Regional

China Passes New Cryptography Law as Part of Greater Effort to Develop and Apply Blockchain Technologies

Introduction

On 26 October 2019, China's top legislative body, the Standing Committee of the National People's Congress, voted to adopt the Cryptography Law of People's Republic of China (中华人民共和国密码法) ("**Cryptography Law**"). The law will come into force on 1 January 2020.[1]

The Cryptography Law came just two days after Chinese President Xi Jinping announced that the country should accelerate the development of blockchain technology as a core for innovation.[2] China's official state-run news agency, Xinhua, quoted President Xi as saying blockchain would serve "an important role in the next round of technological innovation and industrial transformation". He is also said to have emphasised "deep integration" between blockchain and "other information technologies including artificial intelligence, big data and [the] Internet of Things".

The Chinese government has organised a series of group studies on specific topics, including the use of the internet, big data and artificial intelligence, in an effort to innovate and move up the economic value chain.

In an explanatory note published by the Office of the Cybersecurity Administration on 29 October 2019, it was also mentioned that "cryptography is like the DNA of the cyberspace", by "fully realizing the security requirements of identity anti-counterfeiting, information anti-disclosure, content anti-tampering, and behavioural non-repudiation". While not explicitly named, the reference to the capabilities and functions of blockchain technology could not be missed.

Cryptography already permeates most aspects of modern Chinese life. In the explanatory note published by the Office of the Cybersecurity Administration, it was observed that "commercial cryptography is widely used in all aspects of national economic development and social production and life. In the financial field, the People's Bank of China and the State Cryptographic Administration have established a comprehensive technical system and standard system for commercial passwords and banking services, effectively curbing illegal activities such as bank card forgery and online transaction status counterfeiting; in the field of taxation, VAT anti-counterfeiting, the tax control system uses

[1] Article 44, Cryptography Law
[2] https://www.channelnewsasia.com/news/business/china-passes-cryptography-law-as-gears-up-for-digital-currency-12038596

commercial cryptography technology to protect tax-related information, effectively curbing illegal activities such as tax evasion and tax evasion through tampering with invoice information; in the field of social management, the Ministry of Public Security has issued more than 1.8 billion copies of the second-generation ID card using commercial cryptographic chips, effectively eliminating illegal and criminal acts such as forgery and alteration of identity cards. In addition, commercial cryptography can also be used to protect citizens' sensitive personal information, privacy and corporate trade secrets."

In August 2019, it was announced by the People's Bank of China that it is "close" to issuing its own cryptocurrency.[3]

Against this backdrop, the Cryptography Law is a strong policy statement that China intends to adopt greater institutional efforts to further strengthen and promote the development and application of blockchain technology, and to entrench itself as a leading global player and standard-setter.

Salient points to note from the Cryptography Law would include:

(a) The emphasis on grooming and rewarding cryptography talents, and the express positioning of cryptography as an integral part of local-level development plans;
(b) China's intention to develop and establish standardisation, certification, accreditation and supervisory frameworks, thereby positioning and entrenching itself as a standard-setting body in the field of commercial cryptography; and
(c) According protection to proprietary technology and information, including express prohibitions on forced technology transfers and disclosure of source codes.

Purposes of the Cryptography Law

The Cryptography Law is enacted for the purposes of:

(a) Standardising the application and management of cryptography;
(b) Promoting the development of the cryptography industry;
(c) Safeguarding network and information security, safeguarding national security and social public interests; and
(d) Protecting the legitimate rights and interests of citizens, legal persons and other organizations.

Classifications of Cryptography

The Cryptography Law defines "Cryptography" broadly as "technology, products and services for encrypting and securing information, etc. by means of a specific transformation method".

[3] https://www.bloomberg.com/news/articles/2019-08-12/china-s-pboc-says-its-own-cryptocurrency-is-close-to-release

Under the Cryptography Law, Cryptography is categorised into 3 types: Core Cryptography (核心密码), Common Cryptography (普通密码) and Commercial Cryptography (商用密码).[4]

Core Cryptography and Common Cryptography are used to protect state secrets and in themselves constitute state secrets. They will be uniformly managed by the Cryptography Management Department (密码管理部门) in accordance with the Cryptography Law and other relevant laws, administrative regulations and state regulations.[5]

In contrast, Commercial Cryptography is defined as Cryptography used to protect information that are not state secrets, and can be used by citizens, legal entities (i.e. businesses) and other organisations to protect networks and information security.[6]

Promoting Development of the Cryptography Industry

General provisions

The Cryptography Law sets out in Chapter I a suite of provisions that are intended to foster and promote further developments in China's Cryptography scene, through rewarding talents, strengthening education, increasing economic support and enhancing legal protection for encrypted information.

Article 9 of the Cryptography Law focuses on the rewarding of talents. It provides that the State will "strengthen the training of cryptographic talents and building of cryptography teams", and "organizations and individuals who have made outstanding contributions to the work of cryptography will be commended and rewarded in accordance with relevant state regulations."

On the other hand, Article 10 focuses on the strengthening of education in cryptography. It provides that the State will "strengthen cryptography education and incorporate cryptography education into the national education system as well as civil service education and training systems, and enhance cryptography awareness of citizens, legal entities and other organisations."

Article 11 mandates local governments to incorporate cryptography works into their development plans. It provides that "People's government at the county level and above shall incorporate cryptography work into the national economic and social development plans at the same level, and the required funds shall be included in the financial budget."

[4] Article 6, Cryptography Law
[5] Article 7, Cryptography Law
[6] Article 8, Cryptography Law

Commercial Cryptography

In addition, Chapter III of the Cryptography Law also sets out specific provisions aimed at promoting developments for Commercial Cryptography.

Article 21 provides that "The State encourages research and development, academic exchanges, transformation of results and application of commercial cryptography, and improves a unified, open, competitive and orderly commercial cryptographic market system to encourage and promote the development of Commercial Cryptography". The people's governments at all levels and their relevant departments are instructed to abide by the principle of non-discrimination and treat enterprises engaging in commercial cryptography research, production, sales, service, import and export, activities, *including foreign-invested enterprises* (collectively "**Commercial Cryptography Practitioners**") in accordance with the law, and *forced transfers of cryptographic technology* by administrative agencies and their staff using administrative methods *are strictly prohibited***.**

Safeguarding Network and Information Security/ Safeguarding National Security and Social Public Interests

Core Cryptography and Common Cryptography

As highlighted above, Core Cryptography and Common Cryptography are used to protect state secrets and in themselves constitute state secrets.[7] Chapter II of the Cryptography Law sets out the security standards that Cryptography Work Institutions (defined as institutions engaged in the research, production, service, testing, equipment, use and destruction of Core Cryptography and Common Cryptography) must comply with.

Article 14 provides that state secret information transmitted through wired and wireless communications as well as information systems for storing and processing of state secret information must be encrypted with Core Cryptography and Common Cryptography. Article 33 provides that failure to use Core or Common Cryptography as may be required may in accordance with Article 14 may attract warning and sanctions imposed by various State Organs on the recommendation of the Cryptography Management Department.

Article 16 provides that the Cryptography Management Department has supervisory oversight of Cryptography Work Institutions.

Article 17 further provides that the Cryptography Management Department will, in collaboration with relevant government departments, establish a collaborative mechanism for security monitoring and early

[7] Article 7, Cryptography Law

warning, security risk assessment, information notification, major event consultation and emergency response to ensure the security management of Core Cryptography and Common Cryptography. An obligation is also imposed on Cryptography Work Institutions to report any leaks, security hazards or major issues discovered that may affect the security of Core or Common Cryptography for timely investigation, resolution and elimination of security hazards.

Commercial Cryptography

The concern for safeguarding of national security and social public interests is also present in Chapter III which is dedicated to Commercial Cryptography.

Article 21 is book-ended by the principle that "scientific research, production, sales, service and import and export of Commercial Cryptography shall not impair national security, social public interests or the legitimate rights and interests of others." Violation of this principle could trigger legal sanctions under the Cybersecurity Law as other applicable laws and regulations.[8]

Article 26 also provides that Commercial cryptographic products that may implicate national security, national economy and people's livelihood, and social public interests will be listed in a network key equipment and cybersecurity special product catalogue according to law, and may only be sold or supplied after passing the testing and certification of qualified institutions. Violation of this provision may attract warnings and fines.

Standardising Application and Management of Cryptography

The Cryptography Law also sets out various initiatives that China intends to undertake in order to standardise the application and management of Cryptography, in particular in Commercial Cryptography.

Core and Common Cryptography

Article 13 provides that the State shall strengthen the scientific planning, management and use of Core and Common Cryptography, strengthen institution-building, improve management measures, and improve the ability for cryptography to safeguard security.

Article 15 provides that Cryptography Work Institutions must establish comprehensive and secure management protocols, and adopt security measures and accountability systems in accordance with applicable laws, regulations and requirements to ensure the security of Core Cryptography and Common Cryptography.

[8] Article 32, Cryptography Law

Commercial Cryptography

The Cryptography Law sets out a slew of provisions in Chapter III which describe the measures the State intends to undertake to achieve a higher degree of standardisation across Commercial Cryptography Practitioners, both domestic and globally.

Article 22 provides that the State "shall establish and improve on a Commercial Cryptography standardisation system", and further that the State will "support social groups and enterprises to autonomously innovate and create Commercial Cryptography standards that are higher than national standards and industry standards".

Article 23 also provides that the State will push the participation in international standardisation of Commercial Cryptography, participate in the establishment of international standards, and promote the interchangeability between domestic and foreign standards. The State also encourages enterprises, social groups, and educational and scientific research institutions to participate in international standardisation activities for Commercial Cryptography.

Article 25 provides that the State will promote the establishment of Commercial Cryptography verification and certification systems.

Article 36 provides that the sale or provision of Commercial Cryptography products which are not properly assessed or Commercial Cryptography services that are not properly certified may attract sanctions in the form of fines.

Protecting Legitimate Rights and Interests

Given that the last of the four core purposes of the Cryptography Law is "protecting the legitimate rights and interests of citizens, legal persons and other organizations", the Cryptography Law sets out various provisions to protect commercial interests and proprietary cryptographic information.

Article 21 provides that "administrative agencies and their staff shall not use administrative means to force the transfer of commercial cryptography technology".

In a similar vein, Article 31 also provides that "The Cryptography Management Department and relevant departments and their staff shall not require Commercial Cryptography Practitioners and Commercial Cryptography detection and certification agencies to disclose cryptography-related proprietary information such as source code to them, and shall strictly enforce the business secrets and personal privacy that they learnt in the course of performing their duties."

Article 40 provides that staff of relevant government departments or units who abuse their powers, neglect their duties, engage in malpractices for personal gains in cryptographic work, or disclose or illegally provide others with trade secrets and breach personal privacy will face disciplinary actions.

Article 41 also makes clear that the sanctions under the Cryptography Law are imposed in addition to, and will not affect other liabilities, whether civil or criminal, of the transgressor under other relevant laws.

Conclusion

Despite its relatively short length, the Cryptography Law is surprisingly ambitious in scope. It should therefore not be surprising that many provisions of the Cryptography Law are at the present moment mostly guiding principles rather than concrete measures ready for implementation. It is expected that further regulations, guidance and codes of practices will be released in due time to further refine and clarify how these principles will be implemented.

It is therefore perhaps more accurate to view the Cryptography Law as a policy statement of China's intention to step up its efforts to strengthen and promote the development and application of blockchain technology, and to entrench itself as a leading global player and standard-setter.

Developments in this area should be closely monitored, and we will provide further updates on such developments in time to come.

Disclaimer: *Rajah & Tann Singapore LLP Shanghai Representative Office is a foreign law firm licenced by the Ministry of Justice of the People's Republic of China (the "**PRC**"). As a foreign law firm, we may not issue opinions on matters of PRC law. Any views we express in relation to PRC laws and regulations for this matter are based on our knowledge and understanding gained from our handling of PRC-related matters and through our own research, and also from our consultations with PRC lawyers. Therefore, such views do not constitute (and should not be taken as) opinion or advice on PRC laws and regulations.*

Contacts

Rajesh Sreenivasan
Head, Technology, Media & Telecommunications
Rajah & Tann Singapore LLP

D +65 6232 0751

rajesh@rajahtann.com

Benjamin Cheong
Partner, Technology, Media & Telecommunications
Rajah & Tann Singapore LLP

D +65 6232 0738

benjamin.cheong@rajahtann.com

Linda Qiao
Senior International Counsel
Rajah & Tann Shanghai Representative Office

D +86 21 6120 8818

linda.qiao@rajahtann.com

Chia Lee Fong
Chief Representative
Rajah & Tann Shanghai Representative Office

D +86 21 6120 8818

lee.fong.chia@rajahtann.com

Please feel free to also contact Knowledge and Risk Management at eOASIS@rajahtann.com

Our Regional Contacts

RAJAH & TANN | *Singapore*

Rajah & Tann Singapore LLP
T +65 6535 3600
sg.rajahtannasia.com

R&T SOK & HENG | *Cambodia*

R&T Sok & Heng Law Office
T +855 23 963 112 / 113
F +855 23 963 116
kh.rajahtannasia.com

RAJAH & TANN 立杰上海
SHANGHAI REPRESENTATIVE OFFICE | *China*

Rajah & Tann Singapore LLP
Shanghai Representative Office
T +86 21 6120 8818
F +86 21 6120 8820
cn.rajahtannasia.com

ASSEGAF HAMZAH & PARTNERS | *Indonesia*

Assegaf Hamzah & Partners

Jakarta Office
T +62 21 2555 7800
F +62 21 2555 7899

Surabaya Office
T +62 31 5116 4550
F +62 31 5116 4560
www.ahp.co.id

RAJAH & TANN | *Lao PDR*

Rajah & Tann (Laos) Co., Ltd.
T +856 21 454 239
F +856 21 285 261
la.rajahtannasia.com

CHRISTOPHER & LEE ONG | *Malaysia*

Christopher & Lee Ong
T +60 3 2273 1919
F +60 3 2273 8310
www.christopherleeong.com

RAJAH & TANN NK LEGAL | *Myanmar*

Rajah & Tann NK Legal Myanmar Company Limited
T +95 9 7304 0763 / +95 1 9345 343 / +95 1 9345 346
F +95 1 9345 348
mm.rajahtannasia.com

GATMAYTAN YAP PATACSIL
GUTIERREZ & PROTACIO (C&G LAW) | *Philippines*

Gatmaytan Yap Patacsil Gutierrez & Protacio (C&G Law)
T +632 8894 0377 to 79 / +632 8894 4931 to 32
F +632 8552 1977 to 78
www.cagatlaw.com

RAJAH & TANN | *Thailand*

R&T Asia (Thailand) Limited
T +66 2 656 1991
F +66 2 656 0833
th.rajahtannasia.com

RAJAH & TANN LCT LAWYERS | *Vietnam*

Rajah & Tann LCT Lawyers

Ho Chi Minh City Office
T +84 28 3821 2382 / +84 28 3821 2673
F +84 28 3520 8206

Hanoi Office
T +84 24 3267 6127
F +84 24 3267 6128
www.rajahtannlct.com

Our Regional Presence