Regulating The Minefield:

Introduction:

Blockchain technology is an immutable database which stores information in digital form. Blockchain is a decentralised technology, with data being spread amongst several nodes. When a new transaction is processed it is broadcasted to every node in the network. If the majority of nodes validate the transaction, a new block is added to an existing blockchain of validated transactions (meaning blockchain works on a peer-to-peer basis, removing the need for a central authority). Once added to the chain of transactions the blocks cannot be altered.

Blockchain emerged as a method of mitigating the primary concerns associated with smart technology (privacy and security). At present, blockchain is primarily used in approving transactions involving cryptocurrency. However, "the application fields for blockchains seem to be manifold, especially in areas that have historically relied on third parties to establish a certain amount of trust".[1] Blockchain has significant potential as a facilitator in the financial industry, supply chain management, and democratic elections. It has even suggested that "politics and society might be restructured by the blockchain".[2] Particularly throughout Industry 4.0, blockchain will become a more integrated technology.

The immutability and disintermediation of blockchain, along with its potential for a diverse range of applications means blockchain is a unique emerging technology.

An analogy could be drawn to Whack A Mole, where once you have whacked one mole another appears. As Blockchain mitigates the risks of privacy and security, it creates new risks. Such risks provide novel challenges to regulators. These will be discussed throughout, along with potential regulatory strategies.

Critical Regulatory Challenges Associated With Blockchain:

The unknown quantity of blockchain:

Blockchain is a rapidly growing technology with the blockchain market forecasted to grow by almost 63 Billion USD within the next four years.[3] With blockchain becoming increasingly prevalent, and its different uses expected to expand exponentially in unforeseeable ways, the technology represents an unknown quantity. Therefore, regulators are ignorant, meaning

[1] Michael Nofer, Peter Gomber, Dirk Schiereck "Blockchain – A Disruptive Technology" (2017) 59 BISE 183 at 184.

[2] Above n 1 at 186.

[3] "Blockchain Market by Component" (13 August 2022) Markets and Markets <https://www.marketsandmarkets.com/Market-Reports/blockchain-technology-market-90100890.html>

they cannot predict the probability of a blockchain development, or even determine all possible ways blockchain will develop.

For regulators, the accelerated evolution of blockchain produces a real tension between whether to regulate upstream or downstream. Regulating blockchain applications at present risks normative disconnection (that is blockchain develops and is used in other ways, thereby diminishing the value of the regulation). However, regulating blockchain at some future time could be overly reactionary, as significant harm may have to occur for regulators to fully understand the risks associated with a given application.

Alegality of Blockchain?

A critical regulatory challenge is determining whether blockchain is even capable of being regulated. De Filippi posits whether "blockchain operates in its own space where it is neither legal nor illegal", basically summarised, is blockchain alegal? [4]

De Filippi considered alegal matters as "neither legal nor illegal; they merely subsist outside of the legal realm … exceed the intelligibility of the law and cannot be reduced to the legal/illegal binary".[5] Importantly, alegality is not synonymous with difficult to regulate.

The Dao Attack provides an example of how blockchain could be perceived as alegal. The Dao was an investment fund facilitated through a smart contract using blockchain technology. This fund was collectively managed by the investors, instead of a central authority. Every action made in respect of The Dao had to be done on a smart contract transaction. However, the smart contract governing the investment fund had a vulnerability which allowed someone to take $60 million USD from the fund. The Dao was not a registered company in any jurisdiction "but rather subsisted as a decentralized software entity, replicated on the computer of all network nodes".[6] Kiviat suggested "the traditional legal system offered limited recourse, as the lack of a centralized authority combined with the pseudonymity of participants made it virtually impossible for the investors to reclaim their loss through traditional legal means". [7]

The Dao attack provides an example of how blockchain could be perceived as alegal. If this case came before a court, even if regulation prohibited such an action, the regulation could not have been enforced, and any remedy for breach of the regulation would have been of no utility. For regulators, this presents a unique challenge of deciding at the macro-level whether blockchain as a whole is capable of being regulated, and at the micro-level whether in regard to specific actions/instances blockchain is capable of being regulated.

Jurisdictional:

[4] Primavera De Filippi, Morshed Mannan, Wessel Reijers "The alegality of blockchain technology" (2021) 62 Policy Soc 2 at 7.

[5] Above n 4 at 7.

[6] Above n 4 at 14.

[7] Trevor Kiviat "Beyond Bitcoin: Issues in Regulating Blockchain Transactions" (2015) 65 DLJ 569 at 593.

A key trait of blockchain is its decentralisation. However, this means there is no controlling entity, as control is instead divided across multiple nodes globally.

This means that each individual node may be under different jurisdictions, making it difficult to establish which regulations would apply to a given transaction. Disintermediation also means there is no central authority which can be held accountable.

The jurisdictional challenges posed by blockchain are apparent when its decentralisation potential is maximised. Again, the Dao Attack is an illustrative example. This is because the Dao was not a registered company in any jurisdiction and existed on several network nodes spanning across the world. Therefore, it is unlikely the Dao attack could be said to fall within any jurisdiction.

Regulatory effectiveness is an issue, with the key criterion for effectiveness being whether the intervention is likely to achieve its regulatory purpose.[8] The jurisdictional issues creates efficacy challenges for regulators. This is because decentralisation means blockchain can easily act outside the scope of regulatory boundaries, thereby reducing the potential efficacy of the regulation. With each independent jurisdiction favouring differing regulatory tilts – a collaborative approach is not feasible. This leaves regulatory bodies in each jurisdiction grappling with how to maximise the effect of regulation.

Lex cryptographia:

Smart contracts operate as a code, stipulating what can and cannot be done on a particular blockchain. This means that "the parties to a smart contract are making law, implying—or rather coding—the values they take to be fundamental, and initiating the law's automatic execution". [9] As blockchain is immutable, the code that governs cannot be altered and compliance with the code is the only option (like West Coast regulation). In effect, this creates quasi-legal standards (known as lex cryptographia).

If regulators fail to properly engage with the other three challenges discussed, regulation will not be effective. This leaves a gap for an undemocratic, private entity assuming what is effectively regulatory power by using smart contract code to govern the use of that blockchain application - a rather dystopic outcome.

De Filippi emphasized this as a challenge, saying "in a world increasingly reliant on technology and ruled by networks, whoever owns and controls these platforms will always have a significant power".[10] Publicly accountable regulators must overcome other regulatory challenges (described above) so regulation is effective, thereby ensuring they and not private entities assume "significant power".

[8] Roger Brownsword, Morag Goodwin "Law and the Technologies of the Twenty-First Century: Text and Materials" (Cambridge University Press, Cambridge, 2012) at 61.

[9] Katrin Becker "Blockchain Matters—Lex Cryptographia and the Displacement of Legal Symbolics and Imaginaries" (2022) 33 Law Crit. 113 at 118.

[10] Above n 4 at 126.

Potential Strategies To Mitigate Regulatory Challenges:

Regulatory Sandbox Approach:

Mangano is a proponent of the regulatory sandbox approach. Sandboxes are mechanisms used in fintech, to establish a controlled environment to experiment with new technologies.[11] Authorised firms are granted legal exemption to develop the applications of the technology unencumbered, enabling regulators to observe and analyse the developments of the technology in a controlled, transparent ecosystem. This usually occurs on a small scale, for up to six months. Sandboxes are becoming increasingly prevalent in several financial centres in analysing the development of fintech innovations.

The sandbox approach promotes an open dialogue between innovators and regulators; and encourages innovation that complies with the governing rules of that ecosystem. In effect, this means sandboxes function as a crystal ball allowing regulators to see what may be downstream, and therefore enables them to introduce some upstream regulation. Thereby, sandboxes strike a balanced regulatory tilt between facilitation and regulation.

Using the development of Initial Coin Offerings (ICOs) as an example. If the sandbox approach were deployed, it would have allowed regulators to identify equivalence with another aspect of law (at first the dominant use of ICOs was effectively equivalent to an Initial Public Offering). The sandbox could have demonstrated the later, and unforeseeable innovative development of the ICOs into an unprecedented form of a crypto asset. The sandbox would have therefore provided an otherwise unattainable insight into the benefits and risks associated with these unique crypto assets. Regulators would have efficiently reduced risks to investors by introducing some form of investor protection laws, whilst ensuring these protection laws do not cover the crypto asset iteration of an ICO. This is all while allowing the ICO to continue evolving.

However, a sandbox is not an all-encompassing solution. There is insufficient regulatory capacity to place every possible application of blockchain within a controlled ecosystem. Further, the sandbox faces temporal limits as some innovations will be slow burners, and the time they take to develop will be outside the purview of the sandbox.

Blockchain regulating blockchain?

This is the most left-of-field regulatory tactic explored. A potential strategy is to use the unique attributes of blockchain to regulate the use of blockchain itself. As described earlier

[11] Renato Mangano "Blockchain Securities, Insolvency Law and the Sandbox Approach" (2018) 19 Eur 715 at 728.

smart contract code works as a form of West Coast regulation, dictating what can and cannot be done on a particular blockchain.

A potential regulatory solution is that to operate on blockchain in a given jurisdiction you have to be registered. If you are registered within that jurisdiction you have to work within the overarching blockchain of that jurisdiction, which is governed by a smart contract code. The code would be set by a publicly accountable regulator. International Monetary Fund director Christine Lagarde notes that "the same innovations that power crypto-assets can also help us regulate them". [12]

This still allows for private entities to set their own rules governing the use of their blockchain application, as they can use cross-chain smart contracts. But, importantly, these cross-chain smart contracts are subsidiary to the overarching smart contract set by the public regulator, so any cross-chain contract must be consistent with that overarching smart contract code.

In summary, this would mean that to use blockchain for example, in New Zealand you would have to register. By registering you have to work under the primary "blockchain of New Zealand". The "blockchain of New Zealand" would then be governed by a smart contract code set by a public body. Private bodies using blockchain create their own smaller chains under the primary "blockchain of New Zealand", but their subsidiary smart contracts governing their application are constrained by the West Coast regulation of the overarching smart contract.

Finck outlines the process this form of regulation would take saying "law is first created through regulation or legislation and subsequently implemented through cryptographic smart-contracting computer code". [13]

Since blockchain is always evolving, there will likely have to be constant adjustments to regulation. Smart contract code is immutable, so if regulation needed adjustment it would require a new smart contract. Smart contracts can be substituted for another (via "proxy contracts"), so the new adjusted contract would substitute in for the existing contract.

This unorthodox regulatory strategy carries some key benefits. It mitigates the alegality challenge because the code works as a form of West Coast regulation, guaranteeing regulation is effective. The registration element eliminates jurisdictional issues. Mitigating these two challenges, attenuates the lex cryptographia risk (as it ensures that public regulation is effective, and therefore, leaves no room for private entities to set the supreme regulations).

Regulators would have to ensure that the code was open-ended, so it would still allow for new innovative applications to emerge.

[12] Christine Lagarde 'Addressing the Dark Side of the Crypto World' (13 March 2018) IMFBlog <Addressing the Dark Side of the Crypto World – IMF Blog>

[13] Michèle Finck "Blockchain Regulation and Governance in Europe" (Cambridge University Press, 2018) at 74.

However, this regulatory tactic is unprecedented and carries substantial concerns. Using smart contract code as a form of regulation diminishes all flexibility in the law, because the law is quite literally code. Using this inflexible regime means there are no borderline cases in the grey, everything is either allowed or prohibited. De Filippi highlights this as a pertinent concern saying "[legal rules] must be drafted at a higher layer of abstraction so as to be agnostic to the specificities of a case. They must be generic enough to be able to encompass new and unforeseen situations, which are factually different from previous cases, but which are practically or ideologically the same". [14]

Second, smart contract code as the law removes any form of human discretion of how the law ought to apply in a given circumstance. Again, De Filippi voices their concern saying, "human judgement is thus necessary in order to give meaning to the law … to properly appreciate the wording of the law, it is essential to account for the original intentions of the legislator".[15] Using code as law prohibits human discretion, and therefore prevents the common law developing a body of flexible case law which responds to changes in society.

De Filippi said "the prospect of automated legal governance is something that should, to the very least, be examined with great caution."[16] But with blockchain being such a novel technology, does it call for the most novel of regulatory responses? Perhaps this regulatory strategy would be a more viable option when machine learning becomes more prevalent. Machine learning would allow the smart contract code through artificial intelligence to learn and apply more flexible standards, and therefore the code would provide regulation which is more aligned with how traditional legal standards are drafted. But for now, that is merely a future thought.

Follow the leader?

Malta was the first jurisdiction to introduce regulation regarding blockchain.[17] A leading initiative was introducing an optional licence for network operators. This licence certified that a given operator will work within the existing legal infrastructure. The rationale is that this will incentivise people to acquire a licence, because people will only want to deal with verified users.

However, as it is voluntary, it leaves room for a "blockchain black market" to exist. For example, if two people wish to engage in illicit activity they will both ensure they do not acquire a licence - thereby, operating outside the purview of regulations.

To modify the Maltese approach and require a licence to use blockchain technology is an unrealistic idea lacking real-world application, it has been labelled as "absurd".[18] This is

[14] Primavera De Filippi, Samer Hassan "Blockchain Technology as a Regulatory Technology From Code is Law to Law is Code" (2016) 21 First Monday 1 at 17.

[15] Above n 14 at 17.

[16] Above n 14 at 19.

[17] Joshua Ellul, Jonathan Galea, Max Ganado, Stephen Mccarthy, Gordon Pace "Regulating Blockchain, DLT and Smart Contracts: a technology regulator's perspective" (2020) 21 ERA Forum 209 at 216.

[18] Above n 17 at 217.

evidenced through the failure of the New York BitLicence regime. In New York to facilitate virtual currency transactions you needed to acquire a licence. Consequently, many firms moved to other states, with the state infamously only issuing 25 licences within five years of the regime.[19] One would imagine, using licences for blockchain would have a similar chilling effect.

Controlling access points:

Brownsword and Goodwin said, "it will rarely be true to say that an emerging technology finds itself in a regulatory void".[20] Although, not a perfect parallel there is an analogy to be drawn between the internet and blockchain, primarily because both share the unique trait of disintermediation. Finck outlined that regulating certain points of control is a regulatory strategy used in relation to the internet, which could be of equal utility in regulating blockchain. [21]

For regulating blockchain this would require using ISP addresses to "determine whether miners connect to nodes in their area, creating a presumption of participating in blockchain governance".[22] These miners would provide the access point of control for regulators. Blockchain technology is heavily reliant on miners, as these actors add new data to an existing chain and verify the legitimacy of transactions on the ledger. Finck said "contrary to conventional assumptions, miners can be identified relatively easily".[23]

Regulating miners could take two forms. First, regulators could incentivize miners to only process transactions or work on smart contracts that are consistent with regulations. Blockchain mining capital China have reportedly adopted measures similar to this, as they have agreed to subsidize electricity costs for miners who agree to abide with existing law (note: Electricity is a miners largest long-term expense).[24] Second, regulators could impose regulations directly onto miners, with failure to comply subject to punishment.

This strategy carries some distinct advantages. By getting at miners, regulators have control over an indispensable cog in the blockchain wheel. Whether this is enforced by the carrot, or the stick is another question. But ultimately the general rationale of regulating points of control is in my perspective a sound regulatory strategy which is tailored well to dealing with the unique traits of blockchain.

Using ISP addresses also overcomes jurisdictional challenges. So, if a miner who had an ISP address in that jurisdiction they must oblige with domestic regulations.

[19] Matthew Kohen "New York's Relaxed BitLicense Could Still Take Lessons From Wyoming's Permissive Approach" (28 July 2020) JDSUPRA <https://www.jdsupra.com/legalnews/new-york-s-relaxed-bitlicense-could-23441/#:~:text=The%20BitLicense%20was%20intended%20to,had%20only%20issued%2025%20BitLicenses>
[20] Above n 8 at 64.
[21] Above n 13 at 46.
[22] Above n 13 at 49.
[23] Above n 13 at 49.
[24] Above n 13 at 50.

No regulatory strategy?

Finck posited that "If distributed ledgers' real value proposition is in isolation from contemporary legal orders, they are unlikely to succeed".[25] For example, if the Dao Attack becomes a somewhat common occurrence, and people are left without recourse when things go wrong, the technology would lose its appeal. This is sound rationale, for who would want to risk purchasing an investment under an ICO, or selling property under a smart contract if there was no legal remedy if things went wrong? Perhaps, it is not for regulators to introduce regulation for blockchain, but it is for the users of blockchain to bring the technology within the existing legal infrastructure.

However, the risk with this passive regulatory approach is that significant harms like the Dao Attack would have to occur again before blockchain would bring itself within the existing legal system. So, for instances where there is risk of significant harm such a relaxed regulatory tilt is undesirable.

Leaving blockchain to self-correct, also still allows for lex cryptographia by private self-interested entities (as described above).

Conclusion:

Blockchain is a technology with exponential potential in its applications. This potential largely derives from its unique features, it is these points of difference which create novel challenges for regulators.

Jurisdiction, uncertainty and alegality create substantial regulatory challenges. Failure to engage with these challenges, runs the risk of lex cryptographia by private entities. Therefore, engagement by regulators is critical.

At current, deploying regulatory sandboxes is a balanced approach. Sandboxes allow blockchain to evolve as while being constrained by warranted regulation. For now, while blockchain is still in its genesis sandboxes provide the most neutral balance between facilitation and regulation. Should a sandbox forecast to regulators that regulation is necessary, controlling miners as the enforcement mechanism, is in my perspective is the most appropriate response.

2998.

[25] Above n 13 at 86.