International Blockchain Olympiad

Opening Ceremony

Friday 3 July 2020 9:30-10pm

City University (via video conferencing)

Opening Remarks

by Stephen Kai-yi Wong

Barrister, Privacy Commissioner for Personal Data, Hong Kong

Professor YAN Houmin (嚴厚民教授, Dean of the College of Business, CityU), **Gabriel** (CHAN, Programme Director of the event), and **Project Participants**,

- Blockchain is certainly one of the main driving forces for technological innovation and economic growth in this data driven economy.

- As President Xi stressed at a meeting in Beijing in October 2019, blockchain should be promoted as a core technology for innovation.

- The International Blockchain Olympiad has a commendable mission – namely, to support sustainability and maturity in blockchain by working with industry, government, and academic partners.

- Let me extend a warm welcome to all of you from all corners of the globe participating in this annual competition. In the next couple of days, we will have the privilege to see a host of blockchain solutions designed by blockchain talents from around the globe with a view to solving a myriad of problems the world is facing.

- My statutory role as Privacy Commissioner is threefold: an enforcer, educator and a facilitator. In other words, while my office upholds personal data protection, we do not stand in

the way of technological innovation. Instead, we facilitate technological development and innovation in a privacy-friendly manner.

Value of blockchain

- As you will agree, the use of blockchain technology to improve our economic and social well-being has been gaining pace rapidly over the last decade.

- At home, a little over a year ago, the Hong Kong Monetary Authority (**HKMA**) launched the blockchain-based trade finance platform, "eTradeConnect". This platform, developed by a consortium of major banks in Hong Kong, was the first large-scale finance blockchain project in this city[1].

[1] HKMA press release, 'The launch of eTradeConnect and the Collaboration with we.trade', 31 October 2018: https://www.hkma.gov.hk/eng/news-and-media/press-releases/2018/10/20181031-4/

- The "eTradeConnect" project uses blockchain to digitise paper-based documents and automate the trade finance process, to reduce errors and risks of fraud[2].

- Internationally, two weeks ago, UNICEF announced that its Cryptocurrency Fund will place its largest investment of startups in emerging economies – especially companies who use technologies to mitigate hardships on children in the developing world[3].

- The use of cryptocurrency means the transfer of investment funds is almost costless and instantaneous, and provides real-time transparency for UNICEF's donors and supporters.

- In the mainland of China, authorities have established a regulatory regime to foster the healthy development of blockchain technology, including the 'Regulations on the

[2] HKMA, 'Trade Finance': https://www.hkma.gov.hk/eng/key-functions/international-financial-centre/fintech/research-and-applications/trade-finance/
[3] UNICEF press release, 'UNICEF Cryptocurrency Fund announces its largest investment of startups in developing and emerging economies', 19 June 2020: https://www.unicef.org/press-releases/unicef-cryptocurrency-fund-announces-its-largest-investment-startups-developing-and

Management of Blockchain Information Services' (區塊鏈信息服務管理規定) issued by the Cyberspace Administration of China in February 2019.

- As of April 2020, over 700 blockchains were registered in the mainland of China with the Cyberspace Administration of China.

- For example, in Beijing, a smart contract system based on blockchain technology has been launched to enable automatic case filing in the enforcement of mediation agreements. It is believed that the system would make enforcement of mediation more intelligent, transparent and effective.

Privacy Issues of Blockchain

- A blockchain, if designed and built properly, is said to be **tamper-proof** and resistant to modification of the data. There is a high degree of **trust as to the integrity** of the records. A

blockchain is generally highly **transparent** because all transactions are public, traceable and **permanently stored** in the blocks.

- Data in a blockchain is considered **secure and reliable**, without users having to authenticate their identities with other third parties on each occasion.

- However, when a blockchain is used to store personal data, privacy issues may arise.

- For example, the distributed ledger system means that transaction data (possibly some personal data) on the chain could be openly displayed to all participants. This potentially undermines the personal data privacy of the participant.

- In addition, a blockchain is immutable by design. A "block" cannot be deleted or amended even when the data stored in it is obsolete or inaccurate. The retention and continuous

availability of inaccurate or obsolete personal data give rise to compliance difficulties in relation to **data accuracy, data retention and right to erasure**, which are basic principles of personal data protection.

- Furthermore, as a distributed technology, there may **not be a single entity responsible** for the administration of a blockchain. This causes enforcement difficulty in the event of data breach. Individual data subjects may also find it difficult to seek remedy against a violation of privacy right on blockchain.

What steps should be taken

- In a blockchain environment, all participants will likely be deemed as data users, if no single central management of the blockchain can be identified. That means all participants need to carry the burden of complying with data privacy obligations. In other words, all participants of a blockchain

should do their best to protect and respect personal data privacy.

- A few months ago, some people in Hong Kong, we call them doxxers, reportedly uploaded personal data of others to blockchains in order to harass them. This is unlawful and unethical.
- There has yet to be a solution to the privacy issues brought about by the use of blockchains. Compliance with privacy laws alone is not sufficient. The long-term solution therefore lies in **accountability and ethics**, whereby organisations should do what they should do or expected to do in order to be respectful, fair and beneficial to all stakeholders.

- In this regard, conducting the usual **privacy impact assessments and in addition, an ethical data impact assessment** should be a prerequisite for the development and use of blockchains.

- In designing blockchain systems, it is imperative to practise **privacy by design** – that is, to identify and critically evaluate the privacy risks at the design stage of blockchains, and implement measures that will minimise those risks.

- There are seven widely accepted principles for Privacy by Design[4].

  - First, the attention to privacy must be **proactive and preventive**. We must assess, identify, manage and prevent any data protection risks before data breaches occur.

  - Second, it must be **privacy protection by default**. Data protection measures must be integrated into processes and features of the systems. Individuals should not have to take actions for their personal data to be protected, and

[4] Personal Data Protection Commission, Singapore and Privacy Commissioner for Personal Data, Hong Kong, China, 'Guide to Data Protection by Design for ICT Systems', 2019: https://www.pcpd.org.hk//english/resources_centre/publications/files/Guide_to_DPbD4ICTSystems_May2019.pdf

measures to safeguard personal data should be automatically provided as default settings.

- The third principle is **end-to-end security**. Security measures must be considered in the complete Software Development Lifecycle. Good security features and practices can be incorporated at every stage of the Software Development Lifecycle, and from the point that personal data is collected till it is purged from the system. Users should also consider "end-to-end" in terms of how their organisations and vendors work together, as well as how the components of their ICT system – the software, hardware, products, services and platforms – work together. At the same time we should also look out for any vulnerable parts from this "end-to-end" perspective and assess how to strengthen security.

- The fourth principle is **data minimisation**. Do not be tempted to adopt a "collect first and think of what to do

with it later" approach when it comes to personal data. Data minimisation means to strictly collect, store and use personal data that is relevant and necessary for the intended purpose for which data is processed.

- The fifth principle is **user-centric**. Develop and implement ICT systems with individuals in mind – specifically, with the goal of protecting their personal data. Do this through default settings while giving individuals the option to customise settings with informative notices. The interface must be user-friendly, and features such as "just-in-time" notification or layered notices can be applied.

- Sixth is **transparency**. Take an active role in informing individuals on what personal data is collected from them and how it is being used. Also inform users of any third parties processing their personal data. Identify and use the most appropriate means to provide such information,

which could be at different points of interaction with the individual or through "just-in-time" notices.

- And finally, **risk minimisation**. An important aspect of Privacy by Design is to systematically identify and mitigate data protection risk. Risk can be reduced by designing and implementing the right processes and relevant ICT security measures when processing personal data.

- Personal data belongs to individuals. Businesses or organisations utilising personal data cannot conduct their operations merely to meet the minimum regulatory requirements.

- Data ethics can bridge the gap between legal requirements and the stakeholders' expectations, and act as the bedrock for nurturing a new data protection culture in times of technological advance.

Closing

- To conclude, I wish to highlight the importance of two dimensions on which we in Hong Kong have been focussing over the years.

- First, it is about balancing development of ICT against data privacy. Given the nature of new innovations, they are often un-regulated or under-regulated when they first come out. It is important for proponents of such technologies to keep an eye on potential issues of data privacy, however tempting it might be to simply disregard it. Privacy by design is certainly instrumental to achieving privacy protection.

- Second, it is indispensable to build trust between data users and data subjects. If members of the public do not perceive adequate data protection in the innovation, they might defect or refrain from using it altogether.

- Data protection, as expected by all stakeholders, does not only come from effective regulatory frameworks, but is also founded upon trust and confidence among data users and subjects.

- I wish you all a most rewarding interaction and enjoyable competition. Thank you.