

## LEGAL ISSUES IN DISTRIBUTED LEDGER TECHNOLOGY (DLT) & BLOCKCHAIN IN BRUNEI DARUSSALAM

Dr Hakimah Yaacob<sup>1</sup>

### **Abstract**

*Blockchain and Distributed Ledger Technology (DLT) have changed the regulatory landscape globally. Regulators are working hard to create conducive environment for the deployment of DLT and the blockchain. However, robust growth of technology does not come with speedy regulatory changes. This includes reviewing and adapting regulatory requirements or procedures that may unintentionally inhibit innovation or render them non-viable due to lacuna in law. This article is an attempt to analyse the DLT and blockchain from legal perspectives in Brunei. The issues raised in the article warrant considerable merits of law makers' attention. The article concludes with several suggestions and recommendations. The paper employs library research with main references to the policy papers, Act and legislations. Where necessary, the paper makes reference to other countries for comparative purposes. The paper includes several suggestions and recommendations for authority's consideration. The findings suggest that despite of the existing enabling provisions in Brunei, there is a need to have a comprehensive regulations for blockchain and DLT due to excessive big data and other liabilities issues involves.*

**Keywords:** *Distributed Ledger Technology, Legal Issues, Blockchain, Brunei Darussalam*

### **Introduction**

FinTech has gained traction due to its global demand. Based on the KPMG released report, the investment in FinTech worldwide raised more than doubled in 2018. One of the contributors to the figure driven hugely by the acquisition of WorldPay by Vanity and the \$14 billion VC funding round raised by Ant Financial<sup>2</sup>, this is followed by the second quarter with investment involving \$17 Billion PE firm Blackstone's in Refinitive (formerly the financial and risk group

---

<sup>1</sup> Senior Assistant Profesor, Faculty of Islamic Economics and Finance (FEKIm), Universiti Islam Sultan Sharif Ali, Brunei Darussalam. Email: [hakimahunissa2020@gmail.com](mailto:hakimahunissa2020@gmail.com).

<sup>2</sup> KPMG Report on Biannual global analysis of investment in FinTech, retrieved from <https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/02/the-pulse-of-FinTech-2018.pdf>, 4.00pm, 13<sup>th</sup> of February 2020.

of Thomson Reuters) and the \$3.5 billion acquisition of prepaid card company Blackhawk Network by Silver Lake and P2 Capital Partners. In the same year, there are other companies involved in the FinTech investment such as Denmark payments firm Nets merged with German-based Concard is in a multi-billion-dollar deal. At the same time, Nets also carried out a number of other deals, including the acquisition of Poland-based payment firm Dotpay/eCard.<sup>3</sup>

KPMG has reported that in 2018, global investment in FinTech companies hit \$111.8B with 2,196 deals.<sup>4</sup> Deloitte has reported that blockchain is going through a path of diffusion across industries far beyond its initial FinTech applications. More organizations from various sectors such as technology, media, telecommunications, life sciences, health care, and government are expanding and diversifying their blockchain initiatives.<sup>5</sup>

News in 2019 indicates the evolution of JP Morgan stable coin, Libra, Calibra, as well as Central Bank Digital Currencies (CDBC)s from the European Central Bank and The People's Bank of China towards FinTech. With this new development, blockchain has taken a series of steep move into standardising international network and recognising the system worldwide.<sup>6</sup> JP Morgan claimed to issue the 1:1 stable coin value redeemable in fiat currency held by J.P. Morgan.<sup>7</sup> Despite of it's still at prototype, the stable coin has been used among the markets and users under JP Morgan. At the stage of writing of this article, People Bank of China has drafted a law to propose revision that recognise Renminbi to include both a physical form and a digital form. Any individual or entity shall not make or issue any tokenized note or digital

---

<sup>3</sup> Ibid, KPMG Report on Biannual global analysis of investment in FinTech.p39.

<sup>4</sup> Ibid, KPMG Report on Biannual global analysis of investment in FinTech, p60.

<sup>5</sup> Refer to full report at [https://www2.deloitte.com/content/dam/Deloitte/se/Documents/risk/DI\\_2019-global-blockchain-survey.pdf](https://www2.deloitte.com/content/dam/Deloitte/se/Documents/risk/DI_2019-global-blockchain-survey.pdf) , retrieved, 25<sup>th</sup> of October 2020, at 4pm.

<sup>6</sup> Refer to <https://www.jpmorgan.com/solutions/cib/news/digital-coin-payments>, retrieved on 25<sup>th</sup> October 2020, at 3pm.

<sup>7</sup> Ibid, Published - February 14, 2019, retrieved at <https://www.jpmorgan.com/solutions/cib/news/digital-coin-payments>, retrieved on 25<sup>th</sup> October 2020, at 3pm.

tokens that replace the Renminbi's circulation in the market.<sup>8</sup> There seems to be a CBDC recognition in recognizing the creation of coins by the Central Bank. China PBoC has issued almost 3.13 million Central Bank Digital Currency (CBDC) transactions, totaling 1.1 billion yuan (about \$160 million dollars). Users were reportedly underwhelmed by the user interface in the DC/EP wallet. This is to be expected as a central bank often does not have expertise in user facing apps, even though the digital wallets were reportedly designed in association with commercial banks; as the Chinese CBDC uses a two-tier system for distribution.<sup>9</sup> Chinese users are long used to near field communications (NFC) based one tap payments. Alipay and Wechatpay dominate the country's payment landscape with more than \$60 Trillion a year flowing through those rails.<sup>10</sup> 2020 seems to be a promising year to accelerate the Blockchain investment with an increasing focus on companies interested in leveraging the technology to offer specific products. Addressing critical technical issues such as privacy, anonymity, data segregation and scalability will also be a high priority for blockchain investors. During the writing of this article, fear of transmitting the covid-19 virus could accelerate the trend of digital payment apps and reduce the use of cash in society. The spread of covid-19 has intensely motivated the use of digital currencies for its simplicity and able to cut the chain of transmitting disease.<sup>11</sup> This is further supported by the report issued by Bank of International Settlement (BIS) on microbiology research that despite the Scientific evidence suggests that the

---

<sup>8</sup> Refer Article 9 and 13 of the PBoC Bank Regulation available at [http://www.china.org.cn/business/laws\\_regulations/2007-06/22/content\\_1214826.htm](http://www.china.org.cn/business/laws_regulations/2007-06/22/content_1214826.htm) retrieved 9th January 2021 at 5.14 pm.

<sup>9</sup> Refer <https://blockchain.news/news/The-Peoples-Bank-of-China-Seeks-To-Prohibit-The-Creation-of-EYuan-Competing-Digital-Tokens> retrieved 24th Oct 2020, at 2pm.

<sup>10</sup> Ibid.

<sup>11</sup> Refer <https://theconversation.com/cash-and-the-coronavirus-covid-19-is-changing-our-relationship-with-money-138774> retrieved 31 oct 2020, at 3pm.

probability of transmission via banknotes is low, as global pandemic, serious attention are given to the cashless payment.<sup>12</sup>

Autoriti Monetary Brunei Darussalam (AMBD), Brunei's central bank, has issued a 'digital payment roadmap' with the objective to digitally transforming the country's finance sector. Under the title 'Digital Payment Roadmap for Brunei Darussalam 2019-2025', the document lays out key strategies towards a 'Digital Payment Nation' in line with the strategies presented in the Financial Sector Blueprint 2016-2025 (FSBP) and Wawasan 2035's (Vision 2035) aspirations towards a dynamic and diversified economy.<sup>13</sup> AMBD has adopted the regulatory sandbox approach that allows financial institutions and FinTech start-ups to test their innovative financial products and services in a safe environment before rolling out to the public.<sup>14</sup> AMBD's primary objective over this time horizon is to embrace digital transformation to the payments market in Brunei Darussalam, leading to the creation of a digital payment ecosystem involving both users and Payment Service Providers (PSPs), which may be banks or non-banks. This means migrating traditional payment behaviour and processes to innovative electronic channels. The stakeholders include the government, financial institutions, PSPs, telecommunication companies, businesses, retailers and customers.<sup>15</sup> Transforming digital payment comes in four pillars of digitization of payment, regulatory framework, promoting interoperability, greater acceptance and increase in the usage of digital payment and cross border integration between ASEAN countries<sup>16</sup>. Due to its' focus in regulatory reforming being

---

<sup>12</sup> Covid-19, cash, and the future of payments, BIS Bulletin No 3, Raphael Auer, Giulio Cornelli and Jon Frost, published 3<sup>rd</sup> April 2020 available at <https://www.bis.org/publ/bisbull03.pdf>, retrieved 31<sup>st</sup> Oct 2020, at 3.30pm.

<sup>13</sup> For details, refer to <https://www.ambd.gov.bn/Lists/Publications/Displayitem.aspx?ID=66> retrieved 4<sup>th</sup> of May 2020, 3am.

<sup>14</sup> Refer 'Digital Payment Roadmap for Brunei Darussalam 2019-2025', AMBD, p6

<sup>15</sup> Ibid, p4

<sup>16</sup> Ibid, p9

as one of the pillar, this paper intend to highlight several concerns that merits further attention of the policy makers.

### **Literature review**

Due to its rapid growth and unregulated and decentralised, it is a wakeup call from the regulators to ensure the market conduct are controlled. We have seen the growth in regulating market conduct since 2014 and the regulations has evolved fast in dealing with FinTech related activities. Below are several example of the regulations and precedent cases. In May 2014, Google v. Spain has sent shockwave when the European Court of Justice ruled that the European citizens have a right to request that commercial search firms, such as Google, that gather personal information for profit should remove links to private information when asked, provided the information is no longer relevant. Beginning in 2015, European Bankers Association has started to issue opinion on lending based crowd funding. Two months later, Financial Action Task Force (FATF) has issued FATF Guideline on risk based approach (RBA) to virtual currencies. European Supervisory Authorities (ESAs) has issued a joint Committee Report on the use of big data by financial institutions in December 2016. The Third District Court of Appeal in Florida highlights how laws have been evolving around the treatment of crypto currencies, prominent blockchain/digital currency lawyers say. A Florida appellate court reversed the court's prior 2016 decision by finding that crypto currency is indeed a financial or monetary instrument under state law<sup>17</sup>. IOSCO Report on FinTech in February 2017 has led to several reports and research conducted on market infrastructure, payment structure, business models and financial stability implications. In May 2017, Financial Stability Board has issued

---

<sup>17</sup> <https://teris.com/cryptocurrency-blockchain-recent-case-law/> accessed 4<sup>th</sup> of May 2019 at 4pm.

report on FinTech credit, market structure and financial implications on business models. Leveraging on this issue, European Banking Association has daragted recommendations urging the industry to adopt the Cloud Service Providers (CSP). In 2017 alone, we have seen four (4) reports so far being issued as follows;

1. FSB report on financial implications from FinTech.<sup>18</sup>
2. EBA reports on on innovative users of customer data by financial institutions.
3. EBA's approach to financial technology that was issued in August 2017.
4. The EBA's approach to financial technology thatw as issued on August.
5. FSB Report on financial sector syber security regulations, guidance and supervisory practices.
6. FSB report on artificial intelligence and machine learning in financial services.

Reaching 2018, we have seen series of regulations and mandates coming up to control and regulate the market conduct. Due to the high exposure and systemic risks imbued, the regulators have jointly issued additional guidelines and Standards for adoption. In Feb 2018, the Basel Committee has issued the Sound Practices for FinTech developments for banks and bank supervisors. The work was conducted in two main phases. First, the BCBS outlined the current FinTech landscape and supervisory approaches to FinTech developments, using industry research and surveys of member institutions. In the second phase, the BCBS identified the implications for banks and challenges for effective supervision, and conducted more detailed surveys on specific arrangements towards innovation and licensing practices. Began

---

<sup>18</sup> Financial Stability Implications from FinTech, Supervisory and Regulatory Issues, that Merit Authorities' attention, 27 June 2017.

in 2018, we have seen series of supervisory statements and report being published up to 2019.<sup>19</sup> In brief, the paper has covered the evolution of regulatory framework in FinTech related activities. Next part will be discussing the features of FinTech, DLT and blockchain and the implications from legal perspectives.

### **Distributed Ledger Technology (DLT)**

A “Distributed Ledger Technology” (DLT) is an amount of shared and synchronized digital data spread across multiple sites or institutions, with no central administrator or centralized data storage. A distributed ledger is a database that exists across several locations or among multiple participants. By contrast, most companies currently use a centralised database that lives in a fixed location. A centralised database essentially has a single point of failure.

A typical example of DLT is the blockchain system, which can be either public or private. The use of DLT and smart contracts for trade finance may imply several risks from a legal and practical perspective. Sometimes DLT (such as blockchain) operates in a various jurisdictions, with conflicting regulations. By way of example, a smart contract, or more simply, a contract signed by digital means may not be enforced in all the jurisdictions involved.

---

<sup>19</sup> Mar 2018 EU Commission legislative proposal for an EU framework on crowd and peer to peer finance, Mar 2018 EU Commission FinTech action plan, Jun 2018 PRA supervisory statement on algorithmic trading, Mar 2018 ECB guide to assessments of fintech credit institution licence applications, Jul 2018 FSB report on the work of the FSB and international standard-- setting bodies on crypto assets, Oct 2018 PRA, FCA and HMT report on crypto assets, Jul 2018 FCA consultation on loan - based (“peer-to-peer” - -’) and investment-based - crowdfunding platforms, Dec 2018 Basel Committee report on range of regulatory and supervisory practices on cyber security Dec 2018 ECB cyber resilience oversight expectations for financial market infrastructures, Dec 2018 EBA draft guidelines on technology and security risk management, Jan 2019 EBA report on crypto assets, Jan 2019 FCA guidance on crypto assets (regulatory perimeter), Jan 2019 ESAs Joint Committee report on regulatory sandboxes and innovation hubs, Jan 2019 ESAs Joint Committee report on regulatory sandboxes and innovation hubs Feb 2019 FSB report on fintech and market structure in financial services and Feb 2019 FSB Global monitoring report on non-bank financial intermediation. All these are available in <https://www.bis.org/bcbs/publ/d431.pdf>, accessed 4<sup>th</sup> of May 2019.

So, the overall legal scenario remains uncertain, despite some positive initiatives in certain jurisdictions.

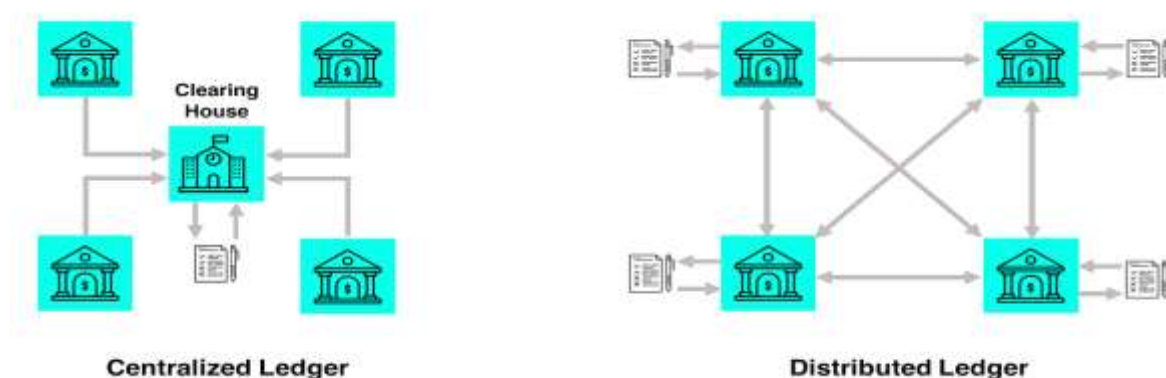


Diagram 1: centralised ledger v blockchain. Source: <https://tradeix.com/distributed-ledger-technology/>

However, a distributed ledger is decentralized to eliminate the need for a central authority or intermediary to process, validate or authenticate transactions. Enterprises use distributed ledger technology to process, validate or authenticate transactions or other types of data exchanges. Typically, these records are only ever stored in the ledger when the consensus has been reached by the parties involved.

All files in the distributed ledger are then time stamped and given a unique cryptographic signature. All of the participants on the distributed ledger can view all of the records in question. The technology provides a verifiable and auditable history of all information stored on that particular dataset.

As pointed above, the “Distributed Ledger Technology” (DLT) is sharing and synchronizing digital data used to spread across multiple sites or institutions, with no central administrator or centralized data storage. The system adopts data digitalization which is covered under Brunei Electronic Transaction Act 2001. This paper submits that in consonance of DLT definition, this may be categorised under sec 2 of “electronic record” which refers to a record generated,



communicated, received or stored by electronic, magnetic, optical or other means in an information system or for transmission from one information system to another;

- a) to facilitate electronic communications by means of reliable electronic records.

Furthermore the act stance with several objectives as follows;

- b) to facilitate electronic commerce, eliminate barriers to electronic commerce resulting from uncertainties over writing and signature requirements, and to promote the development of the legal and business infrastructure necessary to implement secure electronic commerce;
- c) to facilitate electronic filing of documents with government agencies and statutory corporations, and to promote efficient delivery of government services by means of reliable electronic records;
- d) to minimise the incidence of forged electronic records, intentional and unintentional alteration of records, and fraud in electronic commerce and other electronic transactions;
- e) to help to establish uniformity of rules, regulations and standards regarding the authentication and integrity of electronic records; and
- f) to promote public confidence in the integrity and reliability of electronic records and electronic commerce, and to foster the development of electronic commerce through the use of electronic signatures to lend authenticity and integrity to correspondence in any electronic medium.

Based on sec 2 above, this paper submits that any electronic records or digital data generated through decentralised ledger or centralised ledger are recognised under Brunei Law

to serve the objective of ETA 2001 as to facilitate electronic records, communications, commerce and digitalisation.

## Blockchain

Blockchain is one type of Distributed Ledger Technology and refers to a distributed public database which keeps a permanent and incorruptible record of digital transactions. Blockchain are unique in that they cannot be controlled by a single entity and have no single point of failure. Furthermore, blockchains can be programmed to store more than just financial information. This space includes companies involved in developing blockchain applications related to smart contracts, crowd funding, supply chain auditing, crypto currency, identity management, intellectual property and file storage<sup>20</sup>.

### Types of blockchain

			Read	Write	Commit	Example
Blockchain Types	O p e n	Public permissionless	Open to anyone	Anyone	Anyone*	Bitcoin, Ethereum
		Public permissioned	Open to anyone	Authorised participants	All or a subset of authorized participants	Sovrin <sup>21</sup>
	C l o s e d	Consortium	Restricted to an authorized set of participants	Authorized participants	All or a subset of authorized participants	Multiple banks operating a shared ledger
		Private permissioned (enterprise)	Fully private or restricted to a limited set	Network operator only	Network operator only	Internal bank ledger shared

<sup>20</sup> Ibid, KPMG Report on Biannual global analysis of investment in FinTech, p74.

<sup>21</sup> Sovrin is a decentralized, global public utility for self-sovereign identity. *Self-sovereign* means a lifetime portable identity for any person, organization, or thing. It's a smart identity that everyone can use and feel good about. Having a self-sovereign identity allows the holder to present verifiable credentials in a privacy-safe way. Retrieved <https://www.coinmarketplus.com/token/sovrin/> 20<sup>th</sup> March 2020 at 3pm.

			of authorized nodes			between parent company and subsidiaries
--	--	--	---------------------	--	--	-----------------------------------------

*Table 1: \*Requires significant investment either in mining hardware (proof-of-work model) or crypto currency itself (proof-of-stake model). FIGURE 1: Main types of blockchains segmented by permission model Source: Hileman, Garrick and Michel Rauchs. 2017. "Global Blockchain Benchmarking Study." Cambridge Centre for Alternative Finance.*

Permissioned ledgers are mostly used by industry conglomerates. All types of transaction required verification with nodes which require sign in for every block. The right to read data of the ledger may be public, partially public, or restricted to the participants. Private institutions like banks realized that they could use the core idea of blockchain as a distributed ledger technology (DLT), and create a permissioned blockchain (private or federated), where the validator is a member of a consortium or separate legal entities of the same organization. Federated Blockchains operate under the leadership of a group. As opposed to public Blockchains, they don't allow any person with access to the Internet to participate in the process of verifying transactions. Federated Blockchains are faster (higher scalability) and provide more transaction privacy. Consortium blockchains are mostly used in the banking sector. The consensus process is controlled by a pre-selected set of nodes; for example, one might imagine a consortium of 15 financial institutions, each of which operates a node and of which 10 must sign every block in order for the block to be valid. The right to read the blockchain may be public, or restricted to the participants. The term blockchain in the context of permissioned private ledger is highly controversial and disputed.

This is why the term distributed ledger technologies emerged as a more general term. Private blockchains are valuable for solving efficiency, security and fraud problems within traditional financial institutions, but only incrementally. It's not very likely that private

blockchains will revolutionize the financial system. Public blockchains, however, hold the potential to replace most functions of traditional financial institutions with software, fundamentally reshaping the way the financial system works. State of the art public blockchain protocols based on Proof of Work (PoW) consensus algorithms are open source and not permissioned.

Anyone can participate, without permission. Features are as follows;

- 1) Anyone can download the code and start running a public node on their local device, validating transactions in the network, thus participating in the consensus process – the process for determining what blocks get added to the chain and what the current state is.
- 2) Anyone in the world can send transactions through the network and expect to see them included in the blockchain if they are valid.
- 3) Anyone can read transaction on the public block explorer. Transactions are transparent, but anonymous/pseudonymous.

In addition to the above types, there are other types drawn by Chris Scanner (2020)<sup>22</sup> on blockchain as follows;

	Public	Private
Access	Open read/write	Permissioned read and/or write
Speed	Slower	Faster
Security	Proof of Work Other Mechanisms	Proof of Stake consensus Pre-approved participants
Identity	Anonymous Pseudonymous	Know identities
Assets	Native Asset	Any Asset

*Table 2: types of blockchain version 2 Chris Scanner Blog .source <https://thefinanser.com/2015/02/the-FinTech-scene-is-so-hot-its-boiling.html/>*

<sup>22</sup>Adopted from Handbook on Blockchain, via <https://s3.eu-west-2.amazonaws.com/blockchainhub.media/Blockchain+Technology+Handbook.pdf>, at 4pm 3<sup>rd</sup> March 2020.

## **Legal Issues and Implementation in Brunei**

Towards pursuing sophisticated blockchain and DLT system, several legal issues merit attention of the authority as follows;

### Data privacy

Many concerns raised as to the legal implications and impacts in applying FinTech, that worth considerable attention. A bank or companies that applies FinTech, tend to collect large amount of personal data and details of the customer. This may expose customers to data threat, personality theft, data stealing and all sort of cybercrimes. Hence, FinTech companies must ensure compliance with data protection laws and must prove to have adopted appropriate cyber security practices. Brunei has been guided by the Data Protection Policy 2014 (DPP2014) and the Data Protection that was issued under the responsible authority and accountability of the Minister at the Prime Minister's Office (as the Authority) and the compliance to this policy in the Government shall be ensured by the E-Government National Centre (as the Administrator).<sup>23</sup> Data refers all data including personal data in electronic or manual form that suits the criteria under DLT and blockchain.<sup>24</sup> As written in Art 19 of DPP 2014, it is a statutory requirement to conjunctively read the DPP 2014 with the Official Secrets Act (Chap 153), Protective Security Manual, JKDN, 2011 and the United Nations Guidelines concerning Computerized Personal Data Files<sup>25</sup> the UN Guideline has guaranteed ten (10) Principles of recognising protection of Data as enshrined in the DPP2014.

---

<sup>23</sup> Art 5.1 of the DPP 2014

<sup>24</sup> Art 2.1.11, DPP2014.

<sup>25</sup> the United Nations Guidelines concerning Computerized Personal Data Files

### Outsourcing information

In the outsourcing environment, cloud service providers (CSP) are expected to provide sufficient level of transparency.

Failure to do so could result in a material legal and security risk which are systemically imbued into the systems. Cross border transaction often comes within cross-jurisdictional implications towards recognising values and intended transactions. In Biometric authentication is one of the FinTech features. Its authentication is fragile for theft and being copied. Biometric authentication is able to be collected from everyday object the customers touch (Denton 2020). This may poses threat to consumer's rights and lead to cybercrime. As within Brunei context, the biometric protection as executed in several transactions such as the entry and exit the country. ETA 2001 seems to cover the biometric authentication as to be categorised under the electronic records and electronic signature. Sec 2 refers "electronic record" as a record generated, communicated, received or stored by electronic, magnetic, optical or other means in an information system or for transmission from one information system to another. On another note, "electronic signature" means any letters, characters, numbers or other symbols in digital form attached to or logically associated with an electronic record, and executed or adopted with the intention of authenticating or approving the electronic record. Despite of biometric word used in the Act, this paper submits that any record generated digitally or electronically, using by several means, this may fall under the definition of ETA 2001.

### Robo adviser

Robo advisers serves to facilitate in many areas. Robo adviser is still a 'new kids on the block'. Major of its use in FinTech involving advisory that is based on algorithmic and other technology-based programs with human intervention. Mayer Brown explains Robo-advisers as

a platform of advisers involving different levels of customers need. Some interaction may involve only a information and some even goes beyond offering investment portfolios. Others provide advice through investment advisory personnel using interactive platforms and models to generate investment recommendations that are then discussed with the client.<sup>26</sup> Robo advisers are tasked to analyse data, provide advice, conduct due diligence, provide views and information. The use of robo-advisers may expose threat of wrong advise, wrong analysis and incompetent due diligence. Robo-advisor may also be defined as the algorithm that can provide investment services to an investor.<sup>27</sup> A research conducted by World Bank in 2019, has shown that Robo-Adviser provide services beyond advisory which include comprehensive portfolio management services that allow individuals to plan and delegate their investment decisions<sup>28</sup>. In addition to portfolio allocations, the services provided can include portfolio rebalancing and tax management.<sup>29</sup> US has projected the aassets under management in the Robo-Advisors segment are projected to reach US\$682,726m in 2020. Assets under management are expected to show an annual growth rate (CAGR 2020-2024) of 25.3% resulting in a projected total amount of US\$1,683,165m by 2024.<sup>30</sup> Currently, there is no explicit legal framework for

---

<sup>26</sup> Robo-Advisers and Advisers Act Compliance, Mayerbrown, <https://www.mayerbrown.com/-/media/files/perspectives-events/events/2017/03/robo-advisers-and-advisers-act-compliance/files/presentation-slides/fileattachment/170330-chi-webinar-corpsec-roboadviser-slides.pdf>.

<sup>27</sup> Refer to Australian Securities and Investments Commission, Consultation Paper 254 Regulating digital financial advice and Draft Regulatory Guide 000 Providing digital financial product advice to retail clients, March 21, 2016.

<sup>28</sup> Refer Facundo Abraham Sergio L. Schmukler José Tessada, Robo-Advisors: Investing through Machines Research & Policy Briefs From the World Bank Chile Center and Malaysia Hub, published on No. 21, February 2019, retrieved via <http://documents1.worldbank.org/curated/en/275041551196836758/pdf/Robo-Advisors-Investing-through-Machines.pdf>.

<sup>29</sup> Robo-Advisors: Investing through Machines Research & Policy Briefs from the World Bank Chile Center and Malaysia Hub, published on No. 21, February 2019, retrieved via <http://documents1.worldbank.org/curated/en/275041551196836758/pdf/Robo-Advisors-Investing-through-Machines.pdf> at 4pm, 10<sup>th</sup> October 2020.

<sup>30</sup> For details on the figure, refer to <https://www.statista.com/outlook/337/robo-advisors>, retrieved on 30 Oct 2020, at 4pm.

robo advisers. However, robo-advisors could be categorized under the liability of investment companies (where the advice involving investment) where the investment law easily regulated under an investment company. This may attract provisions under the Banking Order 2006, Islamic Banking Order 2008, Companies Act 1956, and Finance Companies Act 2013. Indeed, this paper submits, due to complexity of the robo advisers and what turns out in future, there is a need for robo-adviser law in specific for which should be based on internationally recognized principles. The possibility of giving wrong information and data is relatively high. Robo adviser invites issues of liabilities and prone to legal suit for failure to provide sufficient information required.

#### Nodes of jurisdictional problems

Due to lack of centralised ledger, the ledger may as the nodes of a decentralized ledger stretches throughout different jurisdictions with different regulations with a risk of recognising the existence of blockchain.

#### The service Cloud Providers

The case of *Bodil Lindqvist v Aklagarkammaren i Jonkoping*, (Case C-101/01)<sup>31</sup> held that a data cannot be presumed to be transferred under the word “transfer,” which is not actually defined in the Directive, was intended to cover the loading by an individual of data onto an Internet page. A similar pragmatic approach is required for data on a blockchain to ensure that it is not “transferred” to every jurisdiction in which a node is present, causing unnecessary breaches of privacy regulations. The Lindqvist case indicates that merely uploading personal

---

<sup>31</sup> *Bodil Lindqvist v Åklagarkammaren i Jönköping* (CJEU, 6 November 2003) C-101/01, ECLI:EU:C:2002:513.



data to the Internet would not constitute a ‘transfer’, although that data could be accessed from any part of the world.<sup>32</sup>

### Accountability

The case of *Google Spain v AEPD*<sup>33</sup>, the Court of Justice of the European Union (CJEU) ruled that a search engine could be held accountable for the protection of personal data in respect of third party websites accessible through its service. It was emphasized in this case that the search engine’s activities could be clearly distinguished from those of the original publisher of the data. The harm to the data subject was not a result of the publication, but rather from the widespread availability of this information through a search engine. In *Google v. Spain*<sup>34</sup>, the European Court of Justice ruled that the European citizens have a right to request that commercial search firms, such as Google, that gather personal information for profit should remove links to private information when asked, provided the information is no longer relevant. The Court found that the fundamental right to privacy is greater than the economic interest of the commercial firm and, in some circumstances, the public interest in access to Information.

### ‘Right to be forgotten’ principle

The above principle explains the right to erasure to protect the rights of citizens applies to the controller or search engines like Google Inc. Principles have been developed since 1995, which

---

<sup>32</sup> Ibid

<sup>33</sup> Refer for detail via <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131>

<sup>34</sup> *Google Spain et al. v AEPD, Costeja Gonzales*, C-131/12 (CJEU, 13 May 2014) ECLI:EU:C:2014:317

is recorded in the EU Directive 95/46/EC.<sup>35</sup> In brief, the above principle is briefly explain below;

- a. The rights to be forgotten principle balanced between the citizen's protections of personal data while granting the media freedom of speech despite of moving forward economic growth, rights of citizens must be protected.
- b. The role which the person requesting the deletion plays in public life might also be relevant. And after all, this is about requests to remove irrelevant or outdated links, rather than the content they lead to that balance between the legitimate interests of internet users and citizens' fundamental rights.
- c. Search engines such as Google and other affected companies complain loudly. But they should remember this: handling citizens' personal data brings huge economic benefits to them. It also brings responsibility. These are two sides of the same coin, you cannot have one without the other.
- d. The right to be forgotten is already exists, and it is enshrined in the EU Data Protection Directive from 1995. Article 6 (1) (e) states that all Member States are to ensure that personal data must be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed". In addition, Article 12 (b) provide guarantees for every data subject on the right to obtain from the controller "*as appropriate the rectification, erasure or blocking of data the processing of which does not comply with*

---

<sup>35</sup> Refer Directive 95/46/EC is the reference text, at European level, on the protection of personal data. It sets up a regulatory framework which seeks to strike a balance between a high level of protection for the privacy of individuals and the free movement of personal data within the European Union (EU). To do so, the Directive sets strict limits on the collection and use of personal data and demands that each Member State set up an independent national body responsible for the supervision of any activity linked to the processing of personal data. Refer to [http://publications.europa.eu/resource/cellar/a10a0796-7521-4f45-8685-8e2b05cd65c4.0006.02/DOC\\_2](http://publications.europa.eu/resource/cellar/a10a0796-7521-4f45-8685-8e2b05cd65c4.0006.02/DOC_2), retrieved 28 Oct 2020 at 3am.

*the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data*". Therefore, in lieu of the above, Article 6 (1) (e) and Article 12 (b) of the Directive provides an implied salutation on 'the right to be forgotten'.<sup>36</sup>

- e. The judicial recognition of the right to be forgotten occurred in 2014 with the cornerstone *Google Spain SL v. Agencia Española de Protección de Datos*<sup>37</sup> decision. The Court rationale their decisions on the basis of *Google Spain* was selling advertising space in Spain and since advertising constitutes the main revenue for Google Inc. the two entities are "closely related" and thus Google Inc. is legally bound by the Directive.<sup>38</sup>

The above Right to be forgotten is a universal principle and may be recognised by the local internet provider. Despite of not being recognised in Brunei, the principle is recognisable worldwide. However, the ETA 2001 has given emphasise and acknowledged the 'international origin'.<sup>39</sup> The Act emphasises the recognition of its international origin in interpreting the Act. This is vital in promoting harmonisation, consistency and its implementation must be conducted in bona fide<sup>40</sup>. Further, Questions concerning matters governed by this Act which are not expressly settled in it are to be settled in conformity with the general principles on which this Act is based. When it comes to original origin, this paper submits that it may connote to accept the international norms.

---

<sup>36</sup> For details refer to <http://www.medialaws.eu/the-codification-of-the-right-to-be-forgotten-in-the-digital-era-from-directive-9546ec-to-the-general-data-protection-regulation/> t=retrieved 28Oct 2020 at 2am.

<sup>37</sup> *Google Spain SL v. Agencia Española de Protección de Datos Judgment of the Court (Grand Chamber), 13 May 2014.*

<sup>38</sup> Refer to <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131>, for full decisions by the European Court.

<sup>39</sup> Refer sec 3(2) of ETA 2001.

<sup>40</sup> Good faith.

There are several literatures<sup>41</sup> discussing the legal issues in blockchain and DLT. In Brunei, there are scarce discussion on this matter. The only law available as of to date, is the ETA 2001. However, the Act is silent on the operation of Decentralised Autonomous Organisations (DAOs), which is a subset of blockchain technology and therefore, a proper framework for DAO's is substantial. DAOs requires no human intervention in the process. Inventory, dealing trade, payment of bills, scanning the incoming shipment, invoicing, bills payment are all automated and there is absence of charges for labour and time.<sup>42</sup> However, there is possibility to riode over section 2 of the ETA on 'electronic record' which refers to a record generated, communicated, received or stored by electronic, magnetic, optical or other means in an information system or for transmission from one information system to another. The ReDLT and processes ledger are all automated and

In furtherance of materialising blockchain in future, there is a need of solid legal framework to operate within the blockchain network and real world. If the country were to allow crypto currencies to be implemented, a comprehensive regulatory framework for crypto currencies are required. This may include civil law, taxation, smart contract, data privacy, robo-adviser, etc. these legal framework are paramount to ensure control and supervisions are in place. Setting on the basis that these issues are surrounded with hackers and money laundering, by having a comprehensive framework it facilitates to mitigate crime.

---

<sup>41</sup> Refer to <https://blockchainhub.net/blockchain-law/> retrieved on 19<sup>th</sup> of February 2020 at 4am. The Blockchain & Law Working Group Berlin (BCLAW) is an informal group of lawyers, software developers, and entrepreneurs working with blockchain technology. In a series of meetings, the group has jointly identified a number of legal issues arising from the use of blockchain technology today and in the near future. The aim of the Blockchain & Law Working Group is to discuss those issues in depth within subgroups, based on a multi stakeholder approach

<sup>42</sup> <https://www.investopedia.com/news/daos-and-potential-ownerless-business/> retrieved 3pm 14<sup>th</sup> February

## Conclusion

In pursuing passion towards blockchain and DLT, it is substantial to establish certainty. Legal issues may affect its horizontal implementation. The above issues merits the authority's attention to further horizontalised this new technology. The above issues may have extended consequences as to the algorithmic trust, or trust by default of a legal contract. Open access to public network may affect the trust of legal relationship between the two parties. Therefore solid consensus towards trusted algorithm are required to ensure proof of work on the same protocol. This is important to avoid any arbitrary participants. Despite of n specific legislations concerning blockchain and DLT, there are several enabling provisions amiable for reference. However, due to comprehensive involvement of algorithm of liabilities resulted from rapid technology, this paper stance as comprehensive legal framework are necessary for future betterment.

## References

- AMBD. (2018). AMBD Guideline No. FTU/G-1/2017/1 on FinTech Regulatory Sandbox Report Mar 2018 ECB guide to assessments of fintech credit institution license applications. Brunei Darussalam
- Australian Securities & Investments Commission (2016). Providing digital financial product advice to retail clients. *Consultation Paper 254 Regulating digital financial advice and Draft Regulatory Guide 000*. Retrieved from: <https://download.asic.gov.au/media/3583174/attachment-to-cp254-published-21-march-2016.pdf>. Accessed on 24<sup>th</sup> October 2020.
- CJEU. (2003). Bodil Lindqvist v Åklagarkammaren i Jönköping C-101/01, ECLI:EU:C:2002:513.
- CJEU. (2014). Google Spain et al. v AEPD, Costeja Gonzales, C-131/12 ECLI:EU:C:2014:317. Retrieved from: <https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A62012CJ0131>. Accessed on 24<sup>th</sup> October 2020.
- CJEU. (2014). Google Spain et al. v AEPD, Costeja Gonzales, C-131/12 ECLI:EU:C:2014:31. Retrieved from: [https://curia.europa.eu/jcms/jcms/P\\_106311/en/](https://curia.europa.eu/jcms/jcms/P_106311/en/). Accessed on 24<sup>th</sup> October 2020.

- David, F. & Sarah G. (2019). *Cryptocurrencies: The Underlying Technology/ Cryptocurrencies in Public and Private Law*. Oxford University Press. United Kingdom.
- David, F. (2015). A \$480 Million Mystery: The Saga of Mt. Gox. Retrieved from: <https://www.nasdaq.com/articles/480-million-mystery-saga-mt-gox-2015-08-10>. Accessed on 13<sup>th</sup> February.
- David, M., Kathy, W., Brendan, M., Anjana, R., Jeff, M., Clinton, C., Anton, B., Timothy, B., Linda, F., Kimberley, L., Vanessa, K., Max, E., Wendy, N., & Maria, M. (2016). Distributed ledger technology in payments, clearing, and settlement. *Finance and Economics Discussion Series Division of Research & Statistics and Monetary Affairs, Federal Reserve Board*. Retrieved from: <https://www.fsb.org/wp-content/uploads/R270617.pdf>. Accessed on 10<sup>th</sup> February 2020.
- Deloitte (2019). Deloitte's 2019 Global Blockchain Survey: Blockchain gets down to business. Retrieved from: [https://www2.deloitte.com/content/dam/Deloitte/se/Documents/risk/DI\\_2019globalblockchain-survey.pdf](https://www2.deloitte.com/content/dam/Deloitte/se/Documents/risk/DI_2019globalblockchain-survey.pdf). Accessed on 25<sup>th</sup> of October 2020.
- Diego, O., & John, O. (2014). In Search of an Understandable Consensus Algorithm. *Proceedings of 2014 USENIX Annual Technical Conference, Philadelphia, PA*, Pg 305–319. 108
- EBA. (2019). Crypto assets, Jan 2019 FCA guidance on crypto assets (regulatory perimeter). Retrieved from: <https://www.bis.org/bcbs/publ/d431.pdf>. Accessed on 24<sup>th</sup> October 2020.
- ECB. (2018). Cyber resilience oversight expectations for financial market infrastructures. Retrieved from: [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf) Accessed on 24<sup>th</sup> October 2020.
- ESA (2019). Joint Committee report on regulatory sandboxes and innovation hubs. Retrieved from: <https://esas-joint-committee.europa.eu/Pages/ESAs-publish-joint-report-on-regulatory-sandboxes-and-innovation-hubs.aspx>. Accessed on 24<sup>th</sup> October 2020.
- EU Commission. (2018). Legislative proposal for an EU framework on crowd and peer to peer finance. Retrieved from: <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/1166-Legislative-proposal-for-an-EU-framework-on-crowd-and-peer-to-peer-finance>. Accessed on 24<sup>th</sup> October 2020.
- EU Commission. (2018). EU Commission FinTech action plan, Jun 2018 PRA supervisory statement on algorithmic trading. Retrieved from: <https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/policy-statement/2018/ps1218.pdf?la=en&hash=184D2F8CC94CB9316BC5DF2472A4D9CFD5637EF1>. Accessed on 24<sup>th</sup> October 2020.
- EU. Parliament and of the Council (1995). Directive 95/46/EC. Retrieved from: [http://publications.europa.eu/resource/ellar/a10a0796-7521-4f45-8685%208e2b05cd65c4.0006.02/DOC\\_2](http://publications.europa.eu/resource/ellar/a10a0796-7521-4f45-8685%208e2b05cd65c4.0006.02/DOC_2). Accessed on 24<sup>th</sup> October 2020.
- Facundo, Abraham, S. L. & Schmukler, J. T. (2019). Robo-Advisors: Investing through Machines Research & Policy Briefs from the World Bank Chile Center and Malaysia Hub. Retrieved from: <http://documents1.worldbank.org/curated/en/275041551196836758/pdf/Robo-Advisors-Investing-through-Machines.pdf>. Accessed on 24<sup>th</sup> October 2020.
- FCA. (2018). loan - based (“peer-to-peer”) and investment-based - crowdfunding platforms. Retrieved from: <http://documents1.worldbank.org/curated/en/275041551196836758/pdf/Robo-Advisors-Investing-through-Machines.pdf>. Accessed on 24<sup>th</sup> October 2020.

- FSB. (2018). Crypto-assets: Report to the G20 on work by the FSBV and standard setting bodies. Retrieved from: <https://www.fsb.org/wp-content/uploads/P160718-1.pdf>. Accessed on 30<sup>th</sup> October 2020.
- Godfrey, B. (2020). People's Bank of China Seeks to Prohibit the Creation of Digital Tokens. Retrieved from: <https://blockchain.news/news/The-Peoples-Bank-of-China-Seeks-To-Prohibit-The-Creation-of-EYuan-Competing-Digital-Tokens>. Accessed on 24<sup>th</sup> October 2020.
- Goodin, D. (2018). A 'tamper-proof' currency wallet just got backdoored by a 15-year-old. *arstechnica.com*. Retrieved from: <https://arstechnica.com/information-technology/2018/03/a-tamper-proof-currency-wallet-just-got-trivially-backdoored-by-a-15-year-old/>. Accessed on 13<sup>th</sup> February 2020.
- IAIS.(2017). *FinTech Developments in the Insurance Industry*. Retrieved from: <https://www.iaisweb.org/file/65625/report-on-fintech-developments-in-the-insurance-industry>. Retrieved on 13 February 2020.
- ISDA Whitepaper . (2017). Smart Contracts and Distributed Ledger – A Legal Perspective. Pg 8. Retrieved from: <https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-legal-perspective.pdf>. Retrieved on 13 February 2020.
- KPMG. (2018). Report on Biannual global analysis of investment in FinTech. Retrieved from: <https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/02/the-pulse-of-FinTech-2018.pdf>. Accessed on 13<sup>th</sup> of February 2020.
- KPMG. (). Regulation and supervision of FinTech Ever-expanding expectations
- KPMG. (2018). Report on Biannual global analysis of investment in FinTech. Retrieved from: <https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/02/the-pulse-of-FinTech-2018.pdf>. Retrieved on 13th of February 2020.
- Marc, R. & David, J., (2013). Updating the law of Information Privacy: The new framework of European Union. *Harvard Journal of Law and Public Policy*. Vol 36. Pg 605.
- Martine, R. (2014). The right to be forgotten and the EU data protection reform: Why we must see through a distorted debate and adopt strong new rules soon. *FLA World Library and Information Congress Lyon, France 18 August 2014*. Retrieved from: [https://ec.europa.eu/commission/presscorner/detail/en/SPEECH\\_14\\_568](https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_14_568) . Accessed on: 15th of February 2020.
- Mills, D., Wang, K., Malone, B., Ravi, A., Marquardt, J., , Chen, C., Badev, A., Brezinski, T., Fahy, L., Liao, K., Kargenian, V., Ellithorpe, M., Ng, W., & Baird, M. (2016).Financial Stability Implications from FinTech Supervisory and Regulatory Issues that Merit Authorities. Retrieved from:<https://www.fsb.org/wpcontent/uploads/R270617.pdf>. Accessed on 10th February 2020.
- Misha, K. (2020). Cash and the corona virus: Covid 18 is changing our relationship with money. Retrieved from: <https://theconversation.com/cash-and-the-coronavirus-covid-19-is-changing-our-relationship-with-money-138774>. Accessed on 30<sup>th</sup> October 2020.
- Morgan J.P. (2019). J.P. Morgan creates digital coin for payments. Retrieved from: <https://www.jpmorgan.com/solutions/cib/news/digital-coin-payments>. Accessed on 25<sup>th</sup> October 2020.
- Reuters (2016). Bitcoin Worth \$72M Was Stolen in Bitfinex Exchange Hack in Hong Kong. Retrieved from: <https://www.reuters.com/article/us-bitfinex-hacked-hongkong/idUSKCN10E0KP>. Accessed on 13<sup>th</sup> February 2020.

- Robert, M.M (2014). The inside Story of Mt. Gox, Bitcoin's \$460 Million Disaster. Retrieved from: <https://www.thedomains.com/2014/03/03/wired-the-inside-story-of-mt-gox-bitcoins-460-million-disaster/>. Accessed on 13<sup>th</sup> February 2020.
- Raphael, A., Giulio, C. & Jon, F. (2010). Covid-19, cash, and the future of payments, BIS Bulletin No 3. Retrieved from: <https://www.bis.org/publ/bisbull03.pdf>. Accessed on 31<sup>st</sup> October 2020.
- Robo, A. (2017). Advisers Act Compliance, Mayerbrown. Retrieved from: <https://www.mayerbrown.com/-/media/files/perspectives-events/events/2017/03/robo-advisers-and-advisers-act-compliance/files/presentation-slides/fileattachment/170330-chi-webinar-corpsec-roboadviser-slides.pdf>. Accessed on 24<sup>th</sup> October 2020.