The Money of The Future: A Study of The Legal Challenges Facing Cryptocurrencies

Ahmad Shamsul Abd Aziz [1], Nor Azlina Mohd Noor [2] Omar Farouk Al Mashhour [3]

[1 2] School of Law & Legal and Justice Research Centre, Universiti Utara Malaysia, Sintok, 06010, Kedah, Malaysia
[3]School of Law, Universiti Utara Malaysia, Sintok, 06010, Kedah, Malaysia.
Email: [1] sham@uum.edu.my; [2] norazlyna@uum.edu.my; [3] attorneyomarmash@gmail.com

Abstract

In this article, the authors aim to clarify the ambiguities surrounding important aspects of cryptocurrencies. The use of cryptocurrencies has been increasingly on the rise. Hence, the importance of writing this article which primarily aims to simplify the tricky and complex terms related to this subject. This article has been approached from a conceptual, technical and legal viewpoint. It has been divided into the following three parts: (1) concept of cryptocurrency and its underlying technologies, including all the relevant definitions and meanings; (2) the related mechanism and how blockchain operates in the cryptocurrency world, which requires simplified and easy-to-understand terms and the process that takes place in the so-called blockchain ledger; (3) the legal challenges facing cryptocurrencies. This part pinpoints the most pressing legal issues concerning this virtual form of money. The legal part also aims to highlight the significant results and recommendations for the readers and policymakers to overcome the legal challenges and achieve the ultimate goal of this technology, taking into consideration the risks associated with this digital asset of exchange. In this connection, researchers in different parts of the world have endeavoured to reach and present their findings along with their suggestions and recommendations to improve the current status of this relatively nascent technology.

Keywords: Anonymity, Blockchain, Cryptocurrency, Cybersecurity, Legislation.

1.0 INTRODUCTION

The introduction of cryptocurrency marked a new era in the world's financial system. In the past ten years, cryptocurrency came as an unexpected surprise to the world economy by presenting an unmatched genre of currency, characterised by being fully decentralised and completely different from the other forms of the existing currencies [1]. In 2008, Satoshi Nakamoto, a person or perhaps a group of individuals used this name to present a new method of electronic payment using a peer-to-peer system and a unique decentralised ledger called blockchain to eliminate the need for a third party or an intermediary to handle, authorise and perform transactions. To achieve the ultimate impact of this new technology, the white paper introduced "Bitcoin" which represents the "currency" for circulation and exchange among the users of this digitalized system.

Since its introduction, Bitcoin has gained many supporters, especially after the financial crisis which had a significant impact on people's perception towards banks and governments and caused considerable losses and adversely affected their confidence in regular bank dealing. It has also presented a parallel decentralised financial system and a new business model alongside the blockchain technology being studied by the majority of banks across the globe. Cryptocurrencies are not issued by a centralized body or government, which obviates any chances for manipulation and corruption in the system. However, the protection provided by the government for the official currency is also not provided in case of a legal dispute or fraud. Countries across the globe have reacted differently about cryptocurrencies and their future and the anticipated consequences [2]. Despite their popularity, very few people are sufficiently aware of its mechanism, risks and legal aspect of cryptocurrency [3].

This article seeks to explain the mechanism used for decentralised cryptocurrencies. Understanding how cryptocurrency works would provide a clearer idea for regulators to fully understand cryptocurrencies' eco-system and provide ways to address and interact with such technology rather than ignoring it. The article also identifies the most pressing legal issues facing cryptocurrencies. Providing this essential information aims to give the reader an in-depth understanding of this new and unique virtual currency and its underlying technology. This research uses

"Bitcoin" as the oldest and most popular type of cryptocurrency to explain the commonly adopted mechanism regarding almost all cryptocurrencies [4].

2.0 METHODOLOGY

To achieve the intended objectives, this paper adopts the qualitative approach. The latter approach is suitable for descriptive and exploratory researches [5]. Using the qualitative approach will allow the authors to do an in-depth examination of the existing literature that focused on the mechanism and legal challenges facing cryptocurrencies and analyses these data in order to answer the questions of the research and achieve its objectives [6]. In addition, the study mainly relied on up-to-date secondary data such as journal articles, books, official report, statistics, and many other online sources.

3.0 CRYPTOCURRENCY

The word “cryptocurrency” consists of two parts: "crypto" and "currency" [7]. The word "crypto" reflects the vital role played by cryptography science since its emergence. Nowadays, there are approximately 8,548 cryptocurrencies in the market with approximately $1,589,337,650,660 as a market cap [8]. Cryptocurrencies are intangible and do not exist in reality [9]. Instead, they are virtual and stored on the internet through a unique electronic wallet, accessible only by the owner of the wallet, where the owner concerned has its public and private key [10]. Bitcoin, as the father of all cryptocurrencies, is open source, which means that such a system does not belong to or is controlled by a particular entity or a person [11]. Everyone can own cryptocurrencies and be part of the network. In such open-source software, developers can modify the bitcoin security codes to create their own cryptocurrency projects [12]. Despite having thousands of cryptocurrencies in the market, the majority of cryptocurrencies are based on the same general protocol of bitcoin. Since its emergence, both national and international organisations have issued reports studying cryptocurrencies and their underlying technology. Most of these reports have defined the term “cryptocurrency” and other related terms. The table below provides a few numbers of the definitions mentioned in this regard.

Table 1: Definitions of Cryptocurrency

The International Organizations	**Date**	**The Definition**
The European Parliament	2018	A digital representation of value that (i) is intended to constitute a peer-to-peer (P2P) alternative to government-issued legal tender, (ii) is used as a general-purpose medium of exchange (independent of any central bank), (iii) is secured by a mechanism known as cryptography and (iv) can be converted into legal tender and vice versa” [13].
The International Monetary Fund (IMF)	2016	A digital representation of value, issued by private developers and denominated in their unit of account [14].
Financial Action Task Force (FATF)	2014	A digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value but does not have legal tender status in any jurisdiction. It is not issued nor guaranteed by any jurisdiction and fulfils the above functions only by agreement within the community of users of the virtual currency [15].

Source: Constructed by the authors based on the reports published by the World Bank, IMF and FATF.

As can be seen from the above-mentioned table, different definitions have been provided by international organisations for cryptocurrency. Despite the agreement among them that cryptocurrency represents a "digital representation of value", their definitions still have differences. For instance, the definition provided by the FATF describes cryptocurrency as "a *digital representation of value that does not enjoy a legal currency status under any existing jurisdiction.”* The definitions provided by the international monetary fund, on the other hand, noted that these currencies are "*subset of virtual currencies*", created by "*private developers*" and "*denominated in their account units*." Additionally, the European parliament focused on the mechanism and the convertibility of cryptocurrencies. Hence, it can be seen from the definitions stated that these respective international organisations have failed to provide an

adequate and unified definition for cryptocurrency. Therefore, based on these definitions, it can be seen that the characteristics of cryptocurrency are as stated in figure 1 below:

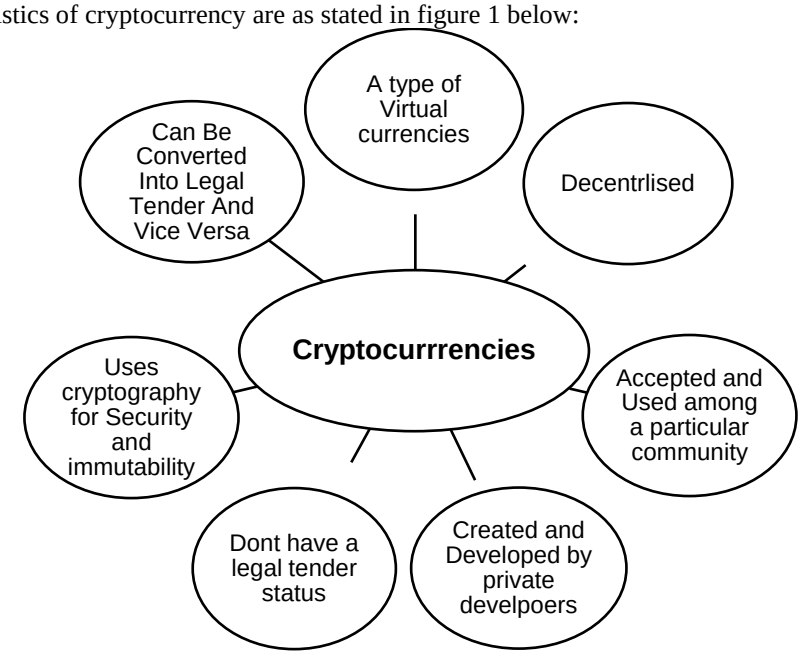

Figure 1. Cryptocurrency's characteristics constructed by the authors based on the definitions provided by the international organisations

The characteristics as showed in Figure (1) represent the results of the explanation provided by international organisations. They referred to them as virtual currencies due to their intangible nature and the absence of any physical existence, and also because of their decentralised nature as they require no third parties to supervise and manage their transactions and the issuance of cryptocurrencies. They are accepted among certain users, who practically trust and use them. They are created by a private developer who introduced cryptocurrencies and identified their features and characteristics. They are not treated as legal tender under any jurisdiction and are used as a cryptography science due to the use of blockchain technology as featured in the characteristics mentioned in the above figure. The researchers define cryptocurrency as "*a convertible virtual currency created and run by a cryptographic decentralised ledger system which is not subject to the control of any central authority. It is used as a medium of exchange that does not have a legal tender status. However, cryptocurrency can be centralised and may have a legal tender status if it were to be legalised under governments' laws and regulations or is created under their authority and control*".

4.0 BLOCKCHAIN

Blockchain represents the basic component of cryptocurrency and the system that has brought them into existence [16]. Due to the unique and undeniably ingenious features of blockchain, it has succeeded to attract and grab the attention of both investors and researchers worldwide. Many reports at both the national and international level have been made. As can be seen from the table below, several definitions have been provided for blockchain. Each one of these definitions has highlighted an important point or aspect.

Table 2.: Definitions of blockchain

The International Organizations	Date	The Definition
European Parliament (Europarl)	2018	"A mechanism that employs an encryption method known as cryptography and uses a set of specific mathematical algorithms to create and verify a continuously growing data structure to which data can only be added and from which existing data cannot be removed that takes the form of a chain of transaction blocks, which functions as a distributed ledger" [17].
The Organization for	2018	"A shared ledger of transactions between parties in a network, not

Economic Co-operation and Development (OECD)		controlled by a single central authority. You can think of a ledger like a record book: it records and stores all transactions between users in chronological order. Instead of one authority controlling this ledger (like a bank), an identical copy of the ledger is held by all users on the network, called nodes" [18].
PricewaterhouseCoopers Advisory (PWC)	2017	"A technology that allows data to be stored and exchanged on a peer-to-peer (P2P) basis. Structurally, blockchain data can be consulted, shared and secured thanks to a consensus-based algorithm. It is used in a decentralized manner and removers the need for intermediaries, or trusted parties" [19].

Source: Constructed by the authors based on the reports published by Europarl, OECD and PWC.

It can be seen that, while the first definition provided by the European parliament has focused mainly on the encryption and security aspects, the second and the third ones have given more attention to the technical part of the blockchain, the decentralisation as well as the peer to peer technology. Therefore, relying on the definitions mentioned above, the researchers define "Blockchain" as "*a unique son of DLT that operates through a shared ledger that saves the data in blocks connected to each other, shaping a chain by relying on the unique technology of cryptography and hashing function. Cryptocurrencies' blockchain operates completely Peer-to-Peer with no need for intermediaries such as central banks and banking institutions."*

Blockchain relies on cryptography science "to encrypt the rule of cryptocurrency within the system itself" [20]. As in traditional currencies, cryptocurrency must ensure that it remains stable, secure and safe from being counterfeited to be widely used. Therefore, to attain this goal, cryptocurrency massively depends on cryptography to protect the system, manage the issuance of the currency, and validate transactions [21]. Blockchain is characterised by being entirely decentralised and transparent [22]. Every transaction added to the blockchain is consistently updated on the blockchain ledger [23]. Not all the information is provided. Most of the stored data, including account names and transactions, are encrypted in the blockchain. Blockchain also transfers from one device to another in a record time against a small fee by a network of nodes or devices in what is called "Mining Process" [24].

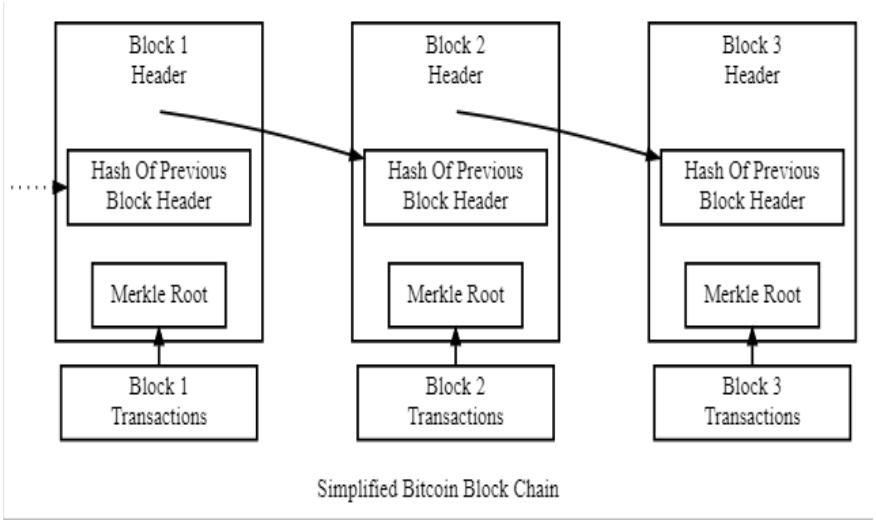

Figure 2: The blocks in the blockchain

As can be seen in [25, Figure. 2] above, all transactions recorded in the blockchain ledger are public. The moment a block of data is attached to the other blocks, its data can never be modified. Any attempts to manipulate them will be readily detected. Thanks to the so-called "cryptographic hash function", any change in any block is likely to prevent the consensus among all the other blocks in the blockchain. The hashing is the process of transforming a standard type of information into an encrypted one. It is explicitly used in its consensus mechanism, and its function is to receive an input and transfer it into a string of numbers.

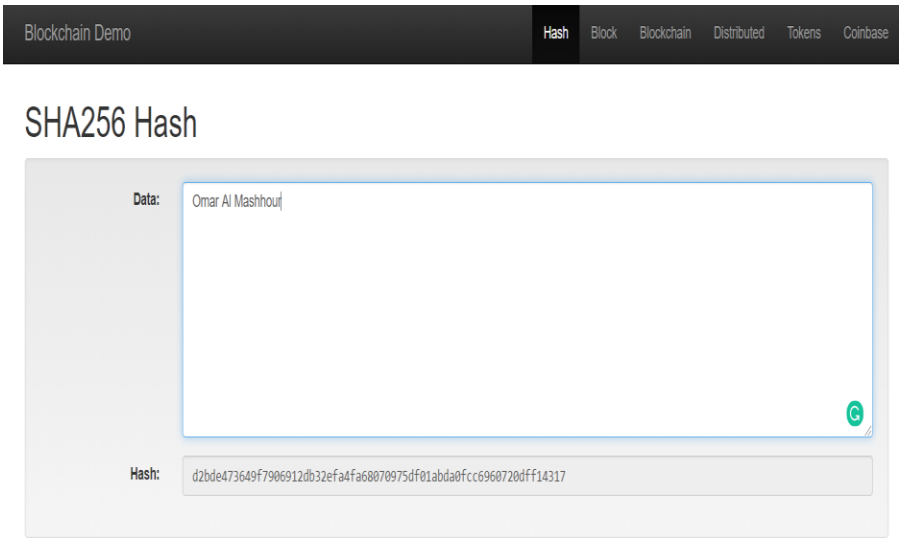

Figure 3: The crypto hash-function

As can be seen in [26, Figure. 3], the name that represents the input has been changed into a string of numbers and letters named "digital fingerprint". In the blockchain, each block receives a unique signature, and every unique signature in a block contributes to the next block's signature. These links between the blocks form a chain of blocks that are impossible to forge. For more details, the reader is referred to [27, Figure. 4].

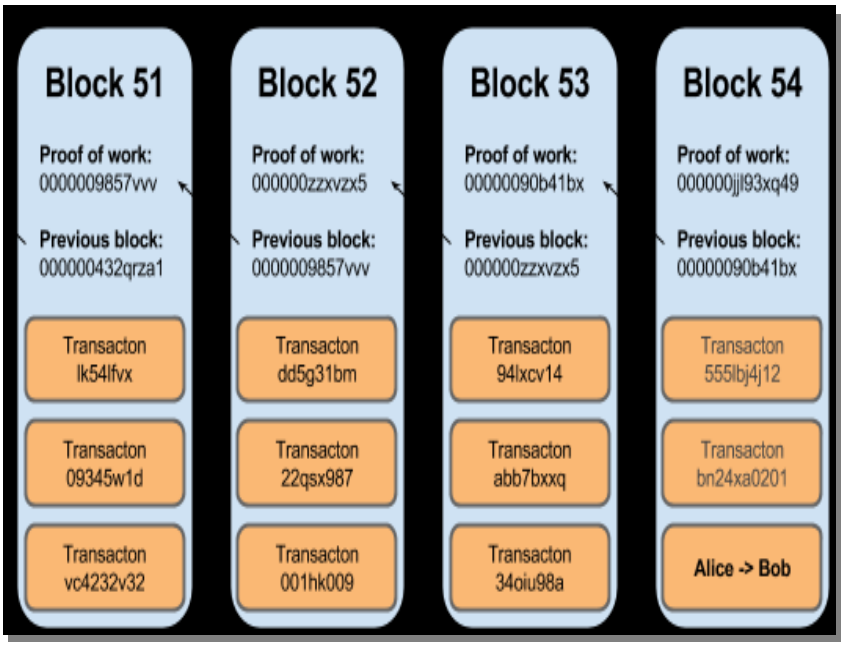

Figure 4: Cryptocurrency's Digital Signature

A small modification made to the data stored inside the block would ultimately lead to a complete change in the signature given to the block, thus making the whole blockchain invalid [28]. If anyone seeks to change a data feed in any block, he/she has to change the signature of the entire subsequent bocks until the end of the chain, which is considered impossible. Each block contains a tree shape of hashed data. For example, if a block contains eight recorded transactions, each one has been hashed separately and given a hash value. Consequently, this hashed value, combined with another value generates a new united hash value. The same process is repeated until one hash-value, referred to as "Merkle root" has been reached.

5.0 MINING PROCESS

Cryptocurrencies are mined through a special program available on the internet. Generally speaking, when a transaction on the "blockchain" is made, it moves to what is called "unverified transaction pool" where all the "unconfirmed transaction" waits to be verified [29]. Those validators on the network are called "miners". Miners are responsible for confirming the transactions and adding them to the blockchain, referred to as "the mining process" [30]. The process of adding a transaction to the blockchain involves solving very complicated mathematical equations that only very high-performance computers can solve. This is called "proof-of-work" [31]. After solving the mathematical issue, the miner will be allocated a reward that will be added to his cryptocurrency wallet. A miner can be one or a group of miners who contribute their computing power to solving this problem [32]. Miners are rewarded with a share of the profits from solving the problem.

6.0 ISSUANCE OF CRYPTOCURRENCY

The power of issuing currency is only limited to the central bank of the country [33]. However, in the case of cryptocurrency, there are two ways of obtaining cryptocurrency. The first is attained by installing a free program, named a mining program that is open to everyone. However, this process requires high specification computers, specially designed to solving such complicated mathematical equations and adding the new transaction to the block. An example of this is the Bitcoin mining application which is available for everyone to download. After succeeding in solving the mathematical puzzle, the program rewards the miner by issuing a cryptocurrency or a portion and adding it to the miner's crypto-wallet [34]. The other way of obtaining cryptocurrency is to have a cryptocurrency wallet through the official website of the cryptocurrency and then obtain cryptocurrencies from a person or somewhere else, such as an authorised exchange.

7.0 THE LIMITATION OF ISSUANCE

Unlike paper money, in which currency issuance is subject to the control of the central bank that has control over the national currency, cryptocurrency issuance is subject to limitation to avoid inflation. The majority of cryptocurrency in the market is limited to a specific number when issuing their currency. Bitcoin, which accounts for around 60% of the cryptocurrency market [35], for instance, has decided to limit the number of bitcoins to 21 million bitcoins [36]. More than 17 million bitcoins have been mined so far. However, bitcoin is not the only cryptocurrency. There are other cryptocurrencies in the market with a limited currency supply, such as Litecoin, which is limited to 84 million [37], XRP, which is limited to almost 100 billion [38] over and above many other types of cryptocurrencies. Meanwhile, some cryptocurrencies have not been decided yet as to the supply limitation, such as Ethereum [39].

8.0 LEGAL ISSUES FACING CRYPTOCURRENCY

8.1 Committing Criminal Activities Using Cryptocurrency

This issue is one of the pressing legal issues facing cryptocurrency to be widely recognized and accepted. The anonymous nature of cryptocurrencies makes them a very attractive tool for criminals to commit some serious criminal activities. Hence, huge attention has been given by governments around the world to regulate cryptocurrencies in order to bring them under monitor and control [40]. Many examples can be provided to demonstrate the illicit use of cryptocurrencies, such as the issue of the dark-web website "Silk Road" [41]. The dark-web online market "Silk Road" offered several illicit goods and items in exchange for cryptocurrencies, especially bitcoin. This dark-website market helped criminals around the world to buy and sell all the illegal items such as weapons and drugs without their identity being exposed using cryptocurrencies as a means of payment. However, in 2013, the United States' government has closed the website and arrested the owner of the website [42].

Silk road represents one example that can be provided for using cryptocurrencies to commit unlawful activities such as money laundering, terrorism financing, tax evasion, bribery and many other illegal activities that can be done, making use of the unique nature of cryptocurrencies such as the decentralization and anonymity. Another example can be provided in the case of *"United States of America v. Michael Mancil Brown" [*43], When the latter committed extortion against the former presidential candidate Mitt Romney. The criminal requested Romney to transfer to him $1 million United States of America dollar (US Dollar)' worth of bitcoin to an account created for this purpose in exchange for not leaking any sensitive information that might affect Romney campaign.

8.2 The Decentralization of Cryptocurrency

Based on the laws in most countries, the currency must be issued by a central body authorized by the law to be fully recognized as a legal tender. This process of printing notes and minting coins by a particular entity will make it difficult to counterfeit the currency [44]. The centralized currency provides the central authorities issuing it the legal power under the law (Central Bank Act) to control the issuance, and circulation of such currency, based on the adopted monetary plan to protect and maintain the economic stability [45]. The legal challenge in the case of cryptocurrency is the decentralized nature, which means that no central authorities control the issuance of cryptocurrencies or monitor the transactions within the eco-system. This issue makes regulating and monitoring efforts quite complicated and tricky [46]. The decentralized nature affects all the aspects of cryptocurrency and related to all the other issues such as tax allocating, volatility, criminal activity, market manipulation and others.

8.3 Lack of Legal Framework

All the currencies worldwide such as US dollar, Euro, Ringgit Malaysia are considered national legal tender currencies. These currencies are regulated and trusted by the people living in the country. On the other hand, cryptocurrencies are not regulated in most countries. The absence of a clear legal framework that addresses all the legal issues could lead to several criminal activities as referred to earlier [47]. Besides, a legal framework for such a novel invention is needed to preserve rights and protects investor and companies alike. Also, the absence of a legal framework will raise several legal points of uncertainly as to legal nature, taxation, inheritance, insolvency, Know Your Customer (KYC) policy, cyber-security, legal dispute, contract, intellectual property and many others. Cybersecurity is also considered one of the issues of paramount importance due to the enormous number of attacks on exchanges causing the loss of millions of dollars [48]. All these issues exist due to the absence of a real legal framework that sets rights and obligations and imposes penalties and punishments. Another problem is the absence of a unified legal approach or structure to regulate cryptocurrencies and their related activities. Each country and international body across the globe has its own opinion about the management, classification or regulation of cryptocurrency. This situation creates a legal gap that allows illegal cross-border activities and facilitates criminals' attempts to evade the laws (such as Tax evasion) by shifting to other jurisdictions where regulation is a bit more lenient [49].

8.4 The Instability in the Value of Virtual Currencies

The volatility issue is also one of the main financial and legal issues facing cryptocurrencies' users because they are intangible and not supported by any tangible assets or precious metals [50]. The main factor determining the value of cryptocurrencies is the supply and demand rule, which reflects the trust that people have in a cryptocurrency [51]. This unstable standard makes it unfavourable for regulators and policymakers since the value can sometimes drop severely due to a statement made by an influential individual or by national or international authorities [52].

Figure 5: The volatility of the bitcoin price in a week

As can be seen in [53, Figure. 5] above, the value of bitcoin can sometimes drop and lose more than a thousand dollars in a week or less. This issue represents a massive risk in the countries that accept or regulate cryptocurrency [54]. It also has a huge influence on the regulators as to whether they accept and regulate cryptocurrencies or not.

8.5 The Probability of Forming Legal Evidence in Court Cases

Transactions in cryptocurrencies are decentralized, anonymous and peer-to-peer, using blockchain technology and its cryptographic hashing to ensure trust in the system. Given their unique nature, it is still vouge and uncertain whether the victim can provide sound evidence that can be recognized or accepted by a court in case of having a legal case like fraud, inheritance, bankruptcy and other criminal activities [55]. Thus, the absence of a legal framework mentioned before represents an essential and pressing issue that regulators must take into account to protect and preserve people's rights from being attacked.

8.6 Digital Inheritance

As stated earlier, the lack of a legal framework that controls cryptocurrency transactions has a huge impact on estate law. With the continuous advancement in the field of technology and the emergence of a new legal field called "digital inheritance", consideration must be given to cryptocurrency as a digital asset that can be inherited since it is an asset having a monetary value [56]. The intangible nature of cryptocurrency makes the inheritance of such asset quite complicated. This issue is considered a matter of serious implications that caused many people to lose their deceased cryptocurrency stored in their crypto-wallet. Several examples can be cited in this regard such as the case of Matthew Moddy, the miner who died in a plane crash leaving cryptocurrency in his crypto wallet, however, the family could not recover this money because they failed to obtain the private key of the to the deceased person's wallet. Therefore, attention must be given to this crucial issue and regulations or guidance must be introduced.

8.7 Cybersecurity

According to a 2020 report made by "Chainalysis," a Blockchain's analytics firm showed that Cryptocurrency scammers raked in $4.3 billion worth of digital money in 2019, more than triple 2018's haul. Cybersecurity has become one of the important issues and a crucial topic that has a huge impact on present-day societies given the need to provide safe and secure access to the internet [57]. Nowadays, it is quite difficult to imagine that people, governments or other entities existing in modern societies can work properly and do their daily tasks without reliance on a computer connected to stable and secure internet. Hence, the internet has become an integral and indispensable part of our life as humans. The unregulated and anonymous nature of cryptocurrencies plays a major role in the huge increase in the number of criminal activities associated with cryptocurrencies [58]. Thus, it can be seen that cryptocurrencies are now considered both a tool and target for criminals to commit a variety of cybercrimes. Since the establishment of cryptocurrency, many cyber-attacks have been carried out against either individuals or exchanges.

Several examples of cybersecurity attacks can be provided, such as the cyber-hacking that occurred to the Japanese based exchange "Mt Gox" which led the company to file for bankruptcy. Around 473 million U.S. dollars' worth of bitcoin (around 850 Bitcoin) was stolen from the company's digital vaults [59]. Another obvious example is what happened to the Hong Kong-based exchange "Bitfinex", where 120 thousand bitcoin (around US $72 million at that time) was stolen by hackers causing the price of bitcoin to plunge just under 23% after the news about this incident had broken out [60]. Moreover, another big cyber-attack occurred against the South Korean exchange Youbit, which closed down and entered into bankruptcy after stealing almost 17% of the exchange bitcoin assets [61].

These are a few examples of serious violations that are still happening around the world. These cyber-attacks can be taken as a reminder about the vulnerabilities of the cryptocurrency platform and the importance of their security level. There are many other types of cybercriminal activities. Phishing is one of the cybercrimes in which criminals use certain tactics to deceive users and entities into believing that they are communicating with genuine and legitimate enterprises. Once the criminal succeeds in deceiving its target, it continues by asking to provide the "Phisher" personal information about the person or the entity such as the log-in information, bank account details (including information about the debit or credit card information), the address, or I.D. number etc. [62]. In the crypto world, the information targeted by the Phisher is the wallet address. An example of phishing can be seen in the statement made on 31st of May 2020 by the Tokyo-based company "Coincheck" which is one of the biggest crypto exchanges in Asia, stating that several phishers have launched attacks against the company's customers. According to the company, several personal information belonging to the customers was leaked out like the name, address, birth dates, and phone numbers

of the customers. However, digital assets have not been stolen or affected.

Malware is also another tool criminal can resort to for committing their criminal activities. Malware refers to malicious software (including viruses, ransomware and spyware etc.) that are designed to damages computers' data or system or to gain unauthorised access to a specific network or device to steal the stored information [63]. On the 11th of July 2020, Cashaa, a Peer-to-Peer trading platform has announced that 336 bitcoins were lost due to an attack launched by hackers. According to Cashaa, the malware was implanted by the hackers into one of the exchange's computers giving the hackers the ability to access it. Another important example of a cyber-crime is the Ponzi scheme, which is a fraudulent investing scam used to deceive people in order to cause them to invest their money by promising these investors a high return at little or zero risks. Ponzi scheme makes its returns for older investors by the money acquired from the new investors. Thus, money is not invested anywhere [64].

9.0 RESULTS

After identifying the meaning of cryptocurrency, blockchain and other components and having explained the mechanism of cryptocurrency, the study has discussed the legal issues facing cryptocurrencies and the need for a workable framework to be adopted and implemented by countries around the world. Criminal activities using cryptocurrencies are one of the challenges that face government agencies and law-enforcement bodies. The unique nature of cryptocurrencies plays a major role in intercepting criminals' attempts to attack, thanks to their unique features such as their anonymous nature and decentralisation. Cybersecurity is a crime that poses a considerable threat to all crypto investors and exchanges alike. The lack of a legal framework that defines cryptocurrency and decides the lawful and unlawful uses of cryptocurrencies is the main weak point in the legislation of most countries. This reflects on all the other legal issues, such as the digital inheritance issue and availability of evidence. In addition, one of the main issues associated with the legal issue and has a great influence on legislators is the volatility that these assets hold and the role of law in affecting its value and stability.

10.0 RECOMMENDATIONS

The study has several recommendations to make for developing better approaches and overcoming these legal challenges. These recommendations can be summed up as follows:

1. Legislators in each country should introduce specific regulations or amend the existing laws and regulations to achieve ultimate benefits and avoid any associated harmful and dangerous risks. The legal movement should also give some attention to the digital inheritance issue and the right of the heirs for these digital assets after the death of the concerned person.
2. Governments should also create a specific body to look into all the issues surrounding cryptocurrencies such as centralised and decentralised exchanges, Initial Coin Offerings (ICOs), and cyber-security issues, in addition to doing further research in the field.
3. Prepare competent judges who are capable of understanding all the related issues surrounding cryptocurrencies and their technologies and ensuring faster and safer judicial processes.
4. The level of awareness about the risks associated with investing or using these assets, such as the volatility and vulnerability of cyber-attacks should be increased.
5. Countries can also start developing their own national cryptocurrencies that are regulated and supervised in an adequate way to maintain and protect these decentralised currencies and ensure the ultimate benefits for their respective countries.
6. More researches should be made on the legal and financial part of cryptocurrency to shed more light on the issue and suggest better solutions.
7. Finally, cryptocurrency is there to stay. It is a technology that was introduced to revolutionise the world we live in, not only financially but also to cover all other sectors.

11.0 CONCLUSION

Cryptocurrencies are among the best discoveries introduced in the last ten years. Their creators have introduced them as a replacement of or a parallel to the present financial system. Despite their enormous benefits and advantages, cryptocurrencies are still viewed as a vogue idea for many people around the world, especially with regard to their

benefits, risks, and mechanism. Cryptocurrencies are considered unique virtual currencies, operating through a decentralised system and using cryptography to provide transparency and protection for the system and manage the generation of money called "blockchain". Blockchain has become a hot topic and a novel technology that succeeded to grab the attention of the majority of governments, banks, corporations around the world.
The cryptocurrency mechanism needs to be explained to the public to provide them with a better understanding of this new technology, its transaction validation, and the mining process so that they are able to add the block to the blockchain and eventually receive the rewards in return. Cryptocurrencies, as a new invention, holds many advantages that might make people's life easier and more secure. However, like any other new inventions, cryptocurrencies are facing a host of legal challenges and obstacles that have to be effectively addressed so that better and safer use of them are attained.

ACKNOWLEDGMENTS

This article is written based on a research that has been carried out under the Fundamental Research Grant Scheme project FRGS/1/2018/SSI10/UUM/03/1 provided by Ministry of Education of Malaysia.

REFERENCES

[1] O. Al Mashhour, A. S. A Aziz and N. A.M Noor, "An Investigation for A Legal Framework Governing Cryptocurrencies Under The Syrian Legislation: An Analytical Study", Journal of Critical Reviews, vol. 7, no. 12, pp. 2761-2767, 2020. Available: http://dx.doi.org/10.31838/jcr.07.13.418.

[2] B. Crowley, "The Legal and Regulatory Issues Surrounding Cryptocurrency", Project Submitted in partial fulfillment of the requirements for Departmental Honors in the Department of Finance, Texas Christian University, 2018.

[3] S. Joshi, N. Khatiwada and J. Giri, "Cryptocurrencies: The Revolution in the World Finance", *NCC Journal*, vol. 3, no. 1, pp. 167-175, 2018. Available: 10.3126/nccj.v3i1.20259 [Accessed 20 February 2021].

[4] A. Narayanan, J. Bonneau, E. Felten, A. Miller and S. Goldfeder, *Bitcoin and cryptocurrency technologies*, 1st ed. Princeton: Princeton University Press, 2016.

[5] E. Babbie, The Practice Of Social Research, 15th ed. United States: Cengage, 2012.

[6] M. Patton, "Qualitative Research", Encyclopedia of Statistics in Behavioral Science, 2005. Available: 10.1002/0470013192.bsa514 [Accessed 20 March 2021].

[7] CryptoDefinitionsStaff, "What Are Cryptocurrencies?", *CryptoDefinitions*, 2020. [Online]. Available: https://cryptodefinitions.com/What-Are-Cryptocurrencies-In-Plain-English/. [Accessed: 20- Feb- 2021].

[8] "All Cryptocurrencies", *CoinMarketCap*. [Online]. Available: https://coinmarketcap.com/all/views/all/. [Accessed: 23- Feb- 2021].

[9] D. Perkins, "Cryptocurrency: The Economics of Money and Selected Policy Issues", Congressional Research Service, Washington, D.C, 2020.

[10] S. Jokić, A. Cvetković, S. Adamović, N. Ristić and P. Spalević, "Comparative analysis of cryptocurrency wallets vs traditional wallets", *Ekonomika*, vol. 65, no. 3, pp. 65-75, 2019. Available: 10.5937/ekonomika1903065j [Accessed 20 February 2021].

[11] T. Brosens, "Why Bitcoin is destined to become a niche asset: A Cryptocurrency Reality Check", Internationale Nederlanden (ING), Amsterdam, 2017.

[12] A. Pîrjan, D. Petroșanu, M. Huth and M. Negoiță, "Research Issues Regarding The Bitcoin And Alternative Coins Digital Currencies", *Journal of Information Systems & Operations Management*, vol. 9, no. 1, p. 3, 2015. Available: http://www.rebe.rau.ro/RePEc/rau/jisomg/SU15/JISOM-SU15-A19.pdf. [Accessed 20 February 2021].

[13] R. Houben and A. Snyers, "Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion", European Parliament, Brussels, 2018.

[14] D. He et al., "Virtual Currencies and Beyond: Initial Considerations", IMF, Washington, D.C., 2016.

[15] The Financial Action Task Force, "Virtual Currencies Key Definitions and Potential AML/CFT Risks", FATF, Paris, 2014.

[16] V. Chhabra, S. Bathla and H. Maheshwari, "An Overview Of Blockchain Technology And Comparison Between Various Cryptocurrencies", *Journal Of Emerging Technologies And Innovative Research*, vol. 6, no. 4, pp. 68-71, 2021. Available: https://www.researchgate.net/publication/332735468_AN_OVERVIEW_OF_BLOCKCHAIN_TECHNOLOGY_AND_COMPARISON_BETWEEN_VARIOUS_CRYPTOCURRENCIES. [Accessed 20 February 2021].

[17] R. Houben and A. Snyers, "Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion", European Parliament, Brussels, 2018.

[18] Organisation for Economic Co-operation and Development, "OECD Blockchain Primer", OECD, Paris, 2018.

[19] PricewaterhouseCoopers Advisory, "Blockchain: a catalyst for new approaches in insurance", PWC, 2017.

[20] A. Narayanan, J. Bonneau, E. Felten, A. Miller and S. Goldfeder, *Bitcoin and cryptocurrency technologies*, 1st ed. Princeton: Princeton University Press, 2016.

[21] S. Seth, "Explaining the Crypto in Cryptocurrency", *Investopedia*. [Online]. Available: https://www.investopedia.com/tech/explaining-crypto-cryptocurrency/. [Accessed: 20- Feb- 2021].

[22] E. Daoud, "Decentralizing Of Transparency: Using Blockchain To Reduce Counterfeiting", *17th International Conference on e-Society 2019*, 2019. Available: 10.33965/es2019_201904l011 [Accessed 20 February 2021].

[23] M. D'Aliessi, "How Does the Blockchain Work?", *Medium*, 2016. [Online]. Available: https://onezero.medium.com/how-does-the-blockchain-work-98c8cd01d2ae. [Accessed: 20- Feb- 2021].

[24] D. Sterry, *Introduction to Bitcoin Mining A Guide For Gamers, Geeks, and Everyone Else*, 1st ed. CoinDL, 2012.

[25] C. O'Neill, "Forks, Merkle Trees, and Bitcoin (Oh My)", Medium, 2018. [Online]. Available: https://medium.com/coinmonks/forks-merkle-trees-and-bitcoin-oh-my-4696079cafaf. [Accessed: 21- Mar- 2021].

[26] A. Brownworth, "Blockchain Demo", Andersbrownworth (SHA256 Hash). [Online]. Available: https://andersbrownworth.com/blockchain/hash. [Accessed: 21- Mar- 2021].

[27] Y. Brikman, "Bitcoin by analogy", Yevgeniy Brikman, 2014. [Online]. Available: https://www.ybrikman.com/writing/2014/04/24/bitcoin-by-analogy/. [Accessed: 21- Mar- 2021].

[28] S. Nadeem, "How Bitcoin mining really works", *freeCodeCamp*, 2018. [Online]. Available: https://www.freecodecamp.org/news/how-bitcoin-mining-really-works-38563ec38c87/. [Accessed: 20- Feb- 2021].

[29] "Unconfirmed Transactions", *Blockchain*. [Online]. Available: https://www.blockchain.com/btc/unconfirmed-transactions. [Accessed: 20- Feb- 2021].

[30] W. Kenton, "Bitcoin Mining Definition", *Investopedia*, 2020. [Online]. Available: https://www.investopedia.com/terms/b/bitcoin-mining.asp. [Accessed: 20- Feb- 2021].

[31] J. Frankenfield, "Proof of Work", *Investopedia*. [Online]. Available: https://www.investopedia.com/terms/p/proof-work.asp. [Accessed: 20- Feb- 2021].

[32] A. Volastro, "CNBC Explains: How to mine bitcoins on your own", *CNBC*, 2014. [Online]. Available: https://www.cnbc.com/2014/01/23/cnbc-explains-how-to-mine-bitcoins-on-your-own.html. [Accessed: 20- Feb- 2021].

[33] "Currency Issuance", *Centralbanksguide*. [Online]. Available: http://www.centralbanksguide.com/Currency+Issuance/. [Accessed: 20- Feb- 2021].

[34] S. Zhu, W. Li, H. Li, C. Hu and Z. Cai, "A survey: Reward distribution mechanisms and withholding attacks in Bitcoin pool mining", *Mathematical Foundations of Computing*, vol. 1, no. 4, pp. 393-414, 2018. Available: 10.3934/mfc.2018020 [Accessed 20 February 2021].

[35] "Global Cryptocurrency Charts", *CoinMarketCap*. [Online]. Available: https://coinmarketcap.com/. [Accessed: 20- Feb- 2021].

[36] A. Meynkhard, "Fair market value of bitcoin: halving effect", *Investment Management and Financial Innovations*, vol. 16, no. 4, pp. 72-85, 2019. Available: 10.21511/imfi.16(4).2019.07 [Accessed 20 February 2021].

[37] G. Mcfarlane, "What Is Litecoin, and How Does It Work?", *Investopedia*, 2019. [Online]. Available: https://www.investopedia.com/articles/investing/040515/what-litecoin-and-how-does-it-work.asp. [Accessed: 20- Feb- 2021].

[38]]A. Levy, "Ripple is sitting on close to $80 billion and could cash out hundreds of millions per month — but it isn't", *CNBC*. [Online]. Available: https://www.cnbc.com/2018/01/16/why-ripple-is-not-cashing-out-its-xrp-holdings.html. [Accessed: 20- Feb- 2021].

[39] "Ethereum price today, ETH marketcap, chart, and info", *CoinMarketCap*. [Online]. Available: https://coinmarketcap.com/currencies/ethereum/. [Accessed: 20- Feb- 2021].

[40] S. Brown, "Cryptocurrency and criminality", *The Police Journal: Theory, Practice and Principles*, vol. 89, no. 4, pp. 327-339, 2016. Available: 10.1177/0032258x16658927 [Accessed 21 February 2021].

[41] N. Christin, "Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace", in *Proceedings of the 22nd international conference on World Wide Web*, 2013, pp. 213-224.

[42] P. Vigna and M. Casey, *The Age Of Cryptocurrency*, 1st ed. Macmillan, 2016.

[43] The case of United States of America V. Michael Mancil Brown (Court of Appeals, Sixth Circuit. 857 F.3d 334 2017).https://www.leagle.com/decision/infco20170515088.

[44] J. Chappelow, "Legal Tender Definition", *Investopedia*. [Online]. Available: https://www.investopedia.com/terms/l/legal-tender.asp. [Accessed: 21- Feb- 2021].

[45] International Monetary Fund, "Monetary Policy and Central Banking", IMF, Washington, D.C., 2019.

[46] P. du Plessis, "The Nature of Decentralized Virtual Currencies: Benefits, Risks and Regulations", Master of International Law and Economics, World Trade Institute., 2014.

[47] Frebowitz, "Cryptocurrency And State Sovereignty", Master's thesis, Naval Postgraduate School, 2018.

[48] T. Massad, "It's Time to Strengthen the Regulation of Crypto-Assets", Brookings Institution, Washington, D.C., 2019.

[49] Frebowitz, "Cryptocurrency And State Sovereignty", Master's thesis, Naval Postgraduate School, 2018.

[50] V. Sapovadia, "Legal Issues in Cryptocurrency", *Handbook of Digital Currency*, pp. 253-266, 2015. Available: 10.1016/b978-0-12-802117-0.00013-8 [Accessed 21 February 2021].

[51] A. Bloomenthal, "What Determines the Price of 1 Bitcoin?", *Investopedia*. [Online]. Available: https://www.investopedia.com/tech/what-determines-value-1-bitcoin/. [Accessed: 21- Feb- 2021].

[52] A. Marshall, "How China Influences Bitcoin Price, Explained", *Cointelegraph*, 2017. [Online]. Available: https://cointelegraph.com/explained/how-china-influences-bitcoin-price-explained. [Accessed: 21- Feb- 2021].

[53] Coinmarketcap, "Bitcoin price today, BTC live marketcap, chart, and info", CoinMarketCap. [Online]. Available: https://coinmarketcap.com/currencies/bitcoin/. [Accessed: 21- Mar- 2021].

[54] A. Guadamuz and C. Marsden, "Blockchains and Bitcoin: Regulatory responses to cryptocurrencies", *First Monday*, vol. 20, no. 12, 2015. Available: 10.5210/fm.v20i12.6198 [Accessed 21 February 2021].

[55] V. Sapovadia, "Legal Issues in Cryptocurrency", *Handbook of Digital Currency*, pp. 253-266, 2015. Available: 10.1016/b978-0-12-802117-0.00013-8 [Accessed 21 February 2021].

[56] O. Al Mashhour and A. Abd Aziz, "The Era of Cryptocurrencies: A Study About the Advantages and Disadvantages", in *The Proceeding of The First Sois Conference on Arts and Humanities (Sicah) 2019 reshaping sustainable development agenda through arts & humanities*, Kedah, 2019, pp. 10-20.

[57] M. O'Connell, L. Arimatsu and E. Wilmshurst, "Cyber Security and International Law", chathamhouse, London, 2021.

[58] J. Bray, "Anonymity, Cybercrime, and the Connection to Cryptocurrency", Master Thesis, Eastern Kentucky University, 2016.

[59] C. Decker and R. Wattenhofer, "Bitcoin Transaction Malleability and MtGox", *Computer Security - ESORICS 2014*, pp. 313-326, 2014. Available: 10.1007/978-3-319-11212-1_18 [Accessed 21 February 2021].

[60] J. Hu, Q. Luo and J. Zhang, "The Fluctuations of Bitcoin Price during the Hacks", *International Journal of Applied Research in Management and Economics*, vol. 3, no. 1, pp. 10-20, 2020. Available: 10.33422/ijarme.v3i1.278 [Accessed 21 February 2021].

[61] J. Detrixhe, "A bitcoin exchange has filed for bankruptcy after latest hack", *Quartz*, 2017. [Online]. Available: https://qz.com/1160573/bitcoin-exchange-youbit-files-for-bankruptcy-in-south-korea-after-latest-hack/. [Accessed: 21- Feb- 2021].

[62] M. Maras, *Computer Forensics: Cybercriminals, Laws, and Evidence*, 2nd ed. Massachusetts: Jones & Bartlett Learning, 2014.

[63] S. Thampi, B. Bhargava and P. Atrey, "Managing Trust in Cyberspace", in *A Comparison of Three Sophisticated Cyber Weapons*, 1st ed., M. Vinay and M. Balakrishnan, Ed. London: Chapman and Hall, 2021, p. 387.

[64] M. Maras, *Computer Forensics: Cybercriminals, Laws, and Evidence*, 2nd ed. Massachusetts: Jones & Bartlett Learning, 2014.