ZIBELINE INTERNATIONAL PUBLISHING

Information Management and Computer Science (IMCS)

DOI : *http://doi.org/10.26480/imcs.02.2019.14.18*

Online ISSN : 2616-5961
CODEN : IMCSBZ

RESEARCH ARTICLE

RESEARCH ON DIGITAL PROTECTION OF INTANGIBLE CULTURAL HERITAGE BASED ON BLOCKCHAIN TECHNOLOGY

Wanni Huang [1*], Fei Dai[2]

[1]College of Tourism & Landscape Architecture, Guilin University of Technology, Guilin, Guangxi, China
[2]Computer science department, University of Otago, Dunedin, New Zealand
**Corresponding Author Email: 102017774@glut.edu.cn, daitr616@student.otago.ac.nz*

ARTICLE DETAILS

Article History:

Received 26 August 2019
Accepted 30 September 2019
Available Online 29 October 2019

ABSTRACT

At present, there are many information security issues in the digitization of intangible cultural heritage (ICH). The digital information of ICH is vulnerable to malicious tampering, stealing or attacks. The blockchain technology has the characteristics of distribution, un-tamper and traceability, which enhances security in the process of protecting digital information. Therefore, this paper discusses the integrity protection and the encryption protection from the perspective of blockchain encryption technology and provides a reference for the network security research of the ICH digital resources.

KEYWORDS

Blockchain technology, Intangible cultural heritage, Digital protection, Encryption.

1. INTRODUCTION

ICH is a variety of social practices, conceptual expressions, expressions, knowledge, skills, tools, handicrafts and cultural sites that are considered by various communities, groups, and individuals as part of their cultural heritage [1]. The protection of ICH is a systematic cultural project, and its basic steps include information mining, information management, information transmission[1], etc. Since the 1990s, the international cultural heritage field has begun to set off a wave of "digitalization". After 2003, many countries began to carry out digital projects of ICH. For a time, internationally, the field of the research of ICH has shifted from culture to information form [2]. Domestic research on the digitalization of ICH has only begun since 2006 [3]. Domestic scholars' research on ICH is mainly carried out from the perspectives of ICH technology research and ICH digital form. In the field of ICH technology research, it focuses on digital imaging technology, 3D technology, VR and AR technology, 3S technology and other aspects. The field of digital morphology research of ICH focuses on the research from the perspective of ICH database, digital museum, and animation games [4].

However, digitalization of ICH not only brings advantages to the protection of ICH but also brings hidden dangers in data security. In China, a firewall will be set in the system to monitor the network, verify identity, defend against suspicious IP packets and illegal user login [5]. Except for the above methods, international research of network security includes the fields of encryption algorithms, system design, security protocols, wireless sensor networks, and smart grids [5,6]. In recent years, with the continuous development of science technology and economy, the blockchain technology had emerged. Blockchain-based information security of network has the characteristics of decentralization, non-tamperability, traceability and high credibility. The integrity and traceability features are better than traditional network security for digital information data protection [7]. Aiming at the digital protection of ICH, this paper studies the digital protection of ICH under blockchain technology from the perspective of encryption technology, and proposes advices of using encryption technology in blockchain technology to protect the digital information of ICH.

2. THE DILEMMA OF INTANGIBLE CULTURAL HERITAGE DIGITAL PROTECTION

Since the 20th century, digital information technology has been gradually applied in the field of cultural heritage protection, using a large number of digital information technologies in the collection and reproduction of cultural heritage scenes, the storage and dissemination of cultural heritage elements. The technology mainly includes digital photography, augmented reality, virtual reality, platform construction, database storage, cloud storage, etc. According to current research, digital information technology has played an important role in promoting the exchange and sharing of world cultural heritage. The advancement of digital information technology such as digital information storage and visual digital conversion has effectively realized the digital protection of ICH. With the further development of research, the cultural connotation of intangible cultural forms such as folklore and craftsmanship were mined by researchers. But most of the inheritance of ICH needs to rely on inheritors, special ecological environment, customs and other factors to realize cultural inheritance and promotion [8].

The protection of the traditional ICH is faced with the constraints of various forms of existence, such as increased protection difficulty, complex environmental factors, and technical conditions. The digital form transformed by a series of technical processing has the characteristics of convenient storage, small space occupation, low resource consumption, well protection and high utilization, which solves the problems of the traditional ICH protection. The development of science and technology turns traditional culture into modernization. It combines digital technology to study the protection of ICH to lay the technical foundation. Digital can realize operations such as moving, sharing and recurring on the internet platform, which gives convenient storage function and reuse function to ICH [9].

With the development of digital information technology, the integration of ICH and digital information technology will become one of the important ways for inheriting and protecting ICH. ICH has the characteristics of changing with social factors, so it needs to seek digital protection, which has become one of the ways to better than traditional protection [10]. However, in the rapidly developing field of digital technology, digitalization and informatization make information exchange frequently and densely. The neglect of security issues may lead to the disclosure, destruction and tampering of information resources. The digital protection of ICH involves database security and data security in terms of network security. Since the protection of ICH under the digitalization involves resource protection of ICH, the digital resources of these ICHs are unique, high-value, and costly to store, and the protection of these digital information resources needs to be paid more attention to their privacy, security, stability, efficiency, etc. Therefore, the digital protection of ICH is primarily faced with the protection of digital resource information of ICH.

As the national cultural ecology changes constantly, the changes in cultural ecology will bring about the fault crisis of ICH [9]. Digital protection is one of the ways to rescue ICH. Because digital protection has the characteristics of absolute efficiency and high utilization rate compared with traditional protection methods, the digital protection of ICH has gradually been accepted and adopted by the society. In recent years, with the continuous development of Internet technology, the digitization of ICH is reflected in Internet platform frequently. The high-speed operation of data information and wide-area communication put forward higher requirements for information security of ICH. The protection of data information resources should pay attention to the further development of database technology and attach importance to the preservation and scientific management of data information.

However, traditional data information and database protection barriers have been repeatedly attacked, and the information in the platform is facing a crisis of data loss and tampering. What is more, the server will be in a state of collapse after being attacked. In order to find a more secure network environment, it is necessary to focus on the root cause of data information storage and database architecture [10]. Blockchain is a technology with high security and it increases the difficulty of malicious attacks to a certain extent and improves the protection of network data information. In terms of data and database, blockchain technology has more security and privacy than traditional data information protection technologies.

3. THE DIGITAL PROTECTION ANALYSIS OF BLOCKCHAIN TECHNOLOGY APPLIED TO INTANGIBLE CULTURAL HERITAGE

A blockchain is a continuously growing distributed database which is jointly maintained by multiple notes. It establishes trust relationships with each other through distributed networks, time-insensitive cryptographic books, and distributed consensus mechanisms, writing the smart contracts manipulate data so as to transit information interconnect to value interconnect [11]. The blockchain technology framework consists of three core application layers: data layer, network layer, and consensus layer. The underlying data layer is used to encapsulate chain structure and data encryption technology, time stamping technology, etc. The network layer is used to encapsulate p2p networking, data dissemination, data verification and other mechanisms.

The consensus layer encapsulates the network node by consensus mechanism algorithm. According to the application of blockchain technology, an additional contract layer encapsulation chain is required to implement various scripts, algorithms and smart contracts[11]. The blockchain is composed of a block header and a block body. The block header is a hash value in the running upper block, and the data of the node receiving algorithm through the whole network is recorded in the block. Each lower-level hash value is derived from a new hash value randomly generated by the upper-level block, and a new random hash value is continuously generated to generate a new region fast and connect to the next block. The structure and dynamic characteristics of the blockchain make it distributed, high-trusted, and timing-fixed.

3.1 Data Integrity Protection for Blockchain Technology

The ICH, which relies on the unique cultural and ecological environment as the background of survival, shows signs of incomplete and near-disappearing material form as the society develops rapidly. The arrival of the digital age enables ICH resources to realize digital resource conversion, digital resource storage and transmission, etc [12]. The network information platform erection, interactive design, 3D scene restoration, augmented reality and other technologies for the protection of ICH are currently used more technical methods. These technical methods mainly apply to ICH information data, if the information data is private. If broken, it will directly cause losses to the data stakeholders [13]. The two algorithms commonly used in algorithm for data information protection in blockchain are hash algorithm and asymmetric encryption algorithm [5]. The two algorithms commonly used for information protection in blockchain are hash algorithm and asymmetric encryption algorithm.

The data integrity protection algorithm for blockchain technology is hash function. The digital signature in the blockchain is mainly implemented by the hash function. The algorithm sets the binary value of arbitrary length into a short and fixed length binary hash value. And it specifies a one-way, irreversible encryption system. The one-way functions commonly used in blockchain technology have a one-way hash function and a one-way trap function, while the hash function uses a one-way hash function. In the hash function, even if the hash function is known for all parameters, it is still not feasible to find the inverse of the function based on known conditions.

The blockchain is formed by a chain structure. The blockchain is connected by blocks. The block in the new block contains a hash pointer. The pointer points to the hash value of the previous block, and the new block is automatically generated. Random numbers and determine the new hash value. Each block in the blockchain can track the hash value of the previous block, combined with the irreversibility of the hash function to encrypt the plaintext into a one-way fixed-length ciphertext, and slight data tampering will cause huge data. Changes, which make it easy to identify data changes and ensure the authenticity of the transmitted data information. In addition, due to the structure of the block connection structure in the blockchain, the change of arbitrary data will cause the block hash value to change and destroy the original blockchain data balance. As a result, it is easy to detect the change. The way of destroying the whole blockchain and tamper data is almost impossible to achieve because hash function in this blockchain ensures the immutability of the data.

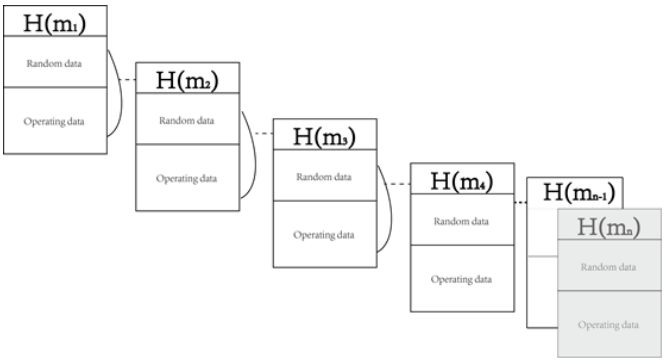

Figure 1: Block and hash

3.2 Data Encryption Signature and Verification Protection of Blockchain Technology

In the blockchain technology, in addition to using the one-way hash function to sign the data digest portion, the elliptic curve cryptosystem is added to encrypt and sign the data information and verify the protection. The algorithm uses different decryption key and encryption key, which cannot be deduced by the decryption. The elliptic curve cryptography algorithm based on the discrete logarithm can realize the functions of private key signature and public key verification. In the elliptic curve algorithm, the blockchain has low requirements of bandwidth and storage due to the shorter length key. Thereby, increasing the operating speed and

environmental adaptability of blockchain. In the blockchain technique, the p of the finite field elliptic curve[18] is generally a large prime number, x, y∈[0, p-1].

$$y^2 = x^3 + ax + b \ (a, b \in F_q) \quad (1)$$

The blockchain technology mainly uses the elliptic curve algorithm secp256k1. secp256k1 is based on the elliptic curve in a limited range. The performance of secp256k1 is 30% higher than other curves after optimization by special algorithm, especially suitable for small speed requirements and low storage capacity's mobile devices. The secp256k1 curve consists of a six-tuple, where the prime number p is proportional to security and inversely proportional to the computational speed [14]. The elliptic curve digital signature algorithm has outstanding advantages for the security attack protection of data information of the same data level. The password operation system only needs small parameters to complete the data protection work, and the key length generated by the cryptosystem is compared with the RSA encryption system, the key length is shorter and has a faster running speed. The hardware requirements are relatively low, and the advantages of the promotion scope are large, the promotion is simple, and the user experience is improved [15].

The elliptic curve digital signature method first needs to randomly generate a key pair according to the cryptosystem, publish K, G and finite fields, and sign the signed data information and output the signature information composed of r and s. The signature information needs to be signed to verify that the signature is valid after receiving. When k is the private key, K is the public key, r is the secret random number, and the ciphertext is m. The blockchain technique uses the elliptic curve algorithm to perform the cryptographic signature. The outstanding advantage of the elliptic curve cryptography algorithm is that it is in the finite field and within the elliptic curve. K can be derived from G at any point k, but K and G cannot be used to derive k. Since the finite field elliptic curve is not a smooth curve but a discrete point, it is almost impossible to derive the private key by the public key and the base point, thereby ensuring the security of the ECDSA cryptosystem.

4. RESEARCH ON DIGITAL PROTECTION OF INTANGIBLE CULTURAL HERITAGE BASED ON BLOCKCHAIN TECHNOLOGY

The most convenient and efficient way to save ICH is to transform it into a digital preservation mode. But digital data is a double-edged sword because digital information resources have security risks. whether from the perspective of passive attacks or active attacks of the data, the security of data information will be accompanied by the development of the digital age. While the digitization of ICH is progressing, the protection of ICH's digital information will not be delayed. In recent years, with the rise of encrypted digital currency, the protection brought by blockchain technology to digital currency circulation has attracted people's attention. Blockchain technology has great potential for digital protection of information [16]. This chapter will discuss the application of ICH from the aspects of digital information security and database security of ICH. The advancement of the digitalization process of ICH will greatly benefit the protection of ICH. At present, the digitization of ICH is mainly stored in the form of audio, video, digital information, etc., and is converted into a digital information resource and stored. In the process of sharing and sharing, ICH's digital information faces security risks.

4.1 The Analysis of Protecting Integrity of Digital Information of ICH by Hash Function in Blockchain Technology

The ICH protection organization stores a large amount of digital information, and most of the ICH is in a state of no successor. Therefore, this part of the digital information is especially valuable. Once this part of the information is lost or malicious tampering will cause it to disappear forever. The digital information of ICH is often in the form of large files. For the protection of digital information of large files, this chapter proposes to protect the digital information of ICH by combining the hash function in blockchain technology, i.e. one-way hash function. The hash function in the blockchain technology has the function of encrypting part of the contents of the large file, and part of the digital information calculated by the one-way hash function can form a fingerprint for subsequent comparison of the integrity of the file [17]. The manner in which the target digital information is protected using a hash function in the blockchain technique is referred to as a digital signature. The unidirectionality of the one-way hash function in the blockchain technique, the fixed hash value, the short hash value, and the weak anti-collision property are applied to the protection of the digital information of ICH, which makes the protection in a fast speed and information could be fast examined. Finally, it protects the integrity of ICH's digital information.

Firstly, combining the unidirectionality with the hash value characteristics to perform digital protection of the ICH. The hash function in blockchain technology is applied to the digital protection of ICH. First, the ICH needs to be digitized. The digital information is calculated for one part of the digital information through a one-way three-type function and forms a new file with the original digital information. The fixed-length hash value calculated by the hash algorithm is embedded in the digital information of the ICH and becomes an indispensable part of the overall data information.

When the digital information of the ICH processed by the one-way hash function encounters an illegal access, since the one-way hash function has the characteristics of unidirectionality and fixed hash value, the attacker will need to solve the NP-hard problem when attempting to perform reverse derivation. At present, within a limited time and within the computing power of today's computers, intruders can't reverse the hash value by inverse operation, that is to say, the target text cannot be recovered through the hash value stolen by the network, thus ensuring the security of the digital resource information of the object and avoid the leakage of important digital information of the ICH.

Secondly, combining weak anti-collision with hash value characteristics for digital protection of ICH. While the network information sender and the receiver both exchange data information of the ICH, the ordinary one-way hash function can calculate a fixed hash value and has the characteristics of a one-way hash function, but if the attacker bypasses the way in which the inverse derivation is turned to break the collision resistance in cryptography, then the digital information exposed on the network at this time is unsafe [18].

The one-way hash function in blockchain technology has weak anti-collision property, and the weak anti-collision function system makes it impossible for an attacker to solve the strong simulation algorithm for rewriting the original file for the function and cannot rewrite the original file at the same time. For the digital protection field of ICH, the hash function in the blockchain technology is used to protect the digital information of the ICH, which can ensure that the digital information received by the digital information receiver is complete and has not been tampered with. Therefore, the hash function in the blockchain technology can ensure the integrity of the data information and ensure the correctness of the information after transmission.

4.2 The Analysis of Elliptic Curve Algorithm in Blockchain Technology Applied to Digital Information Encryption of ICH

The elliptic curve ECDSA used in the blockchain technology not only has the digital signature function of the hash function, but also has the function of performing a series of encryption operations on the digital information. The elliptic curve cryptosystem in the blockchain technology has the characteristics of short key length, small storage requirement space, and extremely fast computing speed. These characteristics make the cryptosystem have limited computing power, high speed requirements, and low software and hardware compatibility. This is especially true for devices with limited storage space, so the algorithm can provide high-performance protection for ICH's digital security issues. The security of the elliptic curve cryptosystem relies on the complexity of the discrete logarithm problem. It is impossible to mathematically solve the elliptic curve cryptography by solving the discrete logarithm, so that its security performance is recognized worldwide. This plays a very important and practical role in the digital protection of ICH, especially the important digital information protection of ICH.

First, the elliptic curve algorithm in the blockchain technique digitally signs the digital information of the ICH. The elliptic curve algorithm in blockchain technology has a digital signature function similar to the hash function, but unlike the hash function algorithm in blockchain technology, the elliptic curve algorithm can generate a key pair to encrypt information. Moreover, key exchange can be realized and a shared key can be generated, which ensures the security of the key exchange and ensures the security of the digital information exchange process. On the other hand, in the process of digital signature, the elliptic curve algorithm uses the hash value calculated by the hash function and adds the random number and the private key to encrypt the information, which can have more complicated than the hash algorithm.

The operation steps, regardless of information data, hash values or slight changes in random numbers, will directly cause changes in digital signatures, and are more sensitive in terms of security detection and protection. These features make the elliptic curve algorithm in blockchain technology extremely secure in protecting digital information. In the process of using the elliptic curve encryption algorithm in the blockchain technology, when the digital information of the national important ICH needs to be transmitted in the network, the elliptic curve algorithm generates random numbers and key pairs by operation, and uses the base point, the random number, the hash value, and the private key sign the target data information[16]. The sender of the information sends the digital signature information of the encrypted value and the public key to the information receiver through the network, and the whole process realizes the process of digital information encryption and digital signature.

The process of digital signature involves the transmission of digital information. The circulation of digital information is prone to security risks. Attackers can steal information such as base points and public keys in this process. Since the elliptic curve algorithm has a more advantageous protection against attacker attacks than the ordinary encryption algorithm, the elliptic curve algorithm in the blockchain technique is about the finite field clock operation. Even if the attacker obtains the information of the elliptic curve E, the public key, and the base point, the imaging of the elliptic curve on the finite field is not a smooth curve, but a series of discontinuous points. When the prime random number generated on the finite field is large enough, the attacker cannot use the stolen information to solve the private key by using the discontinuous point algorithm on the finite field elliptic curve. Therefore, the elliptic curve digital signature technology in blockchain technology is suitable for digital information protection of ICH. And because of the short key length of the elliptic curve but high intensity, the elliptic curve algorithm has much better security performance for digital information encryption than RSA and other cryptosystems.

Second, the elliptic curve algorithm in blockchain technology digitally verifies the digital information of ICH. Since digital information is transmitted at the network layer, this information is publicly available and can be obtained through appropriate technical means. Although the digital signature is used to sign the digital information, if a hacker recalculates the acquired information and simulates the digital signature information with high similarity and sends it to the receiver, then there is a security risk. At this point, the received digital signature needs to be verified to ensure the accuracy and security of the information. The verification of the digital signature information is performed by using the received digital signature information using a private key, a base point, and the others by comparing the operation formula with the product of the random number multiplied by the base point. If the two results are consistent, the digital signature verification is passed, otherwise the digital signature is not passed.

Therefore, the digital information of the ICH is transmitted to the target object on the network, and the signature needs to be verified. The value obtained by modular operation is calculated to verify whether the digital signature information is true, so the correctness of the digital information is confirmed. Verification of the digital signature confirms that the received digital information of ICH is sent by the message owner, so as to avoid data masquerading, malicious tampering, and malicious attacks when ICH digital information is transmitted, shared, and traded on the network, causing economic losses and information leakage.

5. CONCLUSION

Since 1990, the international research field of ICH has gradually entered the digitalization. The digitalization of cultural relics, the digitization of ancient books, and the digitalization of archives have inspired the expansion of digital research in more subject areas. The international ICH digital protection research mainly starts from the three perspectives of digital acquisition, digital preservation and digital development. Among them, digital protection research mainly involves three aspects: digital information organization, retrieval and management, these three aspects mainly carry out the digital information protection of ICH from the perspective of managing and using digital information.

Nowadays, with the rapid development of information technology, the digital protection of ICH is gradually advancing, and more and more important ICHs are using the method of digital protection. However, the development of the Internet and the Internet of Things technology has brought about a growing amount of data in the cyberspace. At the same time, the sharing of massive data brings convenience and security risks. The development of ICH digitalization makes its digital information resources flood the cyberspace. Digital information in cyberspace is at risk of security attacks. The digitalization of ICH brings the security protection problem of digital information resources. Therefore, the article studies and discusses the integrity and encryption of digital information resources of ICH based on blockchain technology.

The digital protection of ICH based on block technology has certain advantages. However, digital protection of ICH still needs to be considered from the perspectives of government policy guidance, market deployment, and social support, such as comprehensively considering the digital protection of ICH to better realize the transformation and inheritance of ICH information resources.

REFERENCES

[1] Hesheng, L., Yi, Y. 2017. The Dilemma and Outlet of China's Intangible Cultural Heritage Protection——Based on the Field Investigation of "Guangchang Meng Opera. Journal of Jiangxi Social Sciences, 37 (6), Pp. 250-256.

[2] Yue, Z., Yaolin, Z. 2017. A Review of Digital Protection of International Intangible Cultural Heritage. Library, (8), Pp. 59-68.

[3] Yunqing, W., Xin, P. 2017. A Summary of the Research on Digital Protection of Intangible Cultural Heritage in China. Archives and Construction, (4), Pp. 9-13.

[4] Ya, Z., Xin, X. 2017. A Review of Digital Research on Intangible Cultural Heritage. Library and Information Service, 61 (2), Pp. 6-15.

[5] Jiang, X., Wei, Z. 2005. Security Research of Network Database in Transmission Process. Computer Science, (11), Pp. 127-129.

[6] Liangbin, Y., Xinli, Z., Yijia, L. 2017. Visualization Analysis of Research Status and Trends in International Cybersecurity in the Past Ten Years. Journal of Information, 36 (1), Pp. 92-100.

[7] Wei, C., Dongxi, X., Liang, X. 2018. Overview of Network Security Technology Based on Blockchain. Telecommunications Science, 34 (3), Pp. 10-16.

[8] Jingyan, Z. 2015. Dilemma and Breakthrough: Exploration of the Industrialization Path of Intangible Cultural Heritage. Learning Forum, 31 (2), Pp. 61-65.

[9] Weijie, W., Yuanping, X. 2018. Status and Development Countermeasures of Digital Protection of Intangible Cultural Heritage of Guizhou Minorities. Journal of Hubei University for Nationalities (Philosophy and Social Sciences), 36 (4), Pp. 119-123.

[10] Yonglin, H. 2015. Protection and Utilization of Intangible Cultural

Heritage in the Digital Background. Cultural Heritage, (1), Pp. 1-10.

[11] Zengjun, Z. 2018. Blockchain Technology Series. Beijing: Mechanical Industry Press, (1), Pp. 1-256.

[12] Xiangyang, S. 2016. Inheritance and Protection of Intangible Cultural Heritage from the Perspective of Digital Technology——Taking the Miao Epic "Ya Lu Wang" as the Center. Guizhou Ethnic Research, 37 (3), Pp. 67-71.

[13] Lan, D., Linlin, C., Li, Z. 2018. Security Architecture of Smart Cloud Manufacturing System Based on Blockchain. Information Technology and Cyber Security, 37 (11), Pp. 34-38.

[14] Mayer, H. 2016. Ecdsa Security in Bitcoin and Ethereum: a Research Survey. Coinfaabrik, 28 (1), Pp. 1-126.

[15] Lauter, K. 2004. The Advantages of Elliptic Curve Cryptography for Wireless Security. IEEE Wireless Communications, 11 (1), Pp. 62-67.

[16] Johnson, D., Menezes, A., Vanstone, S. 2001. The Elliptic Curve Digital Signature Algorithm (ecdsa). International Journal of Information Security, 1 (1), Pp. 36-63.

[17] Fangwei, S., Yan, L. 2015. Digital Protection and Inheritance Strategy of Intangible Cultural Heritage from the Perspective of Cultural Industry. Shandong Social Sciences, (2), Pp. 83-87.

[18] Xiang, C., Yi, Z., Xuecheng, W. 2006. Research on Elliptic Curve Algorithm and Its Application in WPKI. Computer Engineering and Applications, Pp. 110-112.