CRYPTO HEIST AND DATA PRIVACY ISSUES: AN ANALYSIS OF THE LEGAL FRAMEWORK IN MALAYSIA[1]

Nur Adlin Hanisah binti Shahul Ikram[*]

Mohd Yazid bin Zul Kepli[**]

Abstract

The occasional meteoric rise of cryptocurrency prices has led to increasing interest to buy crypto. Cryptocurrencies have entered a bull market and reached a new all-time high (ATH) in 2021. This has motivated cybercriminals to target the vulnerabilities of cryptocurrency platforms and digital wallets, resulting in many problems related to data privacy. One of the largest crypto heists took place in August 2021 whereby $600 million worth of crypto was stolen. This article highlights the legal issues and challenges related to the data protection and data security of cryptocurrencies. The analysis includes the standard expected from Malaysia's legal regime on this matter and a comparison with the practice in the European Union and other advanced jurisdictions. This article proposes that the current legal framework must be improved to ensure better consumer and investors protection.

INTRODUCTION

Many data privacy issues are associated with cryptocurrencies and the blockchain technology behind them. The transparent nature of Bitcoin in which all recorded transactions can be inspected by everyone is problematic from the privacy law perspective and is deterring financial institutions and private investors from adopting this decentralized cryptocurrency.[2] In addition, a study by the New York Times explained how enough pseudonymous location data can lead to the identification of an individual user, and with the immutable record of blockchain, can expose a lifetime of transactions linked to that person.[3]

In addition to Bitcoin (BTC), other top cryptocurrencies like Ethereum (ETH), and Ripple (XRP) also face similar problems. As a solution, privacy coins like Monero (XMR), Dash (DASH), and Verge (XVG) were introduced, and these coins offer better privacy. However, due to their nature, privacy coins have their own set of problems, particularly from the anti-money laundering and the countering of terrorism financing perspective. Some

[1] This research is funded by the FRGS Research Grant entitled 'Developing a new legal and regulatory framework for cryptocurrencies businesses in Malaysia (FRGS/1/2019/SSI10/UIAM/02/10)'

[*] Ph.D. candidate at Ahmad Ibrahim Kulliyyah of Laws, International Islamic University Malaysia. Email: adlinhanisah92@gmail.com.

[**] Associate Professor at Ahmad Ibrahim Kulliyyah of Laws, International Islamic University Malaysia. Email: maritime@iium.edu.my.

[2] Liu, J., Li, W., Karame, G.O., Asokan, N., (2018). Toward Fairness of Cryptocurrency Payments. IEEE Secur. Priv. 16 (3), 81–89.

[3] 'The privacy questions raised by blockchain' (Bradley 14 January 2019) via https://www.bradley.com/insights/publications/2019/01/the-privacy-questions-raised-by-blockchain

research suggested that non-privacy coins can be the currency of choice for criminals due to its high level of anonymity and liquidity.[4]

A discussion on privacy issues related to cryptocurrency should start with Bitcoin. Bitcoin, the first and most well-known cryptocurrency was created by the pseudonym Satoshi Nakamoto in 2009, a decade after the Cypherpunks first discussed the idea of achieving privacy and libertarian ideals by using cryptography. During the discussion, one of the group members proposed for an anonymous, decentralize, digital currency that would allow them to transact efficiently as a medium of exchange, free from government control.[5] Satoshi's view is that the creation of Bitcoin can serve as a solution and address some of the issues with the current financial system like a credit-cycle bubble and financial exclusion.[6]

Unfortunately, the presumed privacy and anonymity associated with cryptocurrency like Bitcoin have resulted in cryptocurrency being the a currency of choice for criminals from drug dealers to extortionists.[7] The illusion of privacy is not real. A study done in 2013 revealed that the profile of almost 40% of Bitcoin users can be identified, despite adopting strict measures as recommended by Bitcoin.[8]

As Bitcoin gained popularity, altcoins[9] started to emerge. For example, Litecoin was released via an open-source client on GitHub by Charlie Lee in 2011, XRP was created by Ripple Labs Inc and released in 2012, and Ethereum was invented by programmer Vitalik Buterin in 2013. Along with Bitcoin, Ether and Ripple are the most widely used.[10] To accommodate the growing demand for cryptocurrencies by the public, several exchanges have been created offering trading services and exchanges between cryptocurrencies and fiat money like Binance, Coinbase, Kraken, and many more. Around the same time, privacy coins were introduced. These coins obscure the user's identity despite using a public blockchain network. Privacy coin like Monero employs various techniques to hide information regarding the transactions by using ring signatures, decoy wallet addresses, a one-time, unique wallet address/key, and stealth addresses.

[4] *see* Niranjan Sapkota and Klaus Grobys, 'Asset market equilibria in cryptocurrency markets: Evidence from a study of privacy and non-privacy coins' (2021) Journal of International Financial Markets, Institutions & Money, Vol. 74, 101402

[5] Reuben Grinberg, 'Bitcoin: An Innovative Alternative Digital Currency' (2011) 4 Hastings Science & Technology Law Journal 159, 162.

[6] David Lee Kuo Chuen and Linda Low, *Inclusive Fintech: Blockchain, Cryptocurrency and ICO* (World Scientific Publishing Co Pte Ltd 2018) x.

[7] See Brenig, C., Accorsi, R., Müller, G., 2015, May. Economic Analysis of Cryptocurrency Backed Money Laundering. In ECIS, and Kethineni, S., Cao, Y., 2020. The Rise in Popularity of Cryptocurrency and Associate Criminal Activity. International Criminal Justice Review 30 (3), 325–344.

[8] Androulaki, E., Karame, G.O., Roeschlin, M., Scherer, T. and Capkun, S., 2013, April. Evaluating user privacy in bitcoin. In International Conference on Financial. Cryptography and Data Security (pp. 34-51). Springer, Berlin, Heidelberg.

[9] The term 'Altcoin' is a combination of two words: 'alt' and 'coin' where alt means 'alternative' and coin means 'cryptocurrency'.

[10] 'What Are Cryptocurrencies like Bitcoin, Ethereum and Ripple? - Back to Basics - IMF F&D Magazine' <https://www.imf.org/external/pubs/ft/fandd/2018/06/what-are-cryptocurrencies-like-bitcoin/basics.htm> accessed 15 August 2021.

Individuals holding cryptocurrencies represent several interests, including technology early adopters, privacy and cryptography enthusiasts, government-mistrusting 'gold bugs', criminals, and speculators.[11] Some of the holders use Bitcoin for tax evasion, money laundering, and as a currency for illegal activities like trade in illegal drugs and child pornography.[12]

Lately, cryptocurrency has gained traction from the public as a medium for investment. Cryptocurrencies use blockchain technology to provide secure, cheaper, and faster payment, improve cross-border payments and enhance financial inclusion.[13] It offers the anonymity of cash while also allowing micropayments for long distances.[14] Buying and selling cryptocurrencies become more mainstream when many digital assets exchanges (DAX) are allowed to operate legally in several countries and many major big companies started to accept cryptocurrency for payment like the Hong Kong-based Pavilion Hotels & Resorts, AXA Insurance, Microsoft, Starbucks, Amazon, VISA, PayPal, airBaltic, Sotheby's, Coca Cola, Lot Polish Airlines, Expedia and Lush.[15] Around 18,000 businesses worldwide accepted cryptocurrencies as a medium of payment nowadays.

When Elon Musk co-founder of Tesla bought $1.5 billion of bitcoin and tweeted "You can now buy a Tesla with Bitcoin", the price exploded. The company accepted Bitcoin as payment because it is provided "more flexibility to further diversify and maximize return' on cash.[16] This tweet has encouraged more people to buy Bitcoin and subsequently, Bitcoin has entered a new bull market with the price of most cryptocurrencies skyrocketing and reaching its all-time high (ATH) in the year 2021.

Many scholars claimed that cryptocurrencies are pseudo-anonymous and secured by cryptography. The holders of the currency have two keys; a public key and a private key which are required to complete a transaction.[17] A public key is the address and can be shared with anyone. The private key is like a password to gain access and it should not be disclosed to others.[18]

In general, crypto holders are not easily identifiable but once they post their personal information online like bank account information (for registration in Digital Asset Exchanges),

[11] Grinberg (n 5) 165.
[12] Grinberg (n 5) 161.
[13] Tobias Adrian, 'Digital Technology: How It Could Transform the International Monetary System' (*International Monetary Fund*, 2021) <https://www.imf.org/en/News/Articles/2021/06/30/sp063021-digital-technology-how-it-could-transform-the-international-monetary-system> accessed 7 September 2021. See also 'Cryptoassets as National Currency? A Step Too Far – IMF Blog' <https://blogs.imf.org/2021/07/26/cryptoassets-as-national-currency-a-step-too-far/> accessed 15 August 2021.s
[14] 'Central Bank Monetary Policy in the Age of Cryptocurrencies - IMF F&D Magazine - June 2018 | Volume 55 | Number 2' <https://www.imf.org/external/pubs/ft/fandd/2018/06/central-bank-monetary-policy-and-cryptocurrencies/he.htm> accessed 15 August 2021.
[15] 'Paying with Bitcoin: These Are the Major Companies That Accept Crypto as Payment | Euronews' <https://www.euronews.com/next/2021/08/29/paying-with-cryptocurrencies-these-are-the-major-companies-that-accept-cryptos-as-payment> accessed 5 September 2021.
[16] 'Tesla Buys $1.5 Billion in Bitcoin, Plans to Accept It as Payment' <https://www.cnbc.com/2021/02/08/tesla-buys-1point5-billion-in-bitcoin.html> accessed 7 September 2021.
[17] 'What Are Cryptocurrencies like Bitcoin, Ethereum and Ripple? - Back to Basics - IMF F&D Magazine' (n 8).
[18] Mohammad Karim Ershadul and Abu Bakar Munir, 'Blockchain Technology : An Introduction in Malaysian Legal and Regulatory Landscape [2018] 2 MLJ Xlv' (2018) 2 Malayan Law Journal Articles 1, 5.

it could leave a trace of digital footprint and other people can identify them. Once the data is embedded in the system, there is a risk of violation of the individual's data privacy.[19] It must be remembered that the hackings of cryptocurrency exchanges happen regularly. There is a need to protect the privacy and trust of the stakeholders to avoid the crisis of confidence because the price of cryptocurrencies depends on its network. In the world of cryptocurrencies, privacy and trust remain a pinnacle concern to organizations and users all around.[20]

THE RISKS AND CHALLENGES

Despite the upsides of cryptocurrencies in their current form, in many cases, the risks and costs outweigh potential benefits. The data on the public blockchain is viewable by all the users, leading to both security and privacy issue.[21] Privacy issues can also be seen in the smart contract as stated by Li Peng et al (2020):

> 'Smart contracts inherit some undesirable blockchain properties. The general smart contract requires every miner to execute every step of every smart contract, which needs the code and data of every contract to be public. Private information cannot be preserved during the validation of state transitions via consensus. Therefore, existing smart contract systems thus lack data confidentiality (e.g., auction bids, financial transactions), which bring serious privacy problems.'[22]

Theoretically, peer-to-peer blockchain technology seems to be quite secure and intact but in reality, it can be a haven for hackers and criminals. Technological breakthroughs related to encryption might destabilise the whole cryptocurrency ecosystem as it is mostly passcode-based.

Cryptocurrency exchanges and wallets are becoming a new target for online theft as banking accounts were. With more people buying crypto and the value keep increasing, the privacy threat they pose must be addressed.[23] Cryptocurrencies exchanges and digital wallet vulnerabilities are susceptible to cyber-attacks such as hacking, phishing, ransomware, cryptojacking, 51% attack, and quantum computing. Aside from cyber-attack, cryptocurrencies also have possibilities of a data leak. This paper argues that a comprehensive legal framework is needed to address the privacy concerns related to cryptocurrency. Below are some of the relevant issues that need to be addressed:

1. Hacking

[19] Wie Liang Sim, Hui Na Chua and Mohammad Tahir, 'Blockchain for Identity Management: The Implications to Personal Data Protection' [2019] 2019 IEEE Conference on Application, Information and Network Security, AINS 2019 30, 30.

[20] Sim, Chua and Tahir (n 18) 30.

[21] Ben Hartwig, 'Cybersecurity in Cryptocurrency: Risks to Be Considered - DATAVERSITY' (*Dataversity*, 2021) <https://www.dataversity.net/cybersecurity-in-cryptocurrency-risks-to-be-considered/> accessed 4 September 2021.

[22] Li Peng, Wei Feng, Zheng Yan, Yafeng Li, Xiaokang Zhou, and Shohei Shimizu, 'Privacy preservation in permissionless blockchain: A survey' (2020) Digital Communications and Networks, Vol. 7, 295-307

[23] Benjamin Powers, '"Panda" Malware Targets Crypto Wallets and Users' Discord, Telegram Accounts' (*Coindesk*, 2021) <https://www.coindesk.com/tech/2021/05/10/panda-malware-targets-crypto-wallets-and-users-discord-telegram-accounts/> accessed 13 September 2021.

One of the main challenges in the cyberworld is hacking activities. Theft of personal data and private keys is a major concern in the cryptocurrency world. Some users decided to use cryptocurrency exchanges to save and keep their digital assets, believing that this will offer them better protection. However, the series of hacking involving cryptocurrency exchanges worldwide on regular basis is a testament that no one is safe from the hackers' threat. Baum (2021) highlights as follow:

> 'Centralized exchange hacks have resulted in over 8 billion dollars' worth of tokens being stolen, out of which over 250 million dollars' worth of tokens were stolen in 2019 alone'.[24]

Recently on 10 August 2021, $600 million cryptos were stolen from Poly Network. It is one of the largest crypto heists of all time. The hackers exploited the vulnerabilities in the organization's system to stole the token. The hacker self-proclaimed do-gooder claims that his action is to highlight the vulnerability of Poly Network technology.[25] The hacker is known as "Mr. White Hat" was reportedly offered $500,000 as a bug bounty for returning the stolen money except for $33 million of tether (which was frozen by its issuers).[26]

There was a second major crypto heist within a week after Poly Network was hacked, where a Japanese cryptocurrency exchange was hit by a cyber-attack and $97 million worth of digital coins were stolen. [27] The company announced that some of its online digital wallets have been compromised. Previously, MtGox collapsed after almost half a billion dollars went missing in 2014, and Coincheck loss $530 million in the 2018 attack.[28]

As systems were hacked and private keys stolen, issues related to customers' personal data must also be addressed. Was this information stolen as well? A clearer legal framework regulating the issue of data protection and privacy for customers of cryptocurrency exchanges must be put in place. A comprehensive legal framework should also consider actions that must be put in place to ensure customers and investors are protected in the event of hacking.

2. Phishing

In 2020, Coincheck, a Japanese DAX suffered a data breach in a spear-phishing attack, leading to the leaking of its users' personal data including emails and other personal details. The

[24] Carsten Baum, Bernardo David, and Tore Kasper Frederiksen, 'P2DEX: privacy-preserving decentralized cryptocurrency exchange' (2021) International Conference on Applied Cryptography and Network Security. Springer, Cham.

[25] 'The Saga behind $610 Million Poly Network Cryptocurrency Theft — Everything We Know about the Mysterious Hacker behind the Attack and What Went down over the Last Three Days | Business Insider India' <https://www.businessinsider.in/investment/news/the-tale-of-610-million-stolen-in-cryptocurrencies-who-stole-it-why-and-what-made-them-return-the-money/articleshow/85300739.cms> accessed 13 September 2021.

[26] Ryan Browne, 'Poly Network: Crypto Platform Asks Hacker to Become Security Advisor' (*CNBC*, 2021) <https://www.cnbc.com/2021/08/17/poly-network-cryptocurrency-hack-latest.html> accessed 13 September 2021.

[27] Ryan Browne, 'More than $90 Million in Cryptocurrency Stolen after a Top Japanese Exchange Is Hacked' (*CNBC*, 2021) <https://www.cnbc.com/2021/08/19/liquid-cryptocurrency-exchange-hack.html> accessed 13 September 2021.

[28] 'Hackers Steal Nearly $100m in Japan Crypto Heist - BBC News' (*BBC News*) <https://www.bbc.com/news/business-58277359> accessed 13 September 2021.

unauthorized third party gained access to Coincheck's registration service Onamae.com and fraudulently accessed users' emails to impersonate the cryptocurrency exchange. Around 200 users who replied to the hacker's emails are said to have their data exposed. Although there is no stolen crypto and no fund has been lost, this breach has resulted in the suspension of the DAX remittance service until the investigation is completed.[29] The average cost of a data breach for the user of bitcoin and other cryptocurrencies is difficult to be estimated.[30] In the context of Malaysia, a stronger legal framework to prevent phishing is needed.

3. Ransomware

Access to important commercial and personal data can be denied by ransomware. Ransomware posed significant risks to cryptocurrency exchanges and digital wallets. The hacker can use malware to damage, disrupt, or hack a device. Ransomware is a type of malware, which designed to block the device until the ransom is paid to the hacker.[31] Hacker usually use ransomware so that they can sell back the personal and business data to the original owner of that data or victim.[32]

The University of Edinburg computer scientist stated that Bitcoin wallets are vulnerable to security hacks but it could be improved by providing better protection of its wallets. A team of the University has discovered that by creating a simple piece of malware that can intercept messages sent between wallets and computers, the users' privacy can be breached and is no longer protected. It is then easy to access the wallet and divert the funds to a different account. The researchers suggested a fix for improving the security of that digital wallet system.[33] The same cannot be said for other cryptocurrencies.

Another example is Panda. "Panda" is a new data-stealing malware that targets crypto wallets and users' discord that was discovered by Trend Micro, a cybersecurity software company. Its associated risks are higher than bank robbery because there is no central authority that can reverse the malicious transactions. The Trend Micro researchers proposed to take basic security measures by keeping the software updated and not open any suspicious links on email to avoid malware or other security breaches.[34] Besides "Panda", "ElectroRAT" malware has been targeting crypto wallets for a year. They lure the victim by operating and designed to look

[29] Yogita Khatri, 'Crypto Exchange Coincheck Says It Suffered a Data Breach, Which May Have Exposed Some Users' Personal Information' (*Yahoo Finance*, 2020) <https://finance.yahoo.com/news/crypto-exchange-coincheck-says-suffered-103522960.html> accessed 12 September 2021.

[30] Hartwig (n 20).

[31] See more *"Chapter 9: Scams, Problems and Challenges"* in Mohd Yazid Bin Zul Kepli and Nur Adlin Hanisah Binti Shahul Ikram, *Cryptocurrency and Digital Assets Law in Malaysia* (Thomson Reuters Asia Sdn Bhd (1278218-W) 2020) 381.

[32] Julian Dossett, 'The History of Hacking Ransoms and Cryptocurrency' (2021) <https://www.cnet.com/personal-finance/investing/the-history-of-hacking-ransoms-and-cryptocurrency/> accessed 13 September 2021.

[33] Andriana Gkaniatsou, 'Bitcoin Wallets Vulnerable to Security Hacks | The University of Edinburgh' (2018) <https://www.ed.ac.uk/news/2018/bitcoin-wallets-vulnerable-to-security-hacks> accessed 4 September 2021.

[34] Powers (n 21).

like legitimate entities. They use fake social media and pay influencers to advertise their apps. Once the user downloads their apps, the "ElectroRAT" was also downloaded. [35]

4. Cryptojacking

Cryptocurrencies use a blockchain system that is regularly updated with the new information of all transactions and combined into a new block. It relies on computing power to produce new block and who supply computing power will be rewarded with cryptocurrency. Cyberhackers maliciously benefits from mining cryptocurrency by using other computing powers without incurring a huge cost, which is known as cryptojacking.[36]

Cryptojacking has become popular among cyber hackers because it is easier to deploy and harder to detect as compared to other types of hacking. It uses Javascript malware to maliciously mine the crypto. Cybercriminals hack computers, tablets, mobile devices, or even servers to install software and secretly use computing powers to mine cryptocurrencies or to access cryptocurrency wallets without the owner's consent.[37]

Previously Coinhive was launched in 2017 and become one of the leading sites to provide Javascript code to mine Monero by using visitors' computing power. The Coinhive's code could be secretly injected into other websites. The site shut down in March 2019.[38] In February 2020, The Japan Times reported that the Tokyo High Court overturned the acquittal of a man accused of cryptojacking. A 32-year-old man who is a website designer used Coinhive mining program for his gain without the visitors' knowledge or consent. The program causes a minor impact on his visitors' computers. The court convicts him and fined him ¥100,000.[39]

5. 51% attack

51% attack happens when a single entity or a collaborated group of miners were able to control 51% of the nodes of the system, the blockchain system is no longer decentralised.[40] Recently, Bitcoin SV suffers a 51% attack for the fifth time in August 2021. Previously, Ethereum Classic was also a victim of 51% attack which disrupted more than 10, 000 blocks and lost million dollars in August 2020, while Bitcoin Gold, ZenCash, Verge, and MonaCoin fell victim in 2018.[41] 51% attack is a well-known and dangerous threat from proof-of-work design consensus, which is design for the members of the network to verify and validate coin

[35] Benjamin Powers, 'This Elusive Malware Has Been Targeting Crypto Wallets for a Year' (*Coindesk*, 2021) <https://www.coindesk.com/tech/2021/01/06/this-elusive-malware-has-been-targeting-crypto-wallets-for-a-year/> accessed 13 September 2021.

[36] 'What Is Cryptojacking & How Does It Work? | Kaspersky' <https://www.kaspersky.com/resource-center/definitions/what-is-cryptojacking> accessed 19 September 2021.

[37] Rob Sobers, 'What Is Cryptojacking? Prevention and Detection Tips | Varonis' (*Varonis*, 2021) <https://www.varonis.com/blog/cryptojacking/> accessed 19 September 2021.

[38] 'What Is Cryptojacking & How Does It Work? | Kaspersky' (n 33).

[39] Kyodo, 'Tokyo Court Convicts Man of Using Website to Install Cryptomining Programs on Computers | The Japan Times' *The Japan Times* (2020) <https://www.japantimes.co.jp/news/2020/02/07/national/crime-legal/tokyo-court-cryptojacking/> accessed 19 September 2021.

[40] See more *"Chapter9: Scams, Problems and Challenges"* in Mohd Yazid Bin Zul Kepli and Nur Adlin Hanisah Binti Shahul Ikram (n 28) 374.

[41] Lachlan Keller, 'Bitcoin SV Suffers A New 51% Attack' (2021) <https://forkast.news/headlines/bitcoin-sv-bsv-suffers-new-51-attack/> accessed 11 September 2021. See also Cali Haan, 'Verge, Bitcoin Gold and MonaCoin Hacked' (*Crowdfundinsider,* 2018) <https://www.crowdfundinsider.com/2018/05/133936-verge-bitcoin-gold-and-monacoin-hacked/> accessed 11 September 2021.

transactions to avoid double-spending. The intruder also can control the network e.g. can modify or stop new transactions from being recorded, prevent transactions from being validated or confirmed.[42] There is no new coin created, only manipulation of the intruders by injecting the fraudulent block into a blockchain. Although some may argue the crypto holders' coins are safe because their private key is secure and completely independent from the attack, the real victims are the customers of the exchanges.[43]

6. Data leak

Recently in May 2021, allegedly there was a personal data leak from the Pi Network mobile app. Pi Network is a Vietnamese cryptocurrency mining app. The valuable personal data is stored in the Know Your Customer's vault. An estimated 10,000 Vietnamese citizen identity cards containing home addresses, contact numbers, and email addresses were put on sale. The selling price is $9,000 which must be paid either using Bitcoin or Litecoin. There is speculation that the Pi app is designed to collect the personal data of its users. However, Justin Wu, the Pi Network's marketing and growth team stated that there are no Vietnamese identity cards were held on Pi Network's servers because the app's Know Your Customer (KYC) was carried out by a third party. There was no evidence of a data leak.[44] According to Vo Do Thang, director of cybersecurity firm Athena, ordinary users could not do much to protect their data. The responsibility should be shifted to whoever let the data leaked in the first place.[45]

Cryptocurrencies depend on the technology behind it, either blockchain or other technology. Most cryptocurrencies are safer because of built-in security which is designed to protect them from an untrusted insider.[46] In general, the public and private keys of cryptocurrency are safe and secure but once the holder interacts with crypto exchanges platforms or digital wallets, the security becomes vital. Why cryptocurrency can be hacked although blockchain is immutable? The blockchain itself is immutable. But the programs used may be vulnerable. The hacker can target the vulnerability of the security to access the keys, he can steal the crypto.[47] This might happen due to faulty software updates. Software updates can be vulnerable due to human error or laziness which poses the system to various security issues.[48] For example, the vulnerability in the smart contract used can be seen in the biggest

[42] 'What Is a 51% Attack? | SoFi' (*SoFi*) <https://www.sofi.com/learn/content/51-attack/> accessed 11 September 2021.

[43] 'Here's Why 51% Attacks Don't Affect Price | Bitcoinist.Com' <https://bitcoinist.com/why-51-attacks-dont-affect-price/> accessed 12 September 2021.

[44] Greg Thomson, 'Mobile Crypto "Mining" App Possibly Connected to Personal Data Leak' (*Cointelegraph*, 2021) <https://cointelegraph.com/news/mobile-crypto-mining-app-possibly-connected-to-personal-data-leak> accessed 16 September 2021.

[45] Phuong Son Luu Quy, 'Personal Data Leak Affects Thousands of Vietnamese - VnExpress International' (*VNExpress International*) <https://e.vnexpress.net/news/news/personal-data-leak-affects-thousands-of-vietnamese-4279503.html> accessed 16 September 2021.

[46] 'The Saga behind $610 Million Poly Network Cryptocurrency Theft — Everything We Know about the Mysterious Hacker behind the Attack and What Went down over the Last Three Days | Business Insider India' (n 22).

[47] Hartwig (n 20).

[48] See more on "*Chapter 9: Scams, Problems, and Challenges*" in Mohd Yazid Bin Zul Kepli and Nur Adlin Hanisah Binti Shahul Ikram (n 28) 373–374.a

crypto heist Poly Network. The hacker managed to steal $610 million worth of crypto.[49] Another example, the vulnerability with the Coincheck KYC system; the reason they suffered a data breach in a spear-phishing attack.[50] According to the University of Edinburg computer scientist, as crypto wallets are vulnerable to ransomware, providing better protection of crypto wallets can enhance its vulnerability.[51]

A situation where the stolen assets were returned to the exchanges like the case of Poly Network[52] is an exceptional case. In most cases, the loss of crypto or fund is not recoverable. There was an order for the exchange to halt remittance services until the investigation is completed like Coincheck[53]. There were also cases of exchanges collapsing after hacking e.g. MtGox etc[54]. Once the exchanges or digital wallets got hacked, it will lead to a crisis of confidence from the public. People will no longer trust the platform to trade crypto. Some people may do not enjoy trading crypto like fiat money because security breaches in the world of cryptocurrency are too risky.[55]

In Malaysia, estimated that more than 1 million people owns cryptocurrencies in 2020. This is because trading in crypto with licensed digital assets exchanges since 2019 is legal, and permissible under Shariah (for Muslims). The permissibility is based on the Shariah Advisory Council (SAC)'s ruling, licensed DAX are subjected to a stringent vetting process to protect the stakeholders' interests. The clarity provided in the legal and Shariah aspects is significant to instil confidence among investors in cryptocurrency trading since Malaysia consists of a Muslim majority population. The leading DAX, Luno Malaysia Sdn Bhd the has reached the size of US $1billion in total transactions as of June 2021. Luno also provides digital wallets for its users.

MALAYSIA LEGAL FRAMEWORK ON CRYPTOCURRENCY

The main regulators for cryptocurrency in Malaysia are Securities Commission Malaysia and Bank Negara Malaysia. On 6 December 2018, the Bank Negara Malaysia work together with the Securities Commission to implement the regulatory framework for the digital asset. It is legal to trade cryptocurrencies and licensed cryptocurrency operators are allowed to operate since 2019.[56] Since then, Luno Malaysia, Sinegy, and Tokenize have started to operate as

[49] 'The Saga behind $610 Million Poly Network Cryptocurrency Theft — Everything We Know about the Mysterious Hacker behind the Attack and What Went down over the Last Three Days | Business Insider India' (n 22).

[50] Khatri (n 26).

[51] Gkaniatsou (n 30).

[52] 'The Saga behind $610 Million Poly Network Cryptocurrency Theft — Everything We Know about the Mysterious Hacker behind the Attack and What Went down over the Last Three Days | Business Insider India' (n 22).

[53] Helen Partz, 'Coincheck Halts Crypto Remittance to Investigate Latest Data Breach' (*Cointelegraph*, 2020) <https://cointelegraph.com/news/coincheck-halts-crypto-remittance-to-investigate-latest-data-breach> accessed 12 September 2021.

[54] Khatri (n 26).

[55] 'Central Bank Monetary Policy in the Age of Cryptocurrencies - IMF F&D Magazine - June 2018 | Volume 55 | Number 2' (n 13).

[56] Mohd Yazid Bin Zul Kepli and Nur Adlin Hanisah Binti Shahul Ikram (n 28) 77.

digital asset exchanges (DAX) in Malaysia.[57] Recently in August 2021, the SC has added MX Global as the fourth registered DAX on the list, known as MX exchange.[58] The SC issued 'Guidelines on Digital Assets' which regulates the trading of digital assets in Malaysia to ensure strong investor protection while avoiding unnecessary barriers to innovation.

There are existing laws to charge the cyber hacker for hacking and stealing cryptocurrency like the Malaysian Penal Code and Computer Crimes Act 1997[59], but in reality, the hackers are hard to be traced and difficult to catch. Rather than focusing on deterrence effects, considering the features of the cryptocurrency, privacy, security, and safety must be put in place. The most relevant law to ensure privacy and security is the Personal Data Protection Act 2010 (PDPA). The PDPA could be used as a benchmark for assessing the adequacy of data protection law in Malaysia. There is a need to analyses the applicability of the PDPA to cryptocurrency trading and platform in Malaysia. As an alternative, binding guidelines issued by the SC on data privacy and security for digital asset exchanges can also be useful.

Cryptocurrency and blockchain were not in the mind of the regulator when they draft the PDPA because cryptocurrency and blockchain technology was in the infancy stage during that time. There are ambiguities whether privacy law applies to cryptocurrency and whether cryptocurrency can be identified as personal data. The PDPA applies to the DAX since DAX collects and processes and the data of its users for commercial purpose[60] i.e., in cryptocurrency trading registration. During registration and verification of these DAX, the user needs to use an email address. For example, Luno accounts have three different levels. In the first level, the users require to confirm contact numbers and basic personal details. In the second level, the users need to scan and upload their IC, and selfie photo within 24 hours. In the third level, the users need to give home address, employment status, occupation, and source of income.[61] Later, the user needs to link bank account with the Luno account to make a deposit or withdrawal.[62] This is how personal data is collected by DAX to ensure the service is more seamless. These personal data are not stored together with the crypto block. It is kept in the different software by the exchanges. Even though the crypto block is immutable, and the transaction is irreversible, the data stored by the exchanges can be changed, or erased.

Cryptocurrency legal framework is still loose at the local and international levels. In the aspects of privacy and security, it can be strengthened by identifying the loopholes specifically concerning cybersecurity attacks to protect stakeholders and crypto holders. The loophole in the framework may be detrimental for exchanges and local consumers' protection

[57] 'SC Registers Three Digital Asset Exchange Operators | The Star' <https://www.thestar.com.my/business/business-news/2019/06/04/sc-registers-three-digital-asset-exchange-operators> accessed 16 September 2021.

[58] 'List Of Registered Digital Asset Exchanges' <https://www.sc.com.my/regulation/guidelines/recognizedmarkets/list-of-registered-digital-asset-exchanges> accessed 16 September 2021.

[59] Section 3,4,5,6 of the CCA.

[60] Section 2 of the Personal Data Protection Act 2010.

[61] 'How Do I Verify My Identity with Luno? | Luno' <https://www.luno.com/help/en/articles/11000019400> accessed 27 September 2021.

[62] 'Deposits and Withdrawals | Luno' <https://www.luno.com/help/en/categories/1000126763> accessed 27 September 2021.

in Malaysia as well as a breach of legal prerequisites for international trade and transactions especially in Europe if it involves European citizens and residents. This is due to fact that the new regulation on data protection in Europe has become the benchmark for other countries to follow.

One of the challenges is to ensure the cryptocurrency trading in Malaysia operates up to the standard placed by the international instrument so that cryptocurrency trading in Malaysia can be competitive and operate in international trade and transactions. This improvement will make the personal data of cryptocurrency holders more protected and more secure from crypto hacks, increase public confidence in cryptocurrency, attract the investors around the world and make Malaysia more competitive and attractive.

THE GDPR AND CRYPTOCURRENCY

The General Data Protection Regulation (GDPR) harmonizes data privacy regulations across Europe when it comes into force on 25 May 2018, replacing the 1995 EU Data Protection Directive 95/46/EC. The GDPR governs all entities that collect and process personal data of European Union citizens and residents regardless of geographical location including cryptocurrency exchanges.[63] The GDPR introduces more specific data protection requirements, extraterritorial scope with strict enforcement, and serious non-compliance penalties.

Some scholars propose that blockchain and GDPR are incompatible because of the blockchain features. Some argue that cryptocurrencies like bitcoin only store public and private keys including transactions data. Therefore, it is not considered personal data. Others argue that cryptocurrencies that use public blockchain should be considered as personal data as they are identifiable once linked with other personal data e.g., when the user interacts with the digital wallet provider, exchange platforms, or merchants who accept crypto as payments. It's quite challenging under the existing legal mechanism to identify whether the cryptocurrency itself is considered as containing personal data or not.

The GDPR applies to crypto exchanges and digital wallet providers if they collect and process the personal data of European users. These users share their data like email address, identification card, phone number, and bank account information to use the exchanges or wallet services. The GDPR introduces regulation on automated decision making[64], cross-border data transfer[65], the requirements of data protection officer, a data breach notification[66], and huge fines and penalties. In the context of cryptocurrency, there are some provisions from the GDPR that can be replicated to improve the legal framework regulating data privacy:

1. Automated decision-making and data profiling

Cryptocurrency exchanges may store personal data by automated means. These personal data can be classified based on categories known as data profiling. Data profiling is often used to

[63] Article 2 of the GDPR.
[64] Article 22 of the GDPR.
[65] Article 44 of the GDPR.
[66] Article 33(3) of the GDPR.

predict the behaviour of the person.[67] It also can be used to make an automated decision for the users for targeted advertising or credit scoring. Although there is a lot of benefit from automated decision making, there are potential risks of lack of intuition, transparency, and fairness and it could be dangerous if it is left unregulated. The GDPR introduces the regulation on automated data processing in Article 22. The article made it compulsory to inform the user that the data will be processed for a legitimate purpose and explicit consent is required before proceeding.

In a certain area like criminal law, automated decision-making could pose a severe danger to the data owner as automated decision-making could be used to evaluate a person based on the personal data given.[68] Such input might be incorrect or discriminatory. In the context of cryptocurrency, automated decision-making might be used for profiling, for advertisement purposes.

Under Malaysia privacy law, there is no provision for automated decision-making. Malaysia should consider including this kind of provision to prevent misuse of automated decision-making and data profiling.

2. Cross border transfer

Cryptocurrency is often used for cross-border payment because it is easier and cheaper compared to fiat money. There are risks for cross-border transfer and it will involve more complex regulations other than domestic regulation. For example, Luno users can make a transfer to Australia, Indonesia, Nigeria, Singapore, South Africa, Uganda, United Kingdom, and Europe. Malaysia may not pass the Europe adequacy test for several reasons including no provision on automated decision-making.[69] Cross border transfer out of Malaysia only allowed to such place as specified on the whitelist by the Minister (upon the recommendation of the Commissioner).[70] Malaysia needs to ensure the legal means of data protection for cross-border transfer is adequate and equivalent to the standard set by section 44 of the GDPR.

3. Data protection by design and default

Article 25 of the GDPR requires the data controller to provide technical and organisational measures to uphold data protection principles including minimal use of personal data for a specific purpose. This can be done by adopting the internal policies and implement measures to meet the principles of data protection by design and default including minimising the processing of personal data, improving pseudonymising of personal data, increasing transparency concerning the functions and processing of personal data, enabling the data subject to monitor the data processing, and improving security features.[71]

[67] Mikella Hurley and Julius Adebayo, 'Credit Scoring in The Era of Big Data' (2016) 18 Yale Journal of Law & Technology 148, 151.

[68] Abu Bakar Munir and Siti Hajar Mohd Yasin, *Personal Data Protection in Malaysia: Law and Practice* (Sweet & Maxwell Asia 2010) 218.

[69] Munir and Yasin (n 66) 218.

[70] Section 129(1) of the PDPA

[71] Janet Toh Yoong San, 'The Impact of the GDPR on Malaysian Businesses - Shearn Delamore & Co' (*Shearn Delamore & Co.*, 2019) <http://www.shearndelamore.com/whatnews/the-impact-of-the-gdpr-on-malaysian-businesses/> accessed 28 September 2021.

In Malaysia, cryptocurrency exchanges like Luno and Tokenize seem to have put proper security and privacy measurements in place. According to Aaron Tang, Luno Malaysia Country Manager, the DAX keeps most of the private keys in physical bank vaults inside safety deposit boxes known as "deep freeze" storage to maximise the safety of its customer's cryptocurrencies. Luno also has its internal security measures by providing the hot wallets co-signing service with London-based firm. In addition, Luno has quite a comprehensive security system by guarding all internal security matters by using firewall policies (to allow minimum permission for different applications and roles to interact) which is not connected to the internet. Luno currently stores 300,000 account holders which consist of more than $1 billion of digital assets including Bitcoin, Ethereum, Ripple, and Litecoin. Tokenize, is another example of DAX which has data protection by design and default by its initiative. Hong Qi Yu, the Tokenize CEO stated that the company conducts the vulnerability and penetration test on an annual basis. The test is conducted by a third party. Tokenize has insured up to US$100 million to protect its assets and investment. [72]

The current practice by Luno and Tokenize in providing privacy by design and default is on their initiative. The PDPA does not have a specific provision for data protection by design and default. The PDPA can include this provision to ensure the rest of DAX in Malaysia have data protection by design and default. This can foster the innovation of cryptocurrency trading by mitigating the risk of a crypto heist and by protecting personal data from data breaches or leaks.

4. Notification on data breach

Article 33(3) of the GDPR requires the company to notify its users within 72 hours in the case of a data breach. On the other hand, section 9 of the PDPA stated that in case of a data breach, the company is obliged to "take practical steps to protect the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure". The "practical steps" is open to interpretations and it must be proportionate with the nature of personal data, where it is stored, any security measures incorporated, any measure taken for ensuring the reliability, integrity, and competence of personnel having access to the personal data, and transfer security.[73] To a certain extent, the PDPA provides certain flexibility to the data collector and data processor to take any measures as a part of damage control. However, cryptocurrency exchanges need to consider the features of blockchain that are decentralized and irreversible, and they must protect and secure the data with maximum security. The notification of the user's data breach might alarm the users, but the users can then take proper action once they are notified. In holding cryptocurrency, the holders must keep the private key safe because it is the only way to access their crypto in a cold wallet, etc. Bryan Gour, cyber innovation architect at City National Bank stated that "One of the best things to do to protect yourself is not to keep your key online where it can be hacked…People should use something called a

[72] Afiq Aziz, 'Luno, Tokenize Pledge Tight Security as Hackers Hit Operators Abroad' (*The Malaysian Reserve*, 2021) <https://themalaysianreserve.com/2021/09/08/luno-tokenize-pledge-tight-security-as-hackers-hit-operators-abroad/> accessed 28 September 2021.

[73] Munir and Yasin (n 66) 101.

hardware wallet, an item that looks like a USB and contains their private code like a Ledger or a Trezor.".[74]

5. The Appointment of Data Protection Officer

The Data Protection Officer (DPO) is a designated independent position responsible to educate the company and its employee about data management and protection including data privacy compliance through training and surveillance. The GDPR makes the necessary appointment of DPO for the entity that collects and processes personal data of European, including cryptocurrency exchanges and digital wallets. The DPO must ensure that the company comply with the data protection laws and ensure that security and privacy measures are in place to avoid hefty fine and penalty. There is no provision on the requirement of appointment of DPO under the PDPA. It needs to be included in Malaysian privacy law to ensure all company collecting and processing personal data for commercial purpose has its person in charge to protect and manage data vaults and at the same time educate and monitor the data activities in the company.

CONCLUSION

Security and privacy must be viewed as essential aspects in this digital world. Failure to ensure this will be disastrous. For example, security and privacy in smart city systems were not viewed as an important aspect until the unexpected large-scale— DDoS attacks and ransomware threats occur, leading to mistrust against the Internet of Things (IoT).[75] The same should not be allowed to happen to cryptocurrency exchanges in Malaysia.

Cryptocurrency has its unique features. In Malaysia, it has gained traction from the public since it is legal and permissible to trade cryptocurrency with four licensed DAX. However, to foster the innovation of cryptocurrency in Malaysia and to secure the DAX from cyberattacks, Malaysia needs to put a proper safeguard in place to mitigate the risk of the crypto heist. In addition, measures to protect investors' interest in cases of crypto heist must also exist. Selected provisions from the GDPR can be adopted into the Malaysian PDPA to strengthen the current privacy law. As an alternative, specific guidelines or policies on the protection of data privacy related to cryptocurrency can be introduced. Public trust will improve when proper safety measure is put in place. In addition, these will make the cryptocurrency market in Malaysia more competitive.

This study has highlighted some of the privacy issues and challenges related to cryptocurrencies, privacy coins and non-privacy coins. On one hand, the transparent nature of public blockchain like Bitcoin inevitably lead to various privacy concerns. On the other hand, increasing the privacy aspect of a blockchain by adopting and including certain technological

[74] 'The Cybersecurity Risks of Cryptocurrency' <https://newsroom.cnb.com/en/personal-finance/wealth-protection/cybersecurity-risks-of-cryptocurrency.html> accessed 11 September 2021.

[75] Hadi Habibzadeh, Brian H. Nussbaum, Fazel Anjomshoa, Burak Kantarci, and Tolga Soyata, 'A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities' (2019) Sustainable Cities and Society, Vol. 50, p.101660.

features like ring signatures, decoy wallet addresses, a one-time, unique wallet address/key and stealth addresses will lead to other problems, especially from the anti-money laundering perspective.

This study has also look at the risks and challenges related to cryptocurrency in general, and special focus is occasionally made specifically on privacy issues. The many challenges including hacking, phishing, ransomware, cryptojacking, 51% attack and data leak remains unsolved.

Analysis was also made on the legal and regulatory framework adopted by Malaysia. The analysis suggested that Malaysia framework is generally proactive from the privacy law perspective but many defects remains. This study suggested that the current legal framework can be improved to ensure better consumers and investors protection by adopting selected provisions from the GDPR.