

# Building a Successful Blockchain Ecosystem for India

---

## Regulatory Approaches to Crypto-Assets

An independent submission to the  
Government of India

December 2018

Nishith M. Desai

Vaibhav Parikh

Jaideep Reddy



---

# Building a Successful Blockchain Ecosystem for India

## **Regulatory Approaches to Crypto-Assets**

---

An independent submission to the Government of India

December 2018

**Nishith M. Desai**

**Vaibhav Parikh**

**Jaideep Reddy**

[blockchain.nda@nishithdesai.com](mailto:blockchain.nda@nishithdesai.com)

---

.....

**Disclosure:** Nishith Desai Associates is advising the Internet and Mobile Association of India in its writ petition in the Supreme Court of India against the Reserve Bank of India circular on Virtual Currencies dated April 6, 2018 (W.P. (C) No. 528 / 2018). However, the scope of the petition is restricted to the said circular, and the Union of India is not a party to it. The enclosed suggestions by the authors are made in an independent capacity, keeping in view the best interests of the public, the government, and the industry. They are not made on behalf of any organisation.

.....

To,  
Shri Subhash Chandra Garg,  
Secretary,  
Department of Economic Affairs,  
Ministry of Finance, Government of India,  
North Block,  
New Delhi - 110001.

December 10, 2018

*Dear Sir,*

Re: Paper titled 'Building a Successful Blockchain Ecosystem for India: Regulatory Approaches to Crypto-Assets'

We are delighted to learn that a High-Level Committee ("**Committee**") constituted under your Chairmanship is working on devising an appropriate legal framework with regard to crypto-assets, also referred to 'cryptocurrencies' or 'virtual currencies'.

As you may be aware, Nishith Desai Associates is a reputed India-centric global law firm and specialises in emerging and futuristic technologies. The authors' brief profiles are attached as **Annexure I** of the enclosed paper.

We have been regularly advising Indian and global entities on crypto-asset and blockchain-related legal issues since the early stages of the industry in India (circa. 2013), and have authored the firm's widely cited research papers on 'Bitcoin' and 'Blockchain'.<sup>1</sup> Recently, under the chairmanship of Lord Meghnad Desai, we have helped the Mauritius Financial Services Commission in developing and drafting an ecosystem for fintech, blockchain and digital assets.

With this background, we wish to present to you the enclosed paper, '*Building a Successful Blockchain Ecosystem for India: Regulatory Approaches to Crypto-Assets*' ("**Paper**"). The Paper puts forth our detailed suggestions to this Committee on the regulatory approaches that can be taken towards crypto-assets.

We note a recent press release by the Ministry of Finance which states that the Committee is considering a "*ban [on the] use of private crypto currencies in India.*"<sup>2</sup> We recognize the concerns of the Committee on the risks associated with crypto-assets. In fact, similar concerns remain true with other financial instruments such as cash and commodities such as gold. We would like to submit that a complete ban will be against the interests of innovation, liberty, and trade. No developed and democratic country has banned crypto-assets.

The G20 leaders in December 2018 have resolved, based on the Financial Action Task Force's (FATF) recommendations in October 2018, to regulate crypto-asset activity in order to ensure that the potential benefits of technology in the financial sector can be realized while risks are mitigated.<sup>3</sup> Countries like Australia, Canada, Japan, Singapore, South Korea, the U.K., and the U.S. have favoured a regulatory approach rather than a ban. A comparative table providing an overview of jurisdictional approaches to crypto-assets is produced at **Annexure II**. We would also like to draw the Committee's attention to the Final Report of the U.K.'s 'Cryptoassets Taskforce', consisting of HM Treasury, the Financial Conduct

---

1. <http://www.nishithdesai.com/information/research-and-articles/research-papers.html>

2. <http://pib.nic.in/newsite/PrintRelease.aspx?relid=184478>

3. [https://g20.org/sites/default/files/buenos\\_aires\\_leaders\\_declaration.pdf](https://g20.org/sites/default/files/buenos_aires_leaders_declaration.pdf), <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>

---

Authority, and the Bank of England (“**U.K. Task Force**”),<sup>4</sup> which considers a balanced yet strong and decisive approach. The said report was released as recently as October 29, 2018.

Drawing from international approaches and the authors’ own experience advising on the application of Indian law to crypto-assets, the enclosed Paper contains two parts:

- i. Reasons why regulation should be considered rather than a ban, and
- ii. Detailed regulatory measures that this Committee can consider. The regulatory measures proposed include:
  - a. The notification of crypto-asset business activity under the Prevention of Money Laundering Act;
  - b. A new licensing regime for crypto-asset business activity. This regime may be introduced either by:
    - i. New legislative provisions, such as under the newly proposed regimes on commodity spot trading and payment systems;
    - ii. Administrative regulations under existing laws including the Payment and Settlement Systems Act, the Non-Banking Financial Company regime, the Foreign Exchange Management Act, the Consumer Protection Act, and/or the Securities Contracts (Regulation) Act; and/or,
    - iii. Statute-backed self-regulation; and,
  - c. The active enforcement and clarification of existing laws with respect to crypto-assets.

Several of these suggested approaches (e.g., notification under the Prevention of Money Laundering Act) can be done with a minimum expenditure of time and resources. If new legislative provisions are introduced, they would help to clearly assign any regulatory vacuum with regard to crypto-assets to a given regulator, which would avoid jurisdictional ambiguity. Since SEBI has competence as regards investor protection, it is one option that can be considered in this connection.

The blockchain industry is intrinsically linked to crypto-assets. A ban on crypto-assets would therefore negatively affect the Indian blockchain software development ecosystem, and not just investors and traders. More and more blockchain players are quietly moving to foreign locations such as Singapore, which is resulting in a loss of skilled workforce.

Having acquired a deep knowledge of this industry, we are convinced that crypto-assets and blockchain technology should not be considered a mere conduit for illegal activities, but have genuine benefits to bring to the nation. These include financial inclusion and the growth of the Indian software ecosystem. We are joined by several eminent persons in this view.

We believe that the primary focus of the regulations should be how to contain the ‘bad actors’ in the digital ecosystem and make India an active participant in Industrial Revolution 4 (IR4). Balanced regulation would help India achieve this goal, whereas a prohibition would be an unfortunate step backward for the nation.

Before taking a decision, we would urge the Committee to conduct public consultations so that all relevant perspectives can be considered. The approach adopted by the Srikrishna Committee on the proposed data protection framework<sup>5</sup> may be followed in this connection.

Thank you for your time and consideration.

---

4. [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/752070/cryptoassets\\_taskforce\\_final\\_report\\_final\\_web.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf)

5. Committee of Experts on a Data Protection Framework for India under the chairmanship of (retd.) Justice B.N. Srikrishna (final report available at [http://meity.gov.in/writereaddata/files/Data\\_Protection\\_Committee\\_Report.pdf](http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf)).

Sincerely,



**Nishith M. Desai**

(nishith@nishithdesai.com)



**Vaibhav Parikh**

(vaibhav.parikh@nishithdesai.com)



**Jaideep Reddy**

(jaideep.reddy@nishithdesai.com)

Lawyers, Nishith Desai Associates.

---

*Copy to:*

Shri Ajay Tyagi,  
Chairman,  
Securities and Exchange Board of India,  
Plot No.C4-A, 'G' Block,  
Bandra-Kurla Complex, Bandra (East),  
Mumbai – 400051.

Shri Ajay Prakash Sawhney,  
Secretary,  
Ministry of Electronics and Information Technology,  
Government of India,  
Electronics Niketan, 6, CGO Complex,  
Lodhi Road, New Delhi – 110003.

Shri Sushil Chandra,  
Chairperson,  
Central Board of Direct Taxes,  
Department of Revenue,  
Ministry of Finance,  
Government of India  
North Block, New Delhi – 110001.

Shri B.P. Kanungo,  
Deputy Governor,  
Reserve Bank of India,  
Central Office Building,  
19<sup>th</sup> Floor, Shahid Bhagat Singh Road  
Mumbai – 400 001.

Dr. Rajiv Kumar,  
Vice Chairman,  
NITI Aayog,  
Sansad Marg,  
New Delhi – 110 001.



## About NDA

At Nishith Desai Associates, we have earned the reputation of being Asia's most Innovative Law Firm – and the go-to specialists for companies around the world, looking to conduct businesses in India and for Indian companies considering business expansion abroad. In fact, we have conceptualized and created a state-of-the-art Blue Sky Thinking and Research Campus, Imaginarium *Aligunjan*, an international institution dedicated to designing a premeditated future with an embedded strategic foresight capability.

We are a research and strategy driven international firm with offices in Mumbai, Palo Alto (Silicon Valley), Bangalore, Singapore, New Delhi, Munich, and New York. Our team comprises of specialists who provide strategic advice on legal, regulatory, and tax related matters in an integrated manner basis key insights carefully culled from the allied industries.

As an active participant in shaping India's regulatory environment, we at NDA, have the expertise and more importantly – the VISION – to navigate its complexities. Our ongoing endeavors in conducting and facilitating original research in emerging areas of law has helped us develop unparalleled proficiency to anticipate legal obstacles, mitigate potential risks and identify new opportunities for our clients on a global scale. Simply put, for conglomerates looking to conduct business in the subcontinent, NDA takes the uncertainty out of new frontiers.

As a firm of doyens, we pride ourselves in working with select clients within select verticals on complex matters. Our forte lies in providing innovative and strategic advice in futuristic areas of law such as those relating to Blockchain and virtual currencies, Internet of Things (IOT), Aviation, Artificial Intelligence, Privatization of Outer Space, Drones, Robotics, Virtual Reality, Ed-Tech, Med-Tech & Medical Devices and Nanotechnology with our key clientele comprising of marquee Fortune 500 corporations.

NDA has been the proud recipient of the RSG - FT award 4 times in a row (2014- 2017) as the 'Most Innovative Indian Law Firm' and in 2016 we were awarded the 'Most Innovative Law Firm - Asia Pacific,' by Financial Times (London.)

We are a trust based, non-hierarchical, democratic organization that leverages research and knowledge to deliver extraordinary value to our clients. Datum, our unique employer proposition has been developed into a global case study, aptly titled 'Management by Trust in a Democratic Enterprise,' published by John Wiley & Sons, USA.

---

## Accolades

A brief chronicle our firm's global acclaim for its achievements and prowess through the years –

- **Legal500:** Tier 1 for Dispute, Tax, Investment Funds, Labour & Employment, TMT and Corporate M&A 2019, 2018, 2017, 2016, 2015, 2014, 2013, 2012
- **Chambers and Partners Asia Pacific:** Band 1 for Employment, Lifesciences, Tax and TMT 2019, 2018, 2017, 2016, 2015
- **IFLR1000:** Tier 1 for Private Equity and Project Development: Telecommunications Networks. 2019, 2018, 2017, 2014
- **AsiaLaw 2019:** Ranked 'Outstanding' for Technology, Labour & Employment, Private Equity, Regulatory and Tax
- **RSG-Financial Times:** India's Most Innovative Law Firm 2017, 2016, 2015, 2014
- **Merger Market 2018:** Fastest growing M&A Law Firm
- **IFLR:** Indian Firm of the Year 2013, 2012, 2011, 2010
- **Asia Mena Counsel's In-House Community Firms Survey 2018:** Only Indian Firm for Life Science Practice Sector
- **Who's Who Legal 2019:** Global Thought Leaders - Nishith Desai (International Corporate Tax and Private Funds,) Dr. Milind Antani (Lifesciences) Vikram Shroff (HR and Employment Law,) and Vaibhav Parikh (Data Practices and Telecommunication)
- **IDEX Legal Awards 2015:** Nishith Desai Associates won the "M&A Deal of the year", "Best Dispute Management lawyer", "Best Use of Innovation and Technology in a law firm" and "Best Dispute Management Firm"

# Contents

<b>1. CRYPTO-ASSETS SHOULD BE REGULATED AND NOT BANNED</b>	<b>01</b>
I. Benefits of the Technology	01
II. Lessons from history	02
III. Counter-productive effects of an outright ban	02
A. Lack of traceability	03
B. Money laundering risk	03
C. Lack of consumer protection	03
D. Lack of market integrity	03
E. Capital flight risk	04
F. Loss of tax revenue	04
G. Lack of enforceability	04
H. Emigration of skilled workforce and startups	04
IV. Crypto-assets essential to blockchain technology	05
V. Susceptibility to legal challenge	06
VI. A balanced approach	07
<b>2. REGULATORY APPROACHES TOWARDS CRYPTO-ASSETS</b>	<b>08</b>
I. Each crypto-asset must be analyzed separately	08
II. Active enforcement of existing laws	09
III. Existing regulatory gap and suggestions to fill the gap	09
A. Nature of the current gap	10
B. Need for KYC/AML and licensing regimes	10
C. Drawing from global precedent	11
D. Who should be covered	11
E. KYC/AML regime - Designation under the PMLA	12
F. New licensing regime	12
i. Legislation	13
ii. Administrative regulation	13
a. Regulations under the PSS Act	14
b. Regulation as 'foreign currency' under the Foreign Exchange Management Act	14
c. Notification as Non-Banking Financial Company (NBFC)	15
d. Regulations under the Consumer Protection Act	15
e. Notifications under the SCRA	16
iii. Statute-backed self-regulation	16
IV. Clarifications and fine-tuning of existing laws	17



A.	FEMA (Export and Import)	17
B.	Information Technology Act	17
C.	Deposit-related laws	18
	i. Collective Investment Schemes	18
	ii. Prize Chits Act and Chit Funds Act	18
	iii. Companies Act and Companies (Acceptance of Deposits) Rules	18
	iv. Banning of Unregulated Deposit Schemes Bill (2018)	18
D.	Taxation	19
<b>3.</b>	<b>SUMMARY</b>	<b>20</b>
	<b>ANNEXURE I</b>	<b>21</b>
	Profiles Of The Authors	21
	<b>ANNEXURE II</b>	<b>22</b>
	Overview of Regulatory Approaches to Crypto-Assets by Significant Jurisdictions	22
	<b>ANNEXURE III</b>	<b>24</b>
	Draft Code of Self-Regulation for Virtual Currency Businesses in India	24



# 1. Crypto-Assets should be Regulated and not Banned

## I. Benefits of the Technology

While crypto-assets pose certain risks such as money laundering (which should be suitably addressed as suggested in this Paper), they are widely acknowledged as a breakthrough technology which enables disintermediation and transparency. The following benefits of crypto-assets have been recognized by Indian government authorities:<sup>1</sup>

- Control and security
- Transparency
- Very low transaction costs
- Instantaneous settlement of transactions
- Reduction of costs of cash
- Ability to provide a more comprehensive and unified source of credit history
- Reduction in instances of tax avoidance.

These features could be hugely beneficial to India which is seeking to be a digitally enabled society and trying to minimize the costs of intermediaries. For instance, India has been estimated by the World Bank in December 2018 to be the largest receiver of inward remittances globally, at USD 79.5 billion for 2018.<sup>2</sup> The same report of the World Bank also noted that the average cost of receiving remittances in South Asia was 5.4%, which would translate to a cost of approximately USD 4.29 billion, or approximately INR 30,600 crore, annually for India. Based on this year's Budget, this amount would fund India's Mid Day Meals scheme for about 3 years,<sup>3</sup> which shows the imperative need to reduce remittance costs. The World Bank report also observed *"[h]armonized regulation and adoption of innovative technologies could lower remittance costs by reducing intermediaries, enabling standardized and verifiable transactions, and smoothing AML/CFT regulatory processes."*

Further, a recent study by Incrypt, a non-profit organisation, based on a survey of 97 blockchain software developers in India, found that open, public blockchains (powered by crypto-assets) can be a new growth driver of the Indian economy, in a similar manner that the IT services industry was.<sup>4</sup> The study has noted that the blockchain ecosystem can drive growth in jobs, capital inflow, solutions to local problems, and technology convergence. The study was specifically focused on core software development activity and blockchain entrepreneurship, and was not aligned with any exchange or organisation dealing with crypto-assets.

---

1. The Report by the Institute for Development and Research in Banking Technology (IDRBT) titled "Applications of Blockchain Technology to Banking and Financial Sector in India" (January 2017); the Report of the Working Group on FinTech and Digital Banking (set up by the Reserve Bank of India) (November 2017); the Report of the "Committee on Digital Payments" constituted by the Ministry of Finance (Watal Committee Report) (December 2016).

2. <https://timesofindia.indiatimes.com/business/india-business/india-to-retain-top-position-in-remittances-with-80-billion-world-bank/articleshow/66998211.cms>, <https://www.knomad.org/publication/migration-and-development-brief-30>

3. [https://www.indiabudget.gov.in/OutcomeBudgetE2018\\_2019.pdf](https://www.indiabudget.gov.in/OutcomeBudgetE2018_2019.pdf)

4. <https://www.incrypt.co/policy>

---

## II. Lessons from history

Like electricity, railways, telecommunications, motor vehicles, aircrafts, mobile phones, and the Internet in the past, many are today concerned about the risks posed by crypto-assets. Like these other technologies, crypto-assets bring substantial benefits as well as risks, and in the early stages of the technology, the risks may appear to outweigh the benefits.

For instance, according to the Smithsonian Magazine, “[a]t the turn of the [20th] century, motor vehicles were handmade, expensive toys of the rich, and widely regarded as rare and dangerous.”<sup>5</sup> Similarly, according to the BBC, “[w]hen Faraday first generated electric power in 1831, there was a widespread fear of electric shocks”, and according to the Economist, “[i]n the 19<sup>th</sup> century, people worried that telegraph wires were affecting the weather, or were a form of black magic. Trains were thought to cause nervous disorders.”<sup>6</sup>

In the Indian context, taxi aggregators like Uber and Ola – which have become everyday services for many – initially faced bans by State governments.

However, with time, the benefits of these technologies and innovations became apparent, and they were regulated accordingly e.g., electricity, motor vehicles, and telecommunications are all now functioning under well-established regulatory regimes. Regulatory provisions were also introduced for taxi aggregators in India.

Today, a ban on the above innovations would be unthinkable to many. History has taught us that the regulation of new and disruptive technologies is more appropriate than prohibition. This applies squarely to crypto-assets.

## III. Counter-productive effects of an outright ban

An outright ban on the use, possession, and/or transfer of crypto-assets by the Central Government is likely not to achieve its objectives. If the objectives are to prevent money laundering, preserve market integrity, and increase consumer protection, regulation along the lines suggested subsequently in this Paper will be more appropriate than a prohibition.

It seems fairly clear that crypto-assets are not a passing fad. This is shown by the global unabated interest in crypto-assets, the acknowledgement of their technological and mathematical breakthroughs by various academic institutions and eminent personalities, and the millions of users in India currently.<sup>7</sup>

Banning the use of crypto assets in India will result in legitimate investments and trading being stopped, with illicit activities likely to continue. This is because crypto-assets are available to anyone using the Internet, without the need for any intermediary. As a result, all trading and usage would remain unreported. This is not mere conjecture, since it has already been shown by press reports after the Reserve Bank of India (RBI) circular dated April 6, 2018 (“**RBI Circular**”) that the prohibition on the use of banking channels for crypto-asset transactions led to an increase in cash transactions, *hawala* transactions, and *dabba* trading.<sup>8</sup> This has been acknowledged by the RBI in its latest Annual Report, which notes that after the RBI Circular, there may be increased usage of cash, dark pools and offshore trading.<sup>9</sup>

A prohibition is likely to be counter-productive for several reasons:

---

5. <https://www.smithsonianmag.com/innovation/when-pedestrians-ruled-streets-180953396/>

6. <https://www.economist.com/leaders/2005/03/23/the-shock-of-the-new>

7. <https://qz.com/india/1451706/modis-india-will-struggle-to-ban-bitcoin-other-cryptocurrencies>

8. [https://www.business-standard.com/article/markets/dabba-trading-comes-to-bitcoin-recent-rally-rbi-rule-add-fuel-to-fire-118072900606\\_1.html](https://www.business-standard.com/article/markets/dabba-trading-comes-to-bitcoin-recent-rally-rbi-rule-add-fuel-to-fire-118072900606_1.html)

9. <https://rbidocs.rbi.org.in/rdocs/AnnualReport/PDFs/OANREPORT201718077745EC9A874DB38C991F580ED14242.PDF>



## A. Lack of traceability

Crypto-assets can be stored and transferred using any device connected to the Internet. If there are no centralized platforms, persons transacting in crypto-assets may do so purely on a peer-to-peer level without any Know Your Customer / Anti-Money-Laundering (KYC/AML) being followed. Further, the Internet Protocol (IP) addresses of devices can be masked using Virtual Private Network (VPN) technology. All of this would make transactions impossible or nearly impossible to trace. Regulators would not be able ascertain the volume of transactions, the identity of parties, and the cross-border movement of crypto-assets.

## B. Money laundering risk

A ban would result in making the entire market for crypto-assets an underground market where trading happens either using cash or other untraceable consideration. This has already been seen in jurisdictions like China which have tried to implement bans.<sup>10</sup> Due to the minimal traceability, the money laundering risk is likely to exponentially increase rather than be mitigated, since unscrupulous elements may see it as an attractive avenue for money laundering.

## C. Lack of consumer protection

Assuming the ban leaves room for limited activity in crypto-assets (e.g., mining or storage), there would be a severe lack of consumer protection for those involved. Since a ban would likely not allow responsible domestic exchanges to operate (such operation is difficult even today as a result of the RBI Circular), those still interested in storing or transacting in crypto-assets may transact through offshore or undesirable domestic avenues. Many offshore businesses may not be responsible or regulated. Even domestically, a rampant grey market is likely to emerge to exploit the interest in crypto-assets and provide an avenue to those still interested in the industry.

Further, individuals would be storing crypto-assets without the help of any trusted party. As a result, since many individuals may not have the capacity or knowledge to maintain adequate cybersecurity practices, they may lose access to their crypto-assets through various means including hacking, loss of private key, compromise of access credentials, and malware attacks. There would be no central entity to look after the interests of consumers and take steps such as consumer education or helping to reverse mistaken transactions.

## D. Lack of market integrity

Similarly, assuming any transactions would still be permissible, any severe restriction, including one such as the current RBI Circular, would increase the speculation and market integrity concerns. In a grey market or purely cash market, there is likely to be price manipulation and limited opportunity for price discovery. Hence, persons holding crypto-assets (whom we understand number nearly 5-6 million currently in India)<sup>11</sup> run the risk of being severely exploited in a cash market.

---

10. <https://bitcoinist.com/china-cryptocurrency-tether-vpn-bypass-ban/>, <https://coingeek.com/crypto-activities-in-china-flourishing-despite-govt-ban/>

11. <https://qz.com/india/1451706/modis-india-will-struggle-to-ban-bitcoin-other-cryptocurrencies/>

---

## E. Capital flight risk

Apps, service providers and financial institutions based outside the country are likely to continue to service crypto-asset trade in India and target the millions of Indians interested in the industry. This has been recognized in the RBI's latest annual report. Not having the opportunity to use domestic platforms or trade domestically, persons interested in getting exposure to this asset class may look to participate in crypto-asset activity abroad, since they would be left holding assets for which they are not able to recoup any fiat currency in India. This would cause capital flight from India and defeat the purposes of the Foreign Exchange Management Act (FEMA).

## F. Loss of tax revenue

With nearly 5-6 million users in India as of date, and a market capitalization of between USD 8.6 (approx. INR 60,000 crore) and 43 billion (approx. INR 3,00,000 crore) in India (based on varied estimates as of May 2018),<sup>12</sup> the crypto-asset industry is a potentially lucrative revenue source for the government. The sale of crypto-assets could provide revenue to the government both in terms of income tax as well as Goods and Service Tax (GST). A ban would deprive the government of this revenue.

## G. Lack of enforceability

An outright prohibition on possession, use and transfer will also be nearly impossible to enforce from a technical perspective. As stated above, various jurisdictions which have imposed sweeping restrictions on Internet-based activity, including crypto-assets specifically, have not been able to enforce such restrictions effectively due to the use of multiple circumvention techniques such as VPNs. A mere ban through a law will be meaningless if it cannot be enforced.

## H. Emigration of skilled workforce and startups

As is well known, India possesses a skilled software development workforce. With the growth of blockchain technology, many Indian software developers have acquired skills in this technology as well. However, the Incrypt report, cited above, found that 84% of the blockchain developers surveyed believed that if the government does not allow crypto-assets, they may move abroad or only work on foreign projects / startups.<sup>13</sup> An outright ban on the use of crypto-assets would hence compel talented blockchain developers and promising startups to leave the country. Many have already started doing so as a result of the RBI Circular.

On the other hand, regulating crypto-assets by insisting on KYC/AML norms and licensing the intermediaries/exchanges would provide the government with a high degree of visibility over crypto-asset transactions. With stringent KYC, every transaction is traceable to a given identity. KYC/AML and licensing regimes would help protect consumers against irresponsible and fraudulent business activity by ensuring capital adequacy, consumer grievance redressal, market integrity, adequate disclosures, and strong cybersecurity. Such norms will also help enforce existing laws such as FEMA and tax laws due to the increased visibility over crypto-asset transactions. Importantly, such an approach will not stifle innovative activity by responsible and law-abiding persons and entities. This will allow the people of India to explore the potential of a new and promising technology, with due safeguards.

---

12. E.g., <https://qz.com/india/1181399/indias-love-for-bitcoin-is-strong-despite-rbi-and-government-warnings/>, <https://medium.com/the-mission/overview-of-the-indian-cryptocurrency-market-7e6e9e4f948a>, <https://coinmarketcap.com/historical/20180506/>

13. Page 22 of the said report.

## IV. Crypto-assets essential to blockchain technology

The government has on several occasions stated that it would like to promote the use of blockchain technology but discourage the use of crypto-assets.<sup>14</sup> However, crypto-assets are essential to blockchain technology. Blockchain without crypto-assets is a severely hampered system since crypto-assets create the incentive for decentralization, the very innovation of blockchain technology. To illustrate, many of the foremost industry implementations of blockchain, such as the Enterprise Ethereum Alliance, a global consortium of over 500 reputed institutions globally, including Accenture, Deloitte, Government of Andhra Pradesh, HP, Infosys, J.P. Morgan, Microsoft and Samsung, use crypto-assets for their implementations.<sup>15</sup> Similarly, a recent report regarding the use of blockchain technology by the local governments of Bankura and Durgapur in West Bengal for an implementation relating to birth certificates, which is a non-financial use case, too uses a crypto-token, 'LYNK'.<sup>16</sup>

The Incrypt report, which represents the voice of the technical blockchain community in India, has stated that the “*blockchain good, crypto bad*” ideology is not correct. Similarly, Sopnendu Mohanty, Chief Fintech Officer of the Monetary Authority of Singapore (MAS), speaking at the G20 forum in July 2018, has stated, “*I want to quash this false narrative that's been going around for the past two years that you can separate blockchain from crypto. You can't.*”

The reason is well explained by the following quotes of renowned experts in the field:

- Andreas Antonopoulos, author of the seminal books ‘The Internet of Money’, ‘Mastering Bitcoin’, and ‘Mastering Ethereum’, and a world-renowned crypto-asset and blockchain expert:

*“[W]hy do blockchains not work without an intrinsic, valuable asset that is the basis for a game theoretical model of security? The reason is simple. A blockchain, as a data structure, is a fairly inefficient data structure. The reason we use a blockchain is to achieve decentralisation. ...The best mechanism we've found so far for decentralising the process of validation is by having a consensus algorithm that depends on competition ... In order to have competition, you need risk and reward. In order to have a reward that is meaningful, you need an intrinsic token. You need something of value that people are trying to get, which keeps them playing fair. If you don't have something of value, you don't have a basis for that competition. Without a basis for that competition, you don't have security. ... Without decentralisation, there's no point in doing a blockchain. You might as well use a replicated database.”<sup>17</sup>*

- Vitalik Buterin, co-founder, Ethereum, which is the second largest blockchain at a market cap of approximately USD 12 billion at the time of drafting, has stated:

*“A public blockchain in particular would require cryptocurrency for it to exist for two reasons. One, to provide an economic incentive for miners. Second, to limit the amount of transactions a person could send by applying economic restrictions such as transaction fees. So if there is no cryptocurrency then at least public blockchains would not work. Private chains could if some kind of solution is developed but the blockchain as a system would be severely restricted.”<sup>18</sup>*

- Computer science researchers Dr. Arvind Narayanan, a professor at Princeton University, U.S.A. and an alumnus of the Indian Institute of Technology, Madras, and Dr. Jeremy Clark, a professor at Concordia University, Canada, in their paper ‘Bitcoin’s Academic Pedigree’, have observed:

---

14. E.g., the 2018 Budget Speech of Hon’ble Finance Minister Jaitley.

15. The Enterprise Ethereum Alliance uses the Ethereum blockchain, which natively has a crypto-asset, Ether.

16. <https://www.ccn.com/indian-state-government-will-issue-birth-certificates-on-a-blockchain/>

17. Extract of the auto-generated transcript of the video by Andreas Antonopoulos titled ‘Bitcoin Q&A: “Blockchain, not Bitcoin”’ available at <https://www.youtube.com/watch?v=r2f0HlaRdgo>.

18. <https://news.bitcoin.com/buterin-ban-russia-stifle-blockchains/>

---

*“In bitcoin, a secure ledger is necessary to prevent double spending and thus ensure that the currency has value. A valuable currency is necessary to reward miners. In turn, strength of mining power is necessary to secure the ledger.”<sup>19</sup>*

It is hence quite clear that crypto-assets present an integral economic incentive to the participants of a secure blockchain. While some kinds of private blockchains may exist without crypto-assets, these are confined to defined sets of parties, and are not open to all. Further such systems rely on trust between participants. Open, public blockchains on the other hand aim to rely largely on mathematics rather than trust, and do not restrict access to participants.

Hence, it would be near impossible to promote blockchain technology while banning the use of crypto-assets. Aiming to do so would be like allowing the Internet but not websites or emails.

## V. Susceptibility to legal challenge

A ban on the possession or trading of crypto-assets would impact the fundamental rights to trade, to privacy and liberty, and to be free from excessive and arbitrary State action,<sup>20</sup> as well as the constitutional right to property.<sup>21</sup> It is well-settled law that restrictions on fundamental rights are required to be proportional and rationally connected to the ends sought to be achieved.<sup>22</sup> Further, the Supreme Court of India has recognized that before a prohibition is imposed, lesser alternatives must be considered.<sup>23</sup>

For instance, in the recent *Puttaswamy* judgment,<sup>24</sup> where a 5-judge Bench of the Supreme Court was ruling on various issues in connection with the Aadhaar scheme, the majority held that the compulsory linkage of bank accounts and mobile numbers for all Aadhaar holders was unconstitutional as it was a sweeping move which was not proportionate to the ends sought to be achieved. They held that less restrictive measures were available and that the possibility of misuse by a few did not warrant a sweeping measure which intrudes on the rights of all.

In the case of crypto-assets, as shown above, a prohibition is likely to worsen the stated concerns rather than mitigate them. Further, several less restrictive alternatives to a ban are available. This is demonstrated by the approach of developed jurisdictions like Australia, Canada, the E.U., Japan, Singapore, South Korea, the U.S., and the U.K. These jurisdictions have opted against any kind of ban, and have instead aimed to mitigate the risks associated with the industry through KYC/AML norms and/or licensing regimes.

A sweeping prohibition depriving the entire population of access to a legitimate technological and financial opportunity, and leaving millions stuck with a ‘dead asset’, based on the danger of misuse by a few, is likely to be found disproportionate to the ends sought to be achieved.

A prohibition may therefore suffer from constitutional challenge.

---

19. <https://queue.acm.org/detail.cfm?id=3136559>.

20. Under Articles 14, 19, and 21 of the Constitution.

21. Under Article 300A of the Constitution.

22. E.g., *Justice K.S Puttaswamy (Retd.) v. Union of India & Ors.*, 2018 SCC OnLine SC 1642; *Papnasam Labour Union v. Madura Coats Limited & Anr.*, (1995) 1 SCC 501.

23. E.g., *State of Gujarat v. Mirzapur Moti Kureshi Kassab Jamat and Others*, (2005) 8 SCC 534

24. 2018 SCC OnLine SC 1642, *supra*.

## VI. A balanced approach

The Managing Director of the International Monetary Fund (IMF), Ms. Christine Lagarde, has stated,

*“just as a few technologies that emerged from the dot-com era have transformed our lives, the crypto-assets that survive could have a significant impact on how we save, invest and pay our bills. That is why policymakers should keep an open mind and work toward an even-handed regulatory framework that minimizes risks while allowing the creative process to bear fruit.”<sup>25</sup> (emphasis added)*

Similarly, the FATF has recommended a risk-based approach towards the regulation of crypto-assets.<sup>26</sup> It has, as recently as October 2018, recommended that crypto-asset service providers be regulated under an AML regime, and be licensed and monitored for this purpose.<sup>27</sup> It has also stated that the risk-based approach does not imply the automatic or wholesale denial of services to crypto-asset businesses without an adequate risk assessment.<sup>28</sup> The G20 leaders have, in their December 2018 declaration, endorsed the FATF recommendations, while stating that they will step up efforts to ensure that the potential benefits of technology in the financial sector can be realized while risks are mitigated.<sup>29</sup> India is a member of all of the above international organisations.

Academic theory too acknowledges that regulatory reactions should balance innovation and trade with consumer interests, and that prohibition is usually an excessive measure.<sup>30</sup>

Therefore, in our view, the only feasible governmental stance is balanced regulation and not any form of prohibition. We submit that the Committee should not consider a prohibition but must instead recommend a detailed regulatory strategy so that consumer interests can be protected while innovation and trade continues.

We have included our suggestions for such a strategy in Section 2 below.

---

25. <https://blogs.imf.org/2018/04/16/an-even-handed-approach-to-crypto-assets/>

26. <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>, <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>. The FATF materials refer to crypto-assets as ‘virtual currencies’ or ‘virtual assets’.

27. <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>

28. <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>

29. [https://g20.org/sites/default/files/buenos\\_aires\\_leaders\\_declaration.pdf](https://g20.org/sites/default/files/buenos_aires_leaders_declaration.pdf)

30. E.g., <https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=3910&context=facpubs>, <https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=2021&context=btlj>, <http://jolt.richmond.edu/jolt-archive/v16i1/article1.pdf>, <http://jolt.richmond.edu/jolt-archive/v16i1/article1.pdf>, <https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?referer=https://www.google.co.in/&httpsredir=1&article=1028&context=aubl>

---

## 2. Regulatory Approaches towards Crypto-Assets

### I. Each crypto-asset must be analyzed separately

What is a crypto-asset? According to the U.K. Task Force, “a cryptoasset is a cryptographically secured digital representation of value or contractual rights that uses some type of DLT [Distributed Ledger Technology] and can be transferred, stored or traded electronically.” Most crypto-assets have the common features that they can be stored in ‘wallets’, and that they can be traded on online platforms or ‘exchanges’. Both retail investors and professional traders may participate in such storage and trade, which comes to resemble participation in the commodities or securities market.

However, while much of the literature on the subject treats all crypto-assets alike for the purpose of legal analysis, there are over 1500 crypto-assets in existence,<sup>31</sup> each with its own unique technical characteristics.

While some, like Bitcoin, are mainly designed for value transfer, others can represent the underlying assets of the issuer (hence resembling securities), while still others can represent a right to use a software platform. Hence, we respectfully submit that any regulatory strategy treating all crypto-assets alike may be insufficient as it would overlook important distinctions between different crypto-assets.

In this light, the regulatory approaches of Switzerland<sup>32</sup> and the U.K.,<sup>33</sup> which classify crypto-assets into categories, may be useful. Both these jurisdictions have recognized **three** types of crypto-assets:

- a. **‘Payment tokens’ or ‘Exchange tokens’** – These tokens are used almost exclusively for value transfer, such as ‘Bitcoin’ and ‘Litecoin’.
- b. **‘Security tokens’ or ‘Asset tokens’** – These tokens represent rights in physical property, company shares, revenue streams, or other underlying assets or value. For instance, ‘DAO Tokens’ were concluded by the U.S. Securities and Exchange Commission (SEC) to be ‘securities’ under U.S. law.<sup>34</sup>
- c. **‘Utility tokens’** – These tokens represent the right of access to a digital product or service. For example, the token ‘Ether’ represents a right of access to the Ethereum network.

Under Indian law, payment tokens like Bitcoins may amount to intangible “goods” or “software”, while security tokens like DAO Tokens may amount to “securities”. Similarly, utility tokens like Ether may, in addition to being intangible “goods”, amount to a license fee paid to use the network. Certain crypto-assets, especially payment tokens, may also amount to “payment systems” requiring authorization, if there is an identifiable ‘operator’. Each crypto-asset and the way it is deployed hence has a different legal and tax import.

Note that a given crypto-asset can fall into more than one of the above categories. For example, the crypto-asset ‘Ether’ can be used both as a payment token and a utility token.

Following a case-by-case approach will allow legally compliant models to thrive, while fraudulent or non-compliant models are prosecuted.

---

31. According to the leading ranking site, coinmarketcap.com.

32. <https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/>

33. [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/752070/cryptoassets\\_task\\_force\\_final\\_report\\_final\\_web.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_task_force_final_report_final_web.pdf), at p. 11.

34. <https://www.sec.gov/news/press-release/2017-131>

## II. Active enforcement of existing laws

As suggested in detail below, since crypto-assets pose certain unique legal questions not fully addressed by existing laws, new legal provisions should be introduced where gaps exist in the current system. However, meanwhile, enforcing existing laws, including the following, on a case-by-case basis will work to effectively regulate a vast amount of crypto-asset activity:

- Consumer Protection Act
- FEMA
- Goods and Services Tax (GST) Acts
- Income Tax Act
- Indian Penal Code
- Information Technology Act
- Payment and Settlement Systems Act (PSS Act)
- Prevention of Money Laundering Act (PMLA)
- Prize Chits and Money Circulation Schemes (Banning) Act (“**Prize Chits Act**”)
- Securities Contracts (Regulation) Act (SCRA)
- Securities and Exchange Board of India (SEBI) Act.

Regulators should carefully assess the applicability of existing laws to each crypto-asset or class of crypto-assets prevalent in India and take suitable steps accordingly.

For instance, rather than taking a blanket approach, the U.S. SEC has carried out various investigations and enforcement actions into different types of crypto-assets, finding that some are ‘securities’ and others are not.<sup>35</sup> Similarly, in India, enforcement action has been taken against allegedly fraudulent businesses like OneCoin<sup>36</sup> and GainBitcoin<sup>37</sup> under the Indian Penal Code and the Prize Chits Act. This shows that action can be taken based on the nature of particular schemes, without impacting the entire industry including *bona fide* businesses. It also shows that existing Indian laws in many cases have teeth to deal with fraudulent action involving crypto-assets.

## III. Existing regulatory gap and suggestions to fill the gap

While many features of crypto-assets can be regulated under existing laws (as shown above), certain gaps exist which merit new legal provisions. This section discusses the nature of such gaps and the new legal provisions that can be considered. Many such suggestions are easy to implement since they involve the mere notification of crypto-asset business activity under the purview of well-established existing regimes (e.g., PMLA).

---

35. <https://www.sec.gov/ICO>

36. <https://timesofindia.indiatimes.com/city/navi-mumbai/one-coin-fraud-18-in-cop-custody/articleshow/58439996.cms>

37. <https://indianexpress.com/article/india/bitcoin-fraud-amit-bhardwaj-director-of-firm-involved-in-rs-2000-crore-scam-arrested-5124244/>

---

## A. Nature of the current gap

Throughout history, new technologies, due to their unique nature, have merited new, *sui generis* regulation for consumer protection e.g., for telecommunications, the Indian Telegraph Act, and for the Internet, the Information Technology Act. A recent example is the RBI's regime governing prepaid payment instruments.

As far as crypto-assets are concerned, we may analyze the nature of the regulatory gap by looking at each of the three categories set out above (payment tokens, utility tokens, and security tokens).

For tokens which are "securities" under the SCRA, only "recognized stock exchanges" may facilitate the trading of such tokens. SEBI will therefore have the jurisdiction to regulate such trading. As far as such tokens are concerned, therefore, the current regulatory regime is sufficient.

However, payment tokens and utility tokens, such as Bitcoin and Ether, are often in the nature of digital "goods",<sup>38</sup> more particularly, intangible software goods. This being the case, the spot trading of such crypto-assets would be treated, under current law, as the sale and purchase of digital goods online, such as the sale and purchase of e-books or music files on e-commerce sites.

Trading on e-commerce marketplaces does not have a *sui generis* regulatory regime, and is by and large regulated by:

- The Consumer Protection Act, for any deficiency in services.
- The RBI's 'Directions for opening and operation of Accounts and settlement of payments for electronic payment transactions involving intermediaries' (2009) ("**Intermediaries Direction**"),<sup>39</sup> if the delivery of the digital goods is not immediate / simultaneous upon payment (DvP).<sup>40</sup>

The same analysis will apply to crypto-asset marketplaces/exchanges and crypto-asset wallet providers which enable the buying, selling and/or storage of utility tokens and payments tokens. There are no statutory KYC/AML requirements or any licensing or capital adequacy requirements which apply to such marketplaces.

In our view, this presents a significant regulatory gap because crypto-asset wallet providers and exchanges are often placed in a position of trust with respect to consumer funds (whether stored in Indian Rupees or crypto-assets). Further, money laundering and fraud risks may arise on platforms which do not voluntarily follow KYC/AML norms and other responsible practices.

A regulatory strategy is therefore necessary to help further the interests of consumer protection and market integrity, and guard against money laundering.

## B. Need for KYC/AML and licensing regimes

Due to the gaps pointed out above, it is necessary to regulate crypto-asset business activity under a new set of legal provisions: (i) a KYC/AML regime, and (ii) a licensing regime.

---

38. This is our interpretation based on the Supreme Court's judgment in *Tata Consultancy Services v. State of Andhra Pradesh*, AIR 2005 SC 371. We note that certain payment tokens, depending on their nature, may amount to "payment systems" or "prepaid payment instruments" requiring authorization under the Payment and Settlement Systems Act. Such tokens would not be able to be very easily traded as "goods" on exchanges, owing to the Know Your Customer (KYC) norms that would have to be followed by a payment system operator when an account changes ownership.

39. <https://www.rbi.org.in/scripts/NotificationUser.aspx?Mode=0&Id=5379>

40. See Clause 2.1, Intermediaries Direction: "For the purpose of these directions, all intermediaries who facilitate delivery of goods/ services immediately/simultaneously (e.g. Travel tickets/movie tickets etc) on the completion of payment by the customer shall not fall within the definition of the expression "intermediaries". These transactions which are akin to a Delivery versus Payment (DvP) arrangement will continue to be facilitated as per the contracts between the merchants and the intermediaries as hitherto and banks shall satisfy themselves that such intermediaries do not fall within the definition of the "intermediaries" when they open accounts other than internal accounts."



- i. **Compliance with KYC/AML norms:** This will help to prevent and detect the use of crypto-assets for money laundering, terrorism financing, fraud, and other economic offences.
- ii. **Licensing regime:** This will help in consumer protection through suitable financial adequacy and prudential measures like reserves and/or insurance, cybersecurity standards, disclosures, and a complaints redressal mechanism. The licensing regime would also work to guard against fraudulent practices of crypto-asset businesses. There should be a suitable threshold of covered entities, under which only entities holding crypto-assets in trust on behalf of consumers are regulated, and exemptions apply for personal use and other suitable categories. To make an analogy, the licensing regime can be broadly compared to the licensing regime for payment system operators.

## C. Drawing from global precedent

When considering the regulatory strategy on crypto-assets, guidance can be drawn from other jurisdictions which have already had detailed deliberations and consultations on this issue.

The Uniform Law Commission in the U.S.<sup>41</sup> has proposed a draft legislation on the subject, the ‘Uniform Regulation of Virtual Currency Businesses Act’ (“**ULC Model Law**”), after considering the views of policy makers, members of the public, non-profit organizations, and leading industry members. The ULC Model Law appears to be a balanced, well-thought out framework that accommodates interests of multiple stakeholders. While the ULC Model Law was framed in the American context, we submit that it can be suitably adapted to the Indian context as necessary. Moreover, crypto-assets are a global concept rather than a jurisdiction-specific one, making global precedents easily adaptable to the Indian context. The latest draft of the ULC Model Law is available at the link provided in the footnote.<sup>42</sup>

## D. Who should be covered

The ULC Model Law regulates “virtual currency business activity”, which refers to exchanging, transferring, or storing virtual currency with or on behalf of individuals or issuing redeemable virtual currency.<sup>43</sup>

We submit that this definition covers the activities which currently under Indian law do not have a specific regulatory regime, and hence is suitable to be adopted in the Indian context. Please note that while the ULC Model Law uses the term ‘virtual currency’, Indian law can use the term ‘crypto-asset’ due to the consensus now emerging on the use of this term (e.g., the Hon’ble Finance Minister’s use of the term in the 2018 Budget Speech). The new regime can also confine its scope to crypto-assets which do not amount to “securities” (since dealing in securities is already regulated by SEBI and under the Companies Act).

41. The Uniform Law Commission was established in 1892 to provide U.S. states with non-partisan, well-conceived and well-drafted legislation, and its members are practicing lawyers, judges, legislators and legislative staff, and law professors.

42. <http://www.uniformlaws.org/Act.aspx?title=Regulation%20of%20Virtual-Currency%20Businesses%20Act>.

43. The full definition reads as below:

“Virtual-currency business activity” means:

- (A) exchanging, transferring, or storing virtual currency or engaging in virtual-currency administration, whether directly or through an agreement with a virtual-currency control-services vendor;
- (B) holding electronic precious metals or electronic certificates representing interests in precious metals on behalf of another person or issuing shares or electronic certificates representing interests in precious metals; or
- (C) exchanging one or more digital representations of value used within one or more online games, game platforms, or family of games for:
  - (i) virtual currency offered by or on behalf of the same publisher from which the original digital representation of value was received; or
  - (ii) legal tender or bank credit outside the online game, game platform, or family of games offered by or on behalf of the same publisher from which the original digital representation of value was received.”

And,

“Virtual-currency administration” means issuing virtual currency with the authority to redeem the currency for legal tender, bank credit, or other virtual currency.”

---

## E. KYC/AML regime - Designation under the PMLA

Since the PMLA is the definitive Indian law on KYC/AML, crypto-asset businesses may be brought under the PMLA as suggested below.

The PMLA regulates “reporting entities”, i.e., any entity which is a “*banking company, financial institution, intermediary or a person carrying on a designated business or profession*”.<sup>44</sup> Currently a “person carrying on a designated business or profession” includes real estate agents, game operators, precious metals dealers, and others.<sup>45</sup>

Significantly, the Central Government has the power to notify any other activities to be regulated as a “designated business or profession”. It is our submission that the Central Government should notify crypto-asset business activity as a “designated business or profession”. This would automatically bring all such businesses within the framework of the PMLA, including the ‘Client Due Diligence’ requirements under Rule 9 of the Prevention of Money-Laundering (Maintenance of Records) Rules.

This would go a long way towards mitigating any money laundering risks associated with crypto-assets.

Meanwhile, the RBI in any event has the power under the Prevention of Money-Laundering (Maintenance of Records) Rules to “*prescribe enhanced or simplified measures to verify the client's identity taking into consideration the type of client, business relationship, nature and value of transactions based on the overall money laundering and terrorist financing risks involved.*”<sup>46</sup> This would appear to be the suitable power of the RBI to require its regulated entities to take enhanced client due diligence measures with respect to crypto-asset businesses.<sup>47</sup> In this manner, the RBI can implement a risk-based approach and alleviate concerns of money laundering, while avoiding a complete prohibition on supporting such businesses. This would enable responsible and credible businesses to operate in a regulated fashion. With such an approach, the current RBI Circular may not be necessary.

Most developed jurisdictions, including Australia, Canada, the E.U., Japan, South Korea, and the U.S., have brought crypto-asset business activity within their AML regimes or recommended heightened AML rules for crypto-asset business activity. Such an approach has also been recommended by the FATF.

## F. New licensing regime

A new licensing regime would mandate obligations such as financial adequacy, audits, and reporting for crypto-asset businesses. As stated above, the licensing regime can be broadly compared to the licensing regime for payment system operators. The licensing regime cannot be expected to be a panacea for all the risks associated with all the crypto-assets. Rather, various existing laws – as pointed out above – will apply to many crypto-asset activities. However, a new licensing regime would be targeted towards further ensuring consumer protection.

---

44. Section 2(wa).

45. Section 2(sa).

46. “9. *Client Due Diligence. ... (14) The regulator shall issue guidelines incorporating the requirements of sub-rules (1) to (13) and sub-rule (15) and may prescribe enhanced or simplified measures to verify the client's identity taking into consideration the type of client, business relationship, nature and value of transactions based on the overall money laundering and terrorist financing risks involved. Explanation.—For the purpose of this clause, simplified measures are not acceptable whenever there is a suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply or where the risk identified is not consistent with the national risk assessment.*”

47. We note that, as of date, this question does not arise due to the RBI Circular.

The question arises as to what legal mechanism should be used to implement such a licensing regime. The possible mechanisms are discussed under three heads: (i) legislation, (ii) administrative regulation, and (iii) self-regulation.

## i. Legislation

The licensing regime for crypto-asset business activity may be brought in through new legislative provisions.<sup>48</sup> Independent, international think-tanks and policy bodies like the Uniform Law Commission and Coin Center have suggested that a new *sui generis* legislation for crypto-assets is a superior approach to administrative regulations under existing laws.<sup>49</sup> The strengths of such an approach are that it increases certainty and is not subject to excessive administrative discretion.<sup>50</sup>

New legislative provisions also have the advantage of clearly designating a given regulator to address the vacuum. This helps avoid any jurisdictional ambiguity that may exist under existing laws and builds up the institutional capacity to effectively regulate the technology.

### *Committee Reports on the PSS Act and Commodity Spot Market*

We note that the ‘Report of Expert Committee on Integration of Commodity Spot and Derivatives Markets’ (chaired by Prof. Ramesh Chand)<sup>51</sup> on the commodity spot market has suggested a new regulatory regime for commodity spot markets in non-agricultural commodities like base metals, precious metals, and energy commodities. Since many crypto-assets can be characterized as “goods” (albeit intangible goods), it is in our view worth considering bringing spot trading of crypto-assets under the new regime proposed by the said committee. For this, crypto-assets of suitable nature will have to be notified as “commodities” under the new regime.

We also note the recent recommendations of the ‘Inter-Ministerial Committee for Finalisation of Amendments of the PSS Act, 2007’ and the proposal of a new Payment and Settlement Systems Bill.<sup>52</sup> The said committee has noted on page 58 of its report (‘Analysis of comments from the Department of Legal Affairs’) that ‘spot exchanges’ would be implicitly covered under the said Bill since *“any exchange which is not authorised under any law and seeks to operate a payment system shall require authorisation under the proposed Bill.”* Hence, the said Bill if passed in its current form is likely to create the requirement of a license for crypto-asset exchanges. This Committee may note this possibility.

Bringing the spot trading of crypto-assets within the umbrella of these proposed regimes, which are already being considered, would save the resources which would have to be expended for an altogether new regime. However, pure crypto-asset wallet or custody providers may not be covered under either of the above regimes since one may argue that they are not operating “payment systems” or facilitating “spot trading”.

## ii. Administrative regulation

Although the legislative route is in our view preferable, an alternative route for the licensing regime is the framing of administrative regulations or directions under existing legislation. However, such regulations or directions need to be confined to the bounds of the parent statute. Here, we may consider various enabling legislations:

48. Since the crypto-asset market is large and the interests of consumers should be protected as soon as possible, and noting that the Parliamentary process is robust but time-consuming, the implementation of the licensing regime through an Ordinance under Article 123 of the Constitution may also be considered. However, such an Ordinance is liable to lapse if not approved within six weeks of Parliament’s reassembly.

49. <https://coincenter.org/entry/state-digital-currency-principles-and-framework>, [http://www.uniformlaws.org/shared/docs/regulation%20of%20virtual%20currencies/2015oct\\_RVCA\\_Mtg%20Draft.pdf](http://www.uniformlaws.org/shared/docs/regulation%20of%20virtual%20currencies/2015oct_RVCA_Mtg%20Draft.pdf)

50. <https://coincenter.org/entry/state-digital-currency-principles-and-framework> at page 5.

51. [https://dea.gov.in/sites/default/files/ReportCommodityDerivativeMarkets042018\\_0.pdf](https://dea.gov.in/sites/default/files/ReportCommodityDerivativeMarkets042018_0.pdf)

52. <https://dea.gov.in/sites/default/files/Payment%20and%20settlement.pdf>

---

## a.Regulations under the PSS Act

Sections 10, 18, and 38 of the PSS Act give the RBI the power to frame regulations, directions, and guidelines. For example, this is the power used by the RBI to promulgate the Master Direction on Prepaid Payment Instruments.<sup>53</sup>

Crypto-asset trading platforms too may be brought within a licensing regime under the PSS Act through such regulations.<sup>54</sup> The first consequence of this such businesses would have to put in place the same robust KYC measures being put in place by banks, NBFCs, and payment system operators, since they would become entities regulated by the RBI.<sup>55</sup> In addition, the RBI can license and audit crypto-asset businesses and regulate their financial adequacy, hence increasing consumer protection.

However, the jurisdiction of the regulation will be constrained to “payment systems” as defined under the PSS Act,<sup>56</sup> and will not cover business models that are not operating payment systems. As a result, some may argue that the regulation should only cover crypto-asset exchanges and not other models where crypto-assets are being held in trust for consumers (e.g., crypto-asset custodians / wallet service providers).

The above approach would require appropriate exemptions to be made in the RBI Circular, since RBI-regulated entities are currently completely prohibited from dealing with, or facilitating trading in, virtual currencies under the said circular.

## b.Regulation as ‘foreign currency’ under the Foreign Exchange Management Act

Under FEMA, the following actions are regulated: dealing in foreign exchange; selling or drawing foreign exchange (current account and capital account transactions); export of goods and services; and realising and repatriating foreign exchange.

Crypto-assets which are not ‘securities’ are likely to fall within the concept of ‘goods’ and ‘software’ under FEMA,<sup>57</sup> and the legal implications under FEMA will then flow accordingly (as discussed in paragraph IV(A) below).

However, FEMA also defines the term ‘currency’. It means “*all currency notes, postal notes, postal orders, money orders, cheques, drafts, travellers cheques, letters of credit, bills of exchange and promissory notes, credit cards or such other similar instruments, as may be notified by the Reserve Bank.*”<sup>58</sup> (emphasis added) Under an RBI notification, “*debit cards, ATM cards, or any other instrument by whatever name called that can be used to create a financial liability*” (emphasis added) amount to ‘currency’.<sup>59</sup>

---

53. [https://rbi.org.in/scripts/BS\\_ViewMasDirections.aspx?id=11142](https://rbi.org.in/scripts/BS_ViewMasDirections.aspx?id=11142)

54. Such regulations can also be introduced under the proposed Payment and Settlement Systems Bill (when passed), since the said Bill would cover crypto-asset exchanges, as discussed above.

55. The RBI’s KYC Directions will apply to such entities. See clause 2(a) of the said Directions: “*The provisions of these Directions shall apply to every entity regulated by Reserve Bank of India, more specifically as defined in 3 (b) (xiii) below, except where specifically mentioned otherwise.*”

56. Under Section 2(1)(i), “*‘payment system’ means a system that enables payment to be effected between a payer and a beneficiary, involving clearing, payment or settlement service or all of them, but does not include a stock exchange.*”

57. See regulation 2(viii), Foreign Exchange Management (Export of Goods & Services) Regulations, 2015 (“*‘software’ means any computer programme, database, drawing, design, audio/video signals, any information by whatever name called in or on any medium other than in or on any physical medium*”).

58. Section 2(h).

59. Notification No. FEMA 15 (R)/2015 - RB

FEMA states that any currency other than Indian currency is ‘foreign currency’. Indian currency is restricted to any currency expressed in Indian rupees. Therefore, if any crypto-asset can be said to “create a financial liability”, it may amount to ‘foreign currency’.

If that is the case, the RBI may regulate the drawing of such crypto-assets under FEMA, such that only ‘authorised persons’ are permitted to deal in foreign currency. This will have the advantage of creating an already well-established regulatory mechanism for those who deal in such types of crypto-assets, since they will be subject to all the safeguards that authorised persons are subject to. On the other hand, the RBI will have to identify which crypto-assets have the feature of creating a financial liability, and which do not.

Also, as stated above, the above approach would require appropriate exemptions to be made in the RBI Circular, since authorised persons, being regulated entities of the RBI, are currently prohibited from dealing with virtual currencies under the said circular.

### c. Notification as Non-Banking Financial Company (NBFC)

Section 45-I of the RBI Act defines the business of an NBFC. An NBFC is defined to include:

1. Various categories of ‘financial institutions’, which term excludes businesses which principally carry on the purchase or sale of any goods or the providing of any services;
2. Companies which receive deposits as their principal business; and,
3. Any non-banking institution or class of institutions notified by the RBI with the previous approval of the Central Government.

‘Crypto-asset business activity’ may often not fall within categories (1) and (2) above, since crypto-asset businesses would principally be service providers, and would rarely be receiving ‘deposits’ (which involves the receipt of ‘money’ and excludes “*amounts received in the ordinary course of business*”) as their principal business.

However, the section gives the RBI, with the prior approval of the Central Government, the power to notify any class of institutions as NFBCs. The RBI and the Central Government may hence consider notifying entities carrying on ‘crypto-asset business activity’ (as defined above) as NBFCs.

This would bring crypto-asset business activity within a well-established regulatory regime, involving licensing, financial adequacy, KYC/AML rules, audits, disclosures, and other consumer-focused requirements.

### d. Regulations under the Consumer Protection Act

The Consumer Protection Act protects consumers against ‘unfair trade practices’, ‘deficiencies’ in services, and ‘defects’ in goods. The term ‘unfair trade practices’ includes false or misleading advertising. As a result, if any crypto-asset business makes misrepresentations to consumers or provides deficient services, consumers have recourse under the Consumer Protection Act.

The National Consumer Disputes Redressal Commission has power under Section 30A of the Consumer Protection Act to make regulations “*to provide for all matters for which provision is necessary or expedient for the purpose of giving effect to the provisions of this Act.*” Therefore, it is open to the National Commission to frame regulations (e.g., create a licensing regime) taking into account the particular consumer protection concerns of the crypto-asset industry. We submit that this avenue may also be considered.

---

## e. Notifications under the SCRA

### *Notification as ‘securities’ under Section 2(h)(ia)*

Crypto-assets having the characteristics of ‘securities’ may be notified under Section 2(h)(ia) of the SCRA as “*such other instruments as may be declared by the Central Government to be securities*”. However, this power should be exercised with care, and all crypto-assets cannot be notified under this power, since some crypto-assets like Bitcoin lack certain features of a ‘security’, such as having an identifiable issuer. As a broad thumb rule, only security tokens should be considered for notification under the SCRA, and not payment tokens or utility tokens.

### *Notification as ‘commodity derivative’ under Section 2(bc)*

Under the SCRA, ‘commodity derivatives’ also amount to ‘securities’. According to a SEBI circular dated September 28, 2016,<sup>60</sup> read with a Central Government notification under the SCRA dated September 27, 2016,<sup>61</sup> the Central Government has notified certain goods for the purpose of the term ‘commodity derivative’ under the SCRA. These include base metals (such as aluminium, brass, and copper), precious metals (gold, silver and platinum), gems and stones (diamond), energy (such as carbon credit, coal, crude oil, and electricity), and other items like cereals and pulses, but do not include any crypto-assets.

The Central Government may at any time choose to bring derivatives contracts in crypto-assets within the SEBI jurisdiction by including crypto-assets in the aforesaid notification. Derivatives in such crypto-assets would then amount to ‘securities’.

If the above powers are exercised, then, under the SCRA, only ‘recognized stock exchanges’ can facilitate the trading of crypto-assets, or derivatives of crypto-assets, amounting to ‘securities’. This would bring such trading within a well-established regulatory regime supervised by SEBI.

## iii. Statute-backed self-regulation

The authors through Nishith Desai Associates had previously submitted a ‘Draft Code of Self-Regulation for Virtual Currency Businesses in India’ to the previous Inter-Disciplinary Committee on the subject, chaired by Shri Dinesh Sharma. The draft code dated July 2017 is attached as **Annexure III**. The draft is largely based on the ULC Model Law, with suitable changes for the Indian context. These include mandating compliance with KYC/AML norms under the PMLA and the RBI’s KYC Direction, and net worth requirements based on those prescribed by the RBI for regulated entities. The draft creates a certification regime and mandates various consumer protection features including capital adequacy, audits, and disclosures.

Self-regulation provides flexibility for changes in norms, which is suitable for the crypto-asset industry owing to its fast-paced nature. The Committee may consider self-regulation backed by a statutory mandate in order to provide statutory backing to the norms, and in turn, facilitate a system of government oversight of the industry.

Self-regulation backed by a statutory mandate has been recognized in India in various contexts including:

- The Advertising Standards Council of India (ASCI) ‘Code for Self-Regulation of Advertising content in India’ supported by Rule 7(9) of the Cable Television Networks Rules, which states,

*“No advertisement which violates the Code for self-regulation in advertising, as adopted by the Advertising Standard Council of India (ASCI), Mumbai for public exhibition in India, from time to time, shall be carried in the cable service.”*

---

60. SEBI/HO/CDMRD/DMP/CIR/P/2016/105

61. S.O. 3068(E) (Ministry of Finance, Department of Economic Affairs)

- The SEBI Act (Section 11(2)(d)) read with the SEBI (Self Regulatory Organizations) Regulations, which enable self-regulatory organizations to lay down codes of conduct specifying standards for their members in the conduct of business. <sup>62</sup>

Similarly, the Committee can consider recommending the statutory backing of a self-regulatory code of conduct to be adopted by crypto-asset businesses. Such statutory backing could be created by inserting suitable provisions under any of the legislative and administrative regulation options (e.g., PSS Act, NBFC regulations, or Consumer Protection Act) suggested above.

Even if self-regulation is not ultimately recommended by the Committee, the Committee may refer to the enclosed draft code at **Annexure III** (which we will be pleased to update if required) for an outline of the norms that may be prescribed under a licensing regime.

## IV. Clarifications and fine-tuning of existing laws

Besides the new regimes that can be introduced as suggested above, certain existing laws are ambiguous in their application to crypto-asset business activity. Clarifications to these laws may be considered along the lines suggested below.

### A. FEMA (Export and Import)

As mentioned above, crypto-assets which are not ‘securities’ are likely to fall within the meanings of ‘goods’ and ‘software’ under FEMA.<sup>63</sup> This is because the definition of ‘software’ under the FEMA regulations is very wide:

*“software’ means any computer programme, database, drawing, design, audio/video signals, any information by whatever name called in or on any medium other than in or on any physical medium”<sup>64</sup>*

If any crypto-assets are considered ‘goods’ under FEMA, the legal implications under FEMA (e.g., compliance for export of goods) will then flow accordingly. However, the RBI has not clarified the classification of crypto-assets under FEMA, leading to ambiguity on the question. The RBI may consider amending its regulations and directions which deal with the export and import of goods in order to clarify their application with respect to crypto-assets.

### B. Information Technology Act

The Information Technology Act, read with the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, is the chief law regarding cybersecurity in India. While the 2011 Rules do lay down fairly stringent cybersecurity requirements for any body corporate handling sensitive personal data, the Central Government may prescribe specific additional measures for crypto-asset business activity if it deems fit. We note that a new data protection Bill is likely to be introduced, and the specific cybersecurity norms may also be prescribed under this Bill, when passed.

62. Rule 15(2)(vi) of the said regulations.

63. Foreign Exchange Management (Export of Goods & Services) Regulations, 2015 and Master Direction – Import of Goods and Services (2016, as amended in 2018). E.g.,

64. Regulation 2(viii) of the Foreign Exchange Management (Export of Goods & Services) Regulations, 2015.

---

## C. Deposit-related laws

### i. Collective Investment Schemes

A 'collective investment scheme' under the SEBI Act is a scheme where the contributions or payments made by the investors are pooled with a view to receive profits, income, or property, and the scheme is managed on behalf of the investors who do not have day-to-day control over the management and operation of the scheme.<sup>65</sup>

'Initial Coin Offerings (ICOs)', or other issuances of crypto-assets, which meet all these elements could be subject to regulation as collective investment schemes. There is some ambiguity as to whether the terms 'contributions' and 'payments' would include crypto-assets.<sup>66</sup>

It is open to SEBI to clarify and enforce this regime in suitable cases, and amend the SEBI (Collective Investment Schemes) Regulations where suitable, to take into account issues specific to the crypto-asset industry. This would bring many types of ICOs and other crypto-asset offerings within a well-established regulatory regime.

### ii. Prize Chits Act and Chit Funds Act

Both the Prize Chits Act and the Chit Funds Act refer to the concept of 'monies'/'money' and 'grain' in their definitions of the terms 'prize chit', 'chit', and 'money circulation scheme'.

Since crypto-assets are not currently 'money' under Indian law, these definitions can be updated to include the term 'valuable thing' (as used in Section 2(c) of the Prize Chits Act), so that the purposes of these Acts can be extended to the schemes involving crypto-assets, among other valuable things.

### iii. Companies Act and Companies (Acceptance of Deposits) Rules

The Companies Act and the Companies (Acceptance of Deposits) Rules regulate the acceptance of 'deposits' by companies from the public. However, the definition of 'deposit' in the said Act and Rules is restricted to the receipt of 'money'. The Committee may consider whether the same should be clarified to include other valuable things like crypto-assets, in order that 'deposits', albeit made in crypto-asset form, are regulated by the Act and Rules. If this path is chosen, such deposits of crypto-assets should still be subject to the exceptions under the definition (e.g., non-interest bearing amounts held in trust, and advances against goods and services).<sup>67</sup>

### iv. Banning of Unregulated Deposit Schemes Bill (2018)

We note that the said Bill proposes to ban all unregulated 'deposits'. The Statement of Objects and Reasons annexed to the Bill states the following as among the main reasons for the introduction of the Bill:

*"[t]he Central legislations such as the Prize Chits and Money Circulation Schemes (Banning) Act, 1978 and the Chit Funds Act, 1982 and the legislations enacted by the State Governments have not been able to completely address the issue of unregulated deposit schemes run by unscrupulous elements."*

---

65. Section 11AA.

66. Certain provisions like Regulation 34 (Money to be kept in separate account and utilisation of money) or Regulation 35 (Investments and segregation of funds) of the SEBI (Collective Investment Schemes) Regulations suggest that the 'contributions' or 'payments' is restricted to 'money'/'funds'.

67. See Rule 2(1)(c)(i) to (xiv), Companies (Acceptance of Deposits) Rules.



Similar to the Companies Act, however, the Bill in its definition of ‘deposits’ only includes the concept of ‘money’, and not other valuable things. The Committee may consider whether this definition should be clarified to include other valuable things like crypto-assets, in order to prevent the acceptance of crypto-assets in connection with fraudulent and unscrupulous schemes.

## D. Taxation

The taxation of crypto-asset-related activity will broadly fall under two heads: Goods and Services Tax (GST) and Income Tax.

Under Section 9 of the Central Goods and Services Tax Act, tax is to be levied “*on all intra-State supplies of goods or services or both*”, and under Section 7, “supply” includes the supply of goods or services or both “*made or agreed to be made for a consideration by a person in the course or furtherance of business.*” The key issues for the tax authority to determine are whether a particular crypto-asset is ‘goods’ or ‘services’, and whether the same is being ‘supplied’, i.e., is in the course of furtherance of ‘business’.

We submit that rather than taking a blanket view, this needs to be decided keeping in mind the facts and circumstances of each crypto-asset and each transaction, since, as mentioned earlier, there are a multitude of crypto-assets, and the types of transactions can vary widely.

Also, situations of double taxation should be avoided, i.e., consumers who use crypto-assets as payment may end up paying GST twice: once on the purchase of the crypto-asset, and again on its use in exchange for other goods and services subject to GST. To avoid such double taxation, some leading jurisdictions like Australia have amended the GST law to exempt purchases of crypto-assets from GST and align the treatment of crypto-assets with money (for tax purposes).<sup>68</sup> The Committee may carefully consider this option for suitable crypto-assets, like payment tokens, in order to avoid double taxation.

Under the Income Tax Act, the key issue is whether income from crypto-assets is treated as ‘capital gains’ or ‘profits and gains of business or profession’. Once again, we submit that rather than taking a blanket view, this needs to be decided keeping in mind the facts and circumstances of each transaction, since individuals and corporates may deal with crypto-assets in a variety of contexts, sometimes as capital assets, and sometimes in the course of business.

---

68. <https://www.ato.gov.au/General/New-legislation/In-detail/Indirect-taxes/GST/GST--removing-the-double-taxation-of-digital-currency/>

---

## 3. Summary

To recap, our suggestions are as follows:

1. An outright ban on crypto-asset activity should not be considered for several reasons. Crypto-assets are essential to blockchain technology, which is a new and disruptive technology that presents both benefits and risks. History has taught us that such technologies should be regulated and not banned, since banning is likely to be counter-productive and may also suffer from legal infirmities. Rather, in line with international consensus, a balanced regulatory approach should be taken to promote the various benefits of the technology and mitigate the risks.
2. For the purpose of legal analysis, all crypto-assets are not alike, and the implications of each should be assessed on a case-by-case basis. Broadly, crypto-assets can be considered to be of three types: payment tokens, security tokens, and utility tokens. Those security tokens which amount to 'securities' will be regulated by SEBI and under the Companies Act. Trading activity with regard to all other crypto-assets falls in something of a regulatory vacuum, although existing laws like the Consumer Protection Act continue to apply to a significant extent.
3. This vacuum should be addressed by introducing: (a) a Know Your Customer / Anti-Money-Laundering (KYC/AML) regime, and (b) a licensing regime, for crypto-asset business activity.
  - a. As regards KYC/AML, businesses dealing with crypto-assets, i.e., providing custody or trading services, can be included within the framework of the PMLA by Central Government notification.
  - b. As regards licensing, a new licensing regime for crypto-asset business activity can be evolved by:
    - i. New legislative provisions, such as under the newly proposed regimes on commodity spot trading and payment systems;
    - ii. Administrative regulation under various laws such as the Consumer Protection Act, PSS Act, NBFC regime, and/or SCRA; and/or,
    - iii. Statute-backed self-regulation.

Administrative regulation under existing laws will be limited by the current scope of the parent statutes, while new legislative provisions may be able to better address the unique nature of crypto-asset activity. In either case, responsibility for such licensing or oversight should be clearly assigned to a given regulatory body to avoid jurisdictional ambiguity. Since SEBI has competence as regards investor protection, it is one option that can be considered in this connection.
4. Meanwhile, existing laws such as the Consumer Protection Act, FEMA, IPC, Information Technology Act, PSS Act, PMLA, Prize Chits Act, deposits-related laws, securities laws, and tax laws should be actively enforced with regard to crypto-asset business activity, since much of such activity is already covered by these laws. The applicability of some of these laws may also be further clarified or fine-tuned with respect to crypto-assets.

*Disclaimer: The suggestions in this Paper are provided in good faith and in public interest. This Paper should not be construed as a legal opinion and the authors accept no liability for the actions or omissions of any person relying upon the same.*

# Annexure I

## Profiles Of The Authors

### Nishith Desai

Nishith Desai is the founder of the research-based and strategy-driven international law firm, Nishith Desai Associates, with offices in Mumbai, Silicon Valley, Bangalore, Singapore, New Delhi, Munich and New York. Mr. Desai is a renowned International Tax, Corporate, and IP lawyer, researcher, published author, and lecturer in leading academic institutions around the world. He specializes in the Financial Services sector and assisted the Government of Mauritius and the Government of India in launching their individual offshore financial centers. Soon after India opened up its economy to the outside world in 1991, he established the first five India-focused funds. He was instrumental in setting the firm's blockchain practice group in 2013.

He was also a member of the Regulatory Committee on Fintech and Innovation Driven Financial Services set up by the Government of Mauritius this year. The said Committee was chaired by Lord Meghnad Desai (House of Lords, U.K.) and recommended a detailed framework for the country to promote and regulate the fintech industry.

### Vaibhav Parikh

Vaibhav Parikh heads the U.S office of Nishith Desai Associates. He also leads the practice areas of Technology, Mergers and Acquisitions, Private Equity, and Crypto-Assets and Blockchain. Vaibhav often plays the role of key advisor to leading crypto-asset exchanges in India and leading financial dailies often turn to him for his views on the subject. Over the years, Vaibhav has been advising many leading Indian e-commerce companies in their operations from a legal and regulatory standpoint. Tying in his expertise in advising several private equity players and venture capitalists in navigating their way to successful investments, Vaibhav has facilitated some of India's largest e-commerce transactions.

### Jaideep Reddy

Jaideep Reddy is a senior member of the firm's Technology Law practice and co-heads its Crypto-Assets and Blockchain practice. He specializes in the legal issues relating to crypto-assets and blockchain technology, privacy and cybersecurity, payments, and other emerging technology law issues. He has authored the firm's research paper on blockchain technology, and led the drafting of the enclosed self-regulatory code of conduct, which is based on international best practices. He is admitted to practice law in India and California, U.S.A. He holds a Masters in Law from the University of California, Berkeley, School of Law and a B.A., LL.B. (Hons.) from the W.B. National University of Juridical Sciences, Kolkata, India.

## Annexure II

### Overview of Regulatory Approaches to Crypto-Assets by Significant Jurisdictions<sup>69</sup>

Jurisdiction	Whether any prohibition imposed	Applicability of KYC/ AML norms	Specific regulatory regime for crypto-assets <sup>70</sup>
<b>Australia</b>	None.	Specifically made applicable to crypto-asset activity.	None, except certain taxation amendments. Existing laws apply.
<b>Canada</b>	None.	Specifically made applicable to crypto-asset activity.	None. Existing laws apply.
<b>China</b>	Yes. There are two main prohibitions: (1) on Initial Coin Offerings (ICOs), and (2) on the conversion of crypto-assets to legal tender, and vice versa, through crypto-asset trading platforms and regulated financial institutions.	Does not arise due to the prohibition.	Prohibition severely limits activity. Existing laws apply to such activity.
<b>E.U.</b>	None.	Specifically made applicable to crypto-asset activity.	None. Existing laws apply.
<b>India</b>	Yes. Prohibition on regulated financial institutions dealing with crypto-assets or facilitating crypto-asset transactions.	Does not arise due to the prohibition.	Prohibition severely limits activity. Existing laws apply to such activity.
<b>Japan</b>	None.	Specifically made applicable to crypto-asset activity.	Crypto-asset exchanges are specifically regulated under the Payment Services Act.
<b>Malta</b>	None.	Specifically made applicable to crypto-asset activity.	Crypto-asset activity is specifically regulated under three new Acts.

69. This overview is based on readily available sources and should not be interpreted as a conclusive statement of the legal status of crypto-assets in any jurisdiction other than India. Further, jurisdictions differ on the terminology used for, and the definitions of, crypto-assets.

70. This column deals with laws or regulations introduced specifically to deal with crypto-assets, and not the extrapolation of existing laws such as securities laws.

<b>Singapore</b>	None.	Existing norms clarified to apply indirectly to crypto-asset activity. New Bill introduced which specifically extends the norms to crypto-asset intermediaries.	None. Existing laws apply.
<b>U.K.</b>	None.	Existing norms clarified to apply indirectly to crypto-asset activity. The U.K. Task Force has stated that the U.K. will soon impose strict KYC/AML norms for crypto-asset activity.	None. Existing laws apply.
<b>U.S.A.</b>	None.	Specifically made applicable to crypto-asset activity.	Varies from state to state. New York and Wyoming have specific regimes for crypto-asset activity.

---

## Annexure III

# Draft Code of Self-Regulation for Virtual Currency Businesses in India

The enclosed self-regulatory code of conduct was prepared in July 2017, as a draft for discussion, on the instructions of the Digital Asset and Blockchain Foundation of India (DABFI). DABFI has since then been subsumed into the Internet and Mobile Association of India (IAMAI) as of November 2017. Further, references to ‘virtual currency’ may be read as references to ‘crypto-assets’, owing to the recent consensus in India on this terminology.

The draft below was based on a multiplicity of sources, indicated in the footnotes as applicable. Where not so indicated, the text was based on a pre-final draft of the ULC Model Law and comments by stakeholders on that draft.<sup>71</sup>

Since the draft was prepared in 2017, we would be pleased to update the draft if the Committee so requires.

---

71. <http://www.uniformlaws.org/Committee.aspx?title=Regulation%20of%20Virtual%20Currency%20Businesses%20Act>

# Code of Self-Regulation for Virtual Currency Businesses in India

## Chapter 1 - General Provisions

### Section 1. Short Title.

- (a) This Code may be called the Code of Self-Regulation for Virtual Currency Businesses in India.
- (b) It shall extend to the whole of India, and shall apply to legal persons outside India that carry on Virtual Currency Businesses activities in India, as defined in this Code.
- (c) It shall come into effect on [...]

### Section 2. Definitions.

- (1) In this Code:
  - (a) “Applicant” means a Virtual Currency Business, existing or proposed, that applies for certification by the Committee under this Code.
  - (b) “Bank” shall have the same meaning as defined in section 2(1)(a) of the Payment and Settlement Systems Act, 2007.
  - (ba) “Board of DABFI” shall mean the governing body of DABFI.
  - (c) “Certified Virtual Currency Business” means a Virtual Currency Business certified by the Committee under this Code.<sup>72</sup>
  - (ca) “chartered accountant” means a chartered accountant as defined in clause (b) of sub-section (1) of section 2 of the Chartered Accountants Act, 1949 who holds a valid certificate of practice under sub-section (1) of section 6 of that Act;
  - (d) “Committee” means the independent body established by DABFI to administer this Code including the granting, administration (including suspension) and withdrawal of certification.<sup>73</sup>
  - (da) “company secretary in practice” means a company secretary who is deemed to be in practice under sub-section (2) of section 2 of the Company Secretaries Act, 1980;
  - (e) “Control”, with all its grammatical variations and cognate expressions, shall:
    - (1) When used in reference to transactions or relationships involving Virtual Currency, mean the power to execute unilaterally or prevent indefinitely Virtual Currency transactions; and,

---

72. The concept of certification is integral to self-regulation and is taken from the ADCCA Code of Conduct, available at <http://adcca.org.au/wp-content/uploads/2016/12/ADCCA-Code-of-Conduct.pdf>.

73. This is taken from the ADCCA Code of Conduct, available at <http://adcca.org.au/wp-content/uploads/2016/12/ADCCA-Code-of-Conduct.pdf>.

- 
- (2) When used in reference to a Virtual Currency Business (as, for example, in Section 6 (a) (3)), include the right to control the management or policy decisions of the Virtual Currency Business exercisable by a person, directly or indirectly, including by virtue of their shareholding, status as a partner, or other management rights or shareholders agreements or partnership agreement or in any other manner.
- (f) “Convertible Virtual Currency” means Virtual Currency that:
- (1) has an equivalent value in Legal tender and can be exchanged for Legal tender or Bank credit; or
  - (2) can be exchanged for an account denominated in Legal tender.
- (g) “DABFI” means the Digital Asset and Blockchain Foundation of India, a [type of entity] duly incorporated under the laws of India.
- (h) “DABFI Certification Mark” means the logo and text described in Appendix 1, to be displayed as described thereunder.<sup>74</sup>
- (i) “Exchange” with its grammatical variations and cognate expressions shall mean to assume Control of Virtual Currency on behalf of a person, at least momentarily, in order to sell, trade, or convert:
- (1) Virtual Currency for Legal tender for one or more forms of Virtual Currency; or
  - (2) Legal tender for one or more forms of Virtual Currency;
- (j) “Executive officer” means an individual who has the management of the whole, or substantially the whole, of the affairs of a Virtual Currency Business, and includes a director, partner or any other person occupying the position of a manager, by whatever name called, whether under a contract of service or not.
- (k) “Government” denotes the Central Government or the Government of a State, as the case may be.
- (l) “in India”, with respect to Virtual Currency Business Activity, means Virtual Currency Business Activity which occurs in India.<sup>75</sup>
- (m) “Legal tender” shall have the same meaning ascribed to that term under the Reserve Bank of India Act, 1934.
- (n) “Net worth” shall have the same meaning as defined in section 2(57) of the Companies Act, 2013.
- (na) “person” shall have the same meaning as defined in section 2 (u) of the Foreign Exchange and Management Act, 1999

---

74. This concept is taken from the ADCCA Code of Conduct, available at <http://adcca.org.au/wp-content/uploads/2016/12/ADC-CA-Code-of-Conduct.pdf>.

75. Companies Act, 2013:

2(42) “foreign company” means any company or body corporate incorporated outside India which–

(a) has a place of business in India whether by itself or through an agent, physically or through electronic mode; and

(b) conducts any business activity in India in any other manner.

Companies (Registration of Foreign Companies) Rules, 2014:

c) For the purposes of clause (42) of section 2 of the Act, “electronic mode” means carrying out electronically based, whether main server is installed in India or not, including, but not limited to–

(i) business to business and business to consumer transactions, data interchange and other digital supply transactions;

(ii) offering to accept deposits or inviting deposits or accepting deposits or subscriptions in securities, in India or from citizens of India;

(iii) financial settlements, web based marketing, advisory and transactional services, database services and products, supply chain management;

(iv) online services such as telemarketing, telecommuting, telemedicine, education and information research; and

(v) all related data communication services,

whether conducted by e-mail, mobile devices, social media, cloud computing, document management, voice or data transmission or otherwise;



- (o) “Record” means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form and includes an ‘electronic record’ as defined under the Information Technology Act, 2000.
- (p) “Standard asset” shall, unless repugnant to the context herein,<sup>76</sup> have the meaning ascribed to it by the Reserve Bank of India in its directions under Section 45JA of the Reserve Bank of India Act, 1934.
- (q) “Store” with its grammatical variations and cognate expressions mean maintaining Control of Virtual Currency on behalf of a person by any person other than that former person.
- (r) “Transfer” means to assume Control of Virtual Currency from or on behalf of a person and to:
- (1) credit the Virtual Currency to the account of another person; or
  - (2) move the Virtual Currency from one account of a person to another account of the same person; or
  - (3) relinquish Control of Virtual Currency to another person;
- (s) “Virtual Currency”, also known as “crypto-currency”:
- (1) means a digital representation of value that:
    - (A) is used as a medium of Exchange, unit of account, or store of value; and
    - (B) is not Legal tender, whether or not denominated in Legal tender; and
  - (2) does not include:
    - (A) the underlying software or protocols governing transfer of the digital representation of value;
    - (B) a transaction in which a merchant grants value as part of an affinity or rewards program, which value cannot be taken from or exchanged with the merchant for Legal tender, or Convertible Virtual Currency; or
    - (C) a digital representation of value used within an online game, game platform, or a family of games sold by the same publisher or offered on the same game platform.
- (t) “Virtual Currency administration” means issuing Virtual Currency with the authority to redeem the currency for Legal tender, Bank credit or other Virtual Currency.
- (u) “Virtual Currency Business” means an individual, a company or a limited liability partnership, duly incorporated under Indian laws, or a duly incorporated non-resident foreign entity carrying out Virtual Currency Business Activity.
- (v) “Virtual Currency Business Activity” means:
- (1) Exchanging, Transferring, or Storing Virtual Currency or engaging in Virtual Currency administration, whether directly or through an agreement with a Virtual Currency control services vendor; or
  - (2) exchanging one or more digital representations of value used within one or more online games, game platforms, or family of games for: (i) Virtual Currency offered by or on behalf of the same publisher from which the original digital representation of value was received; or (ii) Legal tender or Bank credit outside the online game, game platform, or family of games offered by or on behalf of the same publisher from which the original digital representation of value was received.

---

76. This is to guard against the event of the RBI prescribing different definitions for different types of entities under Section 45JA. Currently, the definition appears to be the same for all NBFCs. As of May 25, 2017, this definition reads: “*standard asset*” means the asset in respect of which, no default in repayment of principal or payment of interest is perceived and which does not disclose any problem nor carry more than normal risk attached to the business.”

- 
- (w) “Virtual Currency control services vendor” means a person that has Control of Virtual Currency solely pursuant to agreement with a person that, on behalf of another person, assumes Control of Virtual Currency.
- (2) Words and expressions used in this Code and not defined, but defined in the Payment and Settlement Systems Act, 2007, the Banking Regulation Act, 1949 the Income Tax Act, 1961 and Companies Act, 2013, shall have the meanings assigned to them under the respective legislations where applicable.

## Section 3. Scope.

- (a) Except as otherwise provided in this Code, this Code applies only to the Virtual Currency Business Activities in India of a Virtual Currency Business operating in India.
- (b) In no event shall activities by the following be construed to be “Virtual Currency Business Activity”:
- (1) the Government;
  - (2) a Bank;
  - (3) a person that only contributes connectivity software or computing power to a decentralized Virtual Currency network and is not otherwise engaged in Virtual Currency Business Activity on behalf of other persons;
- Provided that the Committee may issue separate guidelines for 'miners', being those entities who use computing power connected to the decentralized Virtual Currency network to generate fresh Virtual Currency.
- (4) a person that only provides data storage or security services for a Virtual Currency Business and is not otherwise engaged in Virtual Currency Business Activity on behalf of other persons;
  - (5) a person that mines, manufactures, buys, sells, exchanges, or otherwise obtains or relinquishes Virtual Currency solely for personal, family, or household purposes, or for the purpose of any research in Virtual Currency Business Activities which are not for commercial purpose, if the person does not engage in any Virtual Currency Business Activity on another person’s behalf. “Personal, family, or household purposes” include buying or selling Virtual Currency as an investment, researching Virtual Currency or related technologies, and obtaining Virtual Currency as payment for the purchase or sale of goods or services;
  - (6) a person whose Virtual Currency Business Activity in India is reasonably expected to be valued, in the aggregate, on an annual basis, at [INR 1,00,000] or less as measured by the Indian Rupee equivalent of the Virtual Currency;<sup>77</sup> or
  - (7) a Virtual Currency control services vendor.
- (c) The provisions of this Code shall be in addition to and not in derogation of the provisions of any other law for the time being in force.

---

77. This is intended to cover business models where blockchain technology is used and nominal amounts of Virtual Currency are transferred (for example, at least 0.00000001 BTC (less than 1 paisa as of May 2017) is required to access the bitcoin blockchain). This is the case, for example, if land records move to the blockchain. The exception can also cover Virtual Currency Businesses running pilots. If this exception is chosen to be deleted, the former use case (e.g., using nominal amounts of Virtual Currency as part of a non-monetary business model) should be nonetheless be retained. This has been recognized by the ULC, in the ADCCA Code of Conduct, and in independent research. E.g., <https://coincenter.org/entry/state-digital-currency-principles-and-framework>.

## Chapter 2 - Certification

### Section 4. Certification; Eligibility and other Matters.

- (a) Every Applicant shall, subject to provisions of this Code and any other law for the time being in force, be eligible to apply for certification under this Code.
- (b) Any Virtual Currency Business certified under this Code shall display on its website, mobile app, letterhead, and other materials, the DABFI Certification Mark.
- (b) All individuals who are to hold office of Executive Officer, Director, Manager or Partner of a Virtual Currency Business shall have such qualifications as are prescribed by the Committee.

### Section 5. Certification not Transferable or Assignable.

A certification issued under this Code is not transferable or assignable.

### Section 6. Application for Certification.

- (a) Except as provided in Section 8, an application under this Code must be made by an Applicant in a form and medium prescribed by the Committee. The application must:
  - (1) be accompanied by a non-refundable fee of [INR 10,00,000 (Rupees Ten Lakhs only)];  
state whether the Applicant is an entity that is registered with an authority under Indian law and details in respect of the same
  - (2) state the legal name of the Applicant, its current or proposed business address, and any trade name and trademark used or proposed to be used by the Applicant, in conducting its Virtual Currency Business Activity;
  - (3) state the legal name of the Executive officer of the Applicant and any other person that exercises Control over the Applicant's Virtual Currency Business Activity, the residential and business address, and any former name or trade name;
  - (4) describe the current and historical business of the Applicant, including its products and services, associated website addresses, its principal place of business, its projected customer base, specific marketing targets, and the location of each current database server expected to be used with its Virtual Currency Business Activity;
  - (5) a brief description of technology and other protocols that are used in Virtual Currency Business Activity.
  - (6) certificate of compliance by a chartered accountant that the Applicant's Net worth is at least [INR 10,00,00,000 (Rupees Ten Crores only)].<sup>78</sup>
  - (7) disclose:

---

78. The amount has been taken from the RBI's Draft Master Directions on Issuance and Operation of Prepaid Payment Instruments in India (2017), available at [https://www.rbi.org.in/Scripts/bs\\_viewcontent.aspx?Id=3325](https://www.rbi.org.in/Scripts/bs_viewcontent.aspx?Id=3325).

- 
- (A) any authorization or license (in this subsection, “**license**”) granted by the Reserve Bank of India;
  - (B) the date the license expires; and
  - (C) license revocations, suspensions, or other disciplinary actions taken against the Applicant;

(8) disclose criminal convictions of, and pending criminal proceedings against:

- (A) the Applicant;
- (B) a person that exercises Control over the Applicant; and
- (C) a person over which the Applicant exercises Control;

(9) disclose material litigation in which the Applicant or any Executive officer has been involved in the 10-year period preceding the application, determined in accord with generally accepted accounting principles and the extent the Applicant would be required to disclose the litigation in the Applicant’s annual audited financial statements, reports to shareholders, or similar statements or reports;

Explanation: “**Material litigation**” means any material item that, according to Accounting Standard 1 as duly notified by Institute of Chartered Accountants of India, the knowledge of which might influence decisions of the user of the financial statements.

(10) disclose any bankruptcy or similar proceedings in the previous ten years in which the Applicant, an Executive Officer, is a debtor;

(11) state the name and address of each Bank in which the Applicant plans to deposit funds obtained by its Virtual Currency Business Activity;

(12) describe the source of funds and credit to be used by the Applicant to provide Virtual Currency Business Activity in India and demonstrate that the Applicant has the minimum Net worth specified in Section 11;

(13) state the postal address and email address to which communications from the Committee may be sent;

(14) provide a copy of each liability, business-interruption or cyber-security insurance policy maintained by Applicant for itself, its partners, its officers and directors, as applicable, or its customers;

(15) provide a copy of a Government-issued identification document of each Executive officer of the Applicant, together with an employment history and history of any investigation or legal proceeding involving any Executive officer for each for the previous ten years, if applicable;

(16) provide a copy of the charter document of the Applicant, such as the Memorandum of Association, Articles of Association, shareholders agreement, and, Limited Liability Partnership Agreement, as the case may be.

(17) any other information required under this Code, including information in relation to policies, procedures and compliances.

(18) other information that the Committee reasonably may require.

(b) For the purpose of grant of certification to an Applicant, the Committee shall consider introducing or modifying technical specifications of Applicant for eligibility, from time to time

- (c) The Committee may, for reasons recorded in writing, waive a requirement of subsection (a) or permit the Applicant to submit other information instead of the required information.

## Section 7. Security.

- (a) Before a certification is issued under this Code, the Applicant must deposit with the Committee funds, a letter of credit, a bank guarantee, or other security satisfactory to the Committee that:
- (1) secures the Applicant's faithful performance of its duties under this Code; and
  - (2) is in an amount the Committee specifies based on the nature and extent of risks in the Applicant's Virtual Currency Business model, but shall not exceed 10,00,00,000 (Rupees Ten Crores only) .
- (b) The security deposited with the Committee pursuant to this section shall constitute a trust fund maintained by the Committee for the benefit of customers of the relevant Virtual Currency Business. So long as the relevant Virtual Currency Business is solvent, such Virtual Currency Business shall be entitled to receive any interest paid on the security.<sup>79</sup>
- (c) The security is collectible by the Committee:
- (1) for the benefit of any claim against the relevant Virtual Currency Business on account of its Virtual Currency Business Activity with a customer; or
  - (2) pursuant to Section 19(d)(3).
- (d) The security must cover claims for a period the Committee specifies, but which must be at least till the expiry of 3 years after the relevant Virtual Currency Business ceases to engage in Virtual Currency Business Activity in India. Within 30 days after such period, the security shall be returned to the formerly Certified Virtual Currency Business or such other person entitled to receive the security as determined by the Committee.
- (e) The Committee may, for reasons recorded in writing, increase the amount of a Certified Virtual Currency Business's security. The Certified Virtual Currency Business must deposit the additional security not later than 30 days after the Certified Virtual Currency Business receives notice of the required increase in a Record from the Committee.
- (f) The Committee may, for reasons recorded in writing, permit an Applicant Virtual Currency Business to substitute or deposit an alternative form of security satisfactory to the Committee.
- (g) A customer of the relevant Virtual Currency Business (in this subsection, a **"claimant"**) does not have a direct right against the security. Only the Committee may recover on the security. The Committee may retain the recovery for up to 90 days after the Committee recovers on the security and shall in a timely manner handle claims and the distribution of recoveries to claimants.

---

79. Derived from a similar provision in the California Money Transmission Act ([http://leginfo.legislature.ca.gov/faces/codes\\_displayText.xhtml?lawCode=FIN&division=1.2.&title=&part=&chapter=3.&article=](http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=FIN&division=1.2.&title=&part=&chapter=3.&article=)). The ULC requirement of security is based on various U.S. states' money transmission laws. In the alternative, interest can be credited to an Consumer Protection Fund, similar to CWF under Central Excise Act - <http://consumeraffairs.nic.in/forms/contentpage.aspx?lid=73>

---

## Section 8. Action by Committee.

(1) When an application under Section 6 has been determined to be complete in accordance with Section 9(c) to the satisfaction of the Committee, the Committee shall notify the Applicant in a Record not later than [30] days after its decision to approve or deny the application has been made. If the Committee does not notify the Applicant of its decision before the 31st day after the application was complete, the application is deemed approved; and the Committee shall issue the certification, unless the Committee Records the reasons in writing for not issuing such certification.

*Provided that* no application shall be rejected without affording the Applicant a reasonable opportunity of being heard.

(2) The certification shall take effect on the first day following the expiration of the 45 day period if the Applicant by that time has complied with the security requirements of Section 7.

(3) If the Applicant is unable to comply with requirement for security as per Section 7 of this Code within 30 days from the date of the application, the application shall be treated as incomplete.

(4) If the Applicant fails to comply with the requirement of security within 30 days from the date of communication by the Committee, the application shall be treated as having been rejected.

## Section 9. Issuance of Certification.

(a) When an Applicant files an application, the Committee shall investigate or cause to be investigated the:

(1) financial condition and responsibility of the Applicant;

(2) relevant financial and business experience, character and general fitness of the Applicant; and

(3) the competence, experience, character, and general fitness of the Executive officers, directors, partners, managers, and persons in Control of the Applicant.

(4) compliance with applicable laws in India

(b) The Committee, for reasons recorded in writing, may conduct an investigation of the business premises of the Applicant, including facilities and devices for storage of Virtual Currency or credentials for use in Virtual Currency Business Activity, and data associated with it wherever those facilities may be located.

(c) An application is not complete until the Committee has all information required by this Code, and has completed any investigation under subsections (a) and (b). The Committee shall intimate the Applicant when it determines that the application is complete.

(d) Absent good cause which it shall so record in writing, the Committee shall issue a certification to an Applicant if the Applicant has fulfilled all of the conditions set forth in Sections 6 and 8.

(e) An Applicant may appeal the denial of its application in accordance with Section 20(c).

## Section 10. Annual Renewal.

- (a) At least 45 days before each anniversary of certification issuance, the Certified Virtual Currency Business must pay a renewal fee, set by the Committee, of an amount not to exceed INR 10,00,000 (Rupees Ten Lakhs). The Committee, for reasons recorded in writing, may grant an extension of a renewal date.
- (b) A Certified Virtual Currency Business shall submit to the Committee an annual report every year after its certification date (in this section, “**anniversary date**”) in a form and medium prescribed by the Committee, and certified as true and complete by an Executive officer of such business. The renewal report must state or contain, as applicable:
- (1) a copy of the Certified Virtual Currency Business’s most recent annual report and audited annual financial statement;
  - (2) a description of any:
    - (A) material change in the financial condition of the Certified Virtual Currency Business, including its Net worth;
    - (B) particulars and documents relating to litigation involving the Certified Virtual Currency Business, including orders passed by a court, tribunal or authority;
    - (C) any notices received from or proceedings pending with the Reserve Bank of India;
    - (D) Government investigation involving the Certified Virtual Currency Business;
    - (E) data security breach; and
    - (F) material change in information since the date of the audited financial statement submitted under paragraph (1);
    - (G) disclosure if certification has been previously cancelled or suspended by Committee.
  - (3) the number of Virtual Currency transactions conducted or facilitated by it in India for the period since the certification was issued or the last annual report;
  - (4) the rupee-equivalent of Virtual Currency in the Control of the Certified Virtual Currency Business at the end of the month at least 30 days before to the date of the annual report and the total number of customers for whom the Certified Virtual Currency Business had Control of Virtual Currency on the same date;
  - (5) a certificate from a Chartered Accountant or a Company Secretary in practice to the effect that the Certified Virtual Currency Business continues to meet the requirements of Section 11;
  - (6) evidence that the Certified Virtual Currency Business continues to maintain adequate security as required by Section 7; and
  - (7) a list of each location in India where the Certified Virtual Currency Business operates its Virtual Currency Business Activities or operates or uses a server related to the conduct of Virtual Currency Business Activity with residents of India.
  - (8) a list of the number of customer complaints received, number of customer complaints resolved and average time for redressal of each complaint,
- (c) If a Certified Virtual Currency Business does not pay its renewal fee or file its annual report by the due date or by the end of an extension of time granted by the Committee, the certification shall be deemed suspended and, subject to sub-section (d), the certification ceases immediately. The Committee shall communicate such suspension within one week of expiry of the extension of time.

---

The Committee may lift the suspension if, not later than 20 days after the certification was suspended, the Certified Virtual Currency Business:

- (1) files the renewal report and pays the renewal fee; and
  - (2) pays any penalty assessed under Section 19(d).
- (d) The Committee shall provide prompt notice to a Certified Virtual Currency Business of the lifting of any suspension after the Certified Virtual Currency Business has complied with subsection (b) (1) and (2).
- (e) All orders of suspension, lifting of suspension and termination shall be in writing communicated to the Certified Virtual Currency Business and shall also be displayed on the website of DABFI.

## Section 11. Consumer Protection.

- (a) Every Certified Virtual Currency Business shall at all times maintain a minimum Net worth of [INR 10,00,00,000 (Rupees Ten Crores)].<sup>80</sup>
- (b) Every Certified Virtual Currency Business:<sup>81</sup>
- (1) shall hold either:
    - (A) Virtual Currency of the same type and amount as that which is obligated to its customers, or
    - (B) Standard assets of the same amount as that which is obligated to its customers, and, provide evidence of such holdings upon request by a customer or the Committee within 7 days of the request being made to the Certified Virtual Currency Business;
  - (2) shall not, subject to any other law for the time being in force, sell, transfer, assign, lend, hypothecate, pledge, encumber or otherwise use Virtual Currency under its Control except in accordance with the express directions of the respective customer.
  - (c) Where customer funds are received for the purchase of Virtual Currency by a Virtual Currency Business and Virtual Currency is not issued within 24 hours from the time the customer notifies a Certified Virtual Currency Business in writing, with appropriate remittance details of such transfer, the Certified Virtual Currency Business must transfer any such funds to a separate Bank account designated as a trust account (where not already held in such an account in the same fiat currency as provided by the customer). It is intended that only customer funds can be held in that account and funds that the Certified Virtual Currency Business becomes entitled to must be withdrawn from the trust account as soon as practicable and no later than [one month] after the entitlement arises. Unallocated customer funds must be returned to customers within [60] days of receipt.<sup>82</sup>

---

80. This has been taken from the RBI's Draft Master Directions on Issuance and Operation of Prepaid Payment Instruments in India (2017), available at [https://www.rbi.org.in/Scripts/bs\\_viewcontent.aspx?Id=3325](https://www.rbi.org.in/Scripts/bs_viewcontent.aspx?Id=3325).

81. This is taken from the ADCCA Code of Conduct, available at <http://adcca.org.au/wp-content/uploads/2016/12/ADCCA-Code-of-Conduct.pdf>.

82. This is taken from the ADCCA Code of Conduct, available at <http://adcca.org.au/wp-content/uploads/2016/12/ADCCA-Code-of-Conduct.pdf>.



- (d) Certified Virtual Currency Businesses must maintain a risk-based level of insurance cover, to protect against loss of Virtual Currency and Legal tender,

### Option 1<sup>83</sup>

[for not less than [INR 10,00,00,000 (Rupees Ten Crore), and such cover shall protect each customer of the Certified Virtual Currency Business to the extent of at least INR 1,00,000 (Rupees One Lakh)

### Option 2<sup>84</sup>

[up to the full equivalent in Indian Rupees of the Virtual Currency placed under the Control of the Certified Virtual Currency Business or provisional registrant, such value in Indian Rupees being as on the date of the placement].

## Section 12. Compliance with Legal Requirements.

- (a) A Certified Virtual Currency Business shall comply with all laws in force in India that apply to its Virtual Currency Business Activities.
- (b) Without prejudice to subsection (a), a Certified Virtual Currency Business shall comply with the requirements of the below laws (as amended or replaced from time to time) to the maximum extent unless otherwise specified below, regardless of whether such laws would apply to it in the absence of this Code:
- (1) The Reserve Bank of India (Know Your Customer (KYC)) Directions, 2016,<sup>85</sup> except any requirement which is specific to a certain type or types of “Regulated Entities (**REs**)”, and not applicable to REs at large, shall apply to a Certified Virtual Currency Business. For example, paragraph 57(i) which applies to Scheduled Commercial Banks shall not apply to Certified Virtual Currency Businesses.
  - (2) The Competition Act, 2002.
  - (3) The Prevention of Money Laundering Act, 2002.
  - (4) The Information Technology Act, 2000, the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 and other Rules as may be issued from time to time.
  - (5) The Foreign Exchange Management Act, 1999.
  - (6) The Consumer Protection Act, 1986.
  - (7) The Prize Chits and Money Circulation Schemes (Banning) Act, 1978.

---

83. This is taken from the ADCCA Code of Conduct, available at <http://adcca.org.au/wp-content/uploads/2016/12/ADCCA-Code-of-Conduct.pdf>, with a modification.

84. This is required as a disclosure by the ULC.

85. [https://rbi.org.in/Scripts/BS\\_ViewMasDirections.aspx?id=10292](https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10292)

---

# Chapter 3 - Information and Related Matters

## Section 13. Authority to Conduct Inspection

- (a) The Committee may, for reasons recorded in writing and subject to 15 days prior notice, conduct an annual examination of a Certified Virtual Currency Business and such additional examinations as the Committee deems appropriate.
- (b) The Committee, in exceptional circumstances that are clearly articulated, may, for reasons recorded in writing, at any time (and in addition to annual examination), conduct an examination of a Certified Virtual Currency Business without prior notice.
- (b) The Certified Virtual Currency Business shall pay the reasonable costs of an examination under this section.
- (c) Information obtained during an examination under this Code may be disclosed only as provided in Section 16.

## Section 14. Reports and Records.

- (a) A Certified Virtual Currency Business shall maintain a Record of each Virtual Currency Business Activity in which it has engaged in India, for a period of seven years following the date of the activity. The Record must be in a form that will allow the Committee to determine whether the Certified Virtual Currency Business is complying with applicable laws. This subsection requires a Record of:
  - (1) each Virtual Currency Business transaction of the Certified Virtual Currency Business operating in India, including:
    - (A) identity of the customer, if applicable;
    - (B) form of the transaction;
    - (C) amount, date, payment instructions given by the customer, if applicable; and
    - (D) the account number, PAN Number, name and physical address of any parties to the transaction that are customers of the Certified Virtual Currency Business;
  - (2) the aggregate number of transactions and aggregate rupee value of transactions by the Certified Virtual Currency Business in India, for the period the Certified Virtual Currency Business holds a certification under this Code;
  - (3) each transaction in which the Certified Virtual Currency Business exchanges one form of Virtual Currency for Legal tender or another form of Virtual Currency in India;
  - (5) Bank statements and bank reconciliation records for the Certified Virtual Currency Business and the name, account number, and physical address of each Bank used by the Certified Virtual Currency Business in the conduct of its Virtual Currency Business Activity in India, regardless of the physical location of the Bank; and
  - (6) material litigations as defined in this Code and any Virtual Currency Business Activity that the Certified Virtual Currency Business was unable to complete for any reason.
- (b) The records specified in subsection (a) may be maintained in any form in addition to, but not in place of, the form in which the Record was originally made.

- (c) If a Certified Virtual Currency Business maintains its Records outside India, the Certified Virtual Currency Business shall make them available to the Committee on three days' notice in a Record absent good cause.
- (d) All Records maintained by a Certified Virtual Currency Business under this Code are open to inspection by the Committee under this Code.

## Section 15. Cooperation and Data-Sharing Authority.

- (a) Subject to Section 16 and under terms consistent with applicable laws, the Committee shall cooperate, coordinate, jointly examine, consult, and share Records and information with the Government, including any statutory authority or agency thereof, concerning the affairs and conduct of a Certified Virtual Currency Business.
- (b) The Committee shall provide prior notice to a Certified Virtual Currency Business where possible and where prior notice is not possible, notice within 14 days of compliance under sub-section (a) above.

## Section 16. Confidentiality.

- (a) Except as otherwise provided in subsection (b), the following are confidential and not to be disclosed except as required by applicable law:
  - (1) information or reports obtained by the Committee from an Applicant or from a Certified Virtual Currency Business;
  - (2) information contained in or related to a report prepared by, on behalf of, or for the use of the Committee under this Code;
  - (3) trade secrets; and
  - (4) other financial and operational information not otherwise available to the public.
- (b) This section does not prohibit publication of:
  - (1) general information about an Applicant's or Certified Virtual Currency Business's Virtual Currency Business Activity;
  - (2) a list of persons certified under this Code; or
  - (3) the aggregated financial data concerning Applicants and Certified Virtual Currency Businesses.
- (c) An Applicant or a Certified Virtual Currency Business, as the case may be, may submit a request in writing to the Committee and DABFI, that a document or documents, or a part or parts thereof, be treated as confidential. The Committee may accept or reject request for treating information or document as confidential and shall communicate the same in writing with reasons to the Applicant or the Certified Virtual Currency Business, as the case may be.

---

## Section 17. Interim Report.

- (a) Absent good cause, during the term of its certification under this Code, a Certified Virtual Currency Business shall file with the Committee a report detailing any material change in information provided in its application or most recent renewal report to the Committee. Such material change shall include but not be limited to a material change in the Certified Virtual Currency Business's business model for the conduct of its Virtual Currency Business in India. The report must be filed no later than 30 days after the change.
- (b) A Certified Virtual Currency Business shall apply for the prior written permission of the Committee in respect of:<sup>86</sup>
- (1) any takeover or acquisition of Control concerning the Virtual Currency Business, which may or may not result in a change of management;
  - (2) any change in its management which would result in a change in more than 30 per cent of the directors, excluding independent directors, or partners of a Certified Virtual Currency Business.
- Prior approval shall not be required for those directors who get re-elected on retirement by rotation.
- Provided that* a Certified Virtual Business may apply for permission within 30 days after material change has taken place with reasons as to why prior permission could not be obtained. The Committee may, for reasons recorded in writing, grant *post facto* permission.
- (c) The Committee shall, if it is satisfied that the certification hereunder is not prejudiced and all the requirements of the Code are satisfied, grant such permission within 30 days from the date of the application. If such permission is not granted within 30 days, the permission is deemed granted, absent good cause.
- (d) If such permission is denied and the applicant makes the change, the certification under this Code ceases to be of effect.
- (e) Further, if post facto permission, is denied and the Certified Virtual Currency Business proceeds with the actions specified in Section 17(b)(1) or (2), such actions shall be a material non-compliance for the purpose of Section 19.
- (f) Any *post facto* decision shall be communicated in writing with reasons for the decision to the Certified Virtual Currency Business.

---

86. This has been taken from the RBI's Draft Master Directions on Issuance and Operation of Prepaid Payment Instruments in India (2017), available at [https://www.rbi.org.in/Scripts/bs\\_viewcontent.aspx?Id=3325](https://www.rbi.org.in/Scripts/bs_viewcontent.aspx?Id=3325).

## Chapter 4 - Committee and Enforcement

### Section 18. Committee.<sup>87</sup>

- (a) The Committee must consist of at least three people and a maximum of five, each of whom:
- (1) must be independent from the DABFI board;
  - (2) must have demonstrated skills and expertise in matters relating to Virtual Currency and may include eminent former bureaucrats, economists, lawyers, accountants or engineers;
  - (3) must agree to be bound by and follow the terms of reference <sup>88</sup> for the Committee and,
- (b) No DABFI Virtual Currency Business (including its employees, partners, directors, and people with more than 5% shareholding or partnership share in the business) may be a member of the Committee.
- (c) The members of the Committee are to be appointed unanimously by the Board <sup>89</sup> of DABFI.
- (d) The members of the Committee must appoint a chair from their number and may also appoint a deputy chair.
- (e) Except in circumstances where the DABFI board is the respondent in a matter to be determined by the Committee, the DABFI board has the right to appoint an observer to the Committee. The appointed observer will have the right to attend meetings of the Committee but will not be permitted to vote on Committee decisions or contribute to its deliberations. For the avoidance of doubt, the appointed observer may be, but does not need to be, a DABFI Executive officer.
- (f) The Committee will administer this Code according to the following guidelines:
- (1) Jurisdiction: The Committee will only consider matters directly related to granting of certification, monitoring of compliance (including suspension) and withdrawal of certification.
  - (2) Conflicts of interest: Committee members will disclose any conflicts of interest connected to any decision making and the chair or deputy chair will manage the conflict in accordance with the DABFI conflict of interest policy.<sup>90</sup>
  - (3) Fairness and transparency: The Committee's administration of affairs shall adhere to the principles of fairness and transparency, and it shall record each of its decisions and meetings.
  - (4) Risk-based: The Committee will take a risk-based approach in determining how to exercise its powers.
- (g) The Committee will be reimbursed for any DABFI board-approved out-of-pocket expenses incurred in connection with the performance of their duties as Committee members under this Code.
- (h) The Committee may be paid a sitting fee or other remuneration as determined by the DABFI board from time to time

---

87. This clause is broadly based on the ADCCA Code of Conduct, available at <http://adcca.org.au/wp-content/uploads/2016/12/ADC-CA-Code-of-Conduct.pdf>. This is because the ADCCA Code of Conduct provides a framework of enforcement for a self-regulatory code.

88. These terms of reference can contain detailed terms of engagement, such as resignation and dismissal for cause.

89. Since DABFI is not yet a registered entity, this is marked as pending confirmation.

90. A conflict of interest policy broadly along the lines of that of the ADCCA can be adopted.

- 
- (i) The Committee shall maintain accounts of all amounts received and expended or applied under this Code. A copy of these accounts and related documents shall be placed before the Board of DABFI.

## Section 19. Enforcement.<sup>91</sup>

- (a) A Certified Virtual Currency Business must promptly report all incidences of material non-compliance with this Code to the Committee.

- (b) Any person may report an incidence of material non-compliance with this Code to the Committee, describing as much information as practicable about the alleged non-compliance:

provided that any such person must first exhaust their rights under Section 22.

- (c) An incident of non-compliance will be considered material after considering the following:

- (1) the number and frequency of previous similar incidences;
- (2) the impact of the incident or likely incident on the Certified Virtual Currency Business's ability to provide the service as well as its impact on the industry as a whole;
- (3) the extent to which the incident or likely incident indicates that the Certified Virtual Currency Business's arrangements to ensure compliance with those obligations is inadequate; and,
- (4) the actual or potential financial loss to any persons, other than the Certified Virtual Currency Business, arising from the incident or likely incident.

Without prejudice to the foregoing, the following shall be considered material non-compliances:

- (1) any non-compliance resulting in actual financial loss to persons other than the Certified Virtual Currency Business caused in the course of Virtual Business Activities;
  - (2) a non-compliance with the denial of permission as laid out in section 17(b); and
  - (3) non-compliance with any of the laws in relation to Virtual Business Activities as laid out in section 19(b).
- (d) Upon investigation of an incident of material non-compliance brought to its notice under this Section or discovered by it *suo moto*, the Committee may:
- (1) take no action;
  - (2) require that a specific corrective action be undertaken within a nominated period; or
  - (3) withdraw or suspend certification, and, if and to the extent it deems appropriate, require the payment of an amount not to exceed INR 10,00,000 (Rupees Ten Lakhs) for each day of violation;

*Provided that* an order for suspension of certification may be passed only after giving the Certified Virtual Currency Business prior notice and an opportunity of being heard.

- (e) Any amount collected by the Committee under sub-section (d) shall be remitted within 30 days by the Committee to DABFI, for use in connection with its objectives.
- (f) The Committee will not exercise its discretion to cancel, suspend or withdraw certification without first giving the Certified Virtual Currency Business a period of not less than 14 days to respond to the Committee's concerns and provide reasons as to why such action should not be taken.

---

91. This is based on the ADCCA Code of Conduct, available at <http://adcca.org.au/wp-content/uploads/2016/12/ADCCA-Code-of-Conduct.pdf>. In addition, the committee has been granted the power to impose a penalty (S. 19(d)(3) (based on the ULC Model Act).

- (g) In making its decision, the Committee will consider whether the incident of non-compliance is evidence of a systemic failure of business processes, systems or policies such that they are inadequate to ensure consistent compliance with this Code.
- (h) A Certified Virtual Currency Business whose certification has been cancelled, suspended or withdrawn, shall be barred for applying for certification afresh for a period of 2 years.

## Section 20. Legal Status.<sup>92</sup>

- (a) This Code is a contract between DABFI, the members of the Committee, Applicants, and Certified Virtual Currency Businesses, provided that the Committee shall have the right to amend the Code by a vote of 75% of its members and by approval of the Board of DABFI. Such amendment shall be with prior written notice to Certified Virtual Currency Businesses but shall not require their consent.
- (b) This Code shall apply in addition and subordinate to applicable law. For abundant clarity, to the extent that any provisions hereunder conflict with those under law, the latter shall prevail.
- (c) Any dispute arising out of or in connection with this Code between an aggrieved Certified Virtual Currency Business or an Applicant and DABFI, including any questions regarding its existence, validity or termination, shall be referred to and finally resolved by arbitration in accordance with the Arbitration Rules of the Mumbai Centre for International Arbitration (“MCIA Rule”), which rules are deemed to be incorporated by reference into this clause.
- (d) The proceedings in relation to arbitration shall be as follows:
  - i) The seat of arbitration shall be Mumbai.
  - ii) The Tribunal shall consist of three arbitrators.
  - iii) The language of arbitration shall be English.
  - iv) The law governing this arbitration agreement shall be Indian law.
  - v) The law governing the contract shall be Indian law.
- (d) If any provision of this Code or its application to any person or circumstance is held invalid, the invalidity does not affect other provisions or applicability of this Code which can be given effect without the invalid provision or application. To this end, the provisions of this Code are severable.

---

<sup>92</sup>. This is loosely based on the ADCCA Code of Conduct but has been modified.

---

# Chapter 5 - Disclosures and other Protections

## Section 21. Required Disclosures.

- (a) Each Certified Virtual Currency Business shall publicly disclose, and receive the express consent of its customers<sup>93</sup> to, the matters required by subsection (b) and any additional disclosures that the Committee deems reasonably necessary for the protection of the general public.
- (b) Disclosures required by this section shall be made separately from any other information provided by the Certified Virtual Currency Business and in a clear and conspicuous manner in a Record that customers may preserve. A Certified Virtual Currency Business may propose alternate disclosures as more appropriate for the Certified Virtual Currency Business's Virtual Currency Business Activity in India for the Committee's approval.
- (c) The information referred to in subsection (a) is:
- (1) A schedule of all fees and charges that the Certified Virtual Currency Business may assess, the manner that fees and charges will be calculated if not set in advance and disclosed, and, if relevant, the timing of such fees and charges;
  - (2) The extent to which the product or service provided by the Certified Virtual Currency Business is covered by a form of insurance;
  - (3) A notice that any Transfer or Exchange of Virtual Currency normally is irrevocable and any exception to the irrevocability of Transfer or Exchange;
  - (4) A notice describing the Certified Virtual Currency Business's liability for unauthorized, mistaken, or accidental Transfers or Exchanges and, for the purposes of enabling customers to obtain relief, describing the customer's responsibility for providing notice to the Certified Virtual Currency Business of the Transfer or Exchange together with a description of the basis for any recovery by the customer from the Certified Virtual Currency Business and of general error-resolution rights applicable to any transaction;
  - (5) A notice that the date on which a Transfer or Exchange is made and the customer's account is debited may differ from the date or time that the customer initiates the instruction to Transfer or Exchange or makes a Transfer or Exchange of Virtual Currency from one account to another, or from one person to another;
  - (6) Whether the customer has a right to stop a pre-authorized Transfer of Virtual Currency and the procedure to initiate a stop-payment order or to revoke the authorization for subsequent Transfers;
  - (7) The customer's right to receive a receipt, trade ticket, or other evidence of a Transfer or Exchange;
  - (8) The customer's right to at least 30 days' prior notice of a change in the Certified Virtual Currency Business's fee schedule, other terms and conditions of operating, or the policies on the customer's account;
  - (9) A disclosure of the fact that Virtual Currency has not been recognized by the Government of India as legal tender;
  - (10) A disclosure under Section 23(a), if applicable; and,

---

93. This requirement of consent has been added, and is in line with the rules made under the Information Technology Act, 2000.



- (11) A disclosure on applicable taxes in furtherance of Section 22(a)(5).
- (d) At the conclusion of a Virtual Currency transaction involving a customer, the Certified Virtual Currency Business shall furnish to such customer a confirmation in a Record that contains:
- (1) the name and contact information of the Certified Virtual Currency Business, including information a customer may need to file a complaint or ask a question;
  - (2) the type, value, date, precise time, and amount of the transaction; and
  - (3) the fee charged to the customer for the transaction, including any charge for conversion of Virtual Currency to another Virtual Currency or to Legal tender.
- (e) A Certified Virtual Currency Business may elect to furnish a single, daily confirmation for all transactions on that day with a customer instead of a per-transaction confirmation if the Certified Virtual Currency Business discloses its decision to furnish a daily confirmation to the customer in the initial disclosures provided under this Section.

## Section 22. Customer Protection Policies and Procedures.

- (a) A Certified Virtual Currency Business shall establish, implement, publish in a Record available to customers and the Committee, and maintain customer protection policies and procedures as enumerated in this section. The policies and procedures required by this section shall include:
- (1) any action or system of Records required to comply with the provisions of this Code and applicable material provisions of any law applicable to the Certified Virtual Currency Business's Virtual Currency Business Activity in India;
  - (2) procedures for resolving disputes between the Certified Virtual Currency Business and its customers;
  - (3) procedures for detecting and deterring fraud that comply with subsection (b);
  - (4) procedures for customers to report unauthorized, mistaken, or accidental transactions.

and

- (5) providing an explanation of applicable taxes in respect of different transactions and procedures for obtaining undertaking from customers stating that all applicable taxes which need to be paid under law have been paid.
- (b) A Certified Virtual Currency Business shall provide not less than 30 days' advance notice to its customers of any proposed change in its customer protection policies and procedures required by this section that pertain to dispute resolution, complaint filing, or reports of unauthorized, mistaken, or accidental transactions.
- (c) A Certified Virtual Currency Business shall establish and maintain policies and procedures to resolve complaints in a fair and timely manner and provide a notice as soon as reasonably possible of resolution and the reasons for it to the complainant. A Certified Virtual Currency Business shall also appoint a Grievance Redressal Officer whose contact details shall be made easily accessible and will be responsible for addressing issues of complaints.
- (d) These policies and procedures must be made available in a clear and conspicuous manner separately from other disclosures made to customers and in the medium through which the customer contacted the Certified Virtual Currency Business. At a minimum, these disclosures shall include:

- 
- (1) the Certified Virtual Currency Business's mailing address, the telephone number that customers may employ to contact the Certified Virtual Currency Business, and the physical and electronic addresses to which customers may send complaints;
  - (2) a statement that customers may bring complaints to the attention of the Committee;
  - (3) notice of the customers' rights under Section 19(b), and the Committee's mailing address, website, and telephone number; and
  - (4) other information the Committee reasonably requires for an effective complaint system, such as information about what statements of complaint should cover, including information, particulars and documents relating to disputes between a Certified Virtual Currency Business and a consumer.
- (e) For three years from the date of the resolution of a complaint or such lesser period as the Committee may allow, a Certified Virtual Currency Business shall retain a Record of the complaint, resolution of the complaint, and notice to the complainant regarding the resolution of the complaint.
- (f) A Certified Virtual Currency Business shall maintain Records so that customers' Virtual Currency are separately identifiable from the Virtual Currency of the Certified Virtual Currency Business.

## Section 23. Property Interest in Virtual Currency in Control of Certified Virtual Currency Business.<sup>94</sup>

- (a) Except as otherwise provided in this Code, the Virtual Currency in the Control of a Certified Virtual Currency Business on behalf of a customer:
- (1) are held in trust for the entitlement of the customer;
  - (2) are not the property of the Certified Virtual Currency Business; and
  - (3) are not subject to the claims of creditors or purchasers of the Certified Virtual Currency Business:
- [Provided that the Certified Virtual Currency Business and its customers may expressly agree otherwise. In such event, the agreement must clearly define the property interest of the Certified Virtual Currency Business and the customer in the Virtual Currency.]*<sup>95</sup>
- (b) The duties of a Certified Virtual Currency Business with regard to the interests of customers in the Virtual Currency or Virtual Currency credentials held by the Certified Virtual Currency Business for the customers are as agreed by the customers with the Certified Virtual Currency Business to the extent that they are not inconsistent with this Code, or, in the absence of agreement, in accordance with commercial standards performed with due care and in good faith.

---

94. Alternative A-1 from the ULC March 2017 draft has been tentatively chosen.

95. This proviso has been inserted since each Virtual Currency Business has a different business model, and this requirement was objected to by Coinbase ([http://www.uniformlaws.org/shared/docs/regulation%20of%20virtual%20currencies/2017feb28\\_RVCBA\\_Comments\\_Coinbase.pdf](http://www.uniformlaws.org/shared/docs/regulation%20of%20virtual%20currencies/2017feb28_RVCBA_Comments_Coinbase.pdf)). With the proviso, the business is free to have a different structure, as long as that structure is expressly agreed upon. Alternatively, this can be made a disclosure requirement under Section 21.

## Section 24. Mandated Compliance Programs and Policies and Monitoring.

(a) A Virtual Currency Business before submitting its application for certification shall create and maintain the following programs, policies, and monitoring procedures:

- (i) a cybersecurity program,
- (ii) a business continuity program, a disaster recovery program,
- (iii) an anti-fraud program as required by Section 25,
- (iv) an anti-money laundering and prevention of terrorist activity funding program,
- (v) a KYC program that evidences compliance prior to on-boarding new customers,
- (vi) compliance with:
  - (1) this Code; and
  - (2) all applicable laws, including and not limited to those set out in Section 12.

Once certified, the Certified Virtual Currency Business shall keep and preserve Records describing each program, policy, and monitoring procedures at all times.

- (b) Each program, policy, or procedure under subsection (a) must be designed to be adequate for the Certified Virtual Currency Business's contemplated Virtual Currency Business Activity in India, considering all the circumstances of the participants, including its customers, that may be involved and the safe operation of the Virtual Currency Business Activity involved.
- (c) Each program, policy, or procedure of the Certified Virtual Currency Business must be compatible with other programs, policies, and procedures and not conflict with regulations applicable to the Certified Virtual Currency Business under other applicable law. A program, policy, or procedure, if adequate, may be a program, policy, or procedure already in existence at the Certified Virtual Currency Business's Virtual Currency Business, whether adopted by the Certified Virtual Currency Business on its own or required under law.
- (d) A Certified Virtual Currency Business may request advice from the Committee or another source as appropriate as to compliance with this section.
- (e) After the programs, policies, and procedures required by subsection (a) are created and approved by the Committee and officers of the Certified Virtual Currency Business, the Certified Virtual Currency Business must employ a program director with adequate authority and experience to monitor each program, publicize it as appropriate, recommend changes as desirable, and enforce such programs.

Committee shall within two weeks of receiving a request from a Certified Virtual Currency Business under this Section, intimate its decision to such Certified Virtual Currency Business.

- 
- (e) The fact that a particular program, policy, or procedure fails in a given instance or instances to meet its goals is not by itself a ground for liability of the Certified Virtual Currency Business if the program, policy, or procedure was properly created and operated, *provided however* that repeated failures are evidence of a failure to monitor operations properly.

## Section 25. Policies and Procedures to Detect and Deter Fraud and Money Laundering

Without prejudice to the provisions of this Code, each Certified Virtual Currency Business's policies and processes for detecting and deterring fraud, money laundering, and terrorist financing, must include, at a minimum:

- (a) the identification and assessment of the material risks of its Virtual Currency Business operations related to fraud;
- (b) procedures and controls to protect against other material risks identified by the Committee or the Certified Virtual Currency Business;
- (c) procedures for periodic evaluation and revision of the anti-fraud procedures, controls, and monitoring mechanisms; and
- (d) procedures for the identification and assessment of the risks of its Virtual Currency Business operations related to money laundering and terrorist financing.

## Section 26. Limitation of Liability

- (1) Certified Virtual Currency Businesses and Applicants agree that they are solely responsible for Virtual Currency Business Activities and their respective transactions with customers and that DABFI or Committee does not provide products or service to those customers or prospective customers.
- (2) Certified Virtual Currency Businesses and Applicants agree that DABFI and Committee are not liable for any act or omission of a Virtual Currency Business and hold DABFI and Committee harmless against any suit, claim, action, investigation, complaint or other request for compensation to the fullest extent permitted by law.

# Appendix 1: DABFI Certification Mark and Explanatory Text <sup>29</sup>

## 1A: DABFI Certification Mark

The DABFI Certification Mark is shown below. It shall be displayed prominently on all electronic and physical materials of the Certified Virtual Currency Business, so as to catch the attention of a reasonable consumer. It may not be reproduced in any other format or colours and must not be less than 366 by 80 pixels.



[image to be inserted]

*Exercise extreme caution in dealing with any Virtual Currency Business not certified under the Code of Self-Regulation for Virtual Currency Businesses in India adopted by the Digital Asset and Blockchain Foundation of India (DABFI).<sup>97</sup>*



## 1B: DABFI Certification Explanatory Text

The following text explaining the nature and purpose of DABFI certification must be included on the website and mobile app of a Certified Virtual Currency Business:



The Code of Self-Regulation for Virtual Currency Businesses in India is a voluntary scheme that establishes best practice standards for businesses operating in the Indian Virtual Currency industry.

The Code is administered by an independent Committee of the Digital Asset and Blockchain Foundation of India and is available for adoption by businesses operating in India that carry on Virtual Currency Business Activity.

[Company Name] is a member of DABFI and has held certification under the Code since [Month Year]. The full text of the Code of Self-Regulation for Virtual Currency Businesses in India is available at [insert link].



---

96. This is loosely based on the ADCCA Code of Conduct, but has been modified.

97. Since this Code cannot bind non-certified parties, this message is a way of warning consumers that non-certified parties should be dealt with using caution.





# Nishith Desai Associates

LEGAL AND TAX COUNSELING WORLDWIDE

## MUMBAI

93 B, Mittal Court, Nariman Point  
Mumbai 400 021, India

tel +91 22 6669 5000  
fax +91 22 6669 5001

## SILICON VALLEY

220 California Avenue, Suite 201  
Palo Alto, CA 94306-1636, USA

tel +1 650 325 7100  
fax +1 650 325 7300

## BANGALORE

Prestige Loka, G01, 7/1 Brunton Rd  
Bangalore 560 025, India

tel +91 80 6693 5000  
fax +91 80 6693 5001

## SINGAPORE

Level 30, Six Battery Road  
Singapore 049 909

tel +65 6550 9856

## MUMBAI BKC

3, North Avenue, Maker Maxity  
Bandra-Kurla Complex  
Mumbai 400 051, India

tel +91 22 6159 5000  
fax +91 22 6159 5001

## NEW DELHI

C-5, Defence Colony  
New Delhi 110 024, India

tel +91 11 4906 5000  
fax +91 11 4906 5001

## MUNICH

Maximilianstraße 13  
80539 Munich, Germany

tel +49 89 203 006 268  
fax +49 89 203 006 450

## NEW YORK

375 Park Ave Suite 2607  
New York, NY 10152

tel +1 212 763 0080