Public Key Infrastructure Traditional and Modern Implementation

Ohoud Albogami, Manal Alruqi, Kholood Almalki, and Asia Aljahdali
(Corresponding author: Aisa Aljahdali)

College of Computer Science and Engneering, Unversity of Jeddah, Saudi Arabia
(Email: aoaljahdali@uj.edu.sa)

(Received Mar. 25, 2020; Revised and Accepted Oct. 10, 2020; First Online Feb. 16, 2021)

Abstract

The public key infrastructure (PKI) method is used to implement strong authentication, data encryption, and digital signatures. The PKI traditional approaches use certificate authorities (CAs) or web of trust (WoT) models; these approaches have security flaws. An emerging solution for constructing secure PKIs is blockchain. Blockchain is a distributed public ledger that works as transaction records. The development of blockchain-based PKIs has been proposed in several studies. In theory, blockchain meets many PKI requirements and addresses some security problems of traditional approaches. This paper explains the traditional and blockchain-based methods for implementing PKI and discusses their advantages and disadvantages. This paper also analyzes PKI approaches by comparing their features and limitations based on several criteria.

Keywords: Blockchain; Certificate Authority (CA); Public Key Infrastructure (PKI)

1 Introduction

A public key infrastructure (PKI) is the primary building block of many applications that rely on secure and reliable authentication, such as digital signatures and encryption for email, smart cards, and network connections. A PKI ensures that a particular entity is bound to its public key, usually by relying on trusted key servers maintained by certificate authorities (CA) [23]. These authorities issue a certificate for a domain or person that publicly and verifiably binds this entity to a specific key. A standard format for such certificates is X.509 [10]. Traditional PKI setups are mostly centralized and face some problems, such as malicious certificates that can remain undetected and allow attackers to act as a man in the middle [26].

Similarly, the revocation of keys relies on a centralized list maintained by only a few entities, implies a significant amount of trust put into a relatively small CAs. In recent years, the misuse of trust has led to distrusting certificates from specific CAs altogether [13].

One approach toward more transparency in managing certificates has been proposed by [15] and is referred to as log-based PKIs. The proposed public log allows the audit of CA activity for the process of issuing, managing, and revoking certificates but does not provide a fully decentralized approach. The advent of blockchain technology has advanced the concept of such a public log. Blockchain technology presents a mechanism for a public, decentralized, tamperproof, complete, and available list of records. A large number of blockchain-based, decentralized theoretical approaches, for example, [1, 11, 16, 19], have been discussed. They intend to deal with the challenges of traditional PKIs. Implementations of proposed approaches come with different storage types, permission models, and support for certificate formats.

This paper intends to investigate the modern and traditional implementation of PKI, deeply studying the two different approaches and presenting their advantages and limitations.

The paper is organized as follows: Section 2 gives an overview of PKI, Section 3 presents traditional approaches for implementing PKI, while Section 4 investigates the modern approaches for implementing PKI. Finally, a discussion related to the comparison of PKI implementations is presented.

2 Public Key Infrastructure

A PKI is a set of roles, procedures, hardware, and software that manage, distribute, store, and revoke digital certificates and public-key encryption. The goal of a PKI is to securely facilitate the automated transfer of information for various network activities such as sending and receiving emails, internet banking, and e-commerce. PKI confirms the identity of the parties involved in the communication and validates the information being transferred for activities where multiple rigorous proofs are required, not for simple passwords that are inadequate as authentication methods.

A PKI binds public keys with respective identities of entities (users or organizations). The binding is estab-

lished through registration and issuance of certificates that may be carried out by an automated process or under human supervision, depending on the assurance level of the binding [10].

A trusted party called a certification authority (CA) can use the PKI element to establish ownership of a public key. CA issues signing certificates that indicate and bind the identity of the certificate subject to the public key contained in the certificate. The CA uses its private key to sign the certificate. The certificate signing process enables the receiver to verify that the public key was not tampered with or corrupted during transit. The CA hashes the contents, encrypts the hash by using its private key, and includes the encrypted hash in the certificate. The receiver verifies the certificate by decrypting the hash using the CA public key, implementing a separate hash of the certificate, and comparing the two hashes. If they match, the receiver can be sure that the certificate and the public key it contains have not been altered.

3 Traditional Approaches for PKI Implementations

Two traditional approaches used to implement the PKI are certificate authority (CA) and a web of trust (WoT). This section discusses both approaches and their advantages and disadvantages.

3.1 Certificate Authority (CA)

A certificate authority (CA) is an approved entity that distributes and manages digital certificates for a network of users. A digital certificate is a digital document that has been signed by the private key of a trusted authority. The digital certificate that CA issues contain the public key and the identity of the owner. The CA validates and authenticates the identity of the user requesting for the certification by verifying if the public key that will be in the certificate belongs to the user who will own this certificate. This process is called certificate validation [3].

Recent research [4,20] called CA-based PKI as centralized PKI because the CA adopts a centralized infrastructure. The users can trust the CA by verifying the CA's signature. Consequently, users will assume that certificate information is accurate, and the public key belongs to the user identified in the certificate. Several web services are protected through keys signed by CAS.

The CA issues a digital certificate to authorize another CA to distribute certificates that can issue a digital certificate for another CA, forming a chain of trust. Certificates can then be traced backward through this chain. The chained CA certificates are called intermediate CA or sub CA certificates. The top-level CA certificate is called a root CA certificate. Self-signed certificates may be used internally in a large company or used by a small company that does not want the expense of using a CA. A CA's root certificate is self-signed by the CA and is used as a trust anchor in certificate chains [3].

3.1.1 The X.509 Certificate

X.509 is a standard for a digital certificate that is widely used in PKI. The X.509 digital certificate structure is shown in Figure 1. Certificate X.509 has different fields, depending on the version used. The required fields for all versions are version number, serial number, name of the entity associated with the public key (subject), issuer name, validity period, and public key. All this information is signed using the CA's private key. To validate a certificate, a relying party uses the CA's public key to verify the signature on the certificate, checks that the time falls within the validity period, and may also consult a server associated with the CA to ensure that the CA has not revoked the certificate [21].

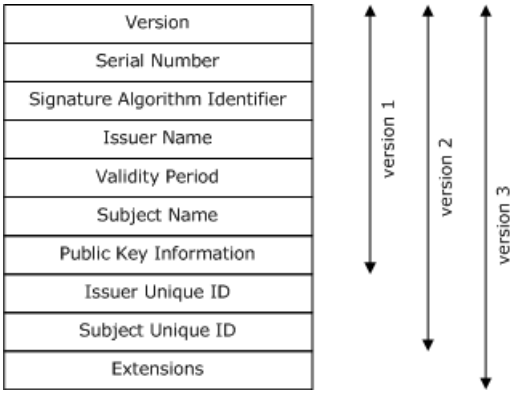

Figure 1: X.509 certificate structure [9]

The advantages of using CA in PKI are as follows:

1) The CA's digital certificate can authenticate the identity of the entity and many enterprise networks and applications using this type of certificate [26].

2) The integrity of the certificate information is guaranteed by verifying the CAs.

3) Integrity: integrity is guaranteed as long as the CA's signature on the digital certificate can be verified.

4) The signature in the certificate also guarantees non-repudiation. Non-repudiation means that the CA who signed the certificate cannot deny it has issued this certificate.

The limitations of using Digital Certificates in public key infrastructure are:

1) CA is vulnerable because of its centralized structure, which could lead to a single point of failure where the whole structure will be affected once a root CA is attacked or tampered with [4,20].

2) There is a concern for the process of certificate verification that uses more than one CA's root public keys. If the attackers add their public keys to that chain of CAs, attackers then issue certificates that will be treated as legitimate certificates [6].

3) CA is highly exposed to different forms of MITM (man-in-the-middle) attacks such as ARP spoofing, DNS spoofing, HTTPS spoofing, and man-in-the-browser.

4) Identification of an anonymous entity that has requested a digital certificate from a CA leaves serious risk for the verifier of the certificate. As a result, the verification process requires a set of verification methods. However, none of these methods can completely guarantee the authenticity of the entity [4,6].

5) In 2017, Symantec, one of the largest CAs, issued a large number of falsified certificates. Google Chrome 70 has stopped support for all certificates issued by Symantec and its affiliates [5].

3.2 Web of Trust (WoT)

In the Pretty Good Privacy (PGP) encryption program, a new concept is introduced named web of trust by Phil Zimmermann in 1991 [18]. The main goal is to authenticate the binding between a public key and the owner of the key. The PKI certificate, which is the centralized hierarchical concept, is only introduced by a CA. Unlike the PKI certificate, WoT is a decentralized public key where each one of the participants in the ecosystem can introduce the public keys of other participants. Any participant in the PGP system is viewed as a CA from the PKI viewpoint. Users of PGP can select the public keys of other users and assign them with different levels of trust. These levels of trust indicate how trustworthy the signature (introduction) of the certificate holder is when he signs public key certificates of other participants. PGP offers four levels of trustworthiness [25]:

1) Full (level 4): The signature of the certificate holder on other users' certificates is fully trusted.

2) Marginal (level 3): The signature of the certificate holder on other users' certificates is trusted to some extent, but it is preferred to find a fully trusted signature.

3) Untrustworthy (level 2): Ignoring signatures on other users' certificates is mandatory if the certificate holder is not trustworthy.

4) Don't know (level 1): There are doubts about the certainty of the certificate holder's signature trustworthiness of other users' certificates. In this case, to send protected information, it is possible to create a "chain of trust" a path from one user to another when confirming the identity is required.

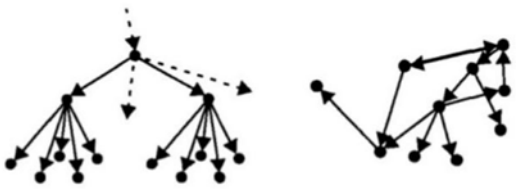

Figure 2: Primary key infrastructure vs. Web of trust [25]

This will cause the publication of a decentralized web of trust for all public keys. As mentioned, each user has a collection of the users' public keys in the ring. In the web of trust, each user encrypts his message, using the recipient's public key and only the private key of the recipient can decrypt the message to ensure confidentiality, and each user digitally signs the information with its own private key when he wants to send a message, then when they verify it using the sender public key to ensure the integrity of the message and that the message was not tampered with and it actually came from the true intended recipient [22].

One of the advantages of using web of trust in public key infrastructure is removing the probability of a central point of failure in PKI's centralized approaches because of its nature as a decentralized system [24]. The limitations of using web of trust in public key infrastructure are:

1) With scalability problem, if a user wants to trust another user not in his group of trusted users, but in one of his group of trusted users, he can simply trust that user and build a secure communication, which is not always a safe way to trust a user.

2) At first, new users must meet in person with another user already in the network of WoT to verify their identities and sign their public key certificates. Therefore, it is difficult for new and remote users to join the network without going through this process [25].

3) In case one of the users lost his private key or the private key gets compromised, WoT provide no way for key revocation. The user has a solution to choose another user on the network to revoke his certificate. It is up to the browser for revocation in some cases [22].

4 Modern Approaches for PKI Implementations

Modern approaches have incorporated blockchain technology with the PKI. This section analyzes two approaches of PKI using blockchain and their advantages and disadvantages.

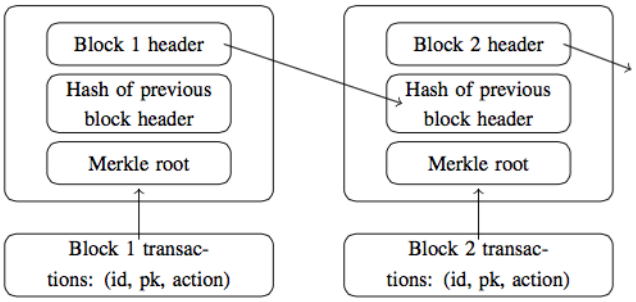

Figure 3: Blockchain PKI structure [9]

4.1 Blockchain-based PKI

A blockchain is a decentralized public ledger to which events are posted and verified by network members. The validation process is called mining in which members compete to complete some proof of work, usually a cryptographic challenge. Blockchain was first introduced as the transaction record for the Bitcoin cryptocurrency. Many blockchains for PKI have been developed, such as the Namecoin blockchain on which Certcoin and PB-PKI are built. Namecoin works as a decentralized domain name server (DNS), which, unlike the Bitcoin blockchain, can store data suitable for larger applications.

The structure of blockchain-based PKI is illustrated in Figure 5. The process of registration, update, and revocation is accomplished by sending a transaction that contains the public key and identity to the blockchain. In the blockchain, each block includes its hash and the hash of previous blocks that creates a reliable ledger that can only be modified by mining the majority of the network. The block can also contain the Merkle root, a hash of a set of transactions. This Merkle root can be used to securely verify transactions, eliminating the need to download the entire blockchain for verification [2]. Blockchain-based PKI has the following advantages:

1) Blockchain is decentralized. No central authority or third-party stores or controls the information. Instead, the information stores and controls the members of the networks.

2) PKIs using blockchain removes the potential points of failure created using CAs.

3) The transaction ledger is unchangeable. Once the transaction is recorded, it cannot be removed or altered.

4) Blockchain-based PKI provides the certificate transparency (CT) property to improve CA-based PKI security through public logging and monitoring of certificates.

5) Blockchain-based PKI also has potential advantages over WoT-based PKI, where the need to establish trust results in a high barrier to entry. The amount of work required to build a web that proves "trustworthiness" to a usefully large proportion of the network is significant. In blockchain-based PKI, entities do not require this web of attesting members, so the work needed to perform as a network member is removed [2].

6) The interaction for a blockchain can be zero-knowledge proofs, where some propositions about the transactions can be proved without revealing all its information [12].

Blockchain-based PKI has the following limitations:

1) Blockchain-based PKI does not provide privacy awareness. Therefore, building a privacy blockchain-based PKI is a complicated task that may have multiple conflicts in its requirements.

2) High resource consumption, such as CPU memory, especially in the mining process [18].

3) Blockchain-based PKIs have a master authority in charge of authentication and trust. The master authority becomes the central part of the network security and the critical point of vulnerability that attackers attack [18].

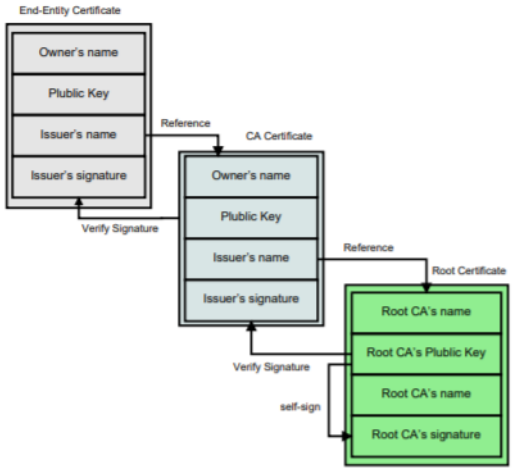

Figure 4: Chain of trust [24]

4.2 Blockchain-based PKI using X.509 Extension

Before introducing blockchain-based PKI, we must briefly discuss the chain of trust to understand types of CAs and to simplify the idea of blockchain. We already discussed CA. We defined CA as a third-party issuing certificates to anyone or any website to guarantee the confidentiality and integrity of the communicating entities' messages [24]. When a user logs in to any social media platform through

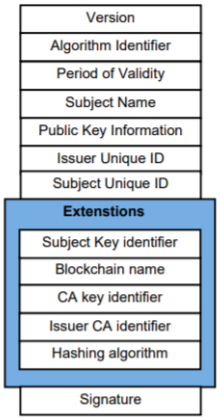

Figure 5: The X.509 hybrid certificate structure [3]

a browser, the browser first validates the platform certificate. Each browser usually has a list of known CAs already trusted and accepts certificates only from those trusted CAs. Root CA and sub CA, which is trusted by root CA, signatures are the only CAs that can issue a certificate that will be trusted to be used [24].

Figure 4 demonstrates how the chain of trust works. The web browser checks the validity of the end-entity certificates, if it's not issued by trust CA, the browser moves forward to check the validity of the CA that issued the certificate to the end entity, and so on, until the browser finally finds a trusted CA or an error is displayed [24]. Blockchain is blocks linked with each other using cryptography, with each block containing the hash of the previous block, a timestamp, and transaction data. Blockchain is a decentralized approach, so it solves the problem of single points of failure that occur in CAs. Blockchain-based PKI is basically an X.509 certificate (Figure 4) with an extension filed contains information about PKI.

The X.509 hybrid certificate structure works with the three types of certificates mentioned before, root CA, sub CA and end-user CA. Blockchain-based PKI is a hierarchy of hybrid certificates and it contains the following fields: Certificate, issued by, issued to, contract ID, and issuer CA ID. Blockchain-based PKI works as follows: the root CA certificate is issued and signed by the root CA and no issuer CA ID, the sub CA must be issued by the root CA and the issuer CA ID is the root CA contract ID. There could be more than one sub CA between root CA and end-user CA. The end-user CA must be issued by the sub CA and the issuer CA ID is the sub CA contract ID. The end-user CA has no contract ID because of the fact that the end user cannot issue certificates.

Blockchain-based PKI has the following advantages over the traditional PKI:

1) Blockchain-based PKI provides a certificate revocation mechanism, and only the parent CA that issued the certificate has the privilege to revoke the certificate and that makes Blockchain-based PKI reliable; because any modification in the network's nodes every other node will be notified [24].

2) The validation process of CAs and certificates are simple and fast [24].

3) Provides a high level of protection against Man in The Middle attack; because when one CA revokes or publishes a public-key of a website or domain on the blockchain th3e modification will be distributed across thousands of nodes which makes it impossible for anyone to tamper the public-key [24].

Table 1: The blockchain hybrid certificate [24]

Cert.	Issued By	Issued To	CA Contract ID	Issuer CA ID
RootCA	RootCA	RootCA	0x1234xxxx	0x00000000
SubCA	RootCA	SubCA	0x5631xxxx	0x1234xxxx
EndUser	SubCA	End user	-	0x5631xxxx

Blockchain-based PKI has the following limitations:

1) Due to the blockchain nature, as the blockchain's size increases more space needed, which may affect the performance [24].

2) The blockchain operation cost depends mainly on the price of the cryptocurrency, for example: In May 2017 Ether price was 85.43 dollars growing 8 times just in 7 months apart December 2017 to be 729.01 dollars [24].

3) If the user lost his/her account's password of the blockchain platform, his/her account becomes irrevocable and he/she will lose the right to access and modify certificates authority data.

5 Discussion

In this section, we analyze the previous PKI approaches by comparing their features and limitations based on several criteria, including system structure, management framework, validation process, revocation process, certificate transparency, level of protection, scalability, privacy, trust, and performance. Table 2 shows a summary of the compression between PKI approaches.

System Structure: The traditional approach CA-based PKI is centralized since it relies on a trusted third party to control the process of issuing, validating, and revoking the certificate. Therefore, the CA is subject to bottleneck, single point of failure, and different attacks because of its centralized structure.

In contrast, the WoT is a decentralized structure in which each participant can introduce the public keys of other participants. The modern approach is also decentralized based on blockchain technology, where a public ledger's linking identity with the public key is distributed over a peer-to-peer network. Decentralization does not have a single point of failure and solves security issues of the central authority.

Table 2: Comparing the discussed techniques based on different factors

Features-approach	**CA**	**WOT**	**PB-PKI**	**Blockchain-based PKI using X059**
System Structure	Centralized	Decentralized	Decentralized	Decentralized
Management Framework	Organized but no real-time monitoring	Complex and no real-time monitoring	Real-time monitoring	Real-time monitoring using a smart contract
Validation process	Simple and fast	Complicated and time-consuming	Simple and fast	Simple and fast through The Smart contract or Web service
Revocation process	Cumbersome, not instant and revocation lists are not immutable	No way for direct revocation	Revocations instantly and the revocation lists are immutable	Revocations instantly and the revocation lists are immutable
Certificate Transparency (CT)	Does not use CT	Does not use CT	Use CT	Use CT
Security (Level of protection)	Low level of protection and exposed to different attacks	Low level of protection and exposed to different attacks	High level of protection	High level of protection
Trust	Has trust issues	Different levels of trust	Trustable	Trustable
Privacy	privacy	Does not consider privacy	High level of privacy	Does not consider privacy
Scalability	No concerns	not always reliable	significant concerns	significant concerns
Performance	Reasonable	Affected by some factors	Affected by some factors	Affected by some factors

Management framework: CA-based PKI is a popular and commonly used approach compared with other methods. The CA has evolved over the years, which makes the management framework in CA well designed, manageable, and organized. Thus, the management process of CA is more precise and adaptable. However, the CA still does not provide real-time monitoring. WoT is the less popular approach because of the complexity in the framework management and registration process. The modern approaches provide real-time monitoring, but the PB-PKI [2] is not suitable for identity management because of its strict privacy and transparency requirements. The management process of blockchain-based PKI [24] is performed using a smart contract for each CA that makes the management of framework straightforward because the smart contract is stored in the blockchain, accessible to every peer in the network and cannot be tampered with.

Validation process: In traditional approaches, the CA's validation process is considered simple with few steps and not time-consuming. Conversely, the WoT model is complicated and time-consuming because new users must meet in person with another user already in the WoT network. In the modern implementation of PKI, both approaches perform a simple validation process without revealing all information in the certificate validation in [24] using the smart contract or Web service.

Revocation process: The CA can revoke the certificate, but the process of revocation is cumbersome and not instant. The CA's revocation lists are not immutable and can be recreated with a different content. In WoT, it does not have a way for direct revocation. The only one solution is to choose another user on the network to revoke the certificate. For modern approaches, they can revoke the certificate instantly and the revocation lists are immutable.

Certificate transparency (CT): The modern implementations of PKI use the certificate transparency (CT) while the traditional PKI implementations do not use it. The CT is an Internet standard providing public logs that record all certificates issued. CT goals are to monitor, auditing, and detecting mistakenly or maliciously issued certificates [14].

Security (level of protection): The security level of the traditional approaches is considered low since the CA and WoT are highly exposed to different attacks,

such as MITM. In many scenarios, CAs had been attacked and issued falsified certificates. The security level of blockchain is high since it has not been attacked until now. Both blockchain and WoT rely on a decentralized structure. However, blockchain is more secure than WoT because it uses a timestamp, immutable ledger, encryption, and consensus protocol such as proof of work and proof of stack.

Trust: CA has trust issues because it was exposed to different attacks. In some cases, the user or organization needs to trust multiple certification centers. In WoT, the users assign different levels of trust (from one to four) to other users. These levels of trust indicate how trustworthy the signature of the certificate holder is. The modern approaches are trusted for many reasons. such peer-to-peer network, transactions being visible and stored in all peers, and trust given only to the parent CA that issued the certificate.

Privacy: The CAs have some level of privacy, but some of the privacy requirements are not included. WoT and blockchain-based PKI [24] do not consider privacy, and a transaction's information is publicly available to the network participants. On the other hand, PB-PKI's privacy requirements are considered in the design phase, which provides a high level of privacy to PB-PKI.

Scalability: There are significant concerns about the scalability in the blockchain-based PKI because of the increase in the chain's size that may affect other aspects of the blockchain [7].

WoT scalability is not always reliable. The users can trust and join other users, not in their group of trusted users. For example, if user A has B in his trusted group and B has C in his trusted group, then user A can trust C. The scalability of CA is better and more efficient when compared with the other approaches.

Performance: The performance here means the time consumed, the consumption of resources, and storage overhead. The CA's performance is reasonable in terms of the consumption of time and resources. CA-efficient storage keeps certificates on individual devices. PKI-based blockchain has factors that affect performance, such as the decentralization system, peer-to-peer networks, and consensus algorithms in which the participants perform most of the work. Thus, blockchains cannot ensure fast and stable data transfer as centralized systems CA.

In the end, the most critical question is, what is the best implementation of PKI' From our point of view, security is the most important thing to consider when configuring a PKI. The system needs a guaranteed and secure management of public keys. In a modern approach, the PKI model using blockchain technology provides a higher level of security than other approaches and removes the potential points of failure created by the use of CAs. Indeed, the modern approach faces some limitations and challenges. However, blockchain is a recent technology that has gained much attention. We believe that blockchain's scalability and performance issues will be overcome soon, especially because of the emergence of a new generation of blockchain 3.0 [17] that focuses on solving these problems.

6 Conclusion

The PKI method is used to implement strong authentication, data encryption, and digital signatures. The traditional approaches of PKI use CAs and WoT models. These approaches have security flaws. An emerging solution to constructing secure PKIs is blockchain. This paper investigates the modern and traditional implementations of PKI. It studies these approaches and presents their advantages and limitations. The paper also provides a comparison between all approaches based on various criteria, such as system structure, management, revocation, validation, privacy, security, and performance. For future research, we will conduct experiments for all approaches against several criteria, evaluate their security, and measure their performance.

References

[1] N. Alexopoulos, J. Daubert, M. Muhlhauser, S. M. Habib, "Beyond the hype: On using blockchains in trust management for authentication," in *IEEE Trustcom/BigDataSE/ICESS*, 2017. DOI: 10.1109/Trustcom/BigDataSE/ICESS.2017.283.

[2] L. M. Axon, and M. Goldsmith, "PB-PKI: A privacy-aware blockchain-based PKI," in *International Conference on Security and Cryptography*, 2016. (`https://doi.org/10.5220/0006419203110318`)

[3] P. Black, R. Layton, "Be careful who you trust: Issues with the Public Key Infrastructure," in *The Fifth Cybercrime and Trustworthy Computing Conference*, 2014. DOI: 10.1109/CTC.2014.8.

[4] Y. Chu, *et al.*, "SS-DPKI: Self-signed certificate based decentralized public key infrastructure for secure communication," in *Digest of Technical Papers - IEEE International Conference on Consumer Electronics*, 2020. DOI: 10.1109/ICCE46568.2020.9043086.

[5] DigiCert, *Replace Your Symantec SSL/TLS Certificates.* (`https://www.digicert.com/blog/replace-your-symantec-ssl-tls-certificates/`)

[6] C. Ellison and B. Schneier, "Ten risks of PKI: What you're not being told about public key infrastructure," *Computer Security Journal*, vol. 16, no. 1, pp. 1-7, 2000.

[7] I. Eyal, *et al.*, "Bitcoin-NG: A scalable blockchain protocol," *Cryptography and Security*, 2015. arXiv:1510.02037.

[8] K. Isirova, O. Potii, "Decentralized public key infrastructure development principles," in *IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, pp. 305-310, 2018.

[9] Mike Jacobs, Michael Satran, *X.509 Public Key Certificates*, May 31, 2018. (`https://docs.microsoft.com/en-us/windows/win32/seccertenroll/about-x-509-public-key-certificates`)

[10] A. T. Kaimov, A. T. Kaimov, *Public Key Infrastructure: A Survey*, 2018. (`https://repository.kbtu.kz/xmlui/handle/123456789/75`)

[11] E. Karaarslan and E. Adiguzel, "Blockchain based DNS and PKI solutions," *IEEE Communications Standards Magazine*, vol. 2, no. 3, pp. 52-57, 2018.

[12] A. E. Kosba, A. Miller, "The blockchain model of cryptography and privacy-preserving smart contracts," in *IEEE Symposium on Security and Privacy (SP'16)*, 2016. DOI: 10.1109/SP.2016.55.

[13] D. Kumar, Z. Wang, M. Hyder, J. Dickinson, G. Beck, D. Adrian, J. Mason, Z. Durumeric, J. A. Halderman, M. Bailey, "Tracking Certificate Misissuance in the Wild," in *IEEE Symposium on Security and Privacy (SP'18)*, 2018. DOI: 10.1109/SP.2018.00015.

[14] B. Laurie, "Certificate transparency," *Communications of the ACM*, vol. 57, no. 10, pp. 40-46, 2016.

[15] B. Laurie, A. Langley, E. Kasper, *Certificate Transparency*, RFC 6962, 2013. (`http://www.rfc-editor.org/info/rfc6962`)

[16] R. Longo, F. Pintore, G. Rinaldo, M. Sala, "On the security of the blockchain BIX protocol and certificates," in *International Conference on Cyber Conflict*, 2017. DOI: 10.23919/CYCON.2017.8240338.

[17] D. D. F. Maesaa, P. Mori, "Blockchain 3.0 applications survey," *Journal of Parallel and Distributed Computing*, vol. 138, pp. 99-114, 2020.

[18] A. Moinet, B. Darties, J. L. Baril, "Blockchain based trust & authentication for decentralized sensor networks," *Cryptography and Security*, 2017. arXiv:1706.01730.

[19] H. Orman, "Blockchain: The Emperors New PKI?," in *IEEE Internet Computing*, vol. 22, no. 2, pp. 23-28, 2018.

[20] B. Qin, *et al.*, "Cecoin: A decentralized PKI mitigating MitM attacks," *Future Generation Computer Systems*, vol. 107, pp. 805-815, 2020.

[21] J. Vacca, *Computer and Information Security Handbook*, 2009. eBook ISBN: 9780080921945.

[22] S. Wilson, "Some limitations of web of trust models," *Information Management & Computer Security*, vol. 6, no. 5, pp. 218-220, 1998.

[23] P. W. Wong, N. Memon, "Secret and public key image watermarking schemes for image," *IEEE Transactions on Image Processing*, vol. 10, no. 10, pp. 1593-1601, 2001.

[24] A. Yakubov, *et al.*, "A blockchain-based PKI management framework," in *IEEE/IFIP Network Operations and Management Symposium*, 2018. DOI: 10.1109/NOMS.2018.8406325.

[25] A. Yakubov, W. M. Shbair and R. State, "BlockPGP: A blockchain-based framework for GPG key servers," in *The Sixth International Symposium on Computing and Networking Workshops*, pp. 316-322, 2018.

[26] J. Yu, M. Ryan, "Evaluating web PKIs," in *Software Architecture for Big Data and the Cloud*, 2017. DOI:10.1016/B978-0-12-805467-3.00007-7.

Biography

Ohoud Albogami received her bachelor's degree in information technology (IT) from King Abdul-Aziz University (KAU), KAS, in 2017. She is currently a master's Student at Jeddah University (JU), KAS. Her current research interest includes clustering, Trust computing systems in vehicular ad hoc networks, and blockchain.

Manal Alruqi graduated from King Abdul-Aziz University with a Bachelor of Science in Information Technology. She is currently a master's student in Computer Science at Jeddah University. Her research interests include Blockchain Technology, Distributed Systems Security, Artificial Intelligence, and Machine Learning.

Kholood Almalki received her undergraduate degree in Information Technology at King Abdul-Aziz University, Faculty of Computing and Information Technology, in 2017. Currently, she is pursuing a master's degree in Computer Science at Jeddah University. She has published a scientific paper in Human-Computer Interaction titled "Anti-procrastination Online Tool for Graduate Students Based on the Pomodoro Technique."

Asia Othman Aljahdali received her Ph.D. degree in computer science at Florida State University in 2017. And a master's degree in information security in 2013. Later on, she worked at King Abdul-Aziz University as assistance Professor. Then, she worked at university of Jeddah as an assistance professor in cybersecurity department. Currently, beside her academic work, she works as cybersecurity consulate for the administration of cybersecurity in Jeddah university. Her current research interests include information security, cryptography, data hiding, network security, IoT security, and Cloud security.