INTERNATIONAL FINANCIAL ARCHITECTURE
FOR STABILITY AND DEVELOPMENT/
CRYPTO-ASSETS AND FINTECH

Regulation of Crypto-asset Exchanges and the Necessity of International Cooperation

Naoyuki Iwashita (Kyoto University)

Submitted on March 15, 2019
Revised on March 27, 2019

Abstract

Bitcoin realized anonymous international fund transfers via the Internet. In 2015, FATF proposed to regulate crypto-asset exchanges for AML / CFT, but it is not achieved in most countries yet.
Due to the wide-spread of crypto-asset investment after the sharp rise in the market price in 2017, the situation is changing. Not only from the viewpoint of AML / CFT but also the perspective of protecting individual investors and preventing cybercrime, the public intervention with crypto-asset exchanges has become more necessary. Attention is to be paid that turbulence of crypto-asset prices distorts the resource allocation of semiconductor production, and mining of crypto-assets is wasting global energy. Information sharing and cooperation among international financial authorities are indispensable.

Challenge

Bitcoin gained much attention from the public after a massive price rise in 2017, and crashed in 2018, spreading recognition of crypto-assets as a high-risk speculative investment. Crypto-assets attracted people as a target of a speculative bubble, and market capitalization reached several hundreds of billion dollars at peak time, as many as 3.5 million users[1] participated in this new market in Japan alone.

Bitcoin was designed for electronic cash which is capable of international, anonymous transactions beyond the financial regulation. It was suitable for money laundering and terrorist financing, and it brought confusion to the global financial order.

In 2015, FATF published guidance[3)] which proposed to regulate crypto-asset exchanges thoroughly and keep records of money-to-crypto conversion, and the subsequent transfer of crypto-assets to avoid money laundering and terrorist financing. However, most countries haven't introduced such regulation to crypto-asset exchanges yet.

Japan pioneered the first comprehensive regulations for crypto-assets as a method of payment and for crypto-asset exchanges in April 2017. This Japanese experience may be precious for G20, too. Japanese authorities have learned a lot of technological knowledge and rigid procedure of "Know Your Customer (KYC)" through surveillance of crypto-asset exchanges.

Today, many crypto-asset exchanges have been established. They have two tasks. First is to exchange legal tender currency to crypto-assets, and second is to keep crypto-assets for their customers. Instead of intractable digital signature technology, customers of exchanges can use ordinary ID and

[1] Counting users of crypto-assets is a controversial issue. According to the report of Chainalysis [1)], Bitcoin blockchain consists of 460 million addresses as of December 2018, but only 27 million addresses actually hold Bitcoin, and there is very little information how these addresses link to actual Bitcoin holders. In 2017, Japanese regulation required crypto-asset exchanges in Japan to perform a strict KYC to every customer. Japan Virtual Currency Exchange Association (JVCEA) aggregated numbers of customers reported from all registered exchanges and disclosed that there are 3.5 million actual crypto-asset holders in Japan [2)].

password to authenticate their trade request.

If both sell-side and buy-side investors are customers of the same exchange, they can make the trade of crypto-asset without blockchain. The settlement can be done within the RDB of the exchange. This kind of transaction is called "off-chain" because the transaction is not written on the blockchain, compared to the traditional "on-chain" transactions [Table 1]. Today, 95 % of crypto-asset transactions are said to be off-chain[2].

[Table 1] Pros /Cons of on-chain and off-chain transaction

Type	On-chain Transaction	Off-chain Transaction
In brief	Transaction method that has been used since the dawn of Bitcoin. A digital signature is generated with a secret key managed by the user himself, and a transaction record including his own address is recorded on the blockchain.	Transaction method whose settlement completes within the RDB of a crypto-asset exchange. Users authenticate with ID and password, instead of a secret key.
Who use it?	● Geeks who have been using Bitcoin from its dawn, ● Users who want anonymous transactions, ● Users who remit or pay across borders, ● Inter-exchange transactions, ● Mining companies.	● Individual investors who are laypersons about crypto-asset transactions, ● Customers of crypto-asset exchanges.
Pros	● Transactions recorded on the blockchain are immutable. ● Transactions can be almost anonymous. ● Even if there are troubles in the exchange, the crypto-assets recorded on the blockchain are safe.	● Nontechnical investors can make transactions with simple authentication such as passwords, and their crypto-assets are at no risk of loss or leakage of secret keys.
Cons	● Each user needs to be technologically skilled in managing his secret key of the digital signature securely. ● Loss or unauthorized use of the user's secret key would result in the total loss of his crypto-assets.	● Risk of losing crypto-assets if a cyber-attack damages an exchange.

Due to the soaring market prices of crypto-assets and increasing investment by individual investors, the amount of value retained at exchanges expanded rapidly. In such circumstance, some crypto-asset exchanges were attacked and lost crypto-assets they kept. All exchanges are venture companies, and the level of risk management was not high enough. **Crypto-asset exchanges around the world were targets of cybercrime** [Table 2].

[2] Based on a comment made by Mr. Gary Gensler, 11th chairman of the Commodity Futures Trading Commission at the fourth meeting of "Study Group on the Virtual Currency Exchange Services" held at Financial Services Agency of Japan [4)], https://www.fsa.go.jp/news/30/singi/20180615-2.html (in Japanese)

[Table 2] Major cyber-attack incidents to crypto-asset exchanges

Attacked Exchange	Nationality	Month / Year	Estimated Loss ($ in millions)	Stolen crypto-assets
Mt.GOX(1)	Japan	June, 2011	9	-
Bitfloor	U.S.	September,2012	0.25	24,000 BTC
Mt.GOX(2)	Japan	February, 2014	480	850,000 BTC
Poloniex	U.S.	March, 2014	0.55	-
BitStamp	U.K.	January,2015	5	19,000 BTC
Bitfinex	Hong Kong	August, 2016	66	119,756 BTC
CoinCheck	Japan	January, 2018	530	526,300,010XEM
BitGrail	Italia	February, 2018	170	15 million NANO
Coinrail	Korea	June, 2018	40	NXPS,ATC,NPER
Bithumb	Korea	June, 2018	31	XRP ?
Zaif	Japan	September, 2018	62	BTC,MONA,BCH
Cryptopia	New	January, 2019	3	ETH ?
QuadrigaCX	Canada	January, 2019	137	inaccessible cold wallets

Once an exchange is attacked, its customers would lose their assets. Crypto-asset investment is quite popular among young people, and the number of investors has increased to a level that cannot be ignored. **Not only from the viewpoint of AML / CFT but also the perspective of protecting individual investors from the cyber-attacks, the public intervention with crypto-asset exchanges has become necessary.**

Moreover, the emerging attention to crypto-assets has led monetary authorities of developed and developing countries to **the discussion of central bank digital currency (CDBC)**. Many central banks have launched CBDC research projects, and some of them are actively moving forward to real emission of CDBC. However, CDBC accompanies many challenges both in legal and economic areas [8].

Bitcoin and similar crypto-assets are using PoW. In this method, miners of crypto-asset play an essential role to sustain the security of crypto-asset. Each miner can earn a reward if it searches hash value more quickly than competitors. For this reason, each miner is incentivized to use fast mining machines. As a result, the overall computing capacity increases, and energy consumption increases.

In the early times of Bitcoin history, PoW or "mining Bitcoin" didn't need such strong computational power. With the soaring price of Bitcoin, mining Bitcoin was considered to be a high-profit business, and a dedicated machine for mining was developed. Miners aiming to win the mining competition employed GPU and ASIC. As a result, **excessive capital investment to the mining business has lead distortion of global resource allocation of semiconductor production.** It caused side effects such as **massive electric power consumption and global environmental problems getting worse.**

Proposal

1. AML / CFT of crypto-asset transaction

In 2015, FATF proposed to regulate crypto-asset exchanges from the viewpoint of AML / CFT. Japan introduced registration of crypto-asset exchanges in 2017. The 5th EU Anti-Money Laundering Directive (AMLD 5) requires extends the scope to virtual currency platforms and wallet providers. Member states are obliged to transpose the modified regulations into national law by the latest January 20th, 2020.

G20 countries should comply with FATF guidance on crypto-asset and introduce the regulation to the crypto-asset exchanges, such as a registration system to ensure to perform a KYC of their customers. If needed, government authorities should examine the exchanges to avoid crypto-assets to be used for money laundering and terrorist financing.

2. Protecting individual investors from cybercrime

Crypto-asset exchange provides various functions such as a market provider, a dealer, custody of crypto-assets. As exchanges keep assets of their customers, they should make every effort for managing financial risk.

G20 countries should supervise crypto-asset exchanges to manage their risk appropriately, including cybercrime risk from the viewpoint of investor protection.

Government interventions can be justified to avoid the damage of individual investors of crypto-assets. **These interventions should also be implemented based on international cooperation. Information sharing is also indispensable.**

From this point of view, Japan has already introduced the regulation to crypto-asset exchanges, investing a lot of human resources, conducted on-site inspections. Thanks to these experiences, Japan's FSA has smoothly responded to cyber-attack cases.

3. Energy consumption of mining crypto-assets

The mining crypto-assets wastes enormous energy resources. The higher the prices of crypto-asset rise, the more energy consumed. From the latter half of 2017 to the beginning of 2018, mining business companies competed to manufacture ASICs and GPUs to strengthen mining capacity [5]. This competition significantly distorted the resource allocation of semiconductor production.

Digiconomist.net was the site pointing out this problem very early [6]. According to the estimate of the site, the power used for mining increased from October 2017 and continued to grow until about June 2018 even as the price of crypto-assets collapsed. As a result, it reached about 70 TWh (Tera-Watt Hour) in terms of one year [Chart 1]. This consumption is almost equal to the electricity used by Austria for one year. The energy spent on mining doesn't create anything useful; it is only wasted. The rise in the price of the Bitcoin means that this waste increases. This is one of the severe problems of crypto-assets.

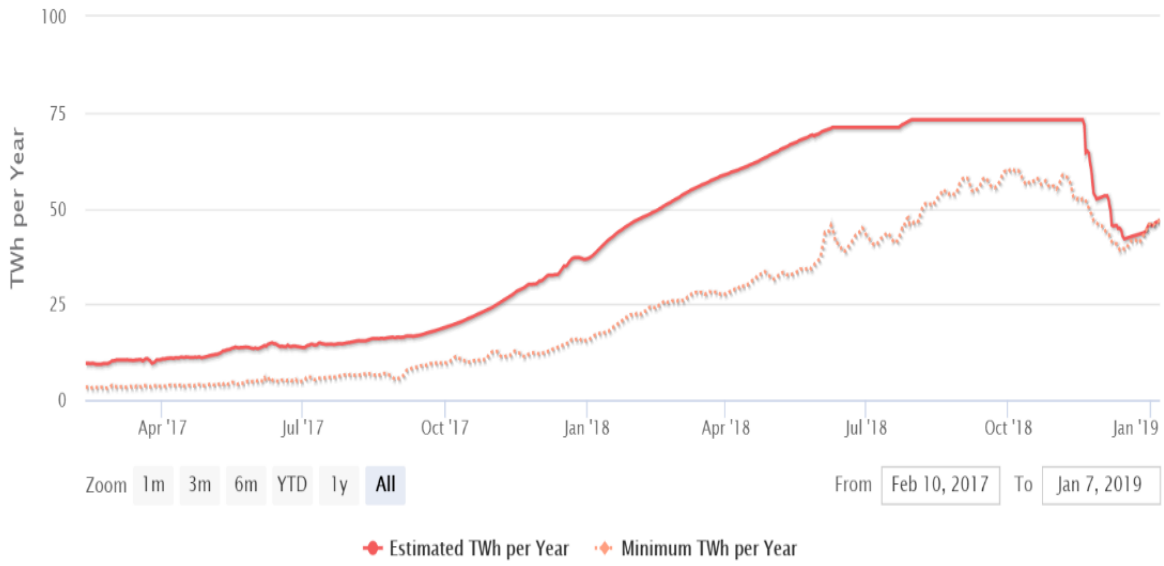
Since the mining machine is a device dedicated to calculating the hash function at high speed, once manufactured, they are not reusable for any other purposes. For this reason, even if the market price collapses in early 2018 and the mining business turned unprofitable, miners cannot stop the working machines. This is why the power consumption did not go down until late 2018.

However, as the miner revenue environment deteriorated further due to the decline in the November 2018 market, mining companies gave up from the mining business one after another. As a result, estimated power consumption has been reduced to about 40 TWh. In the pessimistic scenario assumed in this site one year ago, the power consumption was estimated to exceed 120 TWh at the end of 2018 [Chart 2], but this prediction was not realized and changes to

the desired direction for humanity.

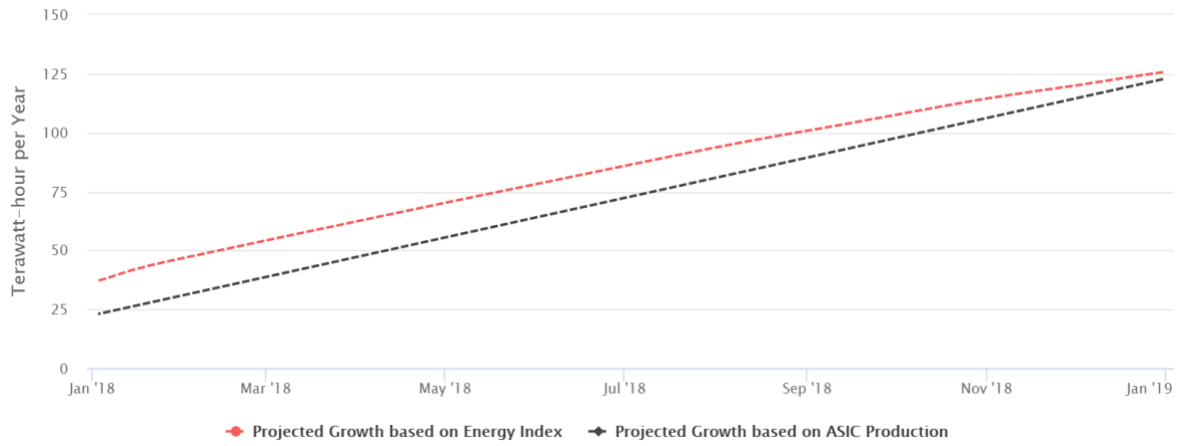
G20 countries should carefully monitor the prices of crypto-assets and mining business if they have an impact on the global environmental problem and lead distortion of global resource allocation.

[Chart 1] Bitcoin Energy Consumption Index



Source: Digiconomist.net

[Chart 2] Estimated future value of electricity consumption (as of the end of 2017)



Source: Digiconomist.net

References

1. Chainalysis: "Mapping the Universe of Bitcoin's 460 Million Addresses," December 19, 2018. https://blog.chainalysis.com/reports/bitcoin-addresses
2. Japan Virtual Currency Exchange Association (JVCEA): " Current status report on virtual currency transaction in Japan," April 10, 2018 (in Japanese). https://www.fsa.go.jp/news/30/singi/20180410-3.pdf
3. Financial Action Task Force: "Guidance for a Risk-based Approach to Virtual Currencies," June 2015. http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf
4. Minutes of the fourth meeting of “Study Group on the Virtual Currency Exchange Services” held at Financial Services Agency of Japan, June 15, 2018. https://www.fsa.go.jp/news/30/singi/20180615-2.html (in Japanese)
5. Bloomberg News, "Nvidia's Crypto Gold Rush Goes Bust in Lackluster Forecast," August 16, 2018. https://www.bloomberg.com/news/articles/2018-08-16/nvidia-gives-disappointing-sales-forecast-on-lower-crypto-demand
6. Alex de Vries, "Bitcoin's Growing Energy Problem," Joule VOLUME 2, ISSUE 5, P801-805, May 16, 2018.
7. Naoyuki Iwashita, "Threats to crypto-assets and countermeasures - Changes of Bitcoin in the process of spread into society - ," Vol.10 No.3 of Journal of Digital Practices, Information Processing Society of Japan (forthcoming).
8. Sergey Drobyshevsky, Elena Sinelnikova, Pavel Trunin,"CBDCs: problems and possible solutions," (forthcoming).