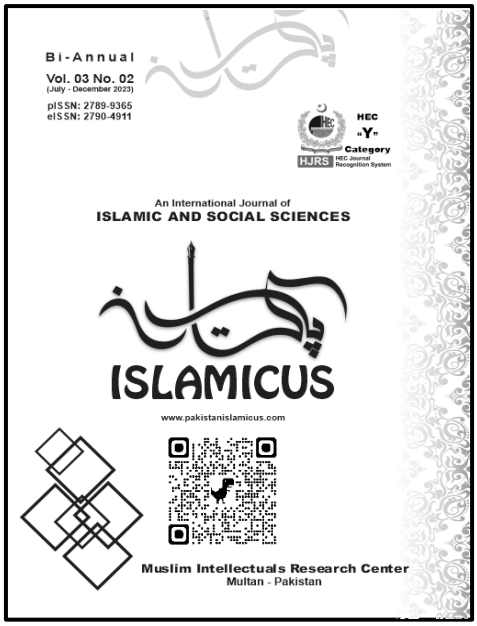
Pakistan Islamicus
An International Journal of Islamic and Social Sciences
(Bi-Annual)
Trilingual: Urdu, Arabic, and English
pISSN: 2789-9365 eISSN: 2790-4911
https://pakistanislamicus.com/index.php/home
Published by:
Muslim Intellectuals Research Center
Multan-Pakistan
website: www.mircpk.net



TOPIC

THE OBSTACLES IN REGULATING CRYPTOCURRENCIES/BITCOIN

AUTHORS

Syed Saqlain Ul Hassan
Faculty of Law,
University of Sialkot, Punjab, Pakistan.
syedsaqlain.hassan@uskt.edu.pk

Saima Sajid
Department of Economics,
GC Women University Sialkot, Punjab, Pakistan.
saima.sajid@gcwus.edu.pk

Sidra Kanwel
Faculty of Law,
University of Sialkot, Punjab, Pakistan.
sidra.kanwel@uskt.edu.pk

How to Cite

Hassan, Syed Saqlain Ul, Saima Sajid, and Sidra Kanwel. 2023.

"THE OBSTACLES IN REGULATING CRYPTOCURRENCIES/BITCOIN".

PAKISTAN ISLAMICUS (An International Journal of Islamic & Social Sciences)

3 (2): 288-298.

Retrieved from:

https://pakistanislamicus.com/index.php/home/article/view/65.

THE OBSTACLES IN REGULATING CRYPTOCURRENCIES/BITCOIN

Syed Saqlain Ul Hassan
Faculty of Law, University of Sialkot, Punjab, Pakistan.
syedsaqlain.hassan@uskt.edu.pk

Saima Sajid
Department of Economics, GC Women University Sialkot, Punjab, Pakistan.
saima.sajid@gcwus.edu.pk

Sidra Kanwel
Faculty of Law, University of Sialkot, Punjab, Pakistan.
sidra.kanwel@uskt.edu.pk

Abstract

This study focuses on exploring the potential of blockchain-based financial applications and the cutting-edge technology "Blockchain"/Bitcoin. The major goal was to describe how blockchain may transform the financial sector. The study covered several intriguing blockchain-related financial applications that may offer varied advantages. The study also clarified the difficulties in implementing blockchains for financial markets.

Keywords: Blockchain, Bitcoin, Cryptocurrencies, Obstacles, Regulations.

Introduction

A cryptocurrency is essentially a form of digital/virtual money that utilizes cryptography (encryption) to ensure that payments are securely sent and received. Examples of cryptocurrencies are Bitcoin, Ethereum, Ripple, and Litecoin, to name a few. Cryptocurrency is not tangible like the banknotes and coins that we are familiar with but rather it exists only electronically on the internet, heavily reliant on a peer-to-peer network of thousands, if not millions, of computers worldwide. As such, and unlike traditional currencies, cryptocurrencies do not have a central issuing authority or regulatory body. Transactions are validated by a network of computers around the world using blockchain technology. Although it is intangible, cryptocurrency has a stored value and can be converted to real money. All that is required is a "*wallet*" to store the cryptocurrency and another party (usually a cryptocurrency exchange) who is willing to exchange the cryptocurrency with real money. (Griffith, T., & Clancey-Shang, D. 2023).

Blockchain Technology

To understand the obstacles in regulating cryptocurrencies, it is imperative that one firstly has a comprehensive understanding of the underlying technology that supports them i.e. the

Blockchain. This is crucial because the advantages associated with Blockchain technology are also the very same reasons why it is extremely difficult to regulate cryptocurrencies that are reliant on that technology. To put it simply, blockchain is essentially a decentralized giant public ledger that is accessible to authorized computers worldwide. It is a form of an electronic database that records every transaction that has taken place where the data is stored in blocks. All these blocks of data are linked/chained together by a cryptographic signature – hence the name "*Blockchain*". (Hooper, A., & Holtbrügge, D. 2020).

The effect of this technology is that there is no longer a need for a centralized regulatory authority (for example, a bank) to oversee the Blockchain and validate the transactions that are taking place. The nature of Blockchain technology, which relies on peer-to-peer networks, is also such that since all the transaction data are chained together, it is practically impossible to hack, forge, or otherwise alter the data within the Blockchain as any slight change to any part of the Blockchain will result in an error on the entire network. As such, it is extremely difficult for an individual to change a transaction within the Blockchain without any of the thousands (if not millions) of the other network users noticing. Therefore, cryptocurrencies work based on trust – not trust in a central regulatory authority like conventional legal tender, but trust in the countless number of users who are within the Blockchain. (Baker, et a, 2023).

Advantages of Cryptocurrencies

1. Decentralization

As explained by '*Satoshi Nakamoto*', the developer of Bitcoin in the groundbreaking paper "*Bitcoin: A Peer-to-Peer Electronic Cash System*" the main aim of cryptocurrencies in general (and Bitcoin in particular), is to allow online payments to be sent directly from one party to another without the need of going through an intermediary/financial institution and at the same time to solve the problem of double-spending (i.e. where digital cash can be spent more than once after having been duplicated or falsified). Nakamoto argues that a financial system that is based on trust in economic agents (i.e. banks) is extremely risky and the way forward is to create an electronic payment "*based on cryptographic proof instead of trust*" which is more secure, (Ozili, P. K. 2022).

By harnessing Blockchain technology, cryptocurrencies have rid themselves of the need for an intermediary such as a bank to oversee and regulate the transactions that are taking place. This can be contrasted with traditional fiat money/legal tender i.e. banknotes and coins whose value is usually backed by the central bank of a country. Cryptocurrencies, on the other hand, are backed by countless computers and users around the world who are constantly maintaining,

updating, and validating the Blockchain to ensure the legitimacy of all transactions that are occurring. The elimination of an intermediary to verify transactions also meant an increase in the speed at which cryptocurrencies can be transacted, unlike the case involving traditional legal tender whereby time-consuming verification by a bank is a pre-requisite before monies can be transferred and received. (Manavi, et al. 2020)

In addition, decentralization would also mean that the risk of theft hacking, or fraud has been significantly reduced as transactions are now being validated and approved by a community of users as opposed to the traditional currency which is heavily reliant on a single authority i.e. the bank which is easily exposed to theft and fraud. In short, no one individual or organization is in charge of the Blockchain to make it susceptible to theft and fraud. At the same time, the problem of double spending is also solved as each transaction on the Blockchain will be validated by other authorized users on the network to ensure that no one is cheating by spending the cryptocurrency twice. (Aspris, A., Foley, S., Svec, J., & Wang, L. 2021)

2. Low Cost

The decentralization nature of cryptocurrencies would be attractive to businesses, in particular those that are involved in cross-border trade, as payments can be made and received almost instantaneously using the internet without the need to go through a bank which might take a few days to clear the payments. This in turn would lower transaction costs and encourage cross-border commerce – a boost to the country's economy. (Hashemi Joo, M., Nishikawa, Y., & Dandapani, K. 2020).

3. **Security**

As mentioned earlier, the Blockchain is a public ledger (or perhaps it can be best described as a public historical document) that records the entire history of the transactions that have taken place. In the context of cryptocurrency, this would mean that every single transaction that has taken place in respect of a particular cryptocurrency e.g. Bitcoin is recorded in the Blockchain. All transactions involving cryptocurrency are secured by cryptography and validated by the Blockchain, which is kept and maintained by countless computers worldwide. Owners of cryptocurrency conduct transactions using what is known as a private key and a public key. (Ghosh, A., Gupta, S., Dua, A., & Kumar, N. 2020).

A private key consists of alphanumerical characters that give a person access and control over his/her cryptocurrency and are only visible to the owner. It allows the owner to "*sign*" (via a digital signature) the cryptocurrency that is being sent to another person. A public key, on the other hand, is derived from the private key and allows other users of the Blockchain to verify the transaction that is taking place and to ensure that the owner has ownership over the

cryptocurrency that he/she is transacting. The Blockchain, therefore, tracks and records all cryptocurrency transactions that are taking place in real-time. The consequence of this is that whenever a cryptocurrency is transacted, it will result in a change to an individual block within the Blockchain, and this, in turn, would mean that the entire distributed ledger is updated and synced in real-time across a multitude of computers worldwide. (Li, et, al 2020).

The fact that any changes to the Blockchain are immediately broadcasted to all users within the global peer-to-peer network makes it difficult for an individual to alter/hack the database and perpetrate theft. An individual would theoretically have to hack every computer (or "*node*") in the network to alter the Blockchain sufficiently to allow him/her to steal cryptocurrencies such as Bitcoin and Ethereum. As such and in comparison, with conventional money which is easily susceptible to theft and hacking of accounts, cryptocurrency is a relatively more secure alternative that is tamper-proof. (Patil, P., Sangeetha, M., & Bhaskar, V. 2021).

4. Access

All that a person needs to transact in cryptocurrency is access to the internet and a suitable device. In this globalized world where more and more people have internet access and the proliferation of mobile phones (particularly smartphones) is rapidly increasing, cryptocurrency is a viable alternative to those who do not have access to traditional exchanges such as a bank. Gone are the days when an individual would have to rely on banks to effect the transfer of their money as all they need now is a mobile device connected to the internet for them to send and receive funds. This is an attractive option, particularly in particular to poor countries where access to banks is limited. An example of this is Kenya, where a recent survey by Citi shows that one in three Kenyans now own a Bitcoin Wallet. (Kumar, et, al. 2021)

5. Anonymity

Every cryptocurrency user is identified not by their real name or address or any other personal details, but rather by a pseudonym that is linked to their cryptocurrency wallet. Therefore, transactions are conducted securely and this significantly reduces the risk of identity theft and fraud (in particular, phishing) that is so prevalent among traditional methods of payment specifically using credit cards. However, it must be stressed that the anonymity accorded by cryptocurrency is a double-edged sword. For reasons that will be discussed further below, the element of anonymity is also one of the main reasons why it has been argued that regulatory control should be exercised over cryptocurrencies. (Peng, et al. 2021)

The Need to Regulate Cryptocurrencies

1. Consumer Protection

Protecting consumers against fraud is perhaps the main reason why some form of oversight should be exercised over cryptocurrencies, more so if we take into account the highly speculative nature of cryptocurrencies and the anonymous identity of the users behind them. The former chair of the United States Federal Reserve, Janet Yellen once described cryptocurrency as "*a highly speculative asset*" because "*it is not a stable source of value, and it doesn't constitute legal tender*" and it is hard to disagree with her statement. Cryptocurrencies such as Bitcoin are essentially generated out of thin air after "*miners*" successfully solve complex mathematical problems and their decentralized nature means that cryptocurrencies are maintained by the Blockchain and not governed by any central bank or government, unlike the situation with traditional legal tender. (Garcia-Teruel, R. M. 2020)

Unlike conventional legal tender, cryptocurrencies are not affected by interest rates, inflation, monetary policy, political stability, and other types of factors that would have a bearing on the value of traditional currency. This is the main reason why cryptocurrency is such a highly speculative asset. Take Bitcoin for example. When it was first launched in 2010, its value was a meager USD0.07 but it shot up exponentially to more than USD17,000.00 in December 2018. At the time of writing (early November 2018), the price of Bitcoin currently stands at approximately USD6,000.00. (Schaupp, et, al 2022).

The highly speculative nature of cryptocurrency means that some sort of regulation must be imposed to protect consumers from being at the mercy of speculators. Many of us in Malaysia would recall the 1997 Asian Financial Crisis where there was a massive plunge in the value of the Ringgit due to currency speculators, resulting in the Ringgit being pegged to the US Dollar at 3.80MYR/USD. For this same reason, regulatory control over cryptocurrencies is critical to ensure consumers are protected from this kind of risk and to minimize the likelihood of cryptocurrency users being defrauded. (Raddatz, et, al, 2023)

2. Security

It has been argued that due to the Blockchain technology that underlies cryptocurrencies such as Bitcoin, no user can steal cryptocurrencies as the thief would have to hack/take control of the entire Blockchain network to sufficiently alter the Blockchain to commit theft. But is the Blockchain as invulnerable as it is claimed to be? History shows otherwise. In early 2014 Mt. Gox (a Bitcoin exchange based in Tokyo, Japan, and the largest in the world at the time) was

the target of a massive hack which resulted in it losing a total of 850,000 Bitcoins valued at a mind-boggling sum more than USD450 million (Liu, X., Khan, M., & Khan, A 2023).

In 2017, a Slovenian-based Bitcoin mining company by the name of NiceHash similarly became a victim of hackers and lost 4,700 Bitcoin worth USD63.92 million. In January 2018, Coincheck (a Bitcoin wallet and exchange service also headquartered in Tokyo, Japan) was hacked resulting in the loss of 500 million NEM tokens (a form of cryptocurrency reliant on Blockchain technology) worth a mammoth sum of USD530 million. All these incidents show us that despite the many assertions about the alleged impregnability of the Blockchain, hackers are still able to find ways to penetrate it and commit theft. This makes cryptocurrency no different, and indeed no safer, than traditional legal tender which are easily exposed to theft and fraud. Under these circumstances, the need for regulation and control is even more pressing to ensure that sufficient security measures are put in place to prevent hacking attacks as discussed above.

3. Anonymity – Conduit for Illegal Activities

As mentioned earlier, cryptocurrency is transacted anonymously whereby the users are not required to disclose their names, addresses, and other personal details compared to traditional methods of transaction involving legal tender. The sender and recipient of cryptocurrency are identified only by an alphanumerical number and nothing else. As such, it is not difficult to see why cryptocurrency has become the favorite medium of exchange among criminals to purchase illegal goods and launder money. Indeed, the focus of most governments around the world in respect of cryptocurrency is to regulate and prevent it from being used to fund criminal activities. (Park, et, al 2023)

To illustrate this, a search conducted on the website www.bitinfocharts.com (which tracks the transactions of cryptocurrencies) shows that as of 3 November 2018, Bitcoin Address No. 1HQ3Go3ggs8pFnXuHVHRytPCq5fGG8Hbhx possesses approximately 69,370.12 Bitcoins worth a staggering USD448,551,934.78! Nobody knows the identity of the individual who owns the aforesaid account and whether that individual is a criminal or otherwise. This goes to show that although anonymity has its advantages in ensuring data protection from theft, it nevertheless presents itself as a tool to be manipulated by criminals for illegal activities. (Poong, Y. 2023).

What happened to the online black market website Silk Road and its creator, Ross Ulbricht is relevant to our present discussion. This website, which deals in illegal guns and drugs, was shut down by the United States Federal Investigation Bureau (FBI) in October 2013 and Ulbricht himself was arrested and subsequently charged, convicted, and imprisoned for offenses ranging

from drug trafficking to money laundering. All transactions on the Silk Road were paid with Bitcoins, with zero regulation and oversight thus attracting the interest of criminals. As stated earlier and as can be seen from what happened to Silk Road, anonymity in transacting with cryptocurrencies is a double-edged sword as it presents law enforcement agencies significant challenges to control and track users that might be using these forms of digital currency in furtherance of criminal activities. (Hanafi, S. F., & Rahman, S. A. 2019).

However, it must be noted that due to the intangible nature of cryptocurrency which only exists on the internet, for a person to realize its value he/she would require what is known as a cryptocurrency exchange which is willing to exchange cryptocurrency for real money. As such, although a cryptocurrency user remains anonymous while he/she is transacting, the anonymity could be at risk of disappearing once he/she "*cashes in*" the cryptocurrency for legal tender at an exchange. This would in turn mean that instead of trying to regulate and control the blockchain (which is pretty much impossible), law enforcement agencies can choose instead to regulate the cryptocurrency exchanges through which cryptocurrency is converted into real money and compel these exchanges to disclose the identity of their customers. This issue will be discussed in further detail below but at this juncture, it is clear that although the element of anonymity accorded by cryptocurrency is laudable, it nonetheless has the unintended consequence of becoming a conduit for illegal activities (Khan, A., & Wu, X. 2021).

The Obstacles in Regulating Cryptocurrencies

In a discussion about the obstacles in regulating cryptocurrencies, it is imperative to note and distinguish between internal and external regulation as cryptocurrencies such as Bitcoin are essentially self-regulating due to the blockchain technology that underlies their existence. The effect of decentralization as discussed above means that cryptocurrencies are maintained and managed by the users themselves through the blockchain (internal regulation), independent of any third-party bank or government. Under these circumstances, unless a regulator can take control of the entire blockchain network on which the existence of a cryptocurrency depends, it is extremely difficult (if not impossible) for external regulation to be imposed on it (Abdelrehim Hammad, A. A., Khan, A., & Soomro, N. E. 2021).

Another challenge in regulating cryptocurrency is due to the very nature of cryptocurrency itself. The problem is simply this – how do you regulate something intangible? Unlike legal tender such as banknotes and coins where circulation is usually regulated by the central bank of a particular country, cryptocurrency only exists in the virtual world as nothing more than an entry in the blockchain. The lack of physical form also means that cryptocurrency can be

transferred with relative ease and under the cloak of anonymity. Under such circumstances, regulators would be hard-pressed in trying to exert some form of regulation over such an asset. (Ramassa, P., & Leoni, G. 2022).

Another hindrance in regulating cryptocurrencies is the fact that any individual with the right knowledge and tools is capable of developing and creating a cryptocurrency by utilizing the blockchain network. This is highlighted by the fact that since the launch of Bitcoin in 2009, there are now (at the time of writing) more than 2000 cryptocurrencies of various names in the market and it is expected that this number will continue to grow in the future. As such, regulating or restricting one cryptocurrency will only result in another cryptocurrency being created under a different name to take its place. This is akin to the Lernaean Hydra, a monster in Greek and Roman mythology where if one of its many heads is cut off, two heads will regrow as a replacement. The ease with which cryptocurrency can be created will therefore present significant challenges to regulators. (Sunny, et, al. 2022)

Regulators will therefore face the challenge of controlling an ever-increasing number of cryptocurrencies, both private and public ones, as this will also have the effect of consuming tremendous manpower and resources which a government simply might not have. Another obstacle in regulating cryptocurrencies is in respect of enforcement. Given that cryptocurrencies work through the blockchain and the blockchain in turn is a globalized public ledger maintained by thousands if not millions of anonymous users worldwide, regulatory challenges will arise in the event of fraud, theft, or technical failure in the cryptocurrencies network. (Teichmann, F. M. 2022).

Law enforcement agencies will face challenges in terms of deciding who, in the vast international, cross-border network of the blockchain, is liable in the event of fraud and theft. The culprit would usually be a resident of another country and he/she is only identified by a lengthy anonymous, alphanumerical number. As an example, let's assume one of the clients of the Tokyo-based Bitcoin exchange Mt. Gox is a Malaysian. How can he/she seek redress for the cryptocurrency that has been lost following the massive hack in 2014? Furthermore, who is to be liable and prosecuted for the hack? Is it the management of Mt. Gox which is based in Tokyo? Or the anonymous hackers who stole the cryptocurrencies? And how are the Malaysian authorities going to identify, arrest, and prosecute the culprit(s)? This example illustrates yet another challenge in regulating digital money which has a global reach and countless pseudo-anonymous users all cloaked by random, lengthy alphanumerical identities (Kahn, A., & Wu, X. 2020).

Other Jurisdictions

In Japan, which is one of the countries where cryptocurrencies are heavily traded, the government has imposed regulations on cryptocurrency exchange businesses in an attempt to exercise some form of oversight and to prevent another Mt. Gox incident from happening in the country. Under the Payment Services Act (Act No. 59 of 2009) which was amended in 2016, cryptocurrency is given a statutory definition, and all cryptocurrency exchange businesses are only allowed to operate on the condition that they are registered with a local Finance Bureau. The Act also imposes, inter alia, requirements that such businesses must separately manage customers' cryptocurrency from their own as well as subject their accounts to review by certified public accountants or accounting firms. (Dhali, at, al 2023).

This can be contrasted with the position in Singapore, where cryptocurrency is not regulated by the authorities. However, as stated by the Deputy Prime Minister in charge of the Money Authority of Singapore (MAS) in August 2017, although MAS does not regulate cryptocurrency *per se*, "*it regulates activities involving the use of virtual currencies that fall under MAS's regulatory ambit*". It is to be noted also that MAS, in November 2017, issued a consultative paper proposing the Payment Services Bill whereby the proposed Bill would extend MAS's regulatory framework to encompass cryptocurrency and require all cryptocurrency traders to be licensed.

Conclusion

The obstacles in regulating cryptocurrency are mainly due to its decentralized nature and the fact that transactions are conducted in a pseudo-anonymous manner. The fact that cryptocurrency is an intangible asset that has no physical form also presents regulatory challenges. However, it must be borne in mind that all these are the very reasons why cryptocurrency has (and indeed will) become a popular medium of exchange. It would take a gargantuan effort for a body to regulate cryptocurrency, not least because of its decentralized nature and the ever-increasing number of cryptocurrencies being produced and made available in the market. Cryptocurrency and its underlying technology, the blockchain were created precisely because of the need to get rid of a central regulatory authority. As such, any attempt to impose any kind of regulation is defeatist to the whole purpose of why cryptocurrency was created in the first place.

It is impractical and indeed expensive for a regulator to try and regulate cryptocurrency and perhaps this is the reason why many countries around the globe have decided not to regulate cryptocurrency itself but rather impose some sort of regulations in the sphere of money

laundering – regulating cryptocurrency exchanges that monetized cryptocurrency into legal tender to prevent it from being used for unlawful activities. It is assets that cryptocurrency is perhaps the medium of exchange for the future due to its many secured features vis-à-vis traditional legal tender. The many advantages of cryptocurrency as discussed above make it an ideal medium of exchange to substitute traditional legal tender as we know it.

As such, cryptocurrency per se should be left unregulated to allow it to retain its many benefits and to develop further. Despite this, however, due to the risk of cryptocurrency being used as a medium of exchange for criminal activities, some sort of regulation must necessarily be imposed on cryptocurrency exchanges as stated above. Cryptocurrency exchanges are the means through which cryptocurrency is monetized and exchanged for cash. Therefore, from a practical and realistic point of view, the public interest is better protected if the government exercises oversight over these exchanges to ensure cryptocurrency is not abused for activities that are detrimental to the public.

References

Abdelrehim Hammad, A. A., Khan, A., & Soomro, N. E. (2021). Digital Economy Barriers to Trade Regulation Status, Challenges, and China's Response. *International Journal of Social Sciences Perspectives*, *8*(2), 41-49.

Aspris, A., Foley, S., Svec, J., & Wang, L. (2021). Decentralized exchanges: The "wild west" of cryptocurrency trading. *International Review of Financial Analysis*, *77*, 101845.

Baker, H. K., Benedetti, H., Nikbakht, E., & Smith, S. S. (Eds.). (2023). *The Emerald Handbook on Cryptoassets: Investment Opportunities and Challenges*. Emerald Publishing Limited.

Dhali, M., Hassan, S., Mehar, S. M., Shahzad, K., & Zaman, F. (2023). Cryptocurrency in the Darknet: sustainability of the current national legislation. *International Journal of Law and Management*, *65*(3), 261-282.

Garcia-Teruel, R. M. (2020). Legal challenges and opportunities of blockchain technology in the real estate sector. *Journal of Property, Planning and Environmental Law*, *12*(2), 129-145.

Ghosh, A., Gupta, S., Dua, A., & Kumar, N. (2020). Security of Cryptocurrencies in blockchain technology: State-of-art, challenges, and prospects. *Journal of Network and Computer Applications*, *163*, 102635.

Griffith, T., & Clancey-Shang, D. (2023). Cryptocurrency regulation and market quality. *Journal of International Financial Markets, Institutions, and Money*, *84*, 101744.

Hanafi, S. F., & Rahman, S. A. (2019). Regulating digital currency: taming the unruly. In *Emerging issues in Islamic finance law and practice in Malaysia* (pp. 265-280). Emerald Publishing Limited.

Hashemi Joo, M., Nishikawa, Y., & Dandapani, K. (2020). Cryptocurrency is a successful application of blockchain technology. *Managerial Finance*, *46*(6), 715-733.

Hooper, A., & Holtbrügge, D. (2020). Blockchain technology in international business: changing the agenda for global governance. *Review of International Business and Strategy*, *30*(2), 183-200.

Kahn, A., & Wu, X. (2020). Impact of digital economy on intellectual property law. *J. Pol. & L.*, *13*, 117.

Khan, A., & Wu, X. (2021). Bridging the Digital Divide in the Digital Economy with Reference to Intellectual Property. *Journal of Law and Political Sciences*, *28*(03), 256-263.

Kumar, A., Abhishek, K., Bhushan, B., & Chakraborty, C. (2021). RETRACTED ARTICLE: Secure access control for the manufacturing sector with the application of the Ethereum blockchain. *Peer-to-Peer Networking and Applications*, *14*(5), 3058-3074.

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A survey on the security of blockchain systems. *Future generation computer systems*, *107*, 841-853.

Liu, X., Khan, M., & Khan, A (2023). The Law and Practice of Global ICT Standardization by Olia Kanevskaia [CUP, Cambridge, 2023, xxvi+ 361pp, ISBN: 978-1-0093-00575,£ 95.00 (h/bk)]. *International & Comparative Law Quarterly*, 1-4.

Moore, D. (2022). *Offensive Cyber Operations: Understanding Intangible Warfare*. Hurst Publishers.

Oxford Analytica. (2021). Fledgling cryptocurrency plans face obstacles in Cuba. *Emerald Expert Briefings*, (oxen-db).

Ozili, P. K. (2022). Decentralized finance research and developments around the world. *Journal of Banking and Financial Technology*, *6*(2), 117-133.

Park, A. H., Ryu, H., Park, W., & Jeong, D. (2023). Forensic investigation framework for cryptocurrency wallet in the end device. *Computers & Security*, 103392.

Patil, P., Sangeetha, M., & Bhaskar, V. (2021). Blockchain for IoT access control, security, and privacy: a review. *Wireless Personal Communications*, *117*, 1815-1834.

Peng, L., Feng, W., Yan, Z., Li, Y., Zhou, X., & Shimizu, S. (2021). Privacy preservation in the permissionless blockchain: A survey. *Digital Communications and Networks*, *7*(3), 295-307.

Poong, Y. (2023). Is it true that a multi-crypto-currency market serves no social purpose other than being a conduit for financial crime and financial instability? *Available at SSRN 4419330*.

Raddatz, N., Coyne, J., Menard, P., & Crossler, R. E. (2023). Becoming a blockchain user: understanding consumers' benefits realization to use blockchain-based applications. *European Journal of Information Systems*, *32*(2), 287-314.

Ramassa, P., & Leoni, G. (2022). Standard setting in times of technological change: accounting for cryptocurrency holdings. *Accounting, Auditing & Accountability Journal*, *35*(7), 1598-1624.

Schaupp, L. C., Festa, M., Knotts, K. G., & Vitullo, E. A. (2022). Regulation as a pathway to individual adoption of cryptocurrency. *Digital Policy, Regulation and Governance*, *24*(2), 199-219.

Sunny, J., Pillai, V. M., Nath, H. V., Shah, K., Ghoradkar, P. P., Philip, M. J., & Shirswar, M. (2022). Blockchain-enabled beer game: a software tool for familiarizing the application of blockchain in supply chain management. *Industrial Management & Data Systems*, *122*(4), 1025-1055.

Teichmann, F. M. (2022). Current trends in terrorist financing. *Journal of Financial Regulation and Compliance*, *30*(1), 107-125.