Use of Blockchain in Public Key Infrastructure (PKI): A Systematic Literature Review

Nouf Aldahwan
Department of Information Systems
College of Computer Sciences
King Khalid University
Abha, Saudi Arabia
naldhwan@kku.edu.sa

Daniyal Alghazzawi
Department of Information Systems
Faculty of Computing and Information Technology
King Abdulaziz University
Jeddah, Saudi Arabia
dghazzawi@kau.edu.sa

***Abstract*—Blockchain technology has revolutionized the way people conduct transactions online. The distributed ledger technology has enabled the recording and tracking of resources and information even without a trustworthy authority as a central figure. Users can exchange transactions that are grouped into blocks following a particular sequence. The distributed append-only ledger allows messages to be recorded without reversal making it one of the most efficient technologies to share critical information and transact resources. An additional technology that has grown to become one of the most preferred security solutions, particularly for e-commerce transactions is Public Key Infrastructure (PKI). PKIs are complex systems comprising of multiple components that require coordination and integration of an organization's business models. PKI uses two digital keys, one public, and another secret to ensure the confidentiality of a transaction, encryption, authentication, and signing of electronic data digitally. In this paper, we illustrated issues related to the PKI field, and then discussed how Blockchain technologies can fix this problem. We also illustrated the problems that occur with Blockchain being implemented.**

***Index Terms*— Blockchain, Public Key Infrastructure (PKI).**

I. Introduction

The world is experiencing unprecedented changes due to the rapid revolution in wireless communication and electronics technologies. The effects of this rapid revolution have been an increase in the number of suitable technologies for every sector and the need to protect and the need to secure data shared on these technologies. Some of these two technologies are Blockchain and Public Key Infrastructure (PKI). Blockchain technology has emerged as one of the ways to share information and tracking resources in a secure and trustworthy manner. The distributed ledger technology records and tracks transactions without a centralized authority. The technology is secured and shared allowing two parties to exchange resources.

The information and resources are exchanged across a peer-to-peer network using assurance mechanisms and cryptographic trust. The technology allows the value-exchange transactions to be grouped into blocks following a particular sequence. The distributed append-only ledger allows messages to be recorded without reversal [1]. The fact that the messages can be recorded irrevocably means that two parties can communicate without central intermediaries. The fact that there are no central intermediaries means that the technology is secure and not easily compromised. Both tangible and intangible resources such as money, lands, houses, digital documents, intellectual property rights, and copyrights can be secured using a Blockchain network. Critical information such as crucial critical sector data can be shared securely through the network. Therefore, Blockchain technology promises transparent systems that are secure and not compromised to enable the sharing of information and resource transfer.

This paper addresses the systematic review to identify, analyze, interpret, compare and evaluate existing Blochchain solutions used to secure PKI.

In this study, we performed a systematic literature review to identify PKI-related issues in the field, and highlighted various Blockchain technology features which could be used to resolve those issues.

The structure of the paper is as follows. Section II, is literature review. Section III offers a summary of our research methodology and intent for undertaking this analysis of the literature. Section IV is split into three parts, section 1 illustrates problems in the PKI domain; section 2 analyzes how to use Blockchain to fix these issues. Part 3 addresses problems

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

related to Blockchain implementation in PKI. Ultimately, the conclusion is concerned with in section V.

II. Literature Review

This section discusses the Blockchain approaches previous literature review to illustrate the need for this SLR.

A. Blockchain Overview

Blockchain is distributed and regulated through a network of nodes by consensus-based protocols. This was first time introduced as a decentralized form of network for peer-to-peer purpose utilizing work proof for transferring money to restrain central authorities from interference with the transactions in general. It constitutes various chains of blocks in the form of data packages that commence with block of genesis that is first block in this system of Blockchain. New models get added in the block chain as it grows. Every block consists of timestamp, value of nonce, list of various transactions, previous bloc's harsh value and computed has values of corresponding blocks. Before adding it to chain, a mechanism of consensus is ensured that most nodes would agree utilizing some procedures and rules on validity of transactions and all new blocks [2].

B. Blockchain Type

Three types of Blockchain exist: private, consortium and public. Private signifies that neither participation nor reading in the process of consensus is permitted till grant of authorization. Consortium means that reading can be either private or public but authorization is required in process of consensus [3].

C. Blockchain Application

The use of Blockchain technology for different network security services determines that the technology is suitable and beneficial in resolving problems encountered with traditional approaches to achieve the required service [1]. The survey also provides Blockchain-based approaches that can help to resolve the problem with traditional approaches for providing the network security services. The survey also identifies the challenges of using Blockchain technology and future directions to guide its use. The security services that the study focuses on include confidentiality, integrity assurance, access control list and privacy, authentication, and data and resource source. The encryption and authentication services, Blockchain features such as non-reproducibility, distributed, and event-recording make the technology suitable for several applications particularly the domain name services (DNS) and PKI. The fact that the technology offers distributed solutions makes it difficult to have a centralized point of failure. Besides, there is no single trusted third party making the technology more trustworthy [1]. An additional of using Blockchain technology to provide encryption and authentication services is the open-source implementation that makes it an efficient and yet cost-effective solution. For privacy services, the survey recommends the use of Blockchain technology approaches such as Zyskind, Fair Access, and Bitcoin to provide efficiency, data ownership control, and scalability. The end-to-end data privacy guarantees are decentralized. Besides, the technology allows change of access rights to data ownership when needed. In the provision of provenance services, traditional approaches are ineffective, complex, and lack centralized controllers. For instance, cloud hardware and software have several layers of interoperability, which results in inefficiency in logging techniques. Blockchain is a shared ledger that records everything in the system. Therefore, the fact that it can record data originality and transactions conducted through the same makes it effective for provenance services. Integrity assurance services ensure that data is not altered or modified at any time by unauthorized services. Blockchain technology can be used to track any individual who tampers with the data, unlike traditional approaches. The technology also provides the integrity of the data and ensures no outsider tampers with the data. However, even though Blockchain technology provides better services, it is time-consuming.

The common risks to Blockchain technology are vulnerability, inability to recover the user key in case it is lost, vulnerable to criminal activities such as money laundering, and leaking of transactions because the privacy protection measures are not robust [4]. However, the authors suggest security enhancements that can make Blockchain technology more efficient. Using secure, efficient, and decentralized smart pool systems can help to address the problems. OYENTE that is used to detect bugs can also help to make the system more secure from hacking

The single-point-of-failure problem can be solved using the block-chain characteristics of non-tampering and distribution, and to solve the identity privacy problem, LEDGERA's privacy-conscious PKI program based on enabled block-chain is proposed. The system achieves this by implementing anonymous digital certificate publishing, which helps separate user registration from authorization, with conditional traceability, to the protection of privacy of users' identities [5]. For instance, the X.509 and PGP traditional PKIs are affected by usability and security issues. Solutions offered by Blockchain can be implemented either independently, or as extensions to the existing traditional PKI methods. Blockchain that have been implemented independently would provide stronger security unlike when implemented as extensions to existing PKIs, which makes them more preferable. However, the adoption of this particular type depends on block-chain advancements concerned with the issue of scalability. Blockchain based solutions have had a problem with scalability, usually brought about by transactional throughput [6].

D. Public Key Infrastructure (PKI) Overview

PKI is the cornerstone and center of building network security, and is the critical assurance of implementing e-commerce defense. PKI technology is used for many ways, including e-mail encryption, virtual private networks, etc. PKI technology uses public key certificate management, connects the user's public key to other user personally identifiable information via a trusted third-party authentication certificate authority, validates user identity on the Internet and sends user identity through CA Digital data is protected to ensure security [7].

PKI needs several CA signatures to each certificate, only in the event of carelessness or compromise. When a CA is

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

compromised, the risk of certificates getting issued to unauthorized users presents itself. Consequently, the security of the corresponding end users is placed at risk. This represents the single-point-of-failure that CAs introduce. Technological advances in Blockchain make it possible to implement trustless systems where immutable ledgers that have fast consensus, and that require no TTPs, are used [8].

SecureGuard as mechanism for certificate verification in public key infrastructure is essential in enhancing efficiency. According to the authors, SecureGuard can handle certificate validation effectively and promptly during TLS handshakes, unlike the current popular certificate validation systems. SecureGuard uses Internet Service Providers (ISPs) that internet accessibility [9]. Besides, ISPs provide security services that enable the blocking of spammers. The study proposes that SecureGuard resolves many limitations that are in the current approaches. It is not time-consuming because it requires less computation time. Besides, it requires less storage size and network bandwidth. Besides, the approach can provide validation for any device because the cryptographic validation is done on the ISP proxy-cache server side.

Security protocols based on PSKs are able to ensure secure communications between two devices. Unfortunately, Blockchain PKIs often substitute flexibility and scalability for decentralization. This can be solved using Conifer, a PKI whose architecture is based on CONIKS, a unified and transparent PKI, and Catena, an agnostic Blockchain for the embedding of permitted logs. This way, Conifer is able to achieve far better performance and scalability, unlike pure Blockchain based approaches [10]. Conifer can also be easily integrated into different applications, and has a design derived from transparency-based and centralized PKIs. With this design, auditable and hard to forge third party activity logs are implemented in order to increase public visibility for third party activities. This would help reduce the possibility that any potentially malicious third parties will carry out attacks against systems using the Conifer PKI. This is mostly due to the fact that certificate authorities have to deposit certificates transparently, where anyone with access to them can do an examination to check for any suspiciousness.

PKI privacy problems can be solved through PTS (Privacy-Preserving Thin-client Scheme) which implements anonymity, thus giving thin clients the ability to normally run as full-node users, while protecting their privacy at the same time. This does away with the need for users working with portable devices to download entire Blockchain for them to be able to perform various operations. To minimize the costs associated with this, an EPTS (Efficient PTS) that employs PIR (Private Information Retrieval) may be implemented [11]. The EPTS utilizes PIR with the aim of protecting the privacy of a user's search during data retrieval from the servers, so as to eliminate the possibility of tracking their search content. As a result, EPTS achieves significantly high security, in addition to comprehensive functionality, which makes it most preferable over existing schemes.

E. Advantages and Disadvantages Related with PKI.

Encryption and public key infrastructure have both advantages and disadvantages. First PKI is all-inclusive. This enables encryption through public key through the use of digital signatures. PKI helps in the management of keys and certificates. PKI is also critical in providing security when transferring digital information [12]. It ensures that transactions remain confidential and the information does not fall in the wrong hands. Besides, it secures the information of consumers particularly their credentials when conducting transactions. One disadvantage of PKI solutions is that the versions of PKI vary and therefore if an organization is using a vendor who becomes bankrupt or stops providing the service; it becomes harder to get services for the future. Besides, there are certificate issued fraudulently that act as substitutes for kernel software. The issued certificates may contain malware imitating code-signing certificates that place data at risk.

III. Research Methodology

This section discusses the methods, methodologies and intent of writing an SLR paper on the PKI domain's current problems and how to solve those problems using Blockhcain technology. Secondly, would it offer researchers help to find out whether the combination of Blockchain and PKI is successful or not? [13].

A. Research Motivation

The research questions based on the motivation that: to outline PKI-related problems, and at the same time presented how Blockchain's technology would provide them with a solution. In addition, those issues were highlighted in this paper which occurs after using Blockchain in PKI (see table I).

TABLE I
Research Questions

Research Question	Motivation
What are issues related to the area?	Plan to deal with the issues faced by PKI.
Plan to fix problems with the PKI Blockchain features used to solve the defined problem.	The goal is to look for Blockchain functionality which will help overcome PKI problems.
What are the problems of Blockchain Implementation at PKI?	The goal is to list the problems that occur during Blockchain implementation at PKI.

B. Research Strategy

We have created search approach in this step to retrieve all the related studies that answer the research question. This approach outlined which sources to search for and how the search terms should be executed.

Using the keywords Blockchain and PKI, we checked papers in Digital Libraries IEEE. After that, we outlined those papers relevant to our search area.

C. Inclusion and Exclusion Criteria

We chose 44 different articles in inclusion which were close to our keyword for research. After reviewing the abstract and the conclusion, we exclude the irrelevant papers and almost 11 papers we consider to be very important to our interests (see table II).

TABLE II
Inclusion and Exclusion Criteria to Select the Researches.

Inclusion Criteria	Exclusion Criteria

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

Include the newest edition of the article if different versions are available.	Eliminate non-journal and non-Conferences papers.
Include the articles published between (Jan- 2018 to 2020).	Eliminate Books, Book Chapters, and Thesis.
Include the articles published in English in electronic format.	Not related to research Questions.

D. Study Selection

The purpose of this step is to select narratively relevant studies that could address the main research questions. We clarify a set of criteria for inclusion and exclusion (see table III).

TABLE III
SELECTED PAPERS.

Study #	Authors	Title	*Year*	*References*
1	Wentong Wang, Xin Liu	BlockCAM: A Blockchain-based Cross-domain Authentication Model	2018	14
2	Abu Shohel, Tuomas Aura	Turning trust around: Smart Contract-assisted Public Key Infrastructure	2018	15
3	Rong Wang, Juan He, Wei-Tek, EnyanDeng	A Privacy-Aware PKI System Based on Permissioned Blockchains	2018	16
4	Thomas Hepp, Fabian Spae, Alexander Schoenhals, Philip Ehret, and Bela Gipp	Exploring Potentials and Challenges of Blockchain-based Public Key Infrastructures	2019	6
5	Elie Kfoury David Khoury	A Privacy-preserving Thin-client Scheme in Blockchain-based PKI	2019	11
6	Ankush Singla Elisa Bertino	Blockchain-based PKI solutions for IoT	2018	17
7	Alexander Yakubov, Wazen M. Shbair, Anders Wallbom, David Sanda, Radu State	A Blockchain-Based PKI Management Framework	2018	5
8	Ankush Singla, Elisa Bertino	Blockchain-based PKI solutions for IoT	2018	18
9	Elie Kfoury David Khoury	Distributed Public Key Infrastructure and PSK Exchange Based on Blockchain Technology	2018	19
10	Tara Salman, Maede Zolanvari, Aiman Erbad, Raj Jain, and Mohammed Samaka,	Security Services Using Blockchains: A State of the Art Survey	2019	1
11	Enis Karaarslan and Eylul Adiguzel	Blockchain Based DNS and PKI Solutions	2018	20

E. Data Extraction

The goal of this step is to answer the research questions by collecting the required data. We gathered from each study the data presented in Table IV.

TABLE IV
DATA EXTRACTION FORM SELECTED PAPERS

Study #	Problem	Solution	*Ref*
1	Bottlenecks and the Complex Certification Delivery	BlockCAM (cross-domain authentication model)	14
2	Certificate Transparency and Dynamic Trust Management	Smart Contract-assisted PKI (SCP)	15
3	Single Point Failure and Poor Efficiency	A privacy-conscious PKI program based on BCs allowed	16
4	-Security and Usability -Cost of operation	-Purely blockchain based solutions -Adding Blockchain doesnot raise the cost	6
5	Privacy Issue	a privacy-preserving Thin-client Scheme (PTS)	11
6	Misbehaving Certificate Authority (CA)	Blockchain-based PKI (open-source Hyperledger Sawtooth)	17
7	SSL /TLS PKI	Blockchain-based PKI (Log-based PKIs, WoT approaches)	5
8	CA-based PKI	Blockchain-based PKI management	18,1
9	Complexity of Certificate Distribution	Distributed PKI platform based on the Ethereum Blockchain.	19
10	WoT-based PKI	Does not need a prior trust. The decision is taken by majority vote.	1
11	CA-based and the WoT-based PKI	The technology has a history of recording events, so it can test whether or not a public key has been documented before.	1

F. Publication Trend

Trend in publishing we mentioned papers in our research that were no older than 2018. We tried to highlight certain high impact factor papers or quotes, so most paper choices were made based on quality publishers such as IEEE.

IV. RESULT

This section describes the actual results obtained from our paper research. They are subdivided into three sections. In part 1 problem are illustrated in the PKI domain along with their short introduction. Blockchain performs in second part work on the solution of these problems. We have proposed a solution here for some problems that are discussed in various primary

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

studies relevant to it. Finally, problem of Blockchain implementation with PKI is discussed in the last part.

RQ1: What are issues related to the area?

1- CA-based PKI Issue

The Certification Authority (CA) is responsible for issuing, retaining, verifying and revoking certificates from the public key. Multiple CAs together form the CA-based Public Key Infrastructure (PKI). Using a PKI reduces trust in the CAs, who have a PKI that causes one to believe and trust in the CAs, which have proven to be a single point of failure on many occasions [18].

2- Secure Socket Layer (SSL)/ Transport Layer Security (TLS) PKI issues

PKI is vulnerable to risks due to potential vulnerabilities of Certificate Authorities (CAs) that could be used to grant unauthorized certificates for end-users. Several recent events suggest that if a CA is violated, the security of future end-users will be at risk [5].

3- Security and Usability

Conventional PKIs, X.509 and PGP in particular, are being plagued by security and accessibility problems. They are not only semantic, as repeated events imply, but allow hackers to cause long term damage [6].

4- Cost of Operation

CAs are required to pay for the services they provide. While the facilities are open, they can only issue domain-validated (DV) certificates. PGP concentrates on establishing trust relationships on a voluntary basis [6].

5- Misbehaving Certificate Authority (CA)

The present PKI is based on the CA, which can become an obstacle and can impact the performance of the cryptographic protocol as compared to the workload produced by verifying cryptographic signatures and certificates. Blockchain has also been used lately to help PKI without a central authority [17].

6- Complexity of Certificate Distribution

PKI and CAs are the main focus of the security technologies already in place. Such solutions include a large infrastructure for the administration of service certificates. Therefore, every device needs to have a client certificate to authenticate itself. The distribution of certificates for many devices is unreliable, costly and almost difficult especially in IoT networks [19].

7- Bottlenecks and the Complex Certification Delivery

The need for network infrastructure and resources is growing due to the growth of the Internet. In a shared networking system where people and organizations exchange their own resources. Avoid unauthorized users of those common services [14].

8- Certificate Transparency and Dynamic Trust Management

The Compromise (CA) and the consequent miss-issue of certificates often raise the value of the validity of the certificates and the dynamic trust management of certificates. Transparency certificate (CT) provides confirmation for given certificates, thereby requiring corrective action on a CA certificate that has been misused. However, the CT and current systems are unable to express the dynamic state of trust [15].

9- Privacy Issue

Due to single point of failure modern centralized PKIs are vulnerable. An effective alternative would be to construct a decentralized PKI without the certificate authority (CA). Trust network is the first step towards achieving a decentralized PKI but it also has other drawbacks, such as lack of motivation and privacy leakage [11].

10- Single Point Failure and Poor Efficiency

The following points apply to PKI. (1) Once managed, the core CA is vulnerable to an attack, the CA root certificate and the CA certificate are no longer validated. (2) Inadequate production of deployed Certificates. The user should first request for CA certificates, the user must customize or install the certificates at his destination on the computer or server [16].

RQ2: Plan to fix problems with the Blockchain features used to solve the defined problem?

1- CA-Based PKI

Blockchain technology as an evolving solution theoretically solves the issues of Conventional PKI systems-including the elimination point of failure and the quick reaction to CA vulnerabilities. In this research, a blockchain-based PKI management system was developed to authorize, validate and Revoke certificates X.509. Assessment and experimental findings show that the architecture proposed is offers moderate maintenance costs for more efficient and robust PKI systems [18].

2- Secure Socket Layer (SSL)/ Transport Layer Security (TLS) PKI

The blockchain-based approach incorporates the advantages of log-based PKIs and WoT techniques, which solves some of the problems with conventional PKIs. The potential fail-of log-PKI solution and implementation problems are resolved on one side by Blockchain. By comparison, the Blockchain -based approach mitigates WoT's need for new certificate holders to demonstrate the trustworthiness of the current network member [5].

3- Security and Usability

On the other hand, strictly Blockchain -based systems provide improved protection and greater versatility. Designated solutions gain improved customer service and scale improved, thus sacrificing future decentralization [6].

4- Cost of Operation

Adding a Blockchain does not raise the cost for clients or consumers, but just by running the ledger it generates funds for miners [6].

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

5- Misbehaving Certificate Authority (CA)

Using open-source Hyperledger Sawtooth to build and applying a Blockchain based PKI. The emerging Blockchain - based solution aids address the current PKI problems such as corrupted and misbehaving CAs [17].

6- Complexity of Certificate Distribution

Distributed Ethereum Blockchain based PKI network. It includes a shared key-store containing all devices ' public keys, and includes a generic protocol for PSK security protocols to protect the channel of communication between two devices. In addition, this innovative program could theoretically remove the confidence need to place on customers by the current PKI / CAs infrastructure [19].

7- Bottlenecks and complicated Certification Transmission

A Blockchain -based cross-domain authentication model called BlockCAM was implemented and a cross-domain verification protocol was developed. BlockCAM uses collaborative Blockchain technology as the identification nodes to create a decentralized network with the root certificate authorities. BlockCAM has decentralizing, transparent and temperature-resistant characteristics [14].

8- Certificate Transparency and Dynamic Trust Management

The study presents Smart Contract Supported PKI (SCP)-a PKI expansion based on the complicated trust network of a smart contract to control PKI. SCP facilitates shared trust in PKI, offers a flexible trust management protocol; ensures a certificate's state of trust and offers end-users a better experience of trust [15].

9- Privacy Issue

The study suggests using the PIR (private information retrieval) method an efficient privacy preservation Thin-Client Scheme, to reduce costs. Security review and functional contrast were then conducted to demonstrate EPTS' high level of safety and robust functionality compared to existing schemes [11].

10- Single Point Failure and Poor Efficiency

The study implements an accepted BC-based privacy-aware PKI program. The program fulfills certificate security and confidentiality requirements, reduces CA architecture, service and maintenance expenses and increase certificate performance in conventional PKI technology service and deployment [16].

RQ3. What are the problems of Blockchain Implementation at PKI?

Given the potential advantages of Blockchain technology, there are still some obstacles that restrict its convenience for the applications of security listed in the preceding sections. Within this part we explain of those problems.

1- Privacy and Anonymity

It is important for security, as the public Blockchain are open and user data is vulnerable to attackers. Thus, the transactions connect the user identity to their public key, the ACL, for most of the methods discussed, or the authenticity details. There are flaws in the Blockchain features of privacy and anonymity. Bitcoin addresses the privacy issue while using the public key of the user as the User ID [1].

2- Computations and Mining Nodes

Security is vital, as public Blockchain are open and user information is available to attackers. Thus, the interactions bind the user identification to their public key, the ACL, or the authenticity information for most of the strategies discussed [1].

3- Communication Overhead

The platform of Blockchain is a peer-to-peer network which can add substantial overheads to the capacities for network traffic and system processing. The transactions and blocks have to be distributed in conventional methods like unicast [1].

4- Scalability

Problems with scalability [1], [20] can occur because under heavy traffic, the system may slow down. Alternative solutions to overcome the scalability issues are being suggested, such as Lightning and Plasma. Transactions in the Lightning network do not require a consensus mechanism when the parties to the transaction trust one another. It will speed up the transaction process; nor will there be written transactions [20].

5- Time Consumption

Building Blockchain authentication and security techniques adds to the time constraint problem, as these techniques are difficult and time consuming. Faster mining and functional techniques are therefore required in order to be able to use the Blockchain in real-time applications [1].

V. Conclusion

Types of Graphics Blockchain opened opportunities which have positive impact on companies currently underway. Blockchain has opened up many opportunities that have a positive impact on companies currently underway. Blockchain has provided a wide range of solutions in companies that are about to remove barriers to plant financing and management.

We discussed the literature review on Blockchain and the public key infrastructure in this paper, and highlighted issues relevant to an environment of PKI. Blockchain is an interesting solution to coping with popular issues faced by PKI, in the context of the literature. Holding the possible efficiencies of both technologies in mind is expected to revolutionize any area of life. Finally, we analyzed the problems currently impeding the practicality of the Blockchain for security applications.

References

[1] Salman, T., Zolanvari, M., Erbad, A., Jain, R., & Samaka, M. (2018). Security services using blockchains: A state of the art survey. IEEE Communications Surveys & Tutorials, 21(1), 858-880.

[2] Niranjanamurthy, M., Nithya, B. N., & Jagannatha, S. (2019). Analysis of blockchain technology: pros, cons and SWOT. Cluster Computing, 22(6), 14743-14757.
[3] Lin, I. C., & Liao, T. C. (2017). A survey of blockchain security issues and challenges. IJ Network Security, 19(5), 653-659.
[4] Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2017). A survey on the security of blockchain systems. Future Generation Computer Systems.
[5] Yakubov, A., Shbair, W., Wallbom, A., & Sanda, D. (2018). A blockchain-based pki management framework. In the First IEEE/IFIP International Workshop on Managing and Managed by Blockchain (Man2Block) colocated with IEEE/IFIP NOMS 2018, Tapei, Tawain 23-27 April 2018.
[6] Hepp, T., Spaeh, F., Schoenhals, A., Ehret, P., & Gipp, B. (2019, April). Exploring Potentials and Challenges of Blockchain-based Public Key Infrastructures. In IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (pp. 847-852). IEEE.
[7] Wang, R., He, J., Liu, C., Li, Q., Tsai, W. T., & Deng, E. (2018, November). A Privacy-Aware PKI System Based on Permissioned Blockchains. In 2018 IEEE 9th International Conference on Software Engineering and Service Science (ICSESS) (pp. 928-931). IEEE.
[8] Dykcik, L., Chuat, L., Szalachowski, P., & Perrig, A. (2018, November). BlockPKI: An Automated, Resilient, and Transparent Public-Key Infrastructure. In 2018 IEEE International Conference on Data Mining Workshops (ICDMW) (pp. 105-114). IEEE.
[9] Alrawais, A., Alhothaily, A., Cheng, X., Hu, C., & Yu, J. (2018). Secureguard: a certificate validation system in public key infrastructure. IEEE Transactions on Vehicular Technology, 67(6), 5399-5408.
[10] Dong, Y., Kim, W., & Boutaba, R. (2018, July). Conifer: centrally-managed PKI with blockchain-rooted trust. In 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) (pp. 1092-1099). IEEE.
[11] Jiang, W., Li, H., Xu, G., Wen, M., Dong, G., & Lin, X. (2018, December). A Privacy-Preserving Thin-Client Scheme in Blockchain-Based PKI. In 2018 IEEE Global Communications Conference (GLOBECOM) (pp. 1-6). IEEE.
[12] Li, Z., Yin, X., Geng, Z., Zhang, H., Li, P., Sun, Y., ... & Li, L. (2013, January). Research on PKI-like Protocol for the Internet of Things. In 2013 Fifth International Conference on Measuring Technology and Mechatronics Automation (pp. 915-918). IEEE.
[13] Kshetri, N. (2017). Can blockchain strengthen the internet of things? IT professional, 19(4), 68-72.
[14] Wang, W., Hu, N., & Liu, X. (2018, June). BlockCAM: A blockchain-based cross-domain authentication model. In 2018 IEEE Third International Conference on Data Science in Cyberspace (DSC) (pp. 896-901). IEEE.
[15] Ahmed, A. S., & Aura, T. (2018, August). Turning Trust Around: Smart Contract-Assisted Public Key Infrastructure. In 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) (pp. 104-111). IEEE.
[16] Wang, R., He, J., Liu, C., Li, Q., Tsai, W. T., & Deng, E. (2018, November). A Privacy-Aware PKI System Based on Permissioned Blockchains. In 2018 IEEE 9th International Conference on Software Engineering and Service Science (ICSESS) (pp. 928-931). IEEE.
[17] Osmov, V., Kurbanniyazov, A., Hussain, R., Oracevic, A., Kazmi, S. A., & Hussain, F. (2019, November). On the Blockchain-Based General-Purpose Public Key Infrastructure. In 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA) (pp. 1-8). IEEE.
[18] Singla, A., & Bertino, E. (2018, October). Blockchain-based PKI solutions for IoT. In 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC) (pp. 9-15). IEEE.
[19] Kfoury, E., & Khoury, D. (2018, July). Distributed Public Key Infrastructure and PSK Exchange Based on Blockchain Technology. In 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) (pp. 1116-1120). IEEE.
[20] Karaarslan, E., & Adiguzel, E. (2018). Blockchain based dns and pki solutions. IEEE Communications Standards Magazine, 2(3), 52-57.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500