Research Square

Preprints are preliminary reports that have not undergone peer review. They should not be considered conclusive, used to inform clinical practice, or referenced by the media as validated information.

Legal Risks and Coping Strategies of Block Chain Managing Trade Secrets: Enlightenment of Chinese Experience

Song Shiyong (Songshiyong2@gmail.com)
Qilu University of Technology

Xing Yuxia
Shandong University of Political Science and Law

Research Article

Keywords: Block Chain, China, Trade Secrets, Management

Posted Date: October 27th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-955903/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Abstract

The management and legal protection of trade secrets is the common goal for all countres. Block Chain was found a huge advantage in protecting trade secrets as an advanced form of mathematical application. To better protect trade secrets for solutions, this study was to find out the legal risks faced with Block Chain. Basic theories of trade secrets and Block Chain were analyzed after reviewed literatures and empirical. The contemporary risks faced were put forward combined in practice. The better ways to protect trade secrets were discussed based on the current judicial practice of China. It was argued that problems of electronic storage and evidence collection of trade secrets would be solved Block Chain protection of trade secrets. Great risks and challenges would be confronted ahead albeit confirmed by the judiciary. It was concluded that a long time was dispensable for Block Chain managing and protecting trade secrets.

I. Introduction

Under the current big data background, it is particularly important to discuss the mode construction and path of protecting trade secrets by using the advantages of Block Chain.

The advantages of Block Chain was not focused as well as trade secrets protection. Mathematics breaded Block Chain, and mathematics promoted mathematics. It was possible for mathematics to transform Block Chain ahead. It was said that Block Chain was an advanced application mode of mathematics. Block Chain was found great advantages and risks for managing and protecting trade secrets. This study was to disclose how Block Chain to manage and protect trade secrets according to cases of China.

Sustainable development is a critical social issue(Song Shiyong,Xing Yuxia,2020), to emphasize the importance of small and medium-sized enterprises for this and it is necessary to prevent immigration problems in the state, to create self-employment opportunities and to ensure sustainability (Mohanty, Jena, and Sipahi, 2021). The welfare centers in the society are among the most dynamic social institutions in the world. Community centers keep people in the center of development, as they have a commitment to regional intervention. To do this, governments provide an institutional link between people and the various private stakeholder coalitions that make up their communities. Community centers also participate in a wide range of social change activities, including advocacy with and on behalf of the community to reform basic social, political and economic conditions (Sipahi, 2019). In this context Block Chain technology is an important sustainable strategy .A greater significance of Block Chain for the transformation of new technology industry was emphasized by Chinese President Xi Jinping, at the 18th collective study held by the Political Bureau of the CPC Central Committee, October 24th, 2019. It was demanded that Block Chain should be regarded as the breakthrough of independent innovation core technology. Thus, Block Chain was officially rose to China's national strategy from then on.

For a long time, Block Chain once was standing national strategies of United Kingdom and Germany. At the end of 2018, Russia officially completed the implementation of the first Block Chain at the government level. There is a subtle change in the attitude of the Korean government towards Block Chain. The crazy obsession of Korean people with digital cash and the influence of international situation prompted the Korean government to strictly ban Block Chain from the beginning, to partially lift the ban in 2018, and then to encourage policies in 2019. It can be said that the application of Block Chain in South Korea has now entered a state-led period.

Block Chain was first applied in China as early as in 2017. When China used its own poverty alleviation fund block from Industrial and Commercial Bank of China. The new model of managing poverty alleviation funds by the chain platform allocated poverty alleviation funds. To realize the Block Chain to issue electronic invoices, Shenzhen and Hangzhou Metro Company cooperated with Tencent and Alipay, respectively. To establish a strategic partnership with Block Chain-based fan participation platform, such top-level teams in the world sports field as Juventus and NBA accepted Bitcoin as the ticket payment method. In 2019, Block Chain electronic deposit was first recognized as evidence of litigation by Hangzhou Internet Court, Zhengjiang, China. It was the first comprehensive application of Block Chain in China's judicial practice.

On May 25, 2020, such deep technology application as big data and Block Chain achievements were stated in the report of Chinese Supreme People's Court made at the Third Session of the 13th National People's Congress, by Zhou Qiang, President of the Supreme People's Court. The standardization level of execution was improved by the application of Block Chain intelligent contract technology in execution (Figure 1).

More than a concept or an application of cryptocurrency in the financial field, Block Chain was moving towards various fields of social governance step by step.

The essence of Block Chain was the application decentralization of distributed database. Four core mature technologies of Block Chain were characterized as distributed P2P ledger (A), consensus mechanism (B), asymmetric encryption technology (C) and intelligent contract (D). Successively, the problems of information asymmetry and peer-to-peer trust mechanism of traditional trading parties would be solved from the aspects of data security preservation (A), security processing and safe application from law (B), objectify the traditional standard of establishment (C) and maintaining trust by relying on reputation into technology to guarantee trust (D). The cost of trust was greatly reduced before. Therefore, post-Block Chain was a magic weapon technology for cryptocurrency. the formation of a new mechanism was accelerated by Block Chain as a new mode of operation in all walks of life.

The field of intellectual property was no exception. It was a particular for the application of Block Chain in intellectual property. On one hand, written and published by open source code, copyright of Block Chain was necessary protected before transferred. On the other hand, such intellectual property as patents, trademarks, copyrights, trade secrets and geographical indications should be better protected by Block Chain. However, there were still limitations and imperfections with Block Chain itself. That so many

technical and legal problems was to be overcome and solved was beyond precedents of the applications above.

Block Chain application of trade secrets were found more typical particularity compared with other intellectual property rights. Due to the unauthorized openness and non-absolute exclusiveness of trade secrets, difficulties and obstacles were still confronted during Block Chain protection of trade secrets.

Ii. Trade Secret Protection Of Block Chain

The ultimate objects of trade secrets protection: business operators, right holders of trade secrets, competitive position of legal holders with trade secrets and market competitive advantage. Protection of trade secrets was critical since it was the core asset of an enterprise. At the same time, the ratio cost of benefit should be considered as well. Such operators as enterprises would regard unnecessary when the cost of protection was far higher than its benefit. Only when enterprises thought certain benefits from trade secrets protection would they stimulate enthusiasm and motivation to protect trade secrets. Block Chain was an optional path with either higher cost or poor protection measures.

A. Contents of trade secret protection

a. Current legal protection

It was necessary to explain the "protection" of intellectual property as trade secrets. In China's national management level, intellectual property standardization was divided into intellectual property management and intellectual property protection. Correspondingly, institutional setup of market supervision bureaus at all levels in China at that time, it was generally set up as Intellectual Property Operation Management Office and Intellectual Property Protection Office. The Intellectual Property Operation Management Office was mainly responsible for the operation and management of intellectual property and the transformation of technological achievements, while the Intellectual Property Protection Office was mainly responsible for building an intellectual property protection system and handling intellectual property disputes. Here, "protection" was a narrow concept. From a broad perspective, the standardization of intellectual property rights was the category of intellectual property rights protection in any case intellectual property rights operation, technological achievements transformation management, standard system construction and dispute resolution. Intellectual property rights protection took the protection of the legitimate rights, interests of intellectual property rights holders and national intellectual property order as its fundamental goal and purpose.

According to Article 123, Civil Code of People's Republic of China, trade secrets was a part of the eight objects of intellectual property rights. Civil Code was China's characterization of the nature of trade secrets at the basic legal level. Civil Code affirmed the general principles of intellectual property protection applicable to trade secrets protection. Cases in points, property rights could be pledged in intellectual property rights stipulated in Article 440 and Article 444, Civil Code. It was argued that time standards for the establishment of pledge rights and standards were also applicable to trade secrets. According to

Article 9, Anti-Unfair Competition Law, People's Republic of China, Articles 9, 10, 11 of Interpretation of the Chinese Supreme People's Court on Several Issues Concerning the Application of Laws in Trial of Civil Cases of Unfair Competition, four elements should be followed with trade secrets protection:

First. Public Secret—– generally not known, but easily obtained by relevant personnel in the field.

Second. Commercial value ——– including realistic and potential commercial value, it will bring competitive advantage to the oblige.

Third. Confidentiality measures ——– Practical protection is dispensable to such commercial value as trade secrets.

Fourth. Protection object ———– Such commercial information as technical information and business information is the main protection object.

b. Protection choice

Here, protection choice referred to legal elements of trade secrets. Illegal trade secrets would not be protected by law until above-mentioned legislation was regard "legality" as the legal component of trade secrets. The fact was a long being a relevant precedent in China's past judicial practice (Tang Qinglin, Huang Mingxin, 2011). In judgments of Shanghai No.1 Intermediate People's Court (2006) Hu Yi Zhong Min Wu (Zhi) Chu Zi No.95 and Shanghai Higher People's Court (2006) Hu Gao Min San (Zhi) Zhong Zi No.92, there was a dispute between Ankecheng Information Service (Shanghai) Co., Ltd. and Shanghai Chenyou Technology Development Co., Ltd.. The judgments infringed the trade secrets in the form of customer lists. Completely different judgments were made by the courts of first and second instance. In the first courts instance, commercial information with mass personal information of natural persons was considered as trade secret of company's customer list. While the second court instance denied such customer list was a trade secret in the end. The second court argued that the company failed to prove natural persons legally. Thus, personal information obtain was the evidence of company's customer list. It was a good awkward illustration of the commercial secrets protected by law. Admittedly, business secrets and commercial information should be kept confidential. The confirm of technical secrets and the legality elements should be the first consideration in the protection of commercial secrets.

B. Block Chain Trade Secrets Protection

a. "Zero knowledge proof" security protection

With rapid development of big data and artificial intelligence technology, data protection was the priority choice for all trade secret holders. The phenomenon of dataization was extended into the storage and transaction of such intellectual property rights method as trade secrets. At the same time, risks were sharply increased due to great changes in acquisition methods of data-based intellectual property rights. Everyone can use the network contents they want at any time. Data contents easy to copy and leak made

it difficult to protect. It was difficult for actual copyright owners to fully prove their value safety even if they were protected. Data contents was feasible used by malicious users with protection.

Block Chain, called as "the fourth industrial revolution", was characterized as integrity, transparency, confidentiality and traceability in the whole process. Block Chain was an important asset in the information age. Such typical problems as illegal copying, forgery and profit distribution of data can be well solved under the trading environment of digital content (Gabin Heo, Dana Yang, Inshil Doh, Kijoon Chae, 2020). It was the first time that human beings created an unrepeatable and forged database in history. At the same time, human beings would independently complete identity verification without relying on any third-party central organization (Wu Wei, 2017). Trade secret obligee would be directly linked with business information once intermediate link removed. More than business information, Block Chain would present hash value encrypted by hash algorithm not expose in content. Thus, the basic requirement of confidentiality was realized (Yekou Youjixiong, 2018). Therefore, Block Chain provided "zero knowledge proof" for trade secrets (Si Yansen, 2009). The subsequent changes about business information were completely presented and traceable well solved the problem of keeping business secrets (Zhang Huaiyin, 2019). Thus, hash value secrecy was guaranteed after trade secret wrote into Block Chain by owners. The outward information in the chain was the fixed-length code and the timestamp indicating the transaction information (Rob Shwarts, Kayvan Ghaffari, 2018). Characterized as high efficiency, low cost, strong confidentiality and traceability, the method well solved problems traditionally difficult confidentiality and high cost of protection.

The complicated and expensive process of traditional registration and confirmation of intellectual property rights would be exempted by the support of brand-new security system from Block Chain. Regional restrictions of intellectual property rights would be broken by Block Chain. Security management and charging were ensured by better technical support from system of security. Optimization of electronic evidence was realized in the aspects of keeping certificates. Thus, evidence and infringement identification were obtained with trade secrets.

b. Evidence for obligee

To characterize tamper resistance and whole-process auditability, Block Chain relies on asymmetric encryption algorithm (Kalpana Singh, Omar Dib, Clément Huyart, Khalifa Toumi, 2020). It can be expressed as decentralization, accountability and security (Joseph Holbrook, 2020). Transactions based on it, Block Chain were completed in the form of intelligent contracts, which were characterized as integrity, verifiability and transparency. It was extremely difficult to tamper with and forge. To prove great potential in management of such intellectual property rights as trade secrets, Block Chain have a great impact on legal practice after solve legal disputation (Gönenç Gürkaynak, İlay Yılmaz, Burak Yeşilaltay, Berk Bengi, 2018). Characteristics of Block Chain above was attributed to "invariance". All participants would complete accurate transaction (or transaction) logs (Kondapally Ashritha, M. Sindhu, K.V. Lakshmy, 2019). With effective evidence of trade secret preservation, the closed-loop evidence would be formed of trade secret proof. Such key issues as ownership source, change process, infringement scope

and value definition of trade secrets would be proved effectively. Thus, comprehensive and efficient technical protection and cross-examination evidence were provided for trade secret obligees.

Iii. Risks Of Block Chain Application

Trade secrets would be no doubt well managed and protected by Block Chain. As an open source technology, Block Chain did not belong to any individual (Gönenç Gürkaynak; İlay Yılmaz, Burak Yeşilaltay, Berk Bengi, 2018). Moreover, based on the nature of its digital content, it was difficult for authors to obtain rights and corresponding benefits from it. At the same time, it would be tampered by malicious users (Gabin Heo; Dana Yang; Inshil Doh; Kijoon Chae, 2020). Thus, many risks would be faced when Block Chain managed and protected trade secrets.

From the perspective of judicial practice, the difficulties in managing and protecting trade secrets lied in proving the essential attributes of trade secrets, infringing trade secrets, and calculating basis of losses after infringing trade secrets. Process transparency, traceability and invariance of Block Chain would solve some problems to a certain extent. For example, security and scalability were still the key problems to be solved in Block Chain (Avinash Kaur Anand Nayyar Parminder Singh, 2020). Especifically, the application of Block Chain in trade secret management and protection would face the following risks.

A. Risk of disclosure

Disclosure

risk in the process of trade secrets (information) uploading did not come from the illegal theft of trade secrets. It was caused by the inherent technical defects of Block Chain and network data services.

The first kind of risk was formed with automatic opening of the database background by obligee in the process of uploading. Trade secret data was represented by hash value in Block Chain platform. It was confidential to the public key personnel in this process unless the owner of private key can obtained according to law. There was an inevitable problem that all confidential data were transparent to the cloud database background that provides services (Zhang Huaiyin, 2019). Just like the access password we set on the network, it was confidential to general visitors, whereas transparent to service providers as well. That such transparency could not be said to be illegally obtained by service providers was reasoned that it was the providers who offer and agree to the network service agreement on their own initiative. Therefore, once such leaks occurred, it was difficult for the providers to pursue the legal responsibility of the network database. Thus, it was called natural risk of actively providing information.

The second type of risk was systemic risk. It was caused by "consensus" mechanism of Block Chain. The original intention of "consensus" was to set a unified standard for smooth progress of transactions. However, such details of transactions as the key information of users could be displayed and obtained by net nodes, especially those of commercial competitors (Muneeb UlHassan, Mubashir Husain Rehmani, Jinjun Chen, 2019). Extremely unfavorable to the protection of trade secrets, to build a consensus model

for shield trade secrets was a goal of Block Chain (Matthew Beising, 2016). Different from transparency risk of data providers, it belonged to the transparency risk of data uplink storage and transaction process of all participants. According to transparency mechanism, with ulterior motives, signature and transaction information on comparison chain would be correlated to a correspondence of real address and signature. Thus, such information as customer list of trade secret holder might be disclosed in the end.

B. Risk of transaction

Trade secrets in the Block Chain were electronic data in nature. Electronic data was often used as electronic evidence in such dispute resolution process as judicial. During the existence of electronic data, risks attack and tampered was existing due to human factors and technical factors (Zheng Yi, 2014). Generally speaking, as a distributed database feature, data tampering was made difficult after Block Chain nature decentralized. When more than 50% of distributed data nodes were successfully control by hackers, code version was tampered before invasion. Hackers would control transactions to be confirmed avoid regulatory detection. Once the trust and security of Block Chain data storage and transaction environment were artificially destroyed, the materialized data content would be tampered.

C. Risk of encryption key

As long as the commercial information was linked in data, transmission and storage in any nodes would be strictly protected by asymmetric encryption technology. There was a high risk of theft during the process of private key storage, transmission and display. The Block Chain was no longer secure once the private key lost or stolen. Anyone who holds the private key would transfer its value maliciously. The consequences of such transfer were serious as usually as immediate and irreversible (Louise Axon, Michael Goldsmith, Sadie Creese, 2018). Especially, once a hacker mastered the private key or attacked more than 50% of nodes or terminals. Thus, the risk of attack would be reality——a lie became a reality. Compared with data content tampering, encryption key risk was related with the trust and security of Block Chain data storage and transaction environment. Encryption key risk was reflected in the risk of programmatic content leakage. Encryption key risk would occur without further change with data content. The purpose of trade secrets obtaining would achieved after the private key leaked.

D. Risk of scalability

With advantages of security and decentralization, Block Chain would be lost in scalability (expansion) of speed and efficiency. Scalability was the biggest pain point after Block Chain industry after it lost the scalability of speed and efficiency. Scalability has become the biggest pain point after confidentiality in Block Chain industry. At present, the basic problem faced by Block Chain was the development of Block Chain in the process of database transactions. Once trade secrets (information) were fully uploaded, the scale of data uploaded by copyright was much larger than before. With the expansion of geometric multiples of distributed database data, the processing speed of Block Chain was much slower than that of traditional mode (Kalpana Singh, Omar Dib, Clément Huyart, Khalifa Toumi, 2020). The risk of poor scalability greatly limited the development of Block Chain.

E. Lack of Legal Supervision

The development history of Block Chain was not long as imamined. Block Chain was developing at an early stage of technology/application now. Trade secrets were related to the survival fate of the obligee. It was feasible in theory to manage and protect trade secrets with Block Chain. With function of keeping certificates, there was a broad prospect for the application of Block Chain. However, no companies engaged in Block Chain business with any uniform standards. Legal supervision was particularly important, especially in such Block Chain strategy nation as China, Britain and Germany. However, it was more critical to effectively supervise too many unpredictable factors in the early Block Chain market. Problems would arise anytime, anywhere in the application of Block Chain. One long process of gradual standardization was a better choice since the standardization of legal supervision was not achieved overnight. The cognition and understanding of Block Chain were still at a low level even at the practice of national legislation, intellectual property administration and justice and lawyers. One national general cognition, acceptance with Block Chain need one gradual process ahead.

F. Risk of trade secrets from Non-obligee

The obligee can only protect trade secrets in the way of self-protection. It was determined by the characteristics of non-statutory authorization and non-publicity of trade secrets. Lack of statutory authorization and publicity, trade secrets were easily infringed. Traditionally, difficult situation of proof would be faced by the obligee of trade secrets when encountered with such a situation. The risk was made more prominent by the emergence of blocks.

The infringer of trade secrets would steal trade secrets with Block Chain to complete information or relevant certification materials. Relevant subsequent research and development would be manufactured with other relevant certificates to pass trade secrets. The process was not necessarily completed by the thief himself, but possibly by associated person or enterprise. The process was even not operated in the place where the right holder located, nor in its business field. It was difficult for the obligee of trade secrets to obtain the evidence. When the trade secret was found to be stolen, the obligee of trade secret would not be able to provide favorable evidence. This was equal to provide the infringement of trade secret infringer with the help of proof. The legitimate rights and interests of the real right holders were seriously infringed.

In the process, more attention should be paid to potential risk as well as legal supervision. To implement the national strategy of Block Chain, more consideration should be paid to maximize efficiency within permitted scope by law instead of blindly restriction. The definition of legal rights was particularly of importance.

Iv. Practice Of "block Chain+intellectual Property"

In the early 21st century of China, Block Chain was started from theoretical concept (Bitcoin) to current practical application. Theoretical concept of Bitcoin took a period of more than ten years. Even Bailey W

and Martin's paper The New Direction of Cryptography in 1976 was regarded as the beginning of Block Chain. It was no more than half a century before.

However, 173,719 Block Chain business enterprises were born with a company named after "Block Chain" (Figure 2). In addition, many companies engaged in Block Chain business but not named with "Block Chain". Most of them named with the keyword "technology". For example, approved by the Ministry of Justice, Beijing Zhongjing Tianping Technology Co., Ltd. focused on the "judicial Block Chain" business. It was the first company providing Block Chain as intellectual property (copyright) of China.

According to the investigation, most Block Chain business companies mainly provided data services with "data storage and evidence collection". The major application scenarios of business companies were copyright protection, electronic data storage and evidence collection. Patents and registered trademarks in intellectual property were rare in Block Chain application scenarios for their legal authorization characteristics. Trade secrets were rare lied their low public awareness and secret characteristics. At present, such intellectual property rights as geographical indications would not consider Block Chain as the main channel for depositing certificates.

Based on risk categories mentioned above, it was found that the Block Chain business was developed in full swing with the support of the national strategy. However, their risks were not uncommon. On the contrary, the risks were particularly prominent due to new types, multiple scope, wide victim groups and great social impact.

A good case in point was a technology company in Zhejiang. This company was mainly engaged in Block Chain business based on Block Chain. One security network was developed to carry out data protection business in the company. The major service areas were intellectual property rights, e-commerce rights protection and financial certificate storage. Their service content was composite of online signature, online certificate storage, evidence data collection and online judicial expertise issuance. Take one science and technology Co., Ltd. in Zhejiang as an example. The company was mainly engaged in Block Chain business, and developed security network based on Block Chain technology to carry out data protection business. The company's main service areas were intellectual property rights, e-commerce rights protection and financial deposit certificate. At the same time, the company would provide online signature, online data storage and evidence collection, online judicial expertise opinion.

At the same time, the company was authorized as the information security level certification and quality management system from Chinese Ministry of public security. The company joined the Block Chain insurance alliance and actively participated in the legislation of Electronic Evidence Standard. The company's business once successfully achieved business docking and direct recognition with judicial expertise center, notary office and internet court. The company could be said perfect in business security and specialization around.

The main business of the companies was copyright Block Chain protection business. One all-round protection system from preventive protection to litigation evidence protection were consisting of a set of

processes as original works preservation, monitoring real-time dynamic confirmed works, copyright owners' feedback, online forensics and one-stop judicial certification. Compared with traditional copyright protection, one all-round protection system was found such outstanding advantages as efficient process, dynamic and comprehensive process and real-time & convenient evidence fixation. In 2018, the first case of Block Chain copyright infringement in China was tried in Hangzhou Internet Court. The evidence storage, evidence collection and verification were fully completed during the case.

Two typical problems were not avoidable when investigating the Block Chain protection of trade secrets. First, the company and Baoquan.com did not deal too many Block Chain business with technical secrets in their daily business. The company was not familiar with the field of trade secrets well. The logistics department of the company was responsible for encryption and storage of data with protected customers. No summary and statistics on business would be afforded to protected customers as well as summary statistics and relevant data. Second, the characteristics of the network system determined that the private data submitted by customers were undisclosed secret data for customers, chain traders and other subjects. However, the data were transparent to Block Chain business and database background, to constraints from internal self-restraint of professional ethics and external constraint of confidentiality agreement with customers.

As the first question mentioned above, trade secrets involved in technical secrets and business secrets. Rather than took risks through Block Chain, customers would keep confidential operation between intranet and external public network. Even if it was provided through Block Chain platform. At present, there was no more solution to effectively prevent secondary disclosure. The above internal and external restraint mechanism was the current peer method all.

Another Block Chain professional company investigated was Beijing Zhongjing Tianping Technology Co., Ltd.. The company was showed involved in certain business of commercial secrets protection Block Chain. To prevent secondary disclosure, clients would determine its identity by internal account. There was no limit on the scope of employees' contact with commercial secrets even not perfectly verified and bound with the employees themselves. Companies were not willing to leave marks in their research. As a common way, physical partition would effectively partition the problem, albeit expensive and troublesome. Data confidential under the chain would be solved by the customer only if customer data were confidentially kept on the chain. However, it was still a realistic issue how to keep the information confidential under the chain.

V. Perfect Block Chain Application

In China, the perfect of legislation and strict enforcement of law were the development trend of trade secret protection at present. To fundamentally solve the problem of evidence obtaining, more attention should be paid to technical problems of trade secret protection (Ledger Insights, 2020). As to the formulation of a unified Trade Secrets Law and Anti-Unfair Competition Law, they were to improve Block

Chain to manage and protect trade secrets in qualified or feasible way (Zhang Huaiyin, 2019). About risks above, Block Chain in trade secret management was suggested to improve in the following aspects.

A. "Standard consensus + compatible consensus plug-in" mode

On September 7, 2018, "Provisions of the Supreme People's Court on Several Issues Concerning the Trial of Cases by Internet Courts" was officially implemented. The status of Block Chain was recognized as evidence of electronic certificate storage in Article 11 of this Judicial Interpretation. It was the first legal confirmation of the legal status of Block Chain as electronic certificate storage in China. In the confirmation, Block Chain was allowed to collect, fix and tamper-proof data as evidence.

By the end of 2019, three internet courts were built in China: Hangzhou, Beijing and Guangzhou. Based on Block Chain, one "unified platform for judicial Block Chain of people's courts" was built in Chinese Supreme People's Court. More than 194 million pieces of data were completed with the work of uploading and storing certificates. Various local courts were stopped with Block Chain as well.

Obviously, the intention of Chinese Supreme People's Court was to build a high starting point, high standard to carry out judicial application in Block Chain electronic deposit. In local people's courts, judicial Block Chain building was allowed to continue to operate, albeit partial suspended. This fact showed the attitude of the Supreme People's Court. Block Chain was applied in judicial practice as a new data technology for electronic certificate storage. The purpose of judicial Block Chain was to make the consensus mechanism universally applicable in a wider scope, to allow local courts to operate Block Chain. There was a mechanism unified Block Chain and local Block Chain in forming a new compatible consensus model. The mechanism would make full use of resources to a certain extent. The universal application characteristics of Block Chain would be conformed as evidence technology support. More choices and convenience would be provided for parties. They were represented as the general trend of China's judicial Block Chain development in the future.

As mentioned above, the pledge of intellectual property rights was stipulated in Article 440, Civil Code of People's Republic of China. It stipulated that the pledge right would be established when the pledge registration was made. Adopted an enumeration mode, article 440 listed such intellectual property rights as patent right, exclusive right to registered trademark and copyright. To three types of intellectual property rights with an unified platform and system, the entries were simple and clear in their application. That was, it could be handled in a unified national registration institution. However, no unified national level platform was ready for the non-statutory publicity, and no uniqueness of intellectual property was absolute rights at present. They were easily held by such trade secrets holders as enterprises themselves. Once being a long-standing historical problem, it was easy to prove litigation involved. More practical significance could be found in the unified work of the Supreme People's Court on Block Chain platform for trade secrets. Once the trade secrets of trade secret owners were standing together with the chain, they would stand together with the national unified registration platform. The pledge registration would be completed by registration formalities once the trade secrets pledged. Thus, efficiency and cost were optimized simultaneously. However, the results were premised that a wider range would be covered by the

judicial Block Chain platform of the Supreme People's Court. The premise of optimization was that the judicial Block Chain platform of the Supreme People's court needed to generally covered. At the same time, the Block Chain platform should have the function of efficient storage and processing of trade secrets (general Block Chain technology cannot achieve the storage and processing capacity of massive data quickly and efficiently). What was more, it can be operated more than judicial certificate storage.

B. Scheme for private key security

Up to now, the social significance and value of Block Chain were hotspot at home and abroad throughout theory and practice. However, data security in Block Chain could not be guaranteed as well as confidentiality requirements by any scheme, nor privacy requirements as data rights holders wanted. Encryption keys protection was still the primary problem faced by Block Chain (Louise Axon, Michael Goldsmith, Sadie Creese, 2018). The risk of encryption keys came from the process of storage and transaction before and after uploading. At present, encryption keys for transportation and transmission were easy to be stolen for its online or in the cloud. Being concealed, encryption keys were difficult to prove especially in the form of cloud storage. Such technical business secrets as technical information and customer information were put in the cloud by enterprises. The storage was equivalent to automatically open to cloud service providers. It was particularly urgent to explore appropriate legal protection for interests of enterprises. What was more, apart from the traditional password, some authentication links of identity or specific biological information would be developed by an encryption key. Some encryption information would be opened during point-to-point transaction. The authentication information could be changed at any time according to needs after transaction completed. Such identity or biological information above as facial expression and gesture can be changed by provider when it destroyed.

C. To build a secret block model

There was a fundamental conflict between the above requirements and the traceability and transparency of the Block Chain. Scholars once discussed the way to balance privacy and security in Block Chain. A user centered and privacy preserving certificate scheme was proposed based on Block Chain. The protocol allowed users to access services without exposing sensitive attributes. Based on efficient short signatures, pair-wise and self-blind credentials were verified on the Block Chain. The scheme realized the anonymity, unlinkability and untraceability of users. In addition, the confidentiality of user attributes was satisfied as well as the unforgeability of user credentials (Kalpana Singh, Omar Dib, Clément Huyart, Khalifa Toumi, 2020). Another case in point, one privacy protection method of license Block Chain based on blind signature was invented to protect trade secrets by users' blind signatures (Li Xianxian, 2019). The inherent transparency and full traceability of Block Chain was ended to a certain extent. At the same time, the technical advantages of Block Chain was affected in a certain extent. Traditional problem of proof was difficult returned once the trade secrets in the chain were stolen, once the traceability and transparency were blocked.

As mentioned above, any information would be accessed on the chain without barriers when loaded into cloud database. Immeasurable risks would be brought to the chain of trade secrets. Background access would record such access information in Block Chain platform as personnel, time and place. Whether there was a preventive mechanism in background access. Generally, the background processing Block Chain information was invisible as specific content on the surface. If you wanted to see it, you needed to open this door. Once you opened and visited it, you would start the traceability process similar to Block Chain, which ensured the security of information to a certain extent. A warning would be given to those who wanted to open and those who could open.

Trade secrets (information) in background database would be accessed or uplinked unlimitedly. In practice, the operation mode was generally based on the confidentiality agreement signed by both parties. However, it was difficult to determine the secret leakage traces caused by access. For example, instead of downloading at the beginning of the uplink, photos taken by visitors would be at risk of leakage. However, the condition was not in the scope of trade secrets confidential measures. Block Chain, as a carrier system of trade secrets information, would minimize the risk with corresponding technical prevention and control.

D. Legislation for trade secret protection

To effectively protect the information, the application of Block Chain should be standardize. In practice, information belong to trade secrets was often lack of legal protection. For example, banking, financial and shopping software downloaded in hand, needed to agree to obtain photos, videos, access address book, location and other protocol contents in the mobile phone before applied. Consumers were often received the prompt that our location information was acquired by a certain software. Few of us would care about the value of the acquired location information. None of us received reward from the enterprise acquired location information. The location information of natural persons was obtained by enterprise backstage. The acquirement showed that the information was valuable. Theoretically, the acquirement should be paid if information was valuable. However, the acquired person would not receive any remuneration from companies. Relevant national legislation lacks mandatory provisions made data leakage and illegal usage rampant. A natural person would give up even if he wanted to defend himself through litigation. It was impossible for a natural person to effectively prove which enterprise obtained what information during which period. Lack of clear legal basis, evidence of infringement was difficult to obtain as well. Data acquisition without cost was a typical behavior of violent plunder and profiteering.

Information protect could be regulated in the following two aspects:

First, Block Chain was penetrate into various fields of network data storage. Original acquisition, intermediate changes could be detailed traced as well as such process data as location and shopping preference. A complete evidence chain was provided for possible data leakage, data payment litigation and dispute resolution.

Second, it was to explore the feasibility of separate legislation formulating on trade secret consent. The basic legal aspects of China's legal norms of trade secrets were Civil Code of People's Republic of China (General Principles of Civil Law till January 1, 2021, Civil Code of People's Republic of China post January 1, 2021) and Anti-Unfair Competition Law of People's Republic of China. The former stipulated that trade secrets were legal objects of intellectual property rights, while the latter stipulated the definition and protection rules of trade secrets. From the perspective of concrete implementation, certain defects could be found in China's trade secret legislation and law enforcement system. It was to be improved urgently.

Subject of infringement should be improved. According to legislative spirit of "Anti-Unfair Competition Law of the People's Republic of China", law direction to the subject of trade secrets infringement of should refer to operators and specific natural persons, legal persons and unincorporated organizations (the third party included). What is more, such malicious acts with specific infringement intentions was included as well as implementers of infringement parties. However, according to Article 1.3, Entry 2, Economic and Trade Agreement between Governments People's Republic of China and the United States of America signed by China and United States on January 15, 2020, China was responsible to define such "operator" infringing trade secrets as natural persons, organizations and legal persons. The definition would obviously expand the concept of "operator". More attention should be paid to the distinction in the process of protecting trade secrets once "operator" was referred in Anti-Unfair Competition Law. It was obviously that "operator" here meant a commercial subject with legal business qualifications in the commercial field. The commercial subject was consistent with the legislative essence of the Anti-Unfair Competition Law. However, Trade Secret Protection Law would be corresponded once "operator" was defined as all natural person organizations and legal persons in a single law mode. It was seemed that China's subsequent legislative mode for trade secrets would like to turn to a separate legislative mode for trade secrets. However, the protection of trade secrets would be practically considered as a broad range of infringing subjects.

Subject of trade secret rights should be protected. According to Article 123 in Civil Code, all civil subjects were entitling to the obligee of trade secrets. However, the obligee's trade secrets were restrict to "commercial information" according to Article 9 in Anti-Unfair Competition Law. Anti-Unfair Competition Law was consistent with the identity of "operator" as a commercial subject, whereas natural persons were excluding in the general civil sense practically. However, as said above, it was of great commercial value for such information as personal location and shopping preferences acquired by ordinary natural persons on Internet. Data providers should be authorized with legal usage through agreements with original right holders and users. The authorization was just legal usage in current situation. However, it was unfair for the providers to be unpaid fundamentally. Data transfer to be authorized would be finally canceled once internet passive consent lacks independently choose. Actually, commercial organizations need to pay for consumers' personal information in countries with relatively complete personal credit information systems. For example, the location information and shopping preference would be obtained by the Japan company after users downloaded a mobile program company developed. The consumer would be got a corresponding value reward of 500 yen after obtaining personal location data for 3 months (Han Ming,

2019). It was showed that personal information of ordinary natural persons was more than the privacy attribute in the traditional civil sense beyond the essence of commercial profit.

The promulgation of China's Civil Code showed that China would adhere the legislative mode of civil and commercial integration, that China would continue to implement the legislative mode of separate law in commercial affairs. Trade secrets were defined as "business information" in Article 9 of Anti-Unfair Competition Law with two layers of meaning. The first was based on the subjective understanding enjoyed by the business subject. The second was based on the objective understanding of commercial behavior. Narrowed scope of civil subject in Article 123 of China's Civil Code, the legislative spirit of Anti-Unfair Competition Law obviously belonged to the first level. However, the category of commercial subject was obviously broken through from the value level of personal information digitization above-mentioned. To define the "commercial information" of commercial secrets was more appropriate and reasonable by commercial behavior. That is, although the digitization of personal information was not provided by commercial subject as stipulated by law, personal providing information of the current era was under the background when do business. In particular, the interpretation of the great significance of spreading the economy was put forward by Premier Li Keqiang, Premier of the State Council of China, during the inspection of Shandong on June 1, 2020. It was more appropriate to understand "business" in terms of business behavior itself. The digital personal information provided by ordinary natural persons was not open to the public as consumers to businesses through Block Chain or other forms. There were still confidentiality requirements beyond commercial profit peer-to-peer. Objectively, basic requirements of trade secrets and conforms should conform the actual situation. It meant that ordinary natural persons would entangled with the substantive obligees of trade secrets in this respect. The situation was impossible to achieve in the scope of the current Anti-Unfair Competition Law. Therefore, a better choice should be chosen the unified and separate legislation of trade secrets in the future.

Vi. Conclusion

As a national strategy of China, Block Chain was gradually applied in such field as cryptocurrency and intellectual property. As Block Chain was still at an early stage, such risk as systematic and non-systematic should be overcome ahead.

The ownership identification of trade secrets should be based on its particularity and universality. Compared with the traditional methods in judicial deposit and evidence collection, great changes had made by the use of Block Chain to protect trade secrets. However, such risks as leakage and tampering were still existing as well as lack of legal supervision. To a certain extent, the judicial Block Chain unified platform led by the Supreme People's Court of China was a relatively closed-loop existence. The encryption verification adopted by the platform ensures its relative security and credibility. In short, to integrate with transparency, traceability and confidentiality in protection trade secrets, intellectual property and electronic certificates, a long period of time development is ahead in realizing the value function of the ordinary Block Chain in Chinese future.

Although China has practiced the protection of trade secrets in Block Chain at the application level, there are still many difficult problems to be solved at the legal level. At present, most countreies has paid great attention to the issue of Block Chain at the national level. Based on the long-term cooperative relationship between China and other countries in intellectual property and the special requirements for the protection of trade secrets in Block Chain, China and other countries can deepen cooperation in this field, learn from each other's strengths and make up for their shortcomings, and achieve a win-win situation in the construction of the belt and road initiative.

Declarations

Acknowledgements

This study was supported:

by Soft Science Project of State IP Office of China (No. SS20-B-27);

by Shandong Province Social Science Planning Research Project of China (Special Project) (No. 20CFZJ05).

Funding : Not applicable

Conflicts of interest : The author has no conflicts of interest

Availability of data and material: Not applicable

Code availability: Not applicable

References

1. Song Shiyong, Xing Yuxia. 2020. “Chinese Intellectual Property Strategy of Sustainable Development in High Education”. Revista Argentina de Clínica Psicológica 2020, Vol. XXIX, N°4, 570-578.
2. Tang Qinglin, Huang Minxin. 2011. Detailed Explanation of Trade Secret Protection Practice and Analysis of 100 Cases(Chinese). Bei Jing : China Legal Publishing Press.
3. Gabin Heo , Dana Yang , Inshil Doh and Kijoon Chae. 2020. “Design of Block Chain System for Protection of Personal Information in Digital Content Trading Environment”. http: //ieeexplore-ieee-org-s.vpn.qlu.edu.cn: 8118/document/9016501.
4. Wu Wei. 2017. Block Chain Actual Combat(Chinese).Bei Jing: Tsinghua University Press.
5. Yekou, Youjixiong. 2018. Block Chain Revolution: The Emergence of Distributed Self-disciplined Society(Chinese). Bei Jing: Oriental Publishing Press.
6. D. R. Jensen.2009. Cryptography: Theory and Practice(Chinese). Bei Jing: Publishing House of Electronics Industry.

7. Zhang Huaiyin. 2019. “Block Chain and Trade Secret Protection in Digital Environment”. Journal of Electronic Intellectual Property (3): 71-78.
8. Rob Shwarts, Kayvan Ghaffari and Block Chain. 2018. “Not Just a Platform for Cryptocurrency but a Potential Method for Protecting Trade Secrets and Other IP”. https: //blogs.orrick.com/trade-secrets-watch/2018/02/16/blockcha...t-a-potential-method-forprotecting-trade-secrets-and-other-ip/, 2018-09-07.
9. Kalpana Singh, Omar Dib, Clément Huyart and Khalifa Toumi. 2020. “A Novel Credential Protocol for 3 Protecting Personal Attributes in Block Chain”, https: //doi.org/10.1016/j.compeleceng.2020.106586.
10. Joseph Holbrook. 2020. “Architecting Your Enterprise Block Chain. https: //doi.org/10.1002/9781119557722.ch3.
11. Gönenç Gürkaynak, İlay Yılmaz, Burak Yeşilaltay and Berk Bengi. 2018. “Intellectual Property Law and Practice in the Block Chain Realm”, https: //doi.org/10.1016/j.clsr.2018.05.027.
12. Kondapally Ashritha, M. Sindhu and K.V. Lakshmy. “Redactable Block Chain Using Enhanced Chameleon Hash Function. http: //ieeexplore-ieee-org-s.vpn.qlu.edu.cn: 8118/document/8728524.
13. Gabin Heo, Dana Yang, Inshil Doh and Kijoon Chae. “Design of Block Chain System for Protection of Personal Information in Digital Content Trading Environment. http: //ieeexplore-ieee-org-s.vpn.qlu.edu.cn: 8118/document/9016501.
14. Avinash Kaur, Anand Nayyar and Parminder Singh. 2020. “Block Chain A Path to the Future. https: //doi.org/10.1002/9781119621201.ch2.
15. Muneeb Ul Hassan Mubashir Husain Rehmani and Jinjun Chen. 2019. “Privacy Preservation in Block Chain Based IoT Systems: Integration Issues, Prospects, Challenges, and Future Research Directions”. https: //doi.org/10.1016/j.future.2019.02.060.
16. Matthew Beising(Translated by Xu Zixuan). 2016. “ To Conquer Wall Street? Block Chain Needs to Protect Trade Secrets”. Business Weekly (Chinese version) (9): 44-46.
17. Zheng Yi. 2014. Research on Cybercrime and Related Problems(Chinese). Wuhan: Wuhan university press.
18. Louise Axon, Michael Goldsmith and Sadie Creese. 2018. “Privacy Requirements in Cybersecurity Applications of Block Chain.https: //doi.org/10.1016/bs.adcom.2018.03.004.
19. Ledger Insights. 2020. “China Believes that Block Chain can Protect Trade Secrets”. https: //www.ledgerinsights.com/china-Block Chain-trade-secrets-intellectual-property/.
20. Louise Axon, Michael Goldsmith and Sadie Creese. 2018. “Privacy Requirements in Cybersecurity Applications of Block Chain”. https: //doi.org/10.1016/bs.adcom.2018.03.004.
21. Xxx. 2019. “Privacy Protection Method and Process of License Block Chain Based on Blind Signature”. http: //www.xjishu.com/zhuanli/62/201811249383.html.
22. Brad Feinstein. 2019. “How does Block Chain Change Sports Industry”.https: //zhuanlan.zhihu.com/p/77258414.

23. Xxx. 2019. “How to Launch Cryptocurrency and Block Chain Projects in the Sports Industry”. http: //m.elecfans.com/article/1007709.html.
24. NehaGupta. 2020. “A Deep Dive Into Security and Privacy Issues of Block Chain Technologies”. https: //doi.org/10.1016/B978-0-12-819816-2.00004-6.
25. Yang Dong. 2017. “Chain Gold has a Law: Block Chain Business Practice and Legal Reference”. Bei Jing: Beihang University Press.
26. StephenCastell. 2018. “The Future Decisions of RoboJudge HHJ Arthur Ian Block Chain: Dread, Delight or Derision”. https: //doi.org/10.1016/j.clsr.2018.05.011.
27. Teresa. 2018. “Trade Secrets of Block Chain Unicorn Circle”. https: //www.sohu.com/a/232798471_100142711.
28. Huru Hasanova, Ui-jun Baek, Mu-gon Shin, Kyunghee Cho and Myung-Sup Kim. 2019. “A Survey on Block Chain Cybersecurity Vulnerabilities and Possible Countermeasures”. https: //doi.org/10.1002/nem.2060.
29. Han Ming. 2019. “People's Daily: The Block Chain Makes the Data ‘Who Owns and Who Benefits’”. http: //Block Chain.people.com.cn/n1/2019/0411/c417685-31024683.html.
30. Fire Wangwang Team. 2020. “What's the Use of the Judicial Block Chain Mentioned in the Supreme Court Report”. https: //www.wanbizu.com/news/20200613458017.html.
31. Sidhant Mohanty, Biswa Mohana Jena, and Esra Sipahi " The Importance of Self Employment in the Context of Small Enterprises: A Case Study of Odisha and Examples from Turkey ", productivity management, vol.26, no.1, pp. 440-457, January 2021.
32. Sipahi, E . (2019). THE ROLE OF SOCIAL WORK IN THE CONTEXT OF INTERNATIONAL DEVELOPMENT: A CROSS-COUNTRY ANALYSIS . R&S - Research Studies Anatolia Journal , 2 (5) , 136-148 . DOI: 10.33723/rs.551503

Figures

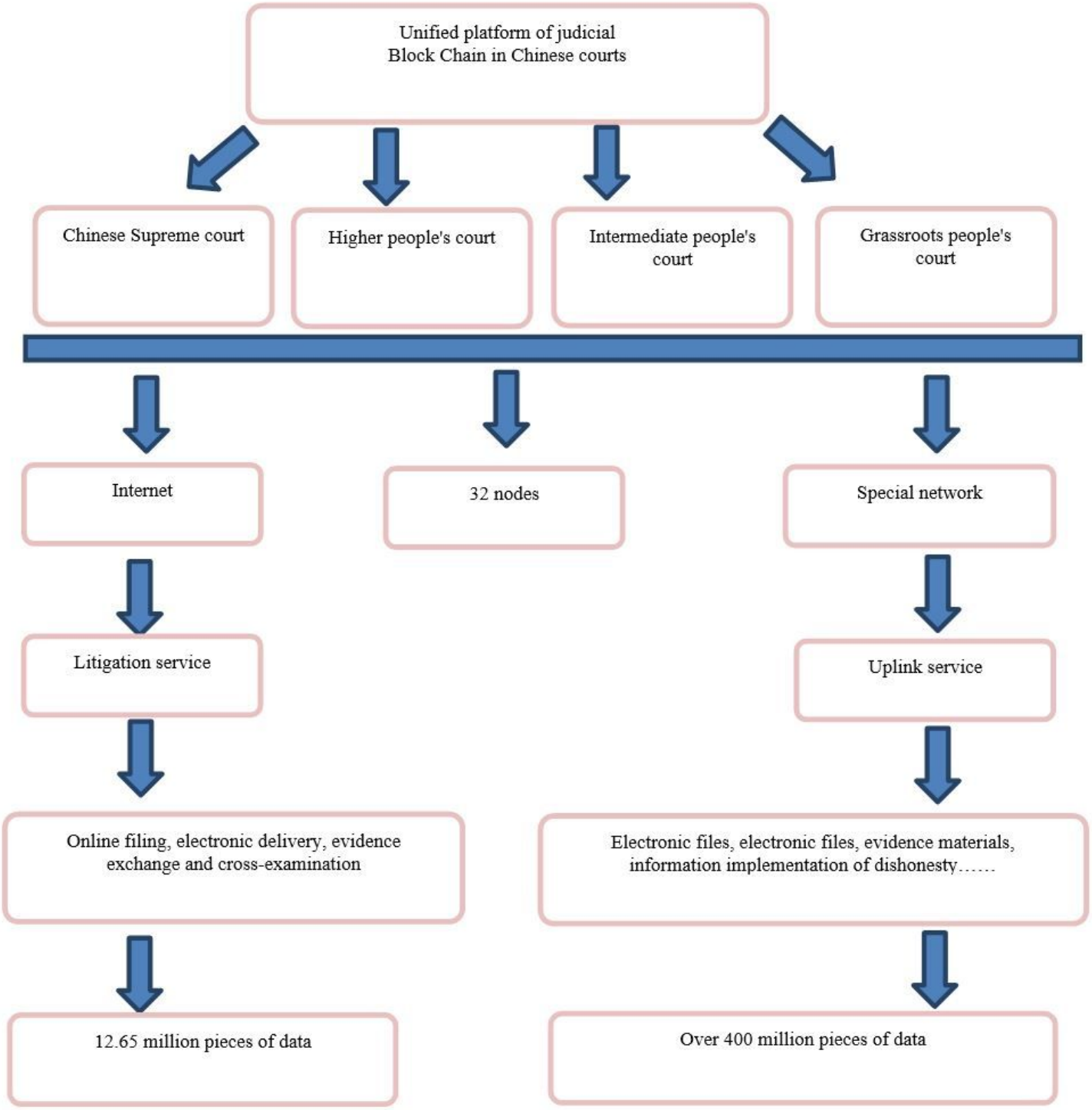

Figure 1

Brief unified platform of judicial Block Chain with Chinese courts in 2019 (May 22, 2020)

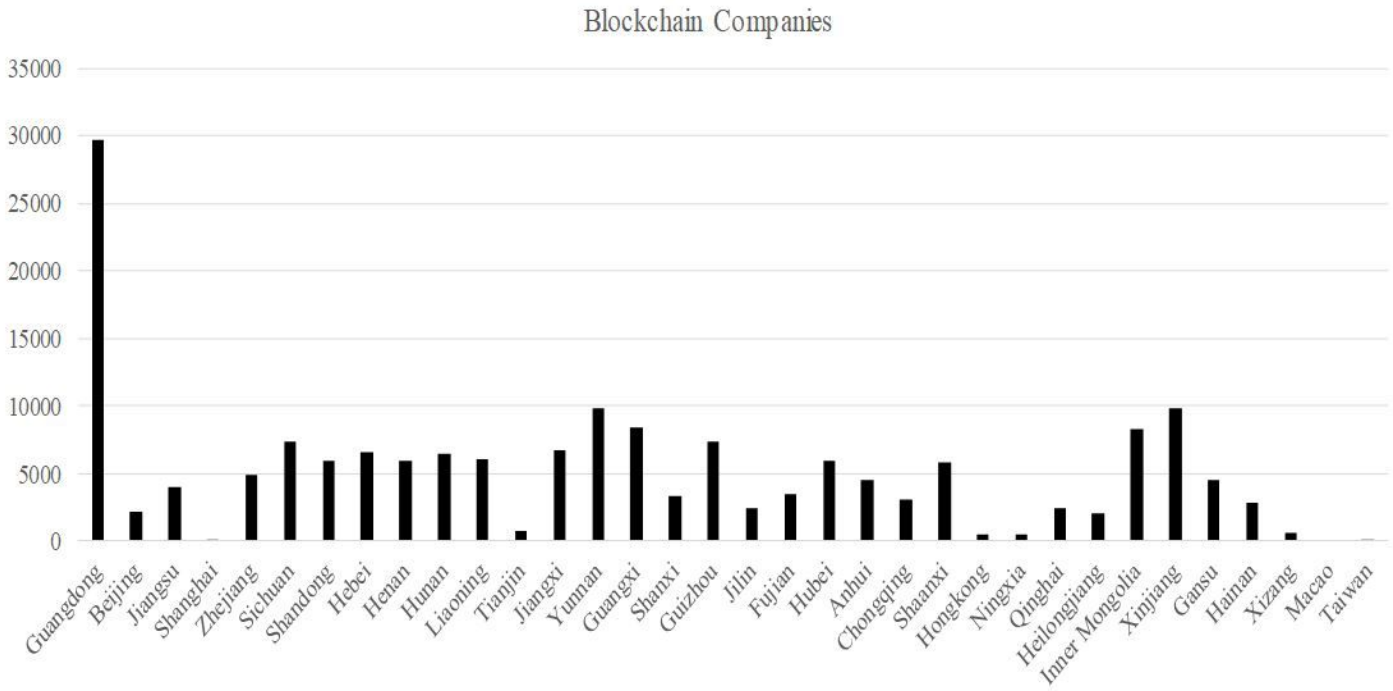

Figure 2

Statistics of Block Chain companies in China sources: data were selected from website of enterprise search https://www.qcc.com/search?key=%E5%8C%BA%E5%9D%97%E9%93%BE, July 4th, 2020.