full related on how PKI developments are evolving from the centralised CA paradigm basis. However, each proposal and prototype takes distance from the centralised origin depending on its operating objective. Therefore, we have divided each analysed work according to its implementation, as follows:

1) Theoretical developments

The theoretical developments of blockchain and of its derivatives provide new ways in which the system works and extend the way blockchain is implemented. The developments presented in our survey focus on identity management implementations and how blockchain could be used to improve the decentralisation of PKI technologies. Sato et al. [34], for example, present a new cryptographic approach that is useful when some users' keys are compromised. Compromised keys can allow attackers to implement double spending or fraudulent branches on the ledger. Consequently, the new approach needs a Centralised Timestamp Authority to create a long-term signature scheme based on Proof of Existence (PoE), which replaces PoW, creating a consensus system based on the order of transaction execution. To store the hashes created by the long-term signatures, a parallel branch must be created and used as a comparison entity. Over the signatures conservation, Zhao et al. [35] created a new system that unifies the ECDSA (Elliptic Curve Digital Signature Algorithm) and Schnorr and Rho signature schemes in a single protocol as aggregate signatures over generic curves. It is worth noting that the aggregate signature differs from multi-signature in that the latter is a signature over another one in the same document. The main idea of the aforementioned new system is to validate the information stored in the block by checking the aggregate signatures (i.e. the block will be rejected if the signatures are invalid or repeated from previous blocks). This system aims to reduce the signature time compared to the creation of blocks in the Bitcoin blockchain and in the blockchains in general. As for the integration of X.509 environment over Bitcoin-based blockchain schemes, Konoplev et al. [36] presents a theoretical development over how X.509 certificates can be decentralised with a blockchain using sets and function definitions. This work aims to prove that blockchain so it can support the storage of certificates, even when the theoretical affirmations omit the creation and revocation of certificates in their demonstration.

Not all theoretical developments are focused on current technologies. An et al. [37] proposes a pseudo-decentralised PKI with blockchain that will be able to resist post-quantum attacks based on Shore quantum-related algorithms. Quantum and post-quantum cryptography schemes are beyond the scope of the present survey; however, the main idea is to use a classical CAs and x.509v3 certificates to create a user's certificates and store them in a blockchain without any consensus protocol, but only with mathematical structures. Theoretically, the proposed blockchain will be embedded with quantum cryptography features. It aims to create a hierarchical CRL system for the blockchain-related CAs, and also of an additional timestamped validation to keep tracking of every certificate stored on that blockchain. This theoretical proposal, however, only explains how to protect a PKI against attacks that exceed classical and quantum cryptography.

Table 1 summarises the aforementioned proposed solutions, highlighting the main features and limitations. Moreover, the summary includes on which topic the solution is oriented and if there is any implementation in addition to their theoretical presentation. Even when these approaches are related to identity and decentralisation, it is important to give them a different treatment from the practical applications explained in the following section.

2) Practical developments

The most important part of this survey depends on how blockchain is used to improve pseudo and full decentralisation concerning identity management. PKI systems could be implemented with blockchain in different ways. To classify the reviewed proposals, we have divided them according to their implementation, as follows:

a: Classical PKI Systems improved with blockchain

This classification shows pseudo-decentralised implementation where traditional CAs are the main part of the implementation to generate the PKI system, besides the use of blockchain. For example, Kakei et al. [38] present cross-certification system for CAs on a PKI based on Hyperledger blockchain. This proposal uses three layers for PKI: 1) users, where all CA existent users are registered, 2) CAs, where all the classic CAs communicate with each other, and 3) the ledger, consisting of entities known as meta-CAs, which functions as the Hyperledger nodes. Layer three stores all the cross-certification references. The Meta-CAs are special CAs themselves, where all the CAs-related certificates are created; creating a trust environment similar to the trust anchor of the classic PKI. The Meta-CAs also trust each other based on a ranking system, in which the most trustworthy Meta-CA is the best ranked one. This proposal creates a system where the transparency of certificate transactions is secured and could be used for all the registered users. Similar to this proposal, Zhao et al. [39] present a system where the cycle of life of each certificate is stored inside a smart contract, while the certificate itself is still stored on the CA side. This means that each certificate has its own smart contract with related metadata to check the certificate validity, not only with the CA, but with the CRL instead. In this proposal, the smart contracts are integrated to the PKI to have a full validation of each certificate since its

TABLE 1: Summary - Reviewed Theoretical Works

Reference	Oriented to	Main Features	Limitations	Consensus Protocol	Current Applicability
[34]	Long-term digital signature.	Validation of blockchain blocks based on Proof of Existence, where long-term Digital Signature is based on two PoE.	Depends on Timestamp Authority to validate the PoE, in blockchain restored only the consensus hash.	PoE.	Not defined.
[35]	Secure blockchain via signatures.	Unified concepts of signature algorithms in an algorithm of partial signatures for bitcoin blockchain, in order to reduce signature and validation time.	Based on Bitcoin blockchain, improves transactions and their storage, not the identity of the issuers.	PoW.	Designed to be integrated over Bitcoin.
[36]	User authentication.	PKI decentralised model scheme for a blockchain standard version with X.509 certificates.	Mathematical and algorithmic model, without implementation. No CRL in the design.	PoW.	Not defined.
[37]	Secure PKI.	PKI model designed to resist post-quantum cryptographic attacks with blockchain validation schemes.	Depends on classic CAs to manage identities, almost a centralised system without consensus algorithm and a CRL leader.	Not Presented.	Not defined.

creation. Another approach created for web-page services is presented by Garba et al. [40], where the domain owners use both CAs and Registration Authorities (RA) to build a blockchain network where the smart contracts store the certificates created after the request made to RAs, which, along with the CAs, are the only entities that can create the smart contracts and validate the information to avoid impersonation between the domain owners. The works of Wang et al. [41] make an improvement over the classical CA, keeping the generation of certificates centralised, but the identities of users and their correspondent certificates in two independent blockchains, managed by the CAs of the network as the nodes of the system. In this case, the consensus protocol is defined by the node administrator in the network. Another approach is presented by Wang et al. [42], where, with an Ethereum implementation, the web pages-related certificates are created by the CA, validating the identity of the server through the DNS system. The purpose is to keep transparency of transactions and revocations of certificates without omitting the CRL system. However, this proposal keeps the transparency of the transactions in one block per certificate, all the system adds overheads and delays in the transactions between the server and the blockchain. The proposal of Fu et al. [43], on the other hand, consists of dividing the emulation of the network on volunteer nodes (called mini-CAs), acting as a blockchain to create a distributed pseudo-CA. Each node performs identity validation for a transaction fee. Despite this pseudo-decentralisation, each node must validate all transactions in the network, as Bitcoin does with these currency transactions.

To avoid Bitcoin's congestion, Guo et al. [44] created a system where the identity is considered as a set of attributes that need to be validated to achieve identity management. Thanks to the smart contract of the Ethereum blockchain, this approach implements a token validation system, where each valid attribute generates a specific token and each information owner grants access to its tokens to other users. In this case, the CA does not act as an identity manager, but rather as an attribute manager, where information is validated by the private key of the information owner and the information user. This prevents MITM attacks. The works of Longo et al. [45] aim to create a decentralised network of CAs, where each CA keeps its properties and become the blockchain nodes to store the certificates the CAs have created. The idea is to create a certificate chain to replace the classical blocks where the CA certificate acts like the first certificate *i*, which issues the first user's certificate *i+1*, which issues the second user certificate in the chain *i+2*, and so on. This theoretical approach keeps the security on the intermediate certificates as if those certificates were classical blockchain blocks. However, the proposal does not implement a CRL system for the certificates in the chain.

b: Modified classical PKI systems

This section explains several approaches of decentralised and pseudo-decentralised identity environments where classical CAs are still an important part of the network, but blockchain and its applications build a new paradigm of decentralised management.

Yan et al. [46] present a system for mobile devices, where the identity of each device is predefined by the manufacturer or acquired by the device from a CA based on some identity feature like the IP of the device. This system, based on X.509v3 certificates, has several types of nodes, differentiating from validators to transactional nodes. Even when the ID of the device is fixed by the International Mobile Equipment Identity (IMEI), a CA is required to validate the identity of the device. While the proposal keeps the classical infrastructure, it omits in its design the CRL to revoke the certificates. Considering the decentralisation of the identity management as a complement to the classic infrastructure, the proposal of Li et al. [18] compares an identity management system with and without CAs. The revocation of certificates is based on external parties. Without the CA, each identity must be verified by internal older

users, like WoT. In both systems, the blockchain stores the transactions between the certificates and not the certificates themselves for tracking purposes.

On the other hand, the proposal of Quin et al. [17] considers the interactions of certificates created by a CA as currency to be transacted in a Bitcoin-based blockchain, using Merkle Patricia trees as a certificate storage system. In this approach, the identity of the user can be modified, and each user can also have more than one certificate for his interactions. In this case, the verification of the validity of each certificate is performed by the number of interactions of each certificate, and the existence of the certificate and the related identity for its revocation. Thinking of signatures, the works of Guo et al. [47] establish a theoretical system where through a Key Management Center (KMC) a user can generate a key pair and store the public one into a blockchain. The main idea is to use the security features of the blockchain to secure each public key signed by the KMC with the ElGamal signature system. For this proposal, the private key remains with the user for all interactions.

A novel technology called Automated Certificate Management Environment (ACME) automatises the issuance of certificates. With those concepts working the proposals of Dykcik et al. [48] and Kfoury et al. [49]. The proposal in [48] is designed to validate DNS names on the Internet using a tandem of multi-signatures, a blockchain and ACME technology. Per domain the network it creates a specific smart contract where all the interactions of the domain are stored. Each certificate is issued by a CA-like system based on ACME, which fulfils the same functions as a classical CA, and validates the certificates based on the approval of a minimal number of network nodes. The CRL is not based on revocation but in the generation of new partial signatures when the domain pays the corresponding renewal fee. On one hand, [49] creates an Ehtereum-based ACME system to verify the x.509 certificates issued for web domains. In this case, the certificates can be issued by the web server or by a registered CA. The idea is also to keep a registration of the transactions of the Web servers with their clients using Oracle services as a secure channel. On the other hand, the proposal of Yakubov et al. [30] discusses the idea of turning smart-contracts into CAs, enabling the smart contract to issue certificates for each user in the network. In this case, the PKI is smart contract-related by default, where certificates exist as creation cases of smart contracts. In addition, the new PKI creates another type of smart contract, which acts as a CRL, keeping the valid certificates in a whitelist (i.e. a structure, where all the members are valid or trustworthy). All this is done to emulate the decentralised functions of the blockchain, while keeping the functions of classical PKIs. A similar approach is presented in the proposal by Li et al. [50], where CAs act as the nodes of the blockchain, and smart contracts store the certificate chain for each certificate issued. The novelty of this proposal lies in the QoS approach, because it proposes a series of economic punishments and rewards for CAs based on their relative behaviour regarding the users.

Boontaetae et al. [22] present a system called Real Digital Identity (RDI), where the identity issuers are a set of public and private organisms and bureaus where the identity of the users is created, and the CA only issues the certificate requested by a user through this set of entities. The trustworthiness of the identity comes from the combination of all user features provided by the entities in tandem, which act as a tree where the nodes are the partial identity entities and the branches are the users requesting their certificates. This proposal claims ownership of physical or virtual assets that are stored in these entities that can be banks, universities, government offices, etc. Finally, in this section, Ahmed et al. [51] propose a system that is called Smart Contract-based PKI (SCP). This proposal uses Ethereum smart contracts to enforce the identity of Web servers through their definitions on DNS services, using CAs as a trust signing servers, and also the nodes of the blockchain. The blockchain in this proposal does not store the certificate or their transactions, but the trust policies are defined by the CA for each certificate issued to achieve certificate transparency.

c: Decentralised PKI systems with blockchain

This section explains all the proposals that avoid using a CA as a main part of the identity management and aim to create a full decentralised system using blockchain.

The works of Patsonakis et al. [52] and its update [53] present a decentralised PKI (DPKI) built from smart contracts that could evolve without generating new branches and also keeping the size of the smart contract inside the blockchain. This design, however, could be called a "Naming Service", because can be used to decentralise DNS services or other services that can be stored into a smart contract. The main contribution of this proposal is the introduction of a cryptographic accumulator: a public additive system that allows to know if an element is part of the initial input of the accumulator (if the evaluated element was accumulated). In this case, the accumulator is based on RSA, meaning that it is necessary to use a TTP to keep the accumulator in the network. The accumulator is used to ensure some transparency over the transactions of the certificates stored in the DPKI.

A similar approach is presented by Axon et al. [54] and it is updated by Plessing et al. [55], where a blockchain-based PKI (PB-PKI) is implemented using a fork of CertCoin [56]. This approach improves the anonymity of the network by disassociating the user's identity from the certificate in order to generate pseudo-obscure identity management. This no-linking process also appears on the key update process. However, as it is shown in [55], the *total-anonymity* concept cannot be achieved directly because the dissociation could lead to identity impersonation. To counteract the weaknesses of PB-PKI, Plessing proposes two additional solutions that are integrated directly in the proposal [54]: a cryptographic asynchronous accumulator (that is based on Merkle trees) and a ring of signatures for the certificates. Mostly, the

accumulator built a Merkle tree while the input elements are accumulated. To improve the storage space of the tree, the intermediate elements are deleted and only the final state is preserved to validation. These improvements make PB-PKI safer and more secure.

Another proposal of decentralised management is presented by Sermpinis et al. [19] in a proposal called DeTract. This proposal allows the web servers to create their own X.509 certificates with uPort, an Ethereum-based identity storage platform, which links physical and Ethereum smart contract addresses, as an identity manager. The deployed blockchain has stored the hash of each certificate with its associated identity while the actual certificates have been stored off-chain. Each transaction must be paid for by the nodes, in Ethereum's gas currency. Each certificate transaction (creation, update, revocation) is performed by the network using the acquired addresses when the user (a web server, in this case) creates their certificate and asks for their storage, obviating the need for a CRL or another centralised system. Another decentralised approach is presented by Toorani et al. [57], that creates a blockchain-based WoT-like system in order to avoid the centralised CRL. This system creates three user types, called units: 1) root, assumed to be honest in all the network developing and a fixed trust definition, 2) intermediates, having a trust definition equal to one, are the units which participate in the network transactions (enrol, update, revocation), and 3) ordinaries, having a trust definition equal to zero, are the users of the network that request the validation and revocation of their certificates. For this proposal, each unit generates its own key pairs and requests to store the public keys into the blockchain to the intermediate units. If ordinary units have the approval of several intermediate units, their keys can be transacted and stored in the blockchain. Otherwise, ordinary units must wait for the approval of the network.

In the proposal of Han et al. [58], the nodes of the blockchain are used as trusted issuers and this trustworthiness (based on a system of relative signatures) allows the creation of a user's certificates. Each certificate is created as a chain of validation from a user-created self-key. This new certificate is distributed between the network and the nodes sign this certificate creating the chain of validations. Only when the nodes have validated the certificate, it is stored in the ledger. It is important to mention that this system works with a limited number of users, in order to improve the speed of certificate generation and validation. On the proposal of Dua et al. [59], it is defined another WoT-like network where the blockchain is used as PGP's signature rings. Based on Ethereum, every identity must have an Ethereum address to interact with the network. In this case, the certificates remain in the network while the signatures of the certificates can be revoked or updated, where the revocation of the signatures and the creation of new ones being an attribute of every certificate smart contract. This meaning that the identities cannot be revoked, only the signatures associated with the identities. Another WoT-like proposal is presented by Schaerer et al. [60], where using a specific Distributed Ledger Technology (DLT) creates a decentralised system that uses graphs to relate identities with their correspondent public keys. This proposed DLT is not lineal (not in chain) but like a tree where the nodes are the stored public keys. To store a new public key, that key must have been invited to the network and be validated by the currently stored public keys. The revocation, on the other hand, depends only on the public key owner. In the same line of thought, and finishing with these WoT-like proposals, the proposal of Anada et al. [61] presents a WoT-like system that uses the modulus elements of RSA where the value N (the multiplication of the two prime numbers p and q defined by RSA theory) of the key pair creation is associated directly with the user identity. This N modulus is used both to validate the key generation, which is going to be stored in the network, and to prove that the identity-related key is available to be approved for the older users in a WoT. This mathematical approach creates a decentralised trusted type network for identity storage.

About other approaches, the proposal of Yang et al. [62] presents the creation of a system where information will be protected on the nodes directly, not just in the communication link. This is a solution for the Named Defined Network (NDN), where each user needs a specific name instead of a classic IP address, and for validation, each network name is linked to a cryptographic signature. These two attributes (the network name and the signature) allow users to identify themselves in the network where the blockchain stores the keys of each network name (as a user or a web server). The validation of each transaction requires 51% of all nodes to consider the transactions as valid, and each node manages an individual blockchain where its own keys are stored to share them with the network. In addition, Tewari et al. [23], with a private and not fully decentralised blockchain, create an identity that does not depend on the user or a centralised entity, but on a set of distributed attributes acquired from various public entities. This system also uses the blockchain to avoid the use of a CRL with timestamped certificates. In this case, instead of using a username and password to validate the users, the registration uses a One-Time-Pad identity validation. Finally, in this section, the proposal of Li et al. [63] creates a ring of signatures based on RSA. The main idea is to use the cryptographic features of RSA to manage the registration and update of the certificates without compromising the register key (the one used to create the original key pair). This development protects the privacy of the users hiding their ID over successive updates where the new public key is related to a pseudonymous stored in the blockchain.

d: PKI revocation system management

This section explains the improvements, not only in the CA specifically, but in the CRL mechanism. The works of Elloh Adja et al. [64] describe an improvement of the validity mechanism on X.509 based on distribution points

to improve the high time delays of blockchain implementations. In this solution, which aims to be fully integrated with X.509 environment distributions in the future, CAs store in the blockchain the revocation information of each issued certificate. These certificates, usually deployed in the context of TLS protocol, are issued by the CAs and maintain the centralised structure of the network. One major improvement for this approach is the client verification for the Web server certificate that is sent on the same channel of the secure data, improving the time of the communication since its beginning for all the systems. Another proposal [65] suggests maintaining the current CA infrastructure by improving the revocation system. This proposal can be used for Web servers or personal users equally. The members of the PKI are the nodes of the blockchain and the smart contracts store the validation of each certificate. All of this is to improve the delays between the server and the user during a TLS connection. Finally, in this section, the proposal of San et al. [66] creates a method based on the Bitcoin blockchain to replace the CRL system, where the information of revocation is stored in the blockchain through a mining work. This system cannot be considered as a PKI, it is only a CRL replacement, where the revocation and the reissuing of certificates is performed through a credential check initiated by the owner, where new IDs are assigned by a CA.

e: CA transparency and auditability

This section explains the works related to the use of blockchain, not for decentralising the identity management, but rather for improving PKI's transparency and auditability.

The works of Chen et al. [67], for example, proposed a layered system called CertChain, in which CAs always create and manage user identities, and a Bitcoin blockchain-based system controls the behaviour of the certificate as a log server. CertChain uses all registered nodes with the highest computing power as "miners", which creates a centralised miner system within the blockchain. Additionally, the verification of the certificate behaviour is done in real time, which avoids the presence of a third-party verifier in the whole system. Another example focused on web page identity is proposed by Madala et al. [15], where a smart contract-based blockchain is used as a database that replaces Google Certificate Environment. This system has CAs as nodes that feed the ledger with certificate chain references. The full certificate information is stored outside the chain (off-chain). To break the security of this proposal, an attacker needs to compromise at least 51% of the CAs in the network to validate the aggregation of new certificates or the signature request. The 51% attack [28] is the only vulnerability according to the Authors. However, that attack is impossible in this case because only the CAs in the network can make this kind of request.

The work presented by Kubilay et al. [68], named CertLedger, proposes a system where a blockchain is used to replace the certificate validation and revocation logs and the CRL, avoiding any CRL spoofing and preserving the entire secure channels since the beginning of the communication. The main idea of this proposal lies on using smart contracts to keep secure all transactions from Web servers' certificates. All of this to prevent the information breach or hijack considering that the classical CAs that create and maintain the certificates can become rogue, or the blockchain could be under the 51% attack. Consequently, the actual security of the system lies in the cryptographic primitives of the architecture.

To keep CAs working properly, the proposal of Matsumoto et al. [69], called Instant Karma PKI (IKP), uses a blockchain as a behavioural control system to incentive good behaviour from the CAs in the network. In this case, the concept 'good behaviour' implies the correct issuing of certificates from the CA (certificates without errors of validation, information or assignment). This means that CAs need to maintain SLA and QoS levels to avoid what the clients call a 'bad reputation', that would relegate the CA to the back of the PKI queue for generating new certificates. Another system in which the blockchain is used as a log ledger is presented in [70], where a new public PKI for Peru is presented. This PKI defines a hierarchy of four types of certificates that are generated by a local CA with RSA-related technologies that are not compatible (at the time of publication) with international certification standards.

In [71], the blockchain is used as a decentralised name server for client-server transactions and identity requests. In this case, the blockchain is used only to store the identity relationship between domains as a related, but without integrating a query system. Finally, in this section, another proposal of a log-related blockchain [72], called blockchain-related PKI (BKI), is designed to be a log manager. In other words, the blockchain stores the transaction logs of the certificates, not the certificates themselves. Instead of using a consensus protocol, the transactions are validated by a Merkle tree, and every transaction has a timestamp with second precision. The idea was developed to avoid a malicious party from modifying the keys of the systems, and hence, to even hijacking the CA. For this proposal, only owners and registered users in BKI can perform each interaction, where the entire system is timestamped.

f: User-related PKI management

In this section, we explain several proposals of management systems that are more focused on how the user interacts with decentralised networks. Although maintains their relationship with the concepts of identity decentralisation. For example, the works in [20] create a system to protect consortium blockchains so that the stored data is no longer transparent. Using a joint system defined for various members of a consortium, the contribution of this proposal is to create a blockchain network that could store the metadata in a safe manner using some homomorphic cryptosystem that is still related to RSA. Another approach for user-centric systems is presented by [73], who proposes

a blockchain-based transparent and trustworthy third-party system to create a secure logging-based framework. The development in this proposal is based on the evaluation of specific algorithms and their experimental execution. In other words, the transactions made by TTPs over some systems have a transparency blockchain to improve the users' knowledge about the TTP transparency. All of that while the privacy of the certificates and the identities related to them is kept. Moreover, clients and users need to interact with blockchain-based PKI systems.

The works in [74] propose a light mobile client, written in Java, to interconnect users with their PKIs. This client, however, is limited to Certcoin-based PKIs. The main idea of Certcoin, defined in [56], is to create a blockchain to securely store users' identities with his related public keys. The client aids to create two private keys (online and offline) to emulate the security implemented in CertCoin. This thin-client performance seems to be more efficient when compared to other existing schemes. Finally, in this section, another proposal is presented in [75]. The proposal describes a system where the identity is based on manager-managed tuples created on hierarchical multi-graphs and then stored on a blockchain. From the blockchain paradigm, this approach acquires security parameters and a pseudo-domain service system that manages all stored tuples to validate the identity of each user.

Table 2 summarises the ideas presented in this section, with their main features and limitations of decentralised PKI approaches. The summary also includes on what section the studied proposal is classified, what topic is oriented the solution and if the solution has planted some form of self-generated or self-signed identity.

III. NEW TRENDS ANALYSIS

Figure 1 shows the classification of the different solutions and proposals about decentralised identity management. As shown in Tables 1 and 2, there are several approaches of how Identity Management as a concept must be implemented and developed. However, we can group them on what final problem they have been designed to solve, all in the context of the Blockchain 3.0 paradigm.

For this analysis, we focus on the practical developments of decentralisation, where user management is the most important feature needed to be improved. However, as it is shown on [7], the broad implementation of centralised systems and x.509 format make it more important to develop solutions to improve and evolve the classic CA infrastructure. Sections II-B2a and II-B2b explains how blockchain is used to bring some transparency over the creation and/or the life cycle of the certificate. Each of these proposals, however, always depends on CA, either for the creation of the identity or of a related certificate. One of the main features of these solutions is the existence and use of the CRL to maintain the registration of the revoked certificates. For these developments, a concept of self-generated certificates or identities does not exist, maybe with the exception of [49], that have some self-signed certificates, but not as a main feature of the proposals. The main goal of the proposals presented on sections II-B2a and II-B2b is to improve the mechanism of how PKI works, introducing decentralisation as a supplementary improvement, but without modifying the inner core in what all the CAs work. The primary limitation of the works described in section II-B2a is their reliance on a traditional centralized infrastructure, including CRL, to maintain the validity of each certificate. In comparison, the works described in section II-B2b introduce modifications to the traditional PKI infrastructure to include a blockchain in the core of the PKI network, in an attempt to create the closest thing to a decentralized network. However, this creates some limitations when CAs are used as nodes in the blockchain, in order to create a smart contract related to network security, which may affect the interactions between users and nodes: users and nodes that were created on a centralized paradigm. Indeed, all of the above means that the implementations presented in section II-B2b still rely on TTPs to maintain system reliability.

A major improvement in PKI, over what was studied in sections II-B2a and II-B2b, is presented in section II-B2c, where the concept of CA and centralisation is avoided with several approaches of blockchain implementation. From certificate-storing blockchain to dual systems to hashes/certificates, the studied proposals allow clients to have a decentralised way to interact with their users (when the users are Web servers), or in a standalone communication. Most of these approaches, however, are designed to emulate the main features of WoT [29] [31]: a group of older network users act as validators/enablers of new users on the network. Despite the well-known capabilities of decentralisation of WoT or any of their studied variations, the possibility that the network can be hijacked and maliciously centralised persists. This vulnerability must be considered, because it is one of the most important impediments to achieving full decentralisation.

The sections II-B2d and II-B2e show improvements focused on the transparency of PKI. The decentralisation of CRL systems allow to keep track of the behaviour of both the certificates and the PKI itself. All of that to maintain the blockchain offered transparency. Even when some of these proposals cannot be considered as PKI per se, their approaches provide the user with the security of knowing how the certificates were generated. That means what their status of operation is and establishment of the connection (especially when it is between the user and a Web server via TLS) and most importantly what their revocation status is. All this to prevent rogue users/certificates from putting all the identity system in danger. However, the emphasis on transparency in these sections makes these proposals vulnerable to the fact that they are not necessarily applicable to decentralized environments, or that they only serve to enhance traditional CA schemes. This means that they do not contribute to the decentralization of identity management as such.

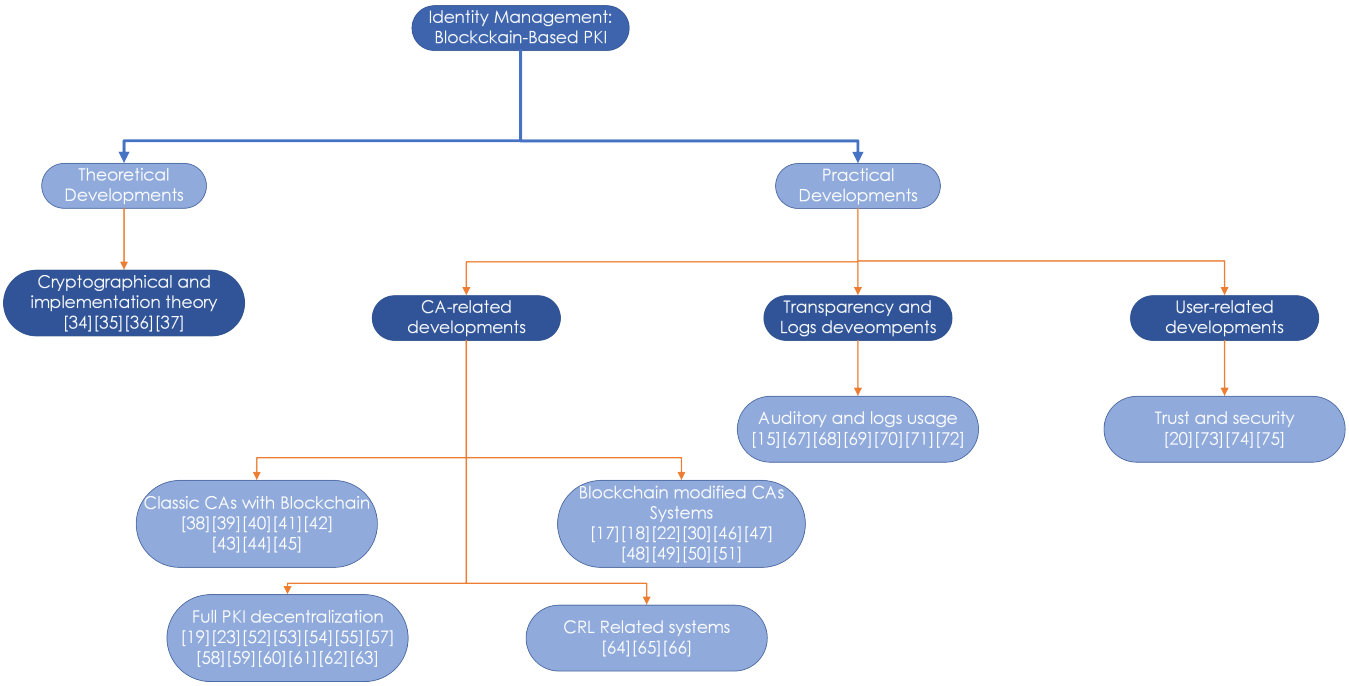

FIGURE 1: Summary of New Trends

Finally, the section II-B2f presents proposals where the user and their interaction with the network is the main objective. This section explains the security that users can achieve with determinate proposals, and how the user must interact with the network through specific clients or encryption to keep their identity secure and safe. However, these proposals are limited only to specific applications of blockchain, which makes it difficult to implement them in other scenarios or in other decentralized systems, even if they share some management characteristics.

This survey analysed 55 works, everyone with different scopes. All of them give an explanation on how blockchain is used to enable the desired decentralisation in identity management. However, most of these works fail to present a decentralisation of identity itself. This means that in almost all cases, there is an entity that creates or issues the identity based on x.509 certificates. The proposals [49], [19], [57], [58] and [63] are the only ones that address the possibility of the creation of an identity by the user himself. As far as we know, there is no project or implementation where users are able to create their own identities; and to be capable of validating it without any entity or without depending on a group of users to have a valid identity.

Other kinds of implementations, known as Self-Sovereign Identity (SSI) systems [76] [77] cannot be included in this survey. Even when SSI considers some form of decentralised identity, it does not work as a PKI (infrastructure to keep and store certificates) in their interactions with the users. The SSI decentralisation is mostly based on mobile devices and their interactions with a blockchain. Besides, the common study fields that all the works shared, it is important to add the user's independence and self-validation techniques to achieve a full decentralised system, where users can be self-represented without the need of entities who tell them who they are, with or without a payment for that service.

IV. CONCLUSION

The analysis of the current trends on the application of blockchain in identity management proves that the technology is used basically like a log of other identity interactions. Most of the works included in this survey show the importance that CA still has when identity is created or used on the Internet. It means that users still depend on third parties (trusted or distrusted, paid or free) to have an actual identity on the network. This implies that current identity systems cannot handle or allow users to create their identities with the features that the users consider significant. To either keep their privacy in online transactions or to securely show who they are. Part of the future works lies on understanding how the actual identity decentralisation could use blockchain as a tool to build an infrastructure that supports all the features studied, including self-created identities. The analysis presented through this survey will be used to build a system where each user will be able to create, manage and validate a self-identity, with the parameters of identification that the user chooses to share and that the network will recognise them as valid.

The step to turn users' identities as autonomous and decentralised is the cornerstone of new and fully decentralised Internet services and the first step on how we must need to understand our relationship with the Internet in the future.

TABLE 2: Summary - Reviewed Practical Works

Related Concept	Ref.	Oriented to	Main Features	Limitations	Consensus Protocol	User Defined Identity
Classical PKI Systems	[38]	CAs validation	Distributed CA implementation for validation of CAs using Hyperledger as transparency core.	WoT-like trust between the meta-CAs, which generate the cross certificates for classical CAs	Not defined	No
	[39]	CA transparency	RootCA transparency system to manage the certificate life cycle	Depends on a third party storage system for each certificate. Depends on CA infrastructure for certification issuing	Not defined	No
	[40]	User registration validation	Blockchain-based PKI for web servers to protect the registration of new users.	The systems depends on CAs and RAs for each transaction	PoW	No
	[41]	User authentication	PKI on a private blockchain with identity independent certificates, divided on two blockchains.	A CA generates all the certificates as an administrator, which defines the consensus method.	Administrator defined	No
	[42]	Web servers Identity	PKI focused on web servers where validation of identity comes from DNS servers with certificate issuers and enablers.	Each browser keeps some headers to validate if chain certificates are stored in the blockchain.	PoW	No
	[43]	User authentication	Create a system of mini-CAs to create and validate distributed CA identity validation via multilevel secret sharing.	Based on Bitcoin features, each node (volunteers) need to validate the work of the previous miners.	PoW	No
	[44]	User authentication	Distributed CA access control system based on identity attributes control via smart-contracts	The system differentiates request contract from store contract, and owner and user of information, with wildcards comparison.	PoS	Based on data, not direct identities
	[45]	User authentication	Prototype suite based on x.509 and blockchain-like ledger to concatenate user certificates with anonymous identities.	Users create the certificate chain, but a CRL-like system is not defined.	Not applicable	No
Modified classical PKI systems	[46]	User authentication	PKI designed for mobile devices' certificates, with self signed certificates via hardware identity.	Depends on a Third party to create the identity (the manufacturer) and validate the certificate.	Not specified	No
	[18]	Certificate storage	Design of a Blockchain-based PKI with and without a CA and analysis of features.	Theoretical design which considers decentralisation as a supplementary part of a PKI.	Not specified	No
	[17]	User authentication	Bitcoin-Based PKI where certificates are used as an ad-hoc currency designed to protect web servers.	Certificate validation is given by the amount of interactions in the network.	PoW, MPT	No
	[47]	Signature management	Blockchain-based KCM to generate keys for certificate generations and hide the identity of the user.	Theoretical design without specific integration to any blockchain-based solution.	Not Specified	No
	[48]	DNS names validation	DNS based PKI with specific CAs and smart-contracts, one for each domain. Every SC has a number of CAs to validate domain servers.	Security based on blockchain security. It depends on a minimal number of nodes (CAs) to validate the authenticity of the system certificates.	PoW	No
	[49]	Web servers validation	Decentralised automatic certificates issuance with Ethereum to validation of web domains through x.509 certificates	Depends on Oracle services and CAs to create the certificates and in the interaction between the user and the web server	PoW	Could have self-signed certificates
	[30]	User authentication	Framework over blockchain which uses CAs as smart-contracts and modified X.509 certificates inside the smart-contract.	Each certificate is part of a global SC in order to transmit the chain of certificates as a classic CA.	Not specified	No
	[50]	User authentication	CA based PKI implemented with smart-contracts to build the certificate chain.	Depends on CAs and measures the behaviour of CAs in order to establish punishments and rewards for communication links.	PoS	No
	[22]	User authentication	CA network model with smart-contracts based on Identity authorities as a service provider and issued by the user.	Use a validation through majority system to solve identity validation between identity authorities with CAs and service providers with customised cryptography.	PoW	No
	[51]	Web servers identity	Smart-contract based PKI which work as a parallel PKI system with QoS definitions.	Web vendors establish trust policies between CA and web browser(user), that vendor can be hijacked by a malicious party and overwrite trust policies between CAs and smart-contracts.	PoW	No

Related Concept	Ref.	Oriented to	Main Features	Limitations	Consensus Protocol	User Defined Identity
Decentralised PKI systems	[52]	PKI generic framework	PKI based system built over smart-contracts based on the access to public keys with an accumulator.	Theoretical design of a PKI with fixed long accumulators for improvement of smart-contract behaviour.	RSA-related random Oracle model.	No
	[53]	PKI generic framework	Update definitions over the works of [52].	The security of the implementation is based on the protocol definitions, also the accumulator needs a TTP for validation.	RSA-related random Oracle model	No
	[54]	User authentication	Decentralised PKI focused on the full anonymity of the user in the system.	Variation of Certcoin (blockchain for certificates) without authentication, but without link identity with certificates.	PoW	No User identities
	[55]	User authentication	Improvements of [54] adding a ring signature and asynchronous accumulator.	There are no privacy defined in the implementation. Also the ring signature need several improvements.	PoC	No
	[19]	User authentication	Framework based on Ethereum facilities to keep hashes stored on a public network with explicit revocation models.	Framework depends on several features on Ethereum (gas, ethers, uPort system). Every transaction is implemented in a generic Ethereum.	Ethereum-related	Yes
	[57]	CRL improvements	WoT-like PKI with user profiles and security thresholds to store the public keys inside the blockchain.	Basic users depend on blockchain nodes users to store their public keys. Consensus depends on users with prefedined trust thresholds.	PBFT	Yes
	[58]	User authentication	Conditional trust framework with certificates chains stored in blockchain.	The security of the system relies on blockchain classic security. User number limited by a binomial distribution.	PoW	Yes
	[59]	User authentication	P2P storing network based on WoT using Ethereum to define a decentralised PKI.	Every identity is based on a Ethereum address. Use a PGP like signature ring. The stability of the network depends on the number of nodes.	Pow	No
	[60]	User authentication	WoT-like tree-designed DLT to store and manage identities through identity claims.	The access to the network is only by invitation. In the DLT is stored a hash related public key.	DLT-defined	No
	[61]	User authentication	Modulus N RSA type PKI to create a WoT validation with RSA and ECC as second public transaction key.	The system is not designed to be implemented in a blockchain directly.	Not Presented	No
	[62]	Name networks communication	Use of blockchain to manage NDN communications like DNS communications focusing on solving the CA compromised problem.	There are multiple blockchains to control network names. Every node manages their own blockchain with their keys.	PoW	No
	[23]	User authentication	X.509 based PKI with identity providers and CAs as blockchain nodes without CRL.	Works on a private non fully decentralised blockchain. Every identity must be validated by a CA before being updated on the blockchain.	PoW	No
	[63]	Signature management	System designed to create a ring signature based on the primitives of RSA to protect identities stored into a blockchain.	Theoretical scheme, not intended implementation.	Not specified	Partial generation
PKI's revocation system	[64]	Certificate validation improvement	Namecoin related system to improve the revocation methods of x.509 certificates.	Not designed for identity decentralisation, intended to be integrated with classical CAs.	Not specified	Not PKI
	[65]	CRL improvements	Blockchain based system designed to store the validation and revocation information into smart contracts.	Susceptible to DoS attacks.	CONS	Not PKI
	[66]	CRL management	System designed to revoke certificates through bitcoin blockchain mining.	Blockchain only for CRL management and improvement. Not designed to manage identities or decentralisation.	PoW	Not PKI
CA transparency	[67]	CA behaviour control via blockchain	Audit Scheme for TLS connections via Blockchain, where CAs manage identity and every transaction is stored as a block with a Merkle tree.	A system based only on trusted CAs as nodes, blockchain stores certificate transactions, not certificates.	Specific designed protocol. Based on Ouroboros.	No

Related Concept	Ref.	Oriented to	Main Features	Limitations	Consensus Protocol	User Defined Identity
CA transparency	[15]	Web servers identity	Hyperledger blockchain which replaces Google Certificate Validator with a blockchain with trustworthy CAs as peers.	The system depends on CAs to generate certificates for the issuers (clients) and for security transactions.	Hyperledger-related	No
	[68]	User authentication	Certificate management system where blockchain is used as a vault for TLS certificates.	Blockchain is used only as a vault, identity is still created in CA and certificate chains.	PBFT	No
	[69]	Web servers identity	Blockchain based system to maintain behavioural control over CAs in the network.	Focused on financial losses, Ethereum used to store server failures based on an SLA, where bad CAs are relegated.	PoW	No
	[70]	User authentication	A new system of hierarchy for signature administration in Peru.	Based on RSAs CA, have problems with interoperability and some vulnerabilities.	Not defined	No
	[71]	Log management	Bitcoin Blockchain based log system acting as a decentralised trustwhorty name server for a centralised client-server identity manager based on CONIKS and Catena.	Blockchain is used only to manage and store the identity relations which are stored in a classic centralised system. Both systems are linked but not interconnected.	PoW	No
	[72]	Logs management	Blockchain-based PKI with CAs to generate key pairs.	Blockchain stores logs instead of certificates or key pairs, in order to protect PKI transactions. The systems need a number of CAs in order to be considered compromised.	PoW	No
User related management	[20]	User data privacy	Blockchain network which stored data over homomorphic cryptography to keep the information private and accessible.	Only designed for consortium blockchains, not intended to deploy on public ones.	Not specified	No
	[73]	Authority trust	Trustworthy third party system based on blockchain to improve TTP transparency.	Transparency designed for TTPs, not intended to be used for any user or certificate storage.	Not specified	No
	[74]	User authentication	Certcoin based application for a PKI used to users administration.	Based on Certcoin, keys recovery made by Shamir parts scheme.	PoW	No
	[75]	User authentication	Tuple system that allows identity management with identity relations graphs with blockchain.	Theoretic approaches based on directed hierarchical multigraphs of managers-managees.	Graph-based protocol	No

REFERENCES

[1] Ravishankar S Bhagavatula, Chandra S Balasubramanian, Francis M Sherwin, Michael A Keresman III, and Jeffry J Bowman. Centralized identity authentication for electronic communication networks. Google Patents, US Patent 7,140,036, November 21 2006.

[2] Liang Yan, Chunming Rong, and Gansen Zhao. Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography. IEEE International Conference on Cloud Computing, Springer, pages 167–177, 2009.

[3] Google. Certificate Transparency. https://certificate.transparency.dev/.

[4] Sara Rouhani and Ralph Deters. Blockchain based access control systems: State of the art and challenges. IEEE/WIC/ACM International Conference on Web Intelligence on - WI '19, pages 423–428, 2019.

[5] Thomas Hepp, Fabian Spaeh, Alexander Schoenhals, Philip Ehret, and Bela Gipp. Exploring Potentials and Challenges of Blockchain-based Public Key Infrastructures. IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pages 847–852, apr 2019.

[6] Christos Patsonakis, Katerina Samari, Aggelos Kiayiasy, and Mema Roussopoulos. On the Practicality of a Smart Contract PKI. 2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON), pages 109–118, apr 2019.

[7] Michael Kuperberg. Blockchain-Based Identity Management: A Survey From the Enterprise and Ecosystem Perspective. IEEE Transactions on Engineering Management, 67(4):1008–1027, nov 2020.

[8] Chong Gee Koa, Swee Huay Heng, Syh Yuan Tan, and Ji Jian Chin. Review of blockchain-based public key infrastructure. Proceedings of the 7th International Cryptology and Information Security Conference 2020, CRYPTOLOGY 2020, 2020:20–31, 2020.

[9] Daniela Pöhn and Wolfgang Hommel. An overview of limitations and approaches in identity management. Proceedings of the 15th International Conference on Availability, Reliability and Security, pages 1–10, aug 2020.

[10] Clemens Brunner, Fabian Knirsch, Andreas Unterweger, and Dominik Engel. A comparison of blockchain-based PKI implementations. ICISSP 2020 - Proceedings of the 6th International Conference on Information Systems Security and Privacy, (February 2021):333–340, 2020.

[11] Damiano Di Francesco Maesa and Paolo Mori. Blockchain 3.0 applications survey. Journal of Parallel and Distributed Computing, 138:99–114, apr 2020.

[12] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf, 2008.

[13] Rui Zhang, Rui Xue, and Ling Liu. Security and Privacy on Blockchain. ACM Computing Surveys, 52(3):1–34, jul 2019.

[14] Moneeb Ahmed, Ihsan Elahi, Muhammad Abrar, Umair Aslam, Iqra Khalid, and Muhammad Asif Habib. Understanding Blockchain. Proceedings of the 3rd International Conference on Future Networks and Distributed Systems - ICFNDS '19, pages 1–8, 2019.

[15] D S V Madala, Mahabir Prasad Jhanwar, and Anupam Chattopadhyay. Certificate Transparency Using Blockchain. 2018 IEEE International Conference on Data Mining Workshops (ICDMW), 2018-Novem:71–80, nov 2018.

[16] Gavin Wood. Ehtereum: A Secure Decentralized Generalized Transaction Ledger. Ethereum Project Yellow Paper, pages 1–32, 2018.

[17] Bo Qin, Jikun Huang, Qin Wang, Xizhao Luo, Bin Liang, and Wenchang Shi. Cecoin: A decentralized PKI mitigating MitM attacks. Future Generation Computer Systems, 107:805–815, 2020.

[18] Yannan Li, Yong Yu, Chunwei Lou, Nadra Guizani, and Lianhai Wang. Decentralized Public Key Infrastructures atop Blockchain. IEEE Network, 34(6):133–139, nov 2020.

[19] Thomas Sermpinis, George Vlahavas, Konstantinos Karasavvas, and Athena Vakali. DeTRACT: a decentralized, transparent, immutable and open PKI certificate framework. International Journal of Information Security, 2020.

[20] Qin Wang, Shiping Chen, and Yang Xiang. Anonymous Blockchain-based System for Consortium. ACM Transactions on Management Information Systems, 12(3):1–25, may 2021.

[21] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2):120–126, 1978.

[22] Pongpayak Boontaetae, Akkarit Sangpetch, and Orathai Sangpetch. RDI: Real Digital Identity Based on Decentralized PKI. 2018 22nd International Computer Science and Engineering Conference (ICSEC), pages 1–6, nov 2018.

[23] Hitesh Tewari, Arthur Hughes, Stefan Weber, and Tomas Barry. X509Cloud — Framework for a ubiquitous PKI. MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM), 2017-Octob:225–230, oct 2017.

[24] Balaji Rajendran. Evolution of PKI ecosystem. 2017 International Conference on Public Key Infrastructure and its Applications (PKIA), pages 9–10, nov 2017.

[25] Hou Liping and Shi Lei. Research on Trust Model of PKI. 2011 Fourth International Conference on Intelligent Computation Technology and Automation, 1:232–235, mar 2011.

[26] Moni Naor and Kobbi Nissim. Certificate revocation and certificate update. IEEE Journal on Selected Areas in Communications, 18(4):561–570, apr 2000.

[27] Paul Black and Robert Layton. Be Careful Who You Trust: Issues with the Public Key Infrastructure. 2014 Fifth Cybercrime and Trustworthy Computing Conference, pages 12–21, nov 2014.

[28] Iuon Chang Lin and Tzu Chun Liao. A survey of blockchain security issues and challenges. International Journal of Network Security, 19(5):653–659, 2017.

[29] Alexander Ulrich, Ralph Holz, Peter Hauck, and Georg Carle. Investigating the openpgp web of trust. Computer Security – ESORICS 2011, pages 489–507, 2011.

[30] Alexander Yakubov, Wazen M. Shbair, Anders Wallbom, David Sanda, and Radu State. A blockchain-based PKI management framework. NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium, pages 1–6, apr 2018.

[31] Alessandro Barenghi, Alessandro Di Federico, Gerardo Pelosi, and Stefano Sanfilippo. Challenging the Trustworthiness of PGP: Is the Web-of-Trust Tear-Proof? Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 9326:429–446, 2015.

[32] Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, and Qiaoyan Wen. A survey on the security of blockchain systems. Future Generation Computer Systems, 107:841–853, jun 2020.

[33] Bhabendu Kumar Mohanta, Soumyashree S Panda, and Debasish Jena. An Overview of Smart Contract and Use Cases in Blockchain Technology. 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), pages 1–4, jul 2018.

[34] Masashi Sato and Shin'ichiro Matsuo. Long-Term Public Blockchain: Resilience against Compromise of Underlying Cryptography. 2017 26th International Conference on Computer Communication and Networks (ICCCN), pages 1–8, jul 2017.

[35] Yunlei Zhao. Practical Aggregate Signature from General Elliptic Curves, and Applications to Blockchain. Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security - Asia CCS '19, pages 529–538, 2019.

[36] A. S. Konoplev, A. G. Busygin, and D. P. Zegzhda. A Blockchain Decentralized Public Key Infrastructure Model. Automatic Control and Computer Sciences, 52(8):1017–1021, dec 2018.

[37] Hyeongcheol An, Rakyong Choi, and Kwangjo Kim. Blockchain-Based Decentralized Key Management System with Quantum Resistance. International Workshop on Information Security Applications, 2(2019):229–240, 2019.

[38] Shohei Kakei, Yoshiaki Shiraishi, Masami Mohri, Toru Nakamura, Masayuki Hashimoto, and Shoichi Saito. Cross-Certification Towards Distributed Authentication Infrastructure: A Case of Hyperledger Fabric. IEEE Access, 8:135742–135757, 2020.

[39] Jian Zhao, Zexuan Lin, Xiaoxiao Huang, Yiwei Zhang, and Shaohua Xiang. TrustCA: Achieving Certificate Transparency Through Smart Contract in Blockchain Platforms. 2020 International Conference on High Performance Big Data and Intelligent Systems, (1):1–6, may 2020.

[40] Abba Garba, Qinwen Hu, Zhong Chen, and Muhammad Rizwan Asghar. BB-PKI: Blockchain-Based Public Key Infrastructure Certificate Management. 2020 IEEE 22nd International Conference on High Performance Computing and Communications; IEEE 18th International Conference on Smart City; IEEE 6th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), pages 824–829, dec 2020.

[41] Rong Wang, Juan He, Can Liu, Qi Li, Wei-Tek Tsai, and Enyan Deng. A Privacy-Aware PKI System Based on Permissioned Blockchains. 2018 IEEE 9th International Conference on Software Engineering and Service Science (ICSESS), 2018-Novem:928–931, nov 2018.

[42] Ze Wang, Jingqiang Lin, Quanwei Cai, Qiongxiao Wang, Jiwu Jing, and Daren Zha. Blockchain-Based Certificate Transparency and Revocation

Transparency. International Conference on Financial Cryptography and Data Security, 10958(2014):144–162, 2019.

[43] Yue Fu, Rong Du, and Dagang Li. Distribution of CA-Role in Block-Chain Systems. International Conference on Cloud Computing and Security, 2:276–285, 2018.

[44] Hao Guo, Ehsan Meamari, and Chien-Chung Shen. Multi-Authority Attribute-Based Access Control with Smart Contract. Proceedings of the 2019 International Conference on Blockchain Technology - ICBCT 2019, Part F1481:6–11, 2019.

[45] Riccardo Longo, Federico Pintore, Giancarlo Rinaldo, and Massimiliano Sala. On the security of the blockchain BIX protocol and certificates. 2017 9th International Conference on Cyber Conflict (CyCon), 2017-June:1–16, may 2017.

[46] Junzhi Yan, Xiaoyong Hang, Bo Yang, Li Su, and Shen He. Blockchain Based PKI and Certificates Management in Mobile Networks. 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pages 1764–1770, dec 2020.

[47] Li Guo and Caihui Lan. A New Signature Based on Blockchain. 2020 International Conference on Intelligent Computing, Automation and Systems (ICICAS), pages 349–353, dec 2020.

[48] Lukasz Dykcik, Laurent Chuat, Pawel Szalachowski, and Adrian Perrig. BlockPKI: An Automated, Resilient, and Transparent Public-Key Infrastructure. 2018 IEEE International Conference on Data Mining Workshops (ICDMW), 2018-Novem:105–114, nov 2018.

[49] Elie F. Kfoury, David Khoury, Ali AlSabeh, Jose Gomez, Jorge Crichigno, and Elias Bou-Harb. A Blockchain-based Method for Decentralizing the ACME Protocol to Enhance Trust in PKI. 2020 43rd International Conference on Telecommunications and Signal Processing (TSP), pages 461–465, jul 2020.

[50] Shaozhuo Li, Na Wang, Xuehui Du, and Aodi Liu. Internet Web Trust System Based on Smart Contract. International Conference of Pioneering Computer Scientists, Engineers and Educators, pages 295–311, 2019.

[51] Abu Shohel Ahmed and Tuomas Aura. Turning Trust Around: Smart Contract-Assisted Public Key Infrastructure. 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), pages 104–111, aug 2018.

[52] Christos Patsonakis, Katerina Samari, Mema Roussopoulos, and Aggelos Kiayias. Towards a Smart Contract-Based, Decentralized, Public-Key Infrastructure. 11261:299–321, 2018.

[53] Christos Patsonakis, Katerina Samari, Aggelos Kiayias, and Mema Roussopoulos. Implementing a Smart Contract PKI. IEEE Transactions on Engineering Management, 67(4):1425–1443, 2020.

[54] Louise Axon and Michael Goldsmith. PB-PKI : a Privacy-Aware Blockchain-Based PKI. Proceedings of the 14th International Joint Conference on e-Business and Telecommunications (ICETE 2017), 4:311 —- 318, 2017.

[55] Paul Plessing and Olamide Omolola. Revisiting privacy-aware blockchain public key infrastructure. ICISSP 2020 - Proceedings of the 6th International Conference on Information Systems Security and Privacy, pages 415–423, 2020.

[56] Conner Fromknecht, Dragos Velicanu, and Sophia Yakoubov. A decentralized public key infrastructure with identity retention. IACR Cryptol. ePrint Arch., 2014:803, 2014.

[57] Mohsen Toorani and Christian Gehrmann. A decentralized dynamic PKI based on blockchain. Proceedings of the 36th Annual ACM Symposium on Applied Computing, pages 1646–1655, mar 2021.

[58] KyungHyun Han and Seong Oun Hwang. A PKI without TTP based on conditional trust in blockchain. Neural Computing and Applications, 6, aug 2019.

[59] Amit Dua, Siddharth Sekhar Barpanda, Neeraj Kumar, and Sudeep Tanwar. Trustful: A Decentralized Public Key Infrastructure and Identity Management System. 2020 IEEE Globecom Workshops (GC Wkshps, pages 1–6, dec 2020.

[60] Jakob Schaerer, Severin Zumbrunn, and Torsten Braun. Veritaa - The Graph of Trust. 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), pages 168–175, sep 2020.

[61] Hiroaki Anada, Takanori Yasuda, Junpei Kawamoto, Jian Weng, and Kouichi Sakurai. RSA public keys with inside structure: Proofs of key generation and identities for web-of-trust. Journal of Information Security and Applications, 45:10–19, apr 2019.

[62] Kan Yang, Jobin J Sunny, and Lan Wang. Blockchain-based Decentralized Public Key Management for Named Data Networking (Invited Paper). 2018 27th International Conference on Computer Communication and Networks (ICCCN), pages 1–9, 2018.

[63] Fengyin Li, Zhongxing Liu, Tao Li, Hongwei Ju, Hua Wang, and Huiyu Zhou. Privacy-aware PKI model with strong forward security. International Journal of Intelligent Systems, (June), 2020.

[64] Yves Christian Elloh Adja, Badis Hammi, Ahmed Serhrouchni, and Sherali Zeadally. A blockchain-based certificate revocation management and status verification system. Computers and Security, 104(January), 2021.

[65] Maurizio Talamo, Franco Arcieri, Andrea Dimitri, and Christian H. Schunck. A blockchain based PKI validation system based on rare events management. Future Internet, 12(2):1–16, 2020.

[66] Aye Mi San, Nopporn Chotikakamthorn, and Chanboon Sathitwiriyawong. Blockchain-based Learning Credential Revision and Revocation Method. Proceedings of the 21st Annual Conference on Information Technology Education, pages 42–45, oct 2020.

[67] Jing Chen, Shixiong Yao, Quan Yuan, Kun He, Shouling Ji, and Ruiying Du. CertChain: Public and Efficient Certificate Audit Based on Blockchain for TLS Connections. IEEE INFOCOM 2018 - IEEE Conference on Computer Communications, pages 2060–2068, apr 2018.

[68] Murat Yasin Kubilay, Mehmet Sabir Kiraz, and Hacı Ali Mantar. CertLedger: A new PKI model with Certificate Transparency based on blockchain. Computers & Security, 85:333–352, aug 2019.

[69] Stephanos Matsumoto and Raphael M. Reischuk. IKP: Turning a PKI Around with Decentralized Automated Incentives. 2017 IEEE Symposium on Security and Privacy (SP), pages 410–426, may 2017.

[70] Maria Encinas, Ronald Martinez, Alvaro Cuno, Alfredo Gallo, Fernando Zapata, and Ricardo Saavedra. The National PKI of Peru: a new certification hierarchy. 2018 37th International Conference of the Chilean Computer Science Society (SCCC), 2018-Novem:1–8, nov 2018.

[71] Yuhao Dong, Woojung Kim, and Raouf Boutaba. Conifer: Centrally-Managed PKI with Blockchain-Rooted Trust. 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pages 1092–1099, jul 2018.

[72] Zhiguo Wan, Zhangshuang Guan, Feng Zhuo, and Hequn Xian. BKI: Towards Accountable and Decentralized Public-Key Infrastructure with Blockchain. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST, 238:644–658, 2018.

[73] Runhua Xu and James Joshi. Trustworthy and Transparent Third-party Authority. ACM Transactions on Internet Technology, 20(4):1–23, nov 2020.

[74] Wenbo Jiang, Hongwei Li, Guowen Xu, Mi Wen, Guishan Dong, and Xiaodong Lin. A Privacy-Preserving Thin-Client Scheme in Blockchain-Based PKI. 2018 IEEE Global Communications Conference (GLOBECOM), pages 1–6, dec 2018.

[75] Nikolaos Alexopoulos, Jorg Daubert, Max Muhlhauser, and Sheikh Mahbub Habib. Beyond the Hype: On Using Blockchains in Trust Management for Authentication. 2017 IEEE Trustcom/BigDataSE/ICESS, pages 546–553, aug 2017.

[76] Jorge Bernal Bernabe, Jose Luis Canovas, Jose L. Hernandez-Ramos, Rafael Torres Moreno, and Antonio Skarmeta. Privacy-Preserving Solutions for Blockchain: Review and Challenges. IEEE Access, 7:164908–164940, 2019.

[77] 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, nov 2018.

DANIEL MALDONADO-RUIZ is an adjunct professor and researcher at the Faculty of Engineering Systems at the Escuela Politécnica Nacional (EPN), Quito-Ecuador. He is also a PH.D. Candidate in Computer Science at EPN. In 2015 he completed a master's degree in Information Security Management at the Universidad de Buenos Aires, Argentina. In 2012 he got his Electronic and Networking and TI engineer degree at the EPN. His current research focuses on identity decentralisation and self-generation using new generation blockchains and smart contracts technologies.

JENNY TORRES is a professor and researcher at the Faculty of Systems Engineering at the Escuela Politécnica Nacional (EPN), Quito-Ecuador. She received her PhD in Computer Science at Sorbona University in France in 2013, and in 2009 she obtained her M.Sc in Computer Science Security at the University Paris-Est Créteil. Before obtaining a SENESCYT scholarship in Ecuador, she completed a master's degree in Management of Networks and Telecommunications at the Universidad de las Fuerzas Armadas ESPE in 2008. In 2006 she got her Computer Systems engineer degree at the EPN. She held the position of associate dean and director of the Doctoral program in Computer at EPN. Currently, she is member of the Incident Response Center CSIRT-EPN, Co-Editor of the Scientific Journal Revista Politecnica (scopus indexed) and General Chair of CSNet 2019.

NOUR EL MADHOUN received her Master's degree in Networks/Computer Science from Sorbonne Université/Télécom ParisTech in 2014, and her Ph.D. degree in Cybersecurity/Computer Science from Sorbonne Université in 2018. In 2019, she joined ISEP - Engineering School, Paris, as an Associate Professor of Cybersecurity in addition to overseeing the engineering cycle - Digital Security and Networks. In 2018, Nour gained industry experience through working as Post-Doctoral researcher at Orange Labs. At Sorbonne Université, she became an ATER in 2017. Her current research focuses on network security, cryptographic protocols, EMV payment, NFC technology, blockchain and smart-contracts technologies. Nour is currently an Associate Professor of Cybersecurity and Blockchain at EPITA - Engineering school in Paris. She is also an Associate Researcher at Sorbonne Université (LIP6-PHARE Team).

MOHAMAD BADRA is an Associate Professor at Zayed University. He received a Ph.D. degree in Security and Networking from TLECOM ParisTECH (ex. ENST). His research interests are in the areas of information security, smart city (smart grid, urban sensing, etc.), wireless sensor networks, with a focus on designing, building, analyzing, and measuring privacy and security protocols and secure architectures for wired/wireless networks. He is the author of several international standards on security exchange and the co-author of many international conference and journal papers.