Graduate School of Public Policy
The University of Tokyo

Philippines' Cryptocurrency Governance and Regulation
Learnings from Japan's Experience

Research Paper

John Dexter C. Valderrama
51-188210

Kawai Yoshihiro
Academic Adviser

Table of Contents

I. Introduction

Cryptocurrency[1] has been a hot topic since its emergence in the global market in 2007; and both the investors and the government can no longer ignore the continuing growth of this decentralized finance. This cryptographic token has promised to become a hard and non-manipulatable money; and its advocates see a future wherein it will substitute fiat money and create the first free and hard world currency.

This virtual asset has attracted much attention for its technological implication; however, it has also raised concerns from regulatory authorities about the safety and soundness of its use. Regulators see the fluctuation of its price as very unstable and find it not suitable as a substitute to fiat money. In addition to that, there is a risk that it can be used to launder money, finance terrorism, or commit other finance-related crimes. Foregoing considered, several countries and international organizations have issued policy initiatives to manage the risk associated to it.

In this paper, the issuances of the different organizations with regard to cryptocurrency regulations will be reviewed and will be related to the cryptocurrency governance and regulation of the Philippines. Also, the hacking of Coincheck that happened in Japan in 2018 and the response of the Financial Service Agency (FSA)[2] will be used as a sample case to identify possible regulatory approach to cryptocurrency-related problems. The purpose of this study is to assess the readiness of the Philippines in relation to regulating cryptocurrency-related transactions. Accordingly, this study will attempt to provide recommendations on how the Bangko Sentral ng Pilipinas (BSP) [3] could respond to the rising demand of cryptocurrency-related transaction and the possible increase in the risk exposure to the financial system in the Philippines.

---

1 Cryptocurrency or Virtual Asset is a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes. FATF (2019).

2 The Financial Service Agency is a Japanese government agency and an integrated financial regulator responsible for overseeing banking, securities and exchange, and insurance sectors in order to ensure the stability of the financial system of Japan. www. fsa.go.jp

3 The BSP is the central monetary authority that function and operate as an independent and accountable body corporate in the discharge of its mandated responsibilities concerning money, banking and credit. The New Central Bank Act (R.A. 7653).

II. Understanding Cryptocurrency through Bitcoin

On October 2008, a document by Satoshi Namoto called a whitepaper was published online. In this document, Bitcoin was introduced as a digital currency based on a specific type of distributed ledger that solves the double-spending problem[4] – a potential flaw in a digital cash scheme. The distributed ledger is updated in groups of transactions called blocks, which are chained sequentially by means of cryptography, hence the name blockchain.

In Bitcoin transaction, there are two groups of participants, i.e., miners – acting as the bookkeepers, and the users – who initiates the transaction. The transaction begins when a user executes a transfer of fund. A user's Bitcoin wallet, which is a program used for interacting with the blockchain, creates a transaction message that contains information about the sender, the recipient, and the amount to be sent. This message, together with the secret/private key, are mathematically mixed by the program to produce a digital signature that are then saved in a small file. This file is broadcasted by the wallet for validation to other computers – called nodes. In validating, the sender's account is checked by the nodes to determine whether it meets the requirement to do the transaction, e.g., there is enough balance to do the transfer. Once the transaction is validated, the file is then stored in a Mempool (memory pool), which is a space for valid but unconfirmed transactions. These transactions are then grouped by miners into blocks. Miners will then compete against each other in guessing a specific number or a correct hash (proof-of-work) in order for their respective blocks to be included in the blockchain. The proof-of-work process is similar to digging up rare numbers using complex mathematical computation, hence called mining. Once a miner guessed the correct hash and the block is successfully included in the blockchain, the transactions therein are then considered confirmed.

It can be observed in Bitcoin transactions that there were transfer of funds without intermediaries that manage the transactions. Rather, every computer that participated in the system holds a copy of the ledger and updates it through a clever system of decentralized verification based on cryptographic hash function. Underlying this system

[4] Double-spending is a potential flaw in a digital cash scheme in which the same single digital token can be spent more than once. Unlike physical cash, a digital token consists of a digital file that can be duplicated or falsified. Banking & Insurance Journal SSRN.

are protocols that aim to align the incentives of all participants to enable a reliable payment technology without a central trusted agent. There are three key aspects to these protocols, to wit:

1. There is a cost to update the ledger (blockchain). This cost arises from the complex mathematical computation to update it. The required "proof-of-work", which is a mathematical evidence that a certain amount of computational work has been done, entails costly equipment and electricity consumption.
2. All miners and users verify all ledger updates. These encourages miners to include only valid transactions, considering that mining is expensive. If any participant found that a ledger update includes an invalid transaction, it will be rejected by the network and the miner's rewards will be voided.
3. The protocol specifies rules to achieve a consensus on the order of updates to the ledger. An example of this is the rule that if there are two distinct blockchain with conflicting transaction history, the longest block or the one with the most work put into it will be considered valid. This rule is generally creating an incentive for individual miners to follow the computing majority of all other miner when they implement updates.

With these key aspects, fraudulent entry in cryptocurrency has been made very costly for individual. A successful double-spend attack may require a substantial share of the computing power of the whole mining community (though this may still be possible). Conversely, quoting the original Bitcoin white paper, a cryptocurrency can overcome the double-spending problem in a decentralized way only if "honest nodes control a majority of [computing] power". BIS Annual Report (2018)

III. International Cryptocurrency Regulatory Initiatives and other Issuances

The Blockchain technology and cryptocurrency have offered technological implication and a promising future. However, these technological advancement carries unresolved questions regarding how it will fit to existing international and domestic laws and regulations. Further, there are uncertainties with regard to its safety and soundness of operation. For example, the swing of cryptocurrency value, i.e., the crazy increase in its price followed by a sudden dip, is an obvious indicator of its instability. Aside from that,

there were also reports of hacking of digital wallets and threats of money laundering and terrorist financing. These instability and irregularity posed concern, not just to investors and regulators, but to the public as well. For the crypto industry to be accepted by the public and become part of the people's daily lives, a level of reasonable and responsible regulation should be embraced. Despite being inherently unregulated, it cannot be denied that it is necessary for regulation to establish a safe, fair and reliable market condition in order for the industry to grow.

At the national level, authorities have taken different approaches and types of actions to address cryptocurrency issues. The difference in the regulation reflected the different market development and related legal and regulatory framework in these nations.

The Financial Stability Board (FSB) on May 2019 published a report on the global work in progress about regulatory and supervisory approaches to cryptocurrency. According to the said report, Standard-setting bodies and other international organizations were working on initiatives to address crypto-related issues. The Financial Action Task Force (FATF) adopted changes to its Recommendations to explicitly clarify that the rules also apply to financial activities involving virtual assets. The amended FATF Recommendation 15 requires that virtual asset service providers be regulated for anti-money laundering and combating the financing of terrorism (AML/CFT) purposes, licensed or registered, and subject to effective systems for monitoring or supervision. These initiatives by the international policy maker focused mainly on investor protection, market integrity, anti-money laundering, bank exposure and financial stability monitoring. Despite the number of concerns, the FSB assessed that cryptocurrency do not pose material risks to global financial stability by this time; however, it may raise possible policy issues beyond financial stability.

The Bank for International Settlements (BIS) issued in June 2018 its Annual Economic Report, wherein some issues regarding cryptocurrencies were discussed. In chapter V. Cryptocurrency: Looking Beyond the Hype of the said report, it can be noted that cryptocurrency is said to promise not only a convenient payment means, but also a novel model of trust. This promise of trust towards the system hinges on several assumptions, i.e., that honest miners control the vast majority of computing power, that users verify the history of all transactions, and that the supply of the currency is predetermined by a

protocol. Although achievable, these assumptions raise issues regarding the cryptocurrency's efficiency and a question of whether trust can truly and always be achieved. A major limitation in terms of efficiency of cryptocurrency is the enormous cost of generating decentralized trust. For example, the verification process requires each users and miners to download all transaction history ever made. This transaction history are huge files and continues to increase its size in every transaction added and substantially grow over time. To download updates, sufficient time, high internet speed and right computer hardware, among others, are needed. To maintain the size and transaction time within a manageable level, cryptocurrency have to put limits on the quantity of transaction. Consequently, controlling the quantity of transaction results to another limitation of cryptocurrency, i.e., congestions. With capacity capped, confirmation of transactions may be delayed, and queues may take several hours; thus, produces an interruption in the payment process.

Another issue raised in the report is the fragile foundation of trust in cryptocurrency. Even though there is verification by all the participants, unknown to them that there can be a rival version of the ledger. Since only one of the two updates can ultimately survive, a transaction rollback may happen, and this shows that the finality of payments made in each ledger version are only probabilistic - yet while the probability that a payment is final increases with the number of subsequent ledger updates, it never reaches 100 percent. BIS Annual Report (2018).

IV. Coincheck Heist and Japan's Supervisory Action

Coincheck is a Bitcoin wallet and a cryptocurrency exchange platform based in Tokyo. This wallet enables users to trade cryptocurrency like Bitcoin (BTC), and XEM[5], among others. Like any other exchange, Coincheck enables users to deposit fiat money or tokens and/or trade them for other tokens or sell them. Exchanges like this typically have easy login features and are user friendly, thus make them practical to use for storing cryptocurrency. However, the simplicity and practicality of these platforms comes with weak information security controls and makes it vulnerable for cyberattacks.

[5] XEM is the native currency of the NEM public blockchain. It is used to pay for transactions on this public blockchain in order to incentivize its network of public nodes that process and record transactions for businesses and users there. https://nem.io/xem/

On January 2018, Coincheck reported that it was hacked and had lost more than $500 million worth of XEM. The company did not detail how their system was breached but said that it was not an inside job, but someone had penetrated their user database and hacked their hot wallets that stored the stolen XEM funds. Hot wallets are online and are convenient to use; however, the downside of it is its vulnerability to cyberattacks. To offset this weakness, hot wallets should come with multi-signature authentication, but Coincheck failed to implement the same.

According to reports, the accounts where the stolen tokens ended up were already identified; however, the owners of these accounts are still unknown. The accounts were labeled with tags to indicate that they were stolen and tracking tools were developed to automatically reject transactions related the said funds. The company had admitted that it failed to employ sufficient security measures to store the stolen cryptocurrency and is considering compensating clients if it fails to recover the stolen tokens. Bloomberg (2018).

The FSA took administrative action against Coincheck after the incident. Business improvement order was issued against the latter and directed it to investigate the root cause of the hacking. The incident also prompted FSA to examine other exchange companies for control weaknesses. All major players in Japan's cryptocurrency industry were forced to spend more resources in order to redesign and recheck their respective security system. Stricter regulations were implemented by the FSA in issuing licenses to exchange companies. Preventive measures, e.g., registration, submission of annual reports, and identification of customers, were also enforced to prevent money laundering or terrorist financing. (Nagata, 2019).

A business improvement order by the FSA against Coincheck is necessary to mitigate the damages and prevent further losses. Like any incident of theft, an immediate investigation about the root cause is needed, not just to identify responsible and accountable person, but also to enable formulation of appropriate control measures and strategy to prevent similar incidents from happening in the future. In addition to business improvement, capital restoration plan (CRP) and corporate governance reform (CGR) can also be directed against the company. The CRP can help the company's capital position and identify how

and where the management will source the funds needed to continue operating. The CGR on the other hand can help the company improve the quality of the oversight function of the management. Good governance can give effect to a revision of existing policies and enhancement of compliance with rules and regulations. Further, if effectively implemented, it can redirect the company's future from possible insolvency into a healthy and stable exchange company.

V. Cryptocurrency in the Philippines

The Philippines is increasingly becoming a crypto-friendly country. Policies to protect investors and promote innovation have been issued by both the private and the public sectors. The country also has an active crypto community and a growing sophisticated and knowledgeable users, traders and enthusiasts. Further, there is a fairly sizable population of expats that enables the exchange of financial technologies and improvement in the payment system. (Helms, 2019).

The BSP has issued regulations on Virtual Currency (VC) exchanges engaged in activities that provide facility for the exchange of fiat currency to VC or vice versa. The guideline states that VCs are not legal tender since they are not backed by a central bank nor a particular commodity and are not guaranteed by any particular country. However, since they are used as a conduit to provide certain financial services, e.g., remittances and payment transactions, entities that provide such services using VCs needs to register with the BSP and adopt adequate measures to mitigate and manage risks associated thereto. The BSP Circular No. 944, s. 2017[6] states that it is the policy of the BSP to provide an environment that encourages financial innovation while at the same time ensure that the Philippines shall not be used for money laundering or terrorist financing activities, and that the financial system and financial consumers are adequately protected. It recognizes the potential of VCs to revolutionize delivery of financial services, in view of their ability to provide a faster more economical transfer of funds.

The Securities and Exchange Commission (SEC) has issued on July 2019 its drafted guideline about its rules on digital asset exchange, inviting comments from exchanges,

[6] BSP. Circular No. 994 dated 06 February 2017

broker-dealers, investment houses, investing public, and other interested parties. Rules were set in the guideline on the registration and operation of Digital Asset Exchange (DAE) - an organized marketplace or facility that brings buyers and sellers and executes trades of securities. Also, the said rule sets anti-money laundering/counter financing of terrorism (AML/CFT) safeguards by enjoining the DAEs to develop and maintain a comprehensive AML/CFT framework.

Other than the guideline for virtual currency exchanges of the BSP and the draft rules on digital asset exchange by the SEC, there is also the Digital Asset Token Offering (DATO) framework to protect investors and promote innovation which was adopted by the Cagayan Economic Zone Authority (CEZA) - a government owned and controlled corporation operating in a special economic zone. According to CEZA, the objective is to provide a clear set of rules and guidelines that will boost innovation while also ensuring proper compliance by actors with the hope that these will promote blockchain and crypto adoption by institutional investors and the financial system.

VI. Conclusion

The birth of the Bitcoin has paved way to the emergence of the blockchain technology. Because of its features, the private sectors are exploring its use and potential application to existing industries. Currently, aside from being used as a medium of exchange or an investment, cryptocurrency, more specifically the blockchain technology, is being applied to smart contracts, video games and supply chain, among others.

The innovation of the industries in the private sector has been rapid in the past decades. Although its growth has brought several advantages, it has also produced several issues, e.g., the technology behind cryptocurrency has innovated information technology but also raise regulatory concerns. To mitigate the risks and protect the general public, the public sector needs to innovate too and catch up with the advancements in private sector. Different nations and international institutions have worked on several initiatives to manage the risks and laid down guidelines to enable the public to safely engage into crypto transaction. These initiatives provided mitigating controls against potential harm and promoted the likely benefits of cryptocurrency.

Despite having preventive controls, some adverse events are inevitable. The Coincheck heist that happened in Japan in early 2018 is a typical theft by way of hacking, which is an inherent risk in any digital and online platform. This kind of problem is not caused by a failure of the blockchain and can simply be addressed by strengthening internal controls, especially the information security, e.g., access controls and computer operation. The business improvement order deployed by the FSA against Coincheck as a response to the heist was proper since the latter has committed negligence in not having sufficient system controls to protect their digital wallets. With regards to the lost XEM funds, Coincheck has said that they will compensate their investors, however there were doubts whether they have sufficient capital to do so. In this case, the FSA can direct the company to have a capital build-up plan showing the actions to be undertaken by the management on how they can address the capital problem to compensate the lost funds and continue its operation.

In the case of cryptocurrency in the Philippines, both the public and the private sector have issued policy initiatives to protect investors and promote the growth of the crypto industry in the country. Government agencies have issued guidelines to register cryptocurrency exchanges and directed them to strictly observe AML/CTF policy. The BSP had set high-level supervisory expectations on banks that are engaging in cryptocurrency activities. Banks were warned about the risks and were directed to engage business only with crypto exchanges that are registered and licensed to operate by the BSP. Domestic investors have also organized themselves and collaborated with international investors in Asia to exchange technology in order to develop and provide clear set of rules and guidelines to boost the crypto industry while ensuring proper regulatory compliance within the region. Although, a lot of preparation and research are still needed, the progress from the private sector shows that the Philippine regulators need to be ready to embrace the crypto-industry and the blockchain technology.

The BSP, in pursue of its policy of providing an environment that encourage financial innovation while adhering to AML/CFT framework, has a duty to ensure that the country have a strong prudential supervision and regulatory framework on cryptocurrency. In order to do these, there must be a clear legal framework that would give the BSP with sufficient jurisdiction over all financial activities, including cryptocurrency, and all

entities engaging therein. With a legal basis, the BSP can effectively execute its mandate and can conduct an examination that would allow it to gather a timely and reliable data. With examination, coupled a with regular monitoring, the BSP can (i) determine if there are proper compliance with regulatory requirement (including appropriate and fairness of disclosure of relevant information), (ii) analyze the condition of the crypto exchange industry and (iii) draft policies, or revised existing ones, to further improve its investor and general public's protection.

Learning from the Coincheck heist, the BSP can direct exchanges to redesign and recheck their respective security system against any cyberattacks. Information security policy applied to the banking system can be applied to the cryptocurrency exchanges. Since the banking system's information security features has been tested through time, there can be a reasonable confidence in its ability to defend the exchanges against cyberattacks. The risk of cyberattack cannot be eliminated as it is an inherent risk associated to digital or online platforms; however, it can be mitigated by employing appropriate information security controls. A regular audit by a Certified Information Security Auditor (CISA) may be required from the exchanges to give a reasonable assurance that they have sufficient IT control against cyberattacks.

Liquidity and capital requirements can also be enforced for additional regulatory safety measure. It is fundamental for financial institutions to maintain a level of liquidity in order to effectively function. Cryptocurrency exchanges can be enjoined to maintain enough fiat money so that it can serve investors anytime the latter decides to withdraw its investment. The level of liquidity to be maintained by the exchanges can be the subject of a future studies of the BSP. With regard to capital requirement, to avoid similar capital dilemma experienced by Coincheck, the BSP can have a policy on capital adequacy requirement similar to that followed by banks and other financial institutions (provided it must cover at least the amount in the hot-wallet fund). In this way, exchanges will have buffer to protect its stakeholders against probable losses from undesirable incidents like theft or hacking.

In addition to strong prudential supervision and regulatory framework, the BSP can also study the potential application of the blockchain technology to the financial system. A dedicated group can be created to conduct research on application of the blockchain

technology to the operation of SMEs and the probable use of cryptocurrency for its capital build up, which would give them more option for their funding needs. Further, the BSP can coordinate with economic zones, e.g., CEZA, to encourage financial activities and innovation in the regional areas. These zones can be used as a testing ground for financial activities, including cryptocurrencies, that may be high risk if implemented in a national level. The sharing of technology and experience can be helpful to both the BSP and these economic zones in order to develop and improve cryptocurrency policies and guidelines in the country.

Many crypto enthusiasts may be against government regulating cryptocurrency. However, they need to understand that the purpose of regulating it is not to limit its potentials, instead, to protect the industry by restricting illicit transaction, and to establish a safe environment to do business. With a safe, fair and reliable market condition, more investors, both from domestic and international, will be encouraged to engage in business in the Philippines' crypto industry; thus, consequently making it flourish and eventually contribute to the economic grow of the country.

VII. References

[1] Financial Stability Board (31 May 2019). Crypto-assets: Work underway, regulatory approaches and potential gaps. Retrieved from: https://www.fsb.org/wp-content/uploads/P310519.pdf

[2] Financial Action Task Force (2019). Virtual Assets and Virtual Asset Service Provider. Retrieved from: https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf

[3] Bank of International Settlement (Jun 2018). V. Cryptocurrencies: Looking beyond the Hype. Retrieved from: https://www.bis.org/publ/arpdf/ar2018e5.pdf

[4] Lin, Peter (28 Aug 2019). "Why Regulation is Best Thing for Crypto". Retrieved from: https://cointelegraph.com/news/why-regulation-is-the-best-thing-for-crypto

[5] Bloomberg (2018). "How to Steal $500 Million in Cryptocurrency". Retrieved from: https://fortune.com/2018/01/31/coincheck-hack-how/

[6] Nagata, Kazuaki (27 Jan 2018). "Cryptocurrency Exchange Coincheck loses 58 billion in Hacking Attack". Retrieved from: https://www.japantimes.co.jp/news/2018/01/27/national/cryptocurrency-exchange-coincheck-loses-58-billion-hacking-attack/

[7] Nagata, Kazuaki (11 Jan 2019). " Hit by tougher standards and Falling Prices, Japan's Cryptocurrency Players Face a Pivotal 2019". Retrieved from: https://www.japantimes.co.jp/news/2019/01/11/business/hit-tougher-standards-falling-prices-japans-cryptocurrency-players-face-pivotal-2019/

[8] Wilson, Thomas and Wada, Takahijo (12 Feb 2018). "Coincheck Heist Sheds Light on Japan's Rush to Create Cryptocurrency Rules". Retrieved from: https://www.reuters.com/article/us-japan-cryptocurrency-regulation/coincheck-heist-sheds-light-on-japans-rush-to-create-cryptocurrency-rules

[9] Martin, Alex (29 Jan 2018) "Financial watchdog raps Coincheck over lax security following massive hack". Retrieved from: https://www.japantimes.co.jp/news/2018/01/29/business/fsa-raps-coincheck-massive-theft-customers-cryptocurrency-assets/

[10] Bangko Sentral ng Pilipinas (06 Feb 2017). Circular No. 944, series of 2017. Guidelines for Virtual Currency (VC) Exchanges. Retrieved from: http://www.bsp.gov.ph/downloads/regulations/attachments/2017/c944.pdf

[11] Security and Exchange Commission (2019). Notice: Rules on Digital Assets Exchange. Retrieved from: http://www.sec.gov.ph/wp-content/uploads/2019/07/2019Notice_RulesinDigitalAsset.pdf

[12] Cagayan Economic Zone Authority (2018). Rules on Digital Asset and Token Offerings (Supplemental Rule to the Financial Technology Solutions and Offshore Virtual Currency Business Rules and Regulations of CEZA of 2018). Retrieved from: http://speza.org/assets/dato_rules_and_regulation.pdf

[13] Gogo, Jeffrey (05 Feb 2019). " Philippines Announces New Cryptocurrency Regelation." Retrieved from: https://news.bitcoin.com/philippines-announces-new-cryptoccurency-regulations/

[14] Helms, Kevin (17 Aug 2019). "Philippines Increasingly Crypto Friendly". Retrieved from: https://news.bitcoin.com/philippines-crypto-friendly/