

# The Need of Blockchain Law in a Cryptocurrency-Based Future: Potential and Possibility of a Purely Blockchain Entity

M Karunanathan# and FAM Imthiyaz

*Faculty of Law, General Sir John Kotelawala Defence University, Sri Lanka*

#mathroth1234@gmail.com

**Abstract** - Blockchain technology first surfaced before ten years ago and it has been the only gaining traction emerged for the last two to three years. Therefore, it is much needed to focus the attention of the governments to implement Blockchain Laws in the present highly digitalized environment. This paper aims to analyse the Blockchain Technology and examine the requirement of a particular legal regime, with its growing popularity among businesses and consumers, as it is a relatively new technology in terms of legislation. This study is largely based on a qualitative approach, a contemporary study on legislations of the countries which follow and do not follow blockchain technology with examining blockchain regulations and relevant scholarly works. The study reveals no consistent policy has yet emerged around the world, except United States. Rather, countries have been left to their own devices, with some, such as those in Europe, incorporating regulation into national legislation and others avoiding the technology altogether. The study concludes by emphasizing the need of a regulatory legal framework for the blockchain technology.

**Keywords—** *Blockchain law, Blockchain technology*

## I. INTRODUCTION- WHAT IS BLOCKCHAIN TECHNOLOGY AND WHY IS IT GAINING TRACTION

Blockchain technology can create a ledger for any type of record. The original Bitcoin blockchain records transfers of funds between different accounts, serving the same purpose as deposit currencies provided by banks. If blockchain technology significantly reduces transaction costs, the current monetary system based on central banknotes and deposit currencies may be replaced by Blockchain Technology. (Makoto Yano 2020). By providing a ledger that nobody administers, a blockchain could provide specific financial services

like payments or securitization without the need for a bank.

Blockchain technology offers a secure and cheap way of sending payments that cut down on the need for verification from third parties and beats processing times for traditional bank transfers. 90% of members of the European Payments Council believe blockchain technology will fundamentally change the industry by 2025. (CB insights 2021).

Blockchain technology also plays a prominent role in the existence of cryptocurrency. A cryptocurrency is a medium of exchange but is digital and uses encryption techniques to control the creation of monetary units and to verify the transfer of funds. Paper money is going away, and Cryptocurrency is a far better way to transfer value than pieces of paper. (Elon Musk 2019) Bitcoin and other digital currencies such as Ethereum use blockchain technology to function. As more and more people start using these digital currencies, the number of blocks will also grow, making the whole system more secure. The system is more efficient and has no transaction cost making the system cheaper too. (Mulligan 2019) However, the nodes on a blockchain may be situated anywhere in the globe and blockchain has the capacity to cross jurisdictional boundaries. This can result in a slew of complicated jurisdictional concerns that must be carefully considered considering the contractual ties at hand. An exclusive controlling law and jurisdiction provision is therefore necessary since it should provide legal certainty to a customer as to which law will be applied to establish the parties' rights and duties, as well as which courts would handle any disputes.

## II. RESEARCH PROBLEM

Investment in virtual currency appears to have gained prominence in recent years. On the contrary, a new generation of blockchains and their applications is currently being developed and deployed. This paper investigates the role that the next generation of blockchains may play in the emerging data-driven society, as well as the need for blockchain laws and policies. In the Internet era, data is expected to become the third major production factor after labour and capital. Blockchain technology enables a new method of owning, sharing, and utilizing data. While the recommendations are being implemented concerning blockchain law, there is still a long way to go to total adoption and full regulation.

This paper seeks to advance the argument that due to Blockchain's ability to cross jurisdictional boundaries, it can pose several complex jurisdictional issues which require careful consideration in relation to the relevant contractual relationships. The principles of contract and title differ across jurisdictions and therefore identifying the appropriate governing law is essential. Accordingly, the paper seeks to provide an overview, scope, and applicability of the concepts in blockchain and emphasize this technology's loophole. Thus, in a decentralized environment, it may be difficult to identify the appropriate set of rules to apply. At its most basic level, every transaction may be subject to the jurisdiction of every node in the network. As a result, the blockchain may be required to comply with a large variety of legal and regulatory frameworks.

Thus, this study specifically focused on the research problem of Why is an exclusive controlling law and jurisdiction provision is therefore necessary for blockchain technology?

### **III. RESEARCH OBJECTIVE**

The objective of this paper is to create awareness regarding blockchain technology and blockchain security threats. Therefore, we should educate ourselves about the blockchain technology and demystify it. If we're able to understand it and implement relevant laws and regulatory statutes and know what we're dealing with, this will help us to manage risks and leverage value. Law enforcers must understand how blockchain technology is exposed to risk through its features and usability and find ways to control it.

Further, the focus of this paper is on the important phases of blockchain technology, analysing the specificities of code, the various benefits and drawbacks of regulation by code, and the ways in which law has, thus far, attempted to regulate code. This paper also investigates the importance of the incorporation of legal norms into code, and on the other, it focuses on the creation of code-based regulation. New kinds of regulation have evolved as a result of the extensive deployment of the global Internet network, which increasingly relies on soft law (i.e., contractual agreements and technological regulations) to govern behaviours. As more and more of our interactions are governed by software, we increasingly rely on technology not only as an aid in decision-making but also to directly enforce rules. Software and this blockchain technology thus end up stipulating what can or cannot be done in a specific online setting more frequently than the applicable law, and frequently, much more effectively. This paper also aims to analyse Blockchain Technology and examine the need for Blockchain Law because, despite its growing popularity among businesses and consumers, blockchain is still a relatively new technology in terms of legislation.

### **IV. RESEARCH METHODOLOGY**

This research is mainly qualitative research carried out by the reference of scholarly books, journals, articles, conference papers, and online resources as secondary sources. Open-domain data were used for the analysis. This paper provides a brief overview of blockchain technology and the debate going over about having no need for the law and common arguments raised in relation thereof. The limitations of the study are that quantitative data is not deeply analysed because only a few countries have recognized the importance of legal certainty and a clear regulatory regime in areas pertaining to blockchain-based applications. The key limitation of the study is the absence of both domestic and international case law and research literature pertains to the main research problem.

### **V. WHY THE WORLD NEEDS THE BLOCKCHAIN LAW**

The Blockchain has been called a haven for criminal activity (NY times 2020). The early focus on Blockchains was on Bitcoin as a private digital currency. The currency which is not controlled by territorial governments. Currency transactions have traditionally been extensively controlled to combat

fraud, money laundering, capital flight, currency manipulation, and terrorist financing. Blockchains are based on complicated technology, yet their essential function is straightforward: giving a widely disseminated but verifiably correct record. Even without a central administrator or master version, anyone can keep a copy of a dynamically updated ledger, but all those copies remain the same. The Blockchain, which is known as the technology most likely to change the next decade of business, deals with an unregulated currency that can easily become a haven for lawlessness, consumer abuses, and financial speculation (Maldonado 2018).

Blockchain-based systems will need to interact with legal procedures and institutions in order to realize their enormous potential and avoid catastrophic disasters. However, unless coders intentionally establish them, there are no legal intervention points for default rules to complete for businesses formed only on the blockchain. On the blockchain, there is no place for default law since it has no purchase. The lack of legal action has both positive and negative consequences. The most obvious legal issue in the case of bitcoins is anonymity. Bitcoin can be used to fund terrorists, buy and sell illegal narcotics, and make regular money "disappear" from legal scrutiny. It's also a means to conceal tax-sensitive transactions. Users can store and exchange precious assets with certainty due to distributed ledger technology. Finding a trustworthy individual or institution, on the other hand, is another matter. Therefore, the world needs Blockchain Law to be the mechanism to work alongside the technical trust architecture of the blockchain.

## **VI. THE LACK OF LEGAL INTERVENTION POINT IN BLOCKCHAIN TECHNOLOGY**

The Blockchain gives its users the ability to avoid the pitfalls of partnership without resorting to organizational legislation, which is something that corporeally constituted entities lack. Entrepreneurs in the real world have every motivation to use business association law to avoid forming a partnership. The 2016 DAO (The DAO was a Decentralized Autonomous Organization that was launched in 2016 on the Ethereum blockchain. After raising \$150 million worth of ether [ETH] through a token sale, The DAO was hacked due to vulnerabilities in its codebase) was a partnership of two or more people to run a business for profit as co-owners. It did not formally form under the

jurisdiction of any state. As a result, it constituted a partnership under business association legislation, and its token holders were potentially exposed to infinite liability.

The Blockchain is a pseudonymous space, and that pseudonymity, along with the Blockchain's "code is law" characteristic, offers participants a level of safety that is not accessible in the real world. As a result, the blockchain eliminates both the penalty and the default from partnership law. Since Lessig's seminal work on "code as law," technology and law have been viewed as two opposing modes of ordering. Software code is a great tool for defining a software-based society's rules. (McKenzie 2017) But, after years of judicial battles, society has figured out how to subject code and digital technology to the rule of law to some extent. The blockchain can, all by itself, perform via contractual means what before now only organizational law could do. Blockchain technology, on the other hand, appears to be a very different beast. They aspire to elude the rule of law since its architectural elements are meant to permit the escape of effective regulation and enforcement. The complicated question is what will happen when gaps appear in the blockchain's nexus of contracts (Fairfield 2014). If the entity only exists on the blockchain, the law fails because there is no way for it to enter the code. However, if identifiable individuals organize entities on the blockchain, a legal intervention point exists at the intersection of the blockchain and the corporeal world, not in the blockchain itself. (Levi, Vasile & Neal 2018).

This Blockchain technology was born in the crypto anarchist underground of the Internet. Thus, Sovereign states all over the world are debating how to regulate the blockchain, inevitably focusing on this intersection as a legal issue. The nature of the blockchain, on the other hand, makes it difficult to apply traditional business law. Indeed, despite their partnership status, businesses created on the blockchain have de facto limited liability when it comes to contract claims.

## **VII. SMART CONTRACTS AND HOW THE BLOCKCHAIN WORKS**

The Blockchain's version of traditional contracts is known as smart contracts. The terms are written in code and stored on a decentralized, immutable blockchain, making them self-executing. The concept of smart contracts was developed independently of

blockchain technology. Smart contracts which are self-contained software agents use Bitcoin's distributed ledger to perform transactions and run autonomously. The same consensus techniques that enable each node to have an identical copy of the ledger also enable it to carry out similar computations in the same order. While Bitcoin uses smart contracts to operate, it restricts their capabilities to simple fund transactions for security reasons (Fairfield 2014)

Ethereum, which debuted in 2015, is the most popular platform for smart contracts today. Ethereum has a Turing-complete programming language, which means that any application that runs on a conventional computer may theoretically be run on the consensus network's distributed computer. The decentralized, international, and pseudonymous character of blockchains creates possible conflicts between digital currency and existing regulations. Anti-money laundering (AML) rules, which impose monitoring duties for financial transactions, are used to demonstrate the idea. That's why it is identified that the significant difference between smart and legal contracts relates to execution and termination, also Smart contracts enforce obligations through autonomous code. Unless an appropriate termination option is written into the program, smart contracts are more difficult to terminate than conventional agreements. Smart contracts are also more dynamic than traditional legal contracts, because performance responsibilities can be altered over time via trusted third-party sources. In terms of clarity, precision, and modularity, smart contracts are advantageous. We might see a world of complex smart contract libraries used not only a la carte in contractual arrangements but also to enable machine-to-machine transactions in the future. (Johnston 2016)

There are some main smart contract restrictions, which are still unaddressed in the current state of the technology. First, there are privacy considerations, which may make them unsuitable for use as a substitute for traditional contracts in transactions requiring confidentiality. Second, smart contracts are insufficient to formalize certain sorts of legal duties. This includes the previously mentioned open-ended provisions of continuous partnerships that must be updated on a regular basis. Third, the pseudonymous nature of the contract's parties, which complicates error rectification and enforcement. Fourth, widespread deployment of smart contracts could

lead to standardization and "automation bias," leading in the acceptance and implementation of flawed contracts with limited modification options. Finally, the primary issue could be the possibility for illicit or immoral behaviour to be enabled by smart contracts and blockchains.

## VIII. PRECEDENCE OF BLOCKCHAIN TECHNOLOGY

A blockchain is frequently referred to as a decentralized ledger. The term "ledger" refers to an old term for a "book of the permanent record." A blockchain is a distributed ledger that was created in a decentralized manner. Many independent entities contribute to the creation of a book of permanent data that is accurate and unfalsifiable in this process. Records that are accurate and unfalsifiable are extremely valuable. A county recorder's office keeps vital records pertaining to real estate (land) ownership as well as debts or liens against it. It would be nearly impossible to trade land and/or lend and borrow money with land as collateral without these records. (Makoto Yano 2020).

Blockchains have demonstrated that such trusted records can be decentralized stored on the Internet. Decentralizing the recording process, which has traditionally been centralized and overseen by the government, is expected to significantly reduce transaction costs (or the cost of creating and maintaining a ledger). That is one of the reasons why many people have embraced blockchain technology. A blockchain allows you to designate the owner of each piece of data, trade data pieces, and market them by creating a data ledge. By replacing the cumbersome, paper-heavy bills of lading process in the trade finance industry, blockchain technology can create more transparency, security, and trust among trade parties globally. The future of money is digital currency. (Bill Gates 2018) The adoption of Blockchain, cryptocurrency, and virtual assets is rapidly increasing, according to a recent Chainalysis (Chainalysis: The Blockchain Data Platform) report, 92 percent of the 154 countries studied had some sort of cryptocurrency activity. The way we work, bank, and live in the future may look very different from how we do now, with some of these technologies underpinning our basic activities. (Povey 2020).

## IX. DRAWBACKS ON BLOCKCHAIN TECHNOLOGY

Recently, wild speculative activities have targeted blockchain currencies and businesses. Blockchain



currencies have been widely used in money laundering and drug trafficking. Social perceptions of blockchain are rather negative as a result of these activities, which have given the blockchain industry the image of a risky business. (Chris Dai 2020). However, if better blockchain laws are developed and a healthy market infrastructure to support the blockchain market is established, the industry will have a bright future. Blockchain laws would be able to contribute to the development of a cyber ecosystem in which the blockchain industry can thrive.

In order to manage IoT (Internet of Thing), large data in a blockchain, a new blockchain on which smart contracts may be performed is required. (A smart contract is a computer program that executes software commands according to the smart contract's specifications for each scenario). As a result, it reduces the expense of dispute resolution that would otherwise be borne by a regular contract; under a standard contract, a disagreement is generally handled by a court. (McKenzie 2017). In modern society, many social obligations are enforced centrally by laws. In a smart contract, in contrast, transactions are enforced by a computer algorithm, which can be expected to wipe out any contractual disputes. This, however, does not imply that the contractual arrangements in a blockchain are free from dispute.

“Blockchain, bitcoin, crypto assets, virtual currencies, a whole new vocabulary describing innovative technology to swiftly transfer value around the world.” The fast-evolving blockchain and distributed ledger technologies have the potential to radically change the financial landscape. But, their speed, global reach and above all - anonymity - also attract those who want to escape authorities' scrutiny.” (Financial Action Task Force). This technology has the potential to improve compliance (for example, DLT can be used to bring more transparency to business transactions and speed up global commerce). However, it has the potential to be advantageous to criminals, the anonymity provided through blockchain can create a haven for bad actors to operate within). While crypto assets do not pose a threat to global financial stability at this point, we remain vigilant to risks, including those related to consumer and investor protection, anti-money laundering, and countering the financing of terrorism. (G20 Finance Ministers and Central Bank Governors Meeting, Fukuoka, Japan, June 9, 2019)

Blockchain laws and regulations are under construction, so this is not clear-cut. Too much regulation stifles growth and adoption at a time when the world is crying out for advancements and improvements in how business is conducted, but too lax an approach allows criminals to run wild and exploit regulatory gaps. (Povey 2020). This is what Joel Reidenberg (1998) has coined Lex Informatica a concept which has subsequently been popularized as “Code is law” by Lawrence Lessig (1999). We could say that with the advent of blockchain technologies, the law is progressively turning into code.

## **X. DEBATE ON WHY DO WE NEED THE LAW OF BLOCKCHAIN?**

Law and technology can influence each other in a variety of ways. The two interact through a complex system of dependencies and interdependencies, as both contribute (to varying degrees) to regulating individual behaviour. The relationship between the two has significantly evolved with the advent of modern information and communication technology, as the latter is increasingly used as a complement or supplement to the former. Lawyers, judges, and policymakers are increasingly surrounded by digital information and software tools that they rely on in their daily work. Recently, new technology has emerged that has the potential to change the way we think about law. The blockchain is the foundational tool for peer-to-peer value creation and trust less transactions. It is a decentralized, secure, and incorruptible database (or public ledger). The technology, which was introduced in 2009 with the Bitcoin network as the underlying infrastructure for a decentralized payment system, (Nakamoto 2009) has rapidly evolved to take on a life of its own.

The blockchain is now used in a wide range of applications, from financial to machine-to-machine communication, decentralized organizations, and peer-to-peer collaboration. The blockchain, as a trustless technology, eliminates the need for trust between parties, allowing the coordination of many individuals who do not know (and thus do not necessarily trust) each other. At the other end of the spectrum, the most recent blockchains have enabled people to upload small snippets of code (so-called smart contracts) directly onto the blockchain, where they can be executed decentralized by every node in the network. Even if they do not reflect any underlying legal or contractual provision, these rules are automatically enforced by the underlying blockchain technology. (De Filippi & Hassan 2016)

Some proponents suggest that blockchain technology could lead to a society where self-enforcing rules would supplant traditional laws (Nakamoto, 2008). Indeed, with the advent of blockchain technology and the introduction of smart contract capabilities on top of it, it becomes increasingly appealing for people to bypass the traditional legal framework of contract law, and to rely on the underlying technical infrastructure provided by the blockchain instead.

A new approach to regulation is known as the codification of law, which entails a growing reliance on code not only to enforce but also to draft and elaborate legal rules. Because smart contracts can be used as both a supplement to and a replacement for legal contracts, the lines between what constitutes a legal or technical rule are becoming increasingly blurred as a result of technological advancements. Indeed, while most smart contracts are not directly associated with a legal contract, depending on how they are entered, they may or may not give rise to an actual contractual relationship in the traditional sense of the term. However, smart contracts can be used to emulate, or at least simulate, the function of legal contracts through technology, effectively turning law into code. (Rodrigues 2018)

Accordingly, as more and more contractual provisions are implemented in the form of a smart contract (as opposed to a legal contract), the blockchain progressively acquires the status of a “regulatory technology”, a technology that can be used both to define and incorporate legal or contractual provisions into code and to enforce them irrespectively of whether there subsists an underlying legal rule. (Buterin 2018)

The blockchain could be the most significant advancement in information technology since the Internet. The blockchain, which was designed to support Cryptocurrency, (digital currency), is something more: a novel solution to the age-old human problem of trust. Excessive or premature application of strict legal obligations will stifle innovation and miss opportunities to use technology to achieve public policy goals. Blockchain developers and legal organizations can collaborate. Each must recognize the other system's distinct affordances. This Blockchain technology has tremendous potential. However, in the absence of effective governance and law, this approach may not promote trust at all. Blockchain-based systems may be completely independent of legal enforcement. This can be counterproductive or even dangerous. And

they are less protected from the reach of the law than they appear. The central question is not how to regulate blockchains, but how blockchains regulate themselves. (Werbach 2018).

## **XI. GLOBAL DATA PROTECTION LAW AND LAW OF BLOCKCHAIN**

The first thing to remember when considering the application of data protection regulations to blockchain/distributed ledger technology is that there is no such thing as a global data protection law. Despite the fact that overarching principles like Article 12 of the Universal Declaration of Human Rights and the OECD Privacy Principles developed in the 1980s provide a common source for many data protection regimes around the world, there is significant variation. Despite this complexity, when it comes to compliance with privacy and data protection standards in the context of blockchain and distributed ledger implementations, there are several fundamental themes that are expected to emerge in most, if not all, jurisdictions. Many data protection rules make it much more difficult to deal with anonymous or pseudonymous data. In many circumstances, data relating to an unidentified individual will fall outside the purview of data protection rules. There are two sorts of prospective creditors for any business: voluntary and involuntary (tort) creditors. In terms of the former, in order for an obligation to arise, the blockchain code would have to describe the terms and circumstances of loans. In that case, Data "controllers" (usually, primary collectors of personal data from end users) and data "processors" (usually, secondary holders of personal the who operate on behalf of data controllers) are clearly defined in several jurisdictions, particularly in the EU are equally responsible for compliance. (McKenzie 2017)

The ramifications of these distinctions will vary based on the Distributed Ledger Technology (DLT) implementation's nature and each participant's level of autonomy. Most public blockchains, on the other hand, have each node deal with the data it gets as a totally independent operator rather than sharing it with other nodes. While many data protection laws are aligned to some extent, this is still a field of law with significant differences between jurisdictions (Johnston 2016). For public and private distributed ledger technology implementations, blockchain laws in their numerous iterations around the world pose a genuine and current compliance barrier. Privacy by

design, which is a motto for privacy regulators around the world, should truly be a key component of any new implementation (Maldonado 2018)

## **XII. BLOCKCHAIN LAW AS AN EVOLVING LAW**

### *A. United States*

The state-by-state regulation of data breach notification is a good example of the US's legal diversity: each state has its own rules governing the circumstances in which entities must notify regulators and individuals of actual or potential data breaches, as well as the processes for such notifications. Aside from healthcare, the financial services industry is one of the most heavily regulated in the United States, which means that public blockchains containing US nodes will have to consider and comply with a wide range of regulations. The United States has yet to develop a consistent legal approach to cryptocurrencies, with laws varying by state. The Financial Crimes Enforcement Network (FinCEN) does not yet consider cryptocurrencies legal tender; however, the Internal Revenue Service (IRS) considers cryptocurrencies to be property. The fragmentation of US privacy and data protection law is perhaps its most distinguishing trait. In practice, there is no overarching legislation governing data protection; instead, data collectors must navigate a tangle of state and federal rules, many of which apply to specific data sets in certain industries.

New York was the first state in the United States to regulate virtual currency enterprises through state agency rulemaking in June 2015. As of 2019, 32 states have introduced or enacted legislation accepting or encouraging the use of Bitcoin and blockchain distributed ledger technology (DLT), with a handful already having done so. Despite some agencies' involvement, the federal government has not used its constitutional pre-emptive right to regulate blockchain to the exclusion of states (as it does with financial regulation), allowing individual states to enact their own laws and regulations.

### *B. UK and the Europe*

The European Union (EU) has taken a constructive and welcoming stance to blockchain technology in general, but it has only recently introduced official law to regulate it. The EU signed the 5th Anti-Money Laundering Directive (5AMLD) into law on January 10, 2020, bringing cryptocurrencies and crypto service providers under regulatory scrutiny for the first time. However, because permissioned DLT

systems involve known and trusted parties, history entries can be changed if a sufficient number of the parties' consent to an erasure. Participants in the Ethereum network, for example, went through a similar procedure to reclaim assets lost in the infamous "DAO attack." "When a data controller (for example, a node in a public blockchain) makes personal data public, exercising the right requires the node to take reasonable steps, including technical measures, to notify other controllers of the erasure request. Controllers must consider the available technology as well as the cost of implementation while fulfilling this requirement.

The right to be forgotten, which is now part of EU law according to Article 17 of the new General Data Protection Regulation, poses a unique challenge for open blockchain systems. Article 17 establishes a "right to be forgotten" for personal data, subject to certain conditions and limitations. These efforts are precursors to a more united approach; the chair of the Financial Stability Board (FSB), based in Switzerland, stated in February 2020 that financial authorities must speed up the process of building a complete regulatory framework for cryptocurrencies. The letter, written to finance ministers and G20 central banks, urged global authorities to act quickly – specifically, to examine the dangers and benefits of stable coins in order to stay up with the crypto market's rapid pace of innovation and development and avoid losing control (Insider Intelligence 2021).

Given the Internet's and Blockchain's opacity, the European Union has found it difficult to establish clear and strict rules (anonymity provided by IP addresses, data being moved quickly, locations disguised via a virtual network, etc.). Sanctions in the cyber world are proving nearly impossible to apply in the same way as sanctions against arms dealers or nuclear proliferation activities. (Povey 2020)

### *C. Australia*

The existing law, the Australian Privacy Act, allows for data offshoring but requires the transferring company to verify that the data is held in line with the standards of Australian privacy law by the recipient. This is often accomplished through contracts that oblige recipients to adhere to certain criteria, but with a public blockchain, this is unlikely to be viable. The heightened focus on cross-border transmission of personal information has been a fundamental component of Australian privacy law since a significant round of legislative amendments in 2014.

Under Australian law, the entity transmitting the data out of Australia is accountable for any breaches by or on behalf of the recipient entity or entities, implying that any Australian node in a public blockchain might face severe liability under present laws (Maldonado 2018)

#### *D. Singapore*

The challenging concerns, such as the treatment of anonymous and pseudonymous data, and questions about the de-identification and re-identification of data, maybe ambiguous in the context of new and emerging technologies like blockchain and DLT implementations. Rather than possessing any specific regions of significant difficulty, the nascence of Singapore's privacy law is a fundamental aspect. Singapore's Personal Data Protection Act was first enacted in 2013; therefore, it does not yet have the same history or precedent in data protection law as other countries, such as those in Europe (Insider Intelligence 2021). Of course, these concerns are not unique to Singapore, as much of the law governing data protection in the Asia Pacific region has also evolved rapidly in the last five to ten years.

#### *E. Sri Lanka*

The Sri Lankan chapter to Blockchain and Cryptocurrency Regulation does not exist. Also, there is currently no consolidated or specialized data protection legislation in Sri Lanka. There are some industry-specific data protection-enabled laws. However, such legislation lacks a definition for the term "data" as well as precise implementation provisions. With the increased use of technology in the Covid-19 epidemic, where practically all social, educational, and local commercial transactions are conducted on the internet, the number of crimes recorded has increased dramatically, according to Comprehensive Error Rate Testing reports (Moody's Analytics 2019) The demand for blockchain laws in Sri Lanka has been steadily growing, highlighting the importance of issues relating to the protection of persons' and other entities' privacy and data. It is not against the law in Sri Lanka to sell or buy cryptocurrencies. But due to its decentralized and anonymous character, CBSL (Central Bank of Sri Lanka) has not issued any licenses or authorizations to any company.

### **XIII. CRYPTOCURRENCY AND BLOCKCHAIN REGULATIONS AROUND THE WORLD**

Some countries, however, believe that accepting cryptocurrencies will lead to a loss of economic

control and a global movement toward decentralized economies. China, Russia, and Colombia are among the countries that have outright outlawed Bitcoin and other cryptocurrencies, making their usage and investment illegal. The cryptocurrency was initially treated with caution in China but has recently received some support. The People's Bank of China banned initial coin offerings and cryptocurrency exchanges in 2017 and attempted to eradicate the industry by making token sales illegal. As a result, the largest exchanges ceased trading. All of this changed in 2019 when a Chinese court ruled that Bitcoin was digital property. Since then, there has been a shift in cryptocurrency adoption, with Chinese President Xi Jinping urging an increase in blockchain development efforts. There is still some skepticism, but China is unquestionably a developing country.

As institutional money enters the market, several economists foresee a significant shift in crypto. Furthermore, there is a chance that crypto will be listed on the Nasdaq, (American stock exchange based in New York City which is ranked second on the list of stock exchanges) which would provide legitimacy to blockchain and its usage as a substitute for traditional currencies. If there isn't a functioning rule of law, to begin with, the blockchain-based rule of law could be a major improvement (Brunner 2020). Several billion individuals in the poor world, for example, do not have access to bank accounts and the benefits that come with them, such as quick payments and credit where Bitcoin and other cryptocurrencies provide a quick solution to the unbanked problem. (Mulligan 2019)

### **XIV. BLOCKCHAIN CODE VS LAW**

The blockchain has ignited the flame of cyber-libertarianism. A conversation regarding blockchain and law can be framed in two ways: Is it possible to have legal and administrative oversight of these technologies? Should they, in fact, be? Governments and large private organizations will not be easily disintermediated, based on the preceding two decades' experience. They developed strategies to limit internet activity if they had a strong desire to do so. A similar trend appears to be emerging for blockchain activities, where the stakes are high enough that governments will not just relinquish control. The first involves breaking the law using cryptocurrencies or stealing cryptocurrency through hacking and other methods. The fact that bitcoin can be used to pay for drugs does not automatically make it illegal; Russian rubles or gold bars can be used in



the same way. Even when transactions are completely digital, peer-to-peer, cross-border, and cryptographically secure, network providers and users might be recognized and subjected to territorial legal obligations. Furthermore, outside of illegal or high-risk activities, there are few incentives for most users to adopt new legal systems where the existing ones are adequate (Ferrari, João & Alexandra 2019).

Already, regulatory battles over blockchain-based systems are raging. The illegality, classification, and legal validity are some major forms of legal controversies. There's also the issue of how other legal systems see distributed ledgers. States are beginning to handle blockchain-based data in the same way they regard traditional records. Delaware passed legislation allowing distributed ledgers to be used for government records as well as regulatory services like tracking business shares. However, there are numerous specific questions to address, and various jurisdictions that must act, just as there are with categorization difficulties. To be sure, there are crucial considerations concerning where to draw the boundary between acceptable and unacceptable technological usage. Criminals and terrorists will try to take advantage of the blockchain, just as they do with other technology. Governments will overreact and impose restrictions that will harm legitimate operations in the process. The point is that these aren't brand-new issues. They should also not be interpreted as proof of a fundamental conflict between the blockchain and the rule of law. New services that do not seek to contravene the law are the more intriguing scenarios. By introducing a powerful new mechanism for trust and compliance, to what extent does the blockchain render existing legal regimes obsolete? And to what extent do existing legal frameworks place undue restrictions on blockchain-based innovation?

Surprisingly, one option for the blockchain to establish more robust confidence is through the judicial system. There are a few ways to combine the distributed, algorithmic trust structures of the blockchain with the human-interpreted, state-backed institutions of law. In some cases, legal assistance will not be required (Lessig 2006). Existing legal arrangements function normally without any integration in other cases where the blockchain is just supplemental.

However, in many circumstances, proactive actions are required to combine the finest features of distributed ledgers and centralized law (Kevin 2017).

#### **XV. UN'S CONCERN ABOUT BLOCKCHAIN LAWS AND REGULATIONS**

Blockchain, for example, is cross border; as a currency and a technology, it transcends national borders and therefore necessitates a united, multilateral legal regulatory approach. It also necessitates those persons working in the public service around the world be more than merely technically savvy; they must be mindful of how their regulations might be interpreted in code. The United Nations Children's Fund has become the first UN entity to possess and trade cryptocurrencies. The UN Children's Fund will now be able to receive, retain, and disperse bitcoin donations through a newly established Cryptocurrency fund. Also "The UN Climate Change Secretariat sees the potential of blockchain technology to contribute to improved climate action and sustainability," said Massamba Thioye, who is in charge of UN Climate Change's DLT and blockchain research. The UN World Food Program conducted a successful pilot in Jordan in 2017 utilizing the Ethereum blockchain to track food aid distribution to 10,000 Syrian refugees. In an area where traditional legal enforcement is impossible, the program provided accountability. We need to be taught how to handle the digital highways upon which our society is currently being created in the same way that we learn the rules of the road before driving. According to studies, just around a third of the public can comprehend the data and statistics that make up the open data movement's outputs. (Mulligan 2019)

From a technical standpoint, the call to inclusion, trust, and multilateralism that blockchain tries to address will continue for many decades, and we will need to find new ways to respond through governments, civil society, academia, non-governmental organizations, and international organizations like the United Nations. According to Cathy Mulligan, Member of the United Nations Secretary General's High-level Panel on Digital Cooperation; and Expert and Fellow, World Economic Forum Blockchain Council has emphasized on the fact that "The regulation of digital technology is a critical subject that requires multilateral attention. Although numerous projects to establish such legislation have been launched around the world, we must widen our understanding of those

efforts as well as human rights concepts across the digital business.” (Mulligan 2019)

We can address our current emergent technologies and have plausible frames of reference for ones that haven't even been thought of yet by developing proper multilateral solutions legally through conventions and treaties. Rather than categorically adopting or rejecting such technologies, we must give them due thought and collaborate to analyse and handle their consequences.

More significantly, codes created in one country under a specific set of laws may affect citizens in another country. It is still uncertain how these instances will be addressed.

#### **XVI. BLOCKCHAIN IMPLEMENTATION IN PANDEMIC**

The COVID-19 has demonstrated that traditional supply chains are not always resilient or adaptable enough to handle a pandemic or other large-scale disaster. Many companies, for example, experienced severe supply chain disruptions during the pandemic, perhaps most notably in the healthcare sector, which was disrupted by shortages of critical medical equipment and supplies. Companies were already looking into the potential of blockchain to update various elements of their supply networks before the COVID-19 pandemic. While there was enthusiasm for using blockchain to usher in a new digital era in the supply chain prior to the pandemic, many organizations believed that implementation could be postponed. The COVID-19 outbreak, on the other hand, has prompted a shift in attitude.

There have been reports of blockchain research and implementation to resolve stubborn supply chain issues since the outbreak. For example, in the early days of virus response, blockchain was considered for applications such as connecting medical providers with needed equipment during the COVID-19 outbreak and potentially producing reliable COVID-19 immunization passports stored on a blockchain. Even the use of blockchain technology to prevent price gouging is being considered. In a related development, blockchain-based contract tracing apps are being developed to improve mobile users' privacy protections by storing digital data in a cryptographically secure manner. Many businesses have yet to realize its potential and the numerous ways in which blockchain may be utilized to improve operations or establish new service offerings, but as

its uses become more widely known, momentum is building. (Brunner 2020).

#### **XVII. CONCLUSION**

The blockchain, like the Internet, is a foundational technology whose ramifications could be felt all over the globe. Law and distributed ledgers, on the other hand, are required to move forward. Blockchain developers cannot ignore the law, but neither can governments ignore the blockchain's growing importance. Adapting the law is one method to close the gap. As regulators, legislators, and courts grapple with the problems and opportunities presented by this basic new technology, some of this will naturally occur. The procedure can be sped up by using more different requirements.

The issue for countries and the judiciary, then, is how to deal with this emerging blockchain technology when they come across it. It's extremely complicated, we're all discovering and attempting to understand it together. There are threats and opportunities, as with all risks. Clearly, we must adhere to regulations and laws; however, what happens when those laws are unstable or unavailable? Similarly, what happens when new technology emerges at such a rapid pace that regulation is unable to keep up? There are so many new products and novel ways of moving value around the world that criminals are poised to exploit that regulator face a formidable challenge in keeping up. Significant capital investments in blockchain technology firms have already begun to be made by public businesses and individual investors. As commercial blockchain installations become a reality, this tendency is expected to accelerate. Transactional attorneys who are responsible for doing due diligence on the purchase and/or sell-side in connection with these investments should be familiar with blockchain technology and the developing business models that are built on it. It's possible that traditional due diligence methods may need to be tweaked. Ownership of data stored on decentralized ledgers and intellectual property ownership of blockchain-as-a-service offers based on open-source blockchain technology platforms, for example, will be distinct challenges. These considerations must be made in the context of the company value proposition and competitive entry barriers.

As a result, the conclusion highlights that there are still legal points of intervention in the blockchain's connection with the actual world, rather than in the

blockchain itself. Governments throughout the world should govern the blockchain, just as they did the Internet before it, and think about how the law might apply to the technology.

### ACKNOWLEDGMENT

We would like to acknowledge the advice and guidance of all the lecturers of the Faculty of Law, Kotelawala Defence University and our parents, family members and friends for the support and encouragement.

### REFERENCES

- Baker McKenzie. (2017) Blockchains and Laws; Are they compatible? <[https://www.bakermckenzie.com/en/-/media/files/expertise/fig/br\\_fig\\_blockchainsandlaws\\_jul17.pdf](https://www.bakermckenzie.com/en/-/media/files/expertise/fig/br_fig_blockchainsandlaws_jul17.pdf)> accessed 21 May 2021
- Cathy Mulligan. (2019) Blockchain and Sustainable Growth <<https://www.un.org/en/un-chronicle/blockchain-and-sustainable-growth>>accessed 25 May 2021
- C.G. Weeramantry (1965) Law of Contracts: Volume I, Stamford Lake Publication
- David Povey. (2020) Cryptocurrency's future: What compliance needs to know, International Compliance Association  
<<https://www.complianceweek.com/risk-management/cryptocurrencys-future-what-compliance-needs-to-know/29734.article>> accessed 21 July 2021
- Donald B. Johnston. (2016) What is the Law of the Blockchain? <<https://www.airdberlis.com/insights/blogs/thespotlight/post/ts-item/what-is-the-law-of-the-blockchain>>accessed 25 May 2021
- Dr. Richard Brunner. (2020) How blockchain technology will impact our legal system  
<<https://www.lexology.com/library/detail.aspx?g=7bc262b3-21df-47c8-9cdd-620367745c32>>accessed 30 May 2021
- Financial Action Task Force, how can criminals misuse virtual assets? <[https://www.fatf-gafi.org/publications/virtualassets/documents/virtual-assets.html?hf=10&b=0&s=desc\(fatf\\_releasedate\)](https://www.fatf-gafi.org/publications/virtualassets/documents/virtual-assets.html?hf=10&b=0&s=desc(fatf_releasedate))> accessed 21 May 2021
- Insider Intelligence. (2021) How the laws & regulations affecting blockchain technology and cryptocurrencies, like Bitcoin, can impact its adoption  
<<https://www.businessinsider.com/blockchain-cryptocurrency-regulations-us-global>>accessed 24 May 2021
- Jaliz Maldonado. (2018) 10 Ways Blockchain Technology Will Change the Legal Industry, The National Law Review, Volume VIII, Number 323  
<<https://www.natlawreview.com/article/10-ways-blockchain-technology-will-change-legal-industry>> accessed 25 May 2021
- Josh A.T. Fairfield. (2014) Smart Contracts, Bitcoin Bots, and Consumer Protection, 71 WASH. & LEE L. REV. ONLINE 35, 46–49  
<<http://scholarlycommons.law.wlu.edu/wlulr-online/vol71/iss2/3>>accessed 21 May 2021
- Laurence Lessig. (2006) Code: Version 2.0 2nd edition
- Makoto Yano. (2020) Blockchain and Crypt Currency Building a High-Quality Marketplace for Crypt Data  
<<https://link.springer.com/book/10.1007/978-981-15-3376-1>> accessed 21 July 2021
- Moody's Analytics. (2019) Exploring Blockchain Implementation in Sri Lanka; Navigating the Opportunities and Challenges  
<<https://www.cfainstitute.org/-/media/regional/arx/post-pdf/2019/04/15/exploring-blockchain-implementation-in-sri-lanka.ashx>>accessed 29 May 2021
- Primavera De Filippi and Samer Hassan. (2016) Blockchain technology as a regulatory technology: From code is law to law is code First Monday, Volume 21, Number 12  
<<https://firstmonday.org/ojs/index.php/fm/article/download/7113/5657>> accessed 21 July 2021
- Quintais, João and Bodó, Balázs and Giannopoulou, Alexandra and Ferrari. (2019). Blockchain and the Law: A Critical Evaluation. Stanford Journal of Blockchain Law & Policy (2)1, Amsterdam Law School Research Paper No. 2019-03, Institute for Information Law Research Paper No. 2019-01, Available at  
<<https://assets.pubpub.org/lmtqgprc/41573938876287.pdf>>accessed 27 May 2021
- Satoshi Nakamoto, Bitcoin: A Peer-To-Peer Electronic Cash System, BITCOIN (2008),  
<<https://bitcoin.org/bitcoin.pdf>>accessed 21 May 2021
- Stuart Levi, Cristina Vasile, MacKinzie Neal (2018) Blockchain & Cryptocurrency Regulation 2021-Legal issues surrounding the use of smart contracts, Global Legal Insights  
<<https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/12-legal-issues-surrounding-the-use-of-smart-contracts>>accessed 24 May 2021

Usha Rodrigues, Law and the Blockchain, 104 Iowa L. Rev. 679 (2018),

Available at: [https://digitalcommons.law.uga.edu/fac\\_artchop/1274](https://digitalcommons.law.uga.edu/fac_artchop/1274) accessed 24 May 2021

Vitalik Buterin. (2018) A Next-Generation Smart Contract and Decentralized

Application Platform, GITHUB <<https://perma.cc/5DTZ-NEZ2>>accessed 25 May 2021

Werbach, Kevin, Trust, But Verify: Why the Blockchain Needs the Law (August 1, 2017). 33 Berkeley Tech. L.J. 489 (2018),

Available at SSRN: <https://ssrn.com/abstract=2844409> or <<http://dx.doi.org/10.2139/ssrn.2844409>>accessed 29 May 2021

Mathumitha Karunanathan is an undergraduate at the faculty of law of General Sir John Kotelawala Defence University. She followed a Diploma in Diplomacy and World affairs at Bandaranaike International Diplomatic Training Institute. She has completed the School Mediation Program by the Ministry of Justice Sri Lanka and the South Asia Program by The Stimson Center US. She's interested in Public International Law, Aviation Law, and is currently focused on the security threats in the cyber domain, blockchain, and cryptocurrency regulation.



Fathima Ameera Mohomad Imthiyaz is an undergraduate at the faculty of law of General Sir John Kotelawala Defence University. She has completed a Diploma in Information Technology. She is trilingual and interested in developing insight into the Law and Policy Dimensions of Ocean Governance. She also has accomplished a Certificate of Leadership Development program by the Lions Club of Kottawa Metro. She is currently following the International Commercial Arbitration Program by The Moot Court Bench Sri Lanka. Her Interest areas are International Maritime Law, Law of Contract, and Information Technology Law.

#### AUTHORS BIOGRAPHIES

