CALL FOR MULTI-STAKEHOLDER COMMUNICATION TO ESTABLISH A GOVERNANCE MECHANISM FOR THE EMERGING BLOCKCHAIN-BASED FINANCIAL ECOSYSTEM

Yuta Takanashi, Shin'ichiro Matsuo, Eric Burger, Clare Sullivan, James Miller, Hirotoshi Sato*

ABSTRACT

Financial regulators around the world regulate financial intermediaries and activities to achieve their regulatory goals including investor/consumer protection, financial stability and prevention of financial crimes, and in so doing address various market failures. These objectives are needed in the social interest regardless of the technologies used by the financial system.

Blockchain technology and any financial ecosystem based on it have technical characteristics including decentralization, autonomization, anonymization and globalization, which could undermine the ability of regulators to achieve regulatory goals. Especially when it comes to preventing financial crimes, these characteristics could have significant negative impact on the ability of regulators. The intergovernmental Financial Action Task Force ("FATF")[1] recognizes these issues and is tackling them by issuing multiple guidelines; however, it seems that such

* Yuta Takanashi is Deputy Director for Fintech and Innovation at the Financial Services Agency (JFSA, Japan's financial regulator) and a Senior Fellow in the Department of Computer Science and McDonough School of Business at Georgetown University; Shin'ichiro Matsuo is a Research Professor of Computer Science at Georgetown University; Eric Burger is a Research Professor of Computer Science at Georgetown University; Clare Sullivan is a Visiting Professor at the Georgetown Law Center; James Miller is a Columbia Institute for Tele-Information Affiliated Researcher at Columbia Business School; Hirotoshi Sato is Vice President in the Digital Transformation Division at Mitsubishi UFJ Financial Group. Opinions presented in this paper belong solely to the Authors and do not represent any positions of the organizations to which they belong. We are grateful to Gary Gensler, Cara LaPointe, Simon Persico, Shigeya Suzuki, and Pindar Wong for their comments on earlier drafts; to James Angel, Paul Brigner, Jessica Gomel-Veksland, John Jacobs, Yuji Kawada, Tatsuya Kurosaka, Deepthi Machavaram, Daisuke Nakao, Robert Wardrop, Taro Watanabe, and colleagues from JFSA for inspiring discussions.

[1] Founded at the 1989 G7 Summit in Paris.

efforts are falling behind rapid technological developments. Thus, financial regulators must discover ways to achieve regulatory goals even in a blockchain-based financial ecosystem. This situation is similar to the case of telecommunication regulators during the rise of the Internet. The Internet complicated their regulatory goals including intellectual property rights protection and contents regulation. Thus, their relevant experiences provide a good reference. In the face of such difficulties in cyberspace, it was suggested to invoke not just law but also social norms, market mechanisms and architecture (software and hardware) to achieve a certain level of oversight. In fact, various stakeholders cooperated towards utilizing these modes of oversight in order to address issues brought by the Internet. Based on the lessons from the Internet, financial regulators should recognize that cooperation between multi-stakeholders would be beneficial for them, and they should actively play a role towards establishing a cooperative environment among stakeholders. Especially because code embedded in a blockchain system could determine the level of oversight on the activities within a blockchain-based financial ecosystem, regulators should consider ways to cooperate with engineering communities developing code despite often disparate incentives and mindsets. Once regulators successfully establish a cooperative relationship with the engineering community and can together develop code that facilitates mechanisms to achieve regulatory goals, they still must empower society to use such code in order to actually achieve regulatory goals, which requires consideration on alignment with social norms and market competitiveness; thus, regulators must cooperate with other stakeholders including businesses and users.

Through these considerations, this paper concludes that regulators should establish multi-stakeholder governance mechanisms within a blockchain-based financial ecosystem by improving cooperation among stakeholders. The final part of this paper provides some thoughts on relevant open questions, which we will continue to work on.

1. INTRODUCTION

In this paper, we will discuss (1) financial regulatory issues raised by blockchain technology, (2) lessons from the Internet as a reference point and (3) ways to deal with regulatory issues via a multi-stakeholder governance approach.

The main contribution of this paper is to reveal the need for regulators to play a role in establishing a multi-stakeholder governance mechanism in order to achieve their regulatory goals. Building upon analysis of implications for regulability from blockchain-based financial activities and lessons from the experience of the Internet in Parts I and II, Part III

discusses why and how should regulators influence code development as well as the way businesses and users use code within the ecosystem. It concludes that regulators need to cooperate with other stakeholders including the engineering community, businesses and users to achieve regulatory goals, and should establish a multi-stakeholder governance mechanism for a blockchain-based financial ecosystem. The final part of this paper provides some thoughts on the key points for establishing such a mechanism, though open questions remain.

PART I: Analysis of Regulatory Issues Raised by Blockchain Technology

2. GOALS OF FINANCIAL REGULATION AND HOW REGULATORS ACHIEVED THEM BEFORE BLOCKCHAIN

Part I aims to convince readers that (1) financial regulatory goals are in the social interest, and (2) blockchain can lead to the creation of a new financial ecosystem that would reduce the ability of regulators to achieve those goals.

Armour and Awrey, in their textbook on financial regulation, explain that financial regulation is justified by the existence of market failures that break the efficient market hypothesis.[2] Although granular discussion of market failures is outside the scope of this paper, we summarize them in the following table:

Table 1. A brief explanation of market failures

Market Failure	Description
Asymmetric Information	When one party of in a transaction has more information than the other, asymmetric information can result. In such a situation, the less-informed party cannot make efficient decisions.[3] This leads to an inefficient market.
Negative Externality	Negative externalities are costs that third parties will suffer from transactions over which they have no control.[4] Because principal parties conducting these

[2] JOHN ARMOUR ET AL., PRINCIPLES OF FINANCIAL REGULATION (2016).
[3] SHAWN CUNNINGHAM, UNDERSTANDING MARKET FAILURES IN AN ECONOMIC DEVELOPMENT CONTEXT (2011).
[4] David J. Bjornstad & Marilyn A. Brown, *A Market Failures Framework for Defining the Government's Role in Energy Efficiency*, 2004-02 JOINT INST. FOR ENERGY AND ENV'T

	transactions will not take such costs into consideration, the rational decision made by these principal parties becomes irrational for the society as a whole.
Public Goods	Public goods have two distinguishing characteristics: (1) one cannot exclude consumption from others, and thus enjoying a "free ride" is possible, and (2) one can consume goods without reducing the quantity of good available to others, and thus the optimal price becomes zero.[5] Because of these characteristics, the provider of the goods cannot generate sufficient benefits for providing the goods, and thus society faces a shortage of such goods.
Imperfect Competition	An efficient competitive market requires three distinctive characteristics: (1) the existence of a large number of small producers, (2) free entry and exit into the market and (3) existence of a large number of well-informed consumers who can change sellers from which they buy products without cost.[6] In the absence of any of these conditions, the market fails to achieve perfect competition.
Irrational Behaviors	All of the other market failures can occur even when parties act rationally; if parties fail to act rationally, the market fails to become efficient.

Financial regulators exist to address these market failures. Each financial regulator articulates its mission and goals in varying parlance, and we do not find a formally agreed list of global regulatory goals; however, Armour and Awrey summarize financial regulatory goals as (1) investor and consumer protection, (2) financial stability, (3) market efficiency, (4) competition, and (5) preventing financial crime.[7]

2.1 Regulatory goals

(2004), https://pdfs.semanticscholar.org/1df8/dc89b3d0f4aa82dffbed34890a6bb63c0ba3.pdf?_ga=2.85888861.592873336.1571741086-1236752378.1571741086.

[5] *Id.*

[6] ARMOUR ET AL., *supra* note 2, at 51-79.

[7] *Id.*

2.1.1 Investor and consumer protection

Investor and consumer protection is a primary goal for financial regulators. In order for investors to assess risks and make an appropriate judgment on a given investment, they need accurate information. However, due to information asymmetry, investors may face difficulties in so doing and move on. In such a situation, regulators can intervene by requiring relevant entities to accurately disclose necessary information to investors to facilitate their decision-making processes.

In addition, investors and consumers rely on financial intermediaries such as banks to make informed judgments; however, there exists an additional problem of **information asymmetry** that prohibits investors and consumers from making appropriate decisions regarding which companies they should rely on or use. Thus, investors and consumers must monitor the companies, leading to "agency cost." Where it may be too high for individual investors and consumers, regulators intervene to eliminate or reduce it by imposing regulations such as licensing requirements. These measures are meant to better ensure that intermediaries conduct their business in a fair and accountable manner.

Furthermore, given that the average consumer or investor may not possess sufficient knowledge and experience and can behave irrationally, risking exploitation, regulators may impose limitations on their behavior.[8]

2.1.2 Financial stability and soundness

As demonstrated by the financial crisis of 2008, the failure of a financial institution can cause a greater failure of the financial system via a domino effect. This is a type of externality that financial regulators must address. In order to minimize the probability of failure of individual financial institutions, financial regulators impose regulations on them including capital requirements. In addition, deposit insurance schemes were introduced to maintain market confidence and protect users of the financial system by preventing bank runs.

However, the financial crisis of 2008 revealed that simply mitigating the probability of failure of an individual financial institution is not sufficient. Deposit insurance does not adequately protect institutional investors such as other banks, which caused the run-like behavior in the market. In addition, it turns out that the domino effect also could occur through correlated investment strategies with deleverage. Thus, after the financial crisis, financial regulators introduced special regulation on

[8] For example, in Japan, regulation imposes leverage limitations for margin trading in foreign exchange markets. *See* CABINET OFFICE ORDER ON FINANCIAL INSTRUMENTS BUSINESS, ETC., Articles 117-1-27 and 28.

systemically important financial institutions ("SIFI"s) and new types of regulations called "macroprudential regulation" that focus on the stability of the system as a whole.

2.1.3 Market efficiency

Investors not only invest in firms directly within the primary market but also invest in financial instruments within the secondary market. Without the secondary market, market prices will not reflect a real-time estimation of the valuation of a given firm. The speed and accuracy at which the market price reflects new information is called "information efficiency," which is important to maintain market liquidity and achieve an efficient allocation of resources.

In addition, information efficiency in the secondary market acts as a real-time monitoring tool for a firm's investment policies, guiding managers of the firm. The more accurate information is made available to the secondary market, the more accurate decisions investors can make.

In this regard, market information can be considered a public good; however, managers tend to be reluctant to disclose information for various reasons. Thus, regulators need to mandate timely, accurate, and adequate disclosure of necessary information.

2.1.4 Competition

Although there are antitrust laws and regulations to promote competition, financial regulators also play a role in promoting fair competition within the financial sector by targeting anti-competitive practices. For example, in the EU, local regulators worked together to create common regulations imposed on financial institutions to promote competition among them throughout the region.

2.1.5 Preventing financial crimes

Armour and Awrey mention that prevention of financial crimes such as insider trading and misstatement in disclosures is a supplement of other regulatory goals, including investor protection. But they also point out that prevention of financial crimes that take advantage of the financial system for socially harmful purposes ("public bad"), e.g. money laundering, should be distinguished as an independent regulatory goal.[9]

Although Armour and Awrey do not provide a regulatory approach towards this preventive goal, financial regulators and other national

[9] ARMOUR ET AL., *supra* note 2.

authorities including financial intelligence units ("FIU"s) take several measures to achieve it.[10] Generally today, regulators criminalize money laundering and regulate financial intermediaries such as banks as gatekeepers for the financial system in order to effectively enforce regulations related to criminal activities.[11] For example, in most jurisdictions, banks are required to conduct Know Your Customer ("KYC") screening when their customers open accounts, as well as ongoing monitoring to report suspicious activities in their accounts to authorities including FIUs.[12] With the information provided, national agencies investigate and prosecute criminal activities. For example, in the US, banks mandated to report suspicious activities reported 958,537 such activities in 2016, per the Financial Crimes Enforcement Network ("FinCEN").[13]

2.2 Costs and benefits

The above section delineates regulatory goals and why regulators need to intervene in markets. However, if the benefits from financial regulation do not exceed the costs of compliance, society cannot enjoy net benefits.[14] Armour and Awrey are aware of this balancing act[15] and point out that, in reality, it is not an easy task to estimate the costs and benefits of regulation due to the complexities of its effects.[16] Notwithstanding the difficulty in understanding costs vs. benefits, regulators still try to assess the impact of their regulatory actions. For example, the Financial Stability Board ("FSB"), a group of financial regulatory authorities, recently established a working

[10] It should be pointed out that making use of financial systems for criminal purposes is only one method for criminals to achieve their purposes. Hence financial regulation is only one part of governmental efforts to prevent such crimes. Regulatory approaches toward non-financial institutions and/or police enforcement actions against individual criminals are also available.

[11] The Financial Action Task Force recommends that national authorities criminalize money laundering, and mandate financial institutions to conduct customer due diligence and report suspicious transactions to the national financial intelligence unit. *See* FINANCIAL ACTION TASK FORCE, THE FATF RECOMMENDATIONS: INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION, http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf (updated June 2019).

[12] *See, e.g.*, Directive (EU) 2015/849 of 20 May 2015 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing [etc], Arts 2, 4, 8 and 11.

[13] *See* FINCEN, SAR STATS – ISSUE 3 – DEPOSITORY INSTITUTIONS (Mar. 2017), https://www.fincen.gov/sites/default/files/sar_report/2017-03-09/SAR%20Stats%203.pdf.

[14] The cost includes not only direct costs for regulated entities but also opportunity costs. For example, if the regulator regulates too much or too soon, people could be disincentivized to take risks to make profits or to generate innovation.

[15] ARMOUR ET AL., *supra* note 2.[16] *Id.*

[16] *Id.*

group to assess the impact of international regulatory standards.[17] In the context of regulation for a blockchain-based financial ecosystem, we need to pay close attention to the risks and benefits in relation to disruptive innovation. In fact, some of the regulators clearly articulate the importance of innovation and pursuit of regulatory goals in the least restrictive manner.[18] In the latter part of this paper, we will discuss this point by reviewing technology neutrality. The bottom line in practice would be that even though it is difficult to accurately assess costs and benefits, regulators make professional judgments in order to maximize the benefits and minimize the costs when they introduce new regulation.

Another point that merits attention is value judgment. Privacy and data access from public authorities present an example. For prevention of financial crimes, regulators need to collect information on who does what and where in order to consistently enforce regulations. However, the more regulators seek data, the greater the concern for the privacy of users of financial services. This is all the more relevant when financial transactions are conducted through Internet infrastructure. For instance, the EU's General Data Protection Regulation ("GDPR") enhances data protection and control of data collected by online service providers,[19] and seeks a socially agreeable balance between competing social interests.

3. CHALLENGES FOR REGULATORS IN ACHIEVING REGULATORY GOALS IN A BLOCKCHAIN-BASED FINANCIAL ECOSYSTEM

In the previous section, we discussed regulatory goals as social interests; however, the advent of a new financial ecosystem based on blockchain technology[20] could have inherent characteristics that would make it difficult for regulators to achieve their goals through traditional regulatory approaches.

---

[17] FINANCIAL STABILITY BOARD, FRAMEWORK FOR POST-IMPLEMENTATION EVALUATION OF THE EFFECTS OF THE G20 FINANCIAL REGULATORY REFORMS (July 3, 2017), http://www.fsb.org/wp-content/uploads/P030717-4.pdf.

[18] For example, European Commission has published on its aim to achieve regulatory goals at minimum cost. *See* EUROPEAN COMMISSION, BETTER REGULATION: GUIDELINES AND TOOLBOX, https://ec.europa.eu/info/law/law-making-process/planning-and-proposing-law/better-regulation-why-and-how/better-regulation-guidelines-and-toolbox_en (last visited Nov. 1, 2019).

[19] Per the GDPR, European citizens can enjoy better control of their personal data collected by online service providers, including an enhanced right to access and the right to be forgotten. *See* EUROPEAN COMMISSION, RIGHTS FOR CITIZENS, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens_en (last visited Nov. 1, 2019).

[20] As we will discuss, this paper mainly focuses on public blockchains as a key technology that will affect regulability within the financial ecosystem.

Some on the more progressive side of the spectrum may believe that society can transcend regulation and push for complete freedom of commerce[21]; however, we believe that regulatory goals are necessary regardless of the technology used in the financial system.

We do not necessarily believe that regulatory goals must be achieved through regulation in traditional ways, but we should find an alternative approach to achieve them to ensure a healthy economic system. In this section, the technical characteristics of blockchain that affect "regulability"[22] of financial services will be discussed in relation to their potential effects on the ability of regulators to achieve each aforementioned regulatory goal.[23]

Regulators worldwide increasingly have paid attention to the emerging market in crypto assets and a potential blockchain-based financial ecosystem. Reflecting this trend, in the Communiqué of the G20 Finance Ministers and Central Bank Governors Meeting held in Buenos Aires on July 21-22, 2018, a group of regulators articulated that "[t]echnological innovations, including those underlying crypto assets, can deliver significant benefits to the financial system and the broader economy. Crypto assets do, however, raise issues with respect to consumer and investor protection, market integrity, tax evasion, money laundering, and terrorist financing. Crypto assets lack the key attributes of sovereign currencies. While crypto assets do not at this point pose a global financial stability risk, we remain vigilant."

Following this statement, the FSB decided to begin collecting data and information to enhance monitoring[24] and recently published a report on the financial stability implications of decentralized financial technologies[25]; at

---

[21] Per "A Cypherpunk's Manifesto," "Cypherpunks deplore regulations on cryptography, for encryption is fundamentally a private act... Even laws against cryptography reach only so far as a nation's border and the arm of its violence. Cryptography will ineluctably spread over the whole globe..." *See* Eric Hughes, *A Cypherpunk's Manifesto* (Mar. 3, 1993), https://www.activism.net/cypherpunk/manifesto.html.

[22] Regulability here is defined as the effectiveness of regulatory approaches that aim to achieve certain regulatory goals. As discussed *infra*, traditional regulatory mechanisms could lose their effectiveness, decreasing regulability unless regulators can find other effective ways to achieve their goals.

[23] It is possible that new technologies could create new or eliminate some regulatory goals by altering the nature of the financial activities in the future; however, it is highly difficult to predict future changes at such a profound scale at this moment. Thus, in this paper and for the sake of simplicity, we assume that the regulatory goals we discuss will remain relevant in the near or foreseeable future even with greater blockchain use in the financial ecosystem.

[24] FINANCIAL STABILITY BOARD, CRYPTO-ASSETS REPORT TO THE G20 ON WORK BY THE FSB AND STANDARD-SETTING BODIES (July 16, 2018), http://www.fsb.org/wp-content/uploads/P160718-1.pdf.

[25] FINANCIAL STABILITY BOARD, DECENTRALISED FINANCIAL TECHNOLOGIES: REPORT ON FINANCIAL STABILITY, REGULATORY AND GOVERNANCE IMPLICATIONS (June 6, 2019), https://www.fsb.org/wp-content/uploads/P060619.pdf.

the same time, in considering appropriate responses to the emergence of a new financial ecosystem based on blockchain technology, it is important for regulators to think outside of the box.

3.1 Regulability for each regulatory goal

3.1.1 Investor and consumer protection and market efficiency

The International Organization of Securities Commissions ("IOSCO") has stated, "existing regulatory models may rely on access through a regulated entity to support many investor protection[s]… but access to crypto-asset platforms currently may not involve such regulated entities."[26] It already is difficult for regulators to impose necessary disclosure regulations on issuers of tokens or to take actions toward misconduct in the market,[27] with respect to protecting investors/consumers and maintaining an efficient market.

While a blockchain-based financial system would be global, regulators can only act within their respective jurisdictions, causing coordination problems across borders. Without universal and globally applicable regulations, achieving current levels of investor and consumer protection will become difficult, as demonstrated by fraud via initial coin offerings ("ICO"s). In many cases, issuers have failed to establish expected services, and their tokens have lost all or nearly all value. An Ernst & Young study found that "71% [of ICO-funded startups] have no offering in the market at all."[28] Amidst this predicament, it is not easy for regulators to impose adequate disclosure requirements on global ICO projects, as securities laws vary from jurisdiction to jurisdiction, and little has been done beyond the issuance of warnings.[29]

To ensure investor and consumer protection, regulators also aim to reduce agency costs by requiring financial intermediaries to follow certain business conduct; however, in a blockchain-based financial ecosystem, code

---

[26] FINANCIAL STABILITY BOARD, CRYPTO-ASSETS REPORT TO THE G20 ON WORK BY THE FSB AND STANDARD-SETTING BODIES (July 16, 2018), http://www.fsb.org/wp-content/uploads/P160718-1.pdf.

[27] In fact, UK researchers concluded that their AI program recognized approximately 236 cases of price manipulation in the crypto assets market from July to November 18, 2018, creating $7 million of transactional volume per day on average. *See* Jiahua Xu & Benjamin Livshits, *The Anatomy of a Cryptocurrency Pump-and-Dump Scheme* (Proceedings of the 28th USENIX Conference on Security Symposium, 2019), https://arxiv.org/pdf/1811.10109.pdf.

[28] *EY Study: Initial Coin Offerings (ICOs): The Class of 2017 – One Year Later*, ERNST & YOUNG (Oct. 19, 2018), https://www.ey.com/Publication/vwLUAssets/ey-study-ico-research/$FILE/ey-study-ico-research.pdf.

[29] IOSCO lists regulators' statements regarding ICOs on its website. *See* https://www.iosco.org/publications/?subsection=ico-statements.

could replace financial intermediaries. In such an environment absent regulators, investors and consumers themselves would need to check if the services and code providing services are sound, safe and trustworthy. This self-responsibility could lead to exploitation of inexperienced investors and consumers.

3.1.2 Financial stability

To ensure financial stability, the appropriate regulators look to financial intermediaries and reduce the probability of their failures by imposing various regulations such as capital requirements. However, in a blockchain-based financial ecosystem built upon code, financial regulators could face difficulties without exercising oversight over the code itself. For example, a single line of code with a simple mistake or bug could be tantamount the failure of a financial institution in payment and settlement systems, which in turn could roil the entire financial system in a worst case scenario.

Even without complete elimination of financial intermediaries, in a highly globalized market based on blockchain, financial regulators would find it difficult to impose necessary regulations across all involved jurisdictions. Autonomous frameworks would further complicate enforcement of regulations. For example, it may prove very difficult to impose stay requirements[30] unless the code of the contract were to allow such limits on an *ex-ante* basis.[31] In the context of macroprudential regulations, diversification in an autonomous blockchain-based financial ecosystem could stymie regulator efforts to appropriately and timely assess the macroprudential risks.

3.1.3 Preventing financial crimes

3.1.3.1 Theoretical consideration of the impact of the blockchain

Financial crimes are a substantial negative externality associated with a financial ecosystem, and it is important to mitigate them through financial regulation.[32] Below we discuss two hypothetical scenarios as shown in

[30] *ISDA Resolution Stay Jurisdictional Modular Protocol*, INTERNATIONAL SWAPS AND DERIVATIVES ASSOCIATION (May 3, 2016), https://www.isda.org/protocol/isda-resolution-stay-jurisdictional-modular-protocol.

[31] Phillip Paech, *The Governance of Blockchain Financial Networks*, 80 MODERN L. REV. 1073 (2017).

[32] Money laundering and other economic crimes cannot be eradicated through financial regulation alone. Rather, the goal of financial regulators is to prevent the financial system from being used by criminals.

Figure 1 to simplify our argument, although one can imagine many other different financial crime scenarios.

In Scenario A, criminals holding "dirty" fiat currency exchange it for crypto assets, which they launder and then exchange for clean fiat currency. Given that, at this moment, the process of exchange between fiat currency and crypto assets cannot be completed on-chain (meaning that a person/entity must conduct exchange in the real world upon entry and exit), regulations intended for the person/entity conducting the exchange theoretically could prevent the laundering of dirty fiat currency through a blockchain network, to the same extent possible with current financial services provided through financial intermediaries;[33] however, in practice, the global nature of a blockchain-based financial ecosystem could dilute the effectiveness of such regulations. The Financial Action Task Force ("FATF"), an international standard-setting body for financial criminal activities, clearly delineates how the global nature of a blockchain-based financial ecosystem gives rise to issues in regulability as "virtual currencies commonly rely on complex infrastructures... often spread across several countries, to transfer funds or execute payments. This segmentation of services means that responsibility for AML/CFT compliance and supervision/enforcement may be unclear. Moreover, customer and transaction records may be held by different entities, often in different jurisdictions, making it more difficult for law enforcement and regulators to access them... And importantly, components of a virtual currency system may be located in jurisdictions that do not have adequate AML/CFT controls. Centralised virtual currency systems could be complicit in money laundering and could deliberately seek out jurisdictions with weak AML/CFT regimes."[34]

In Scenario B, criminals gain crypto assets from illegal activities such as the hacking of exchanges, distribution of ransomware, and sale of illegal information on the dark market, and then launder these dirty crypto assets through a blockchain network. Finally, they exchange clean crypto assets with fiat currency using a centralized exchange. In such a scenario, prevention of the money laundering would entail further difficulties for authorities in the current regulatory regime for the following reasons:

---

[33] Needless to say, even current regulations for financial intermediaries are not perfect in eradicating all money laundering and other financial crimes. However, it is important to achieve at least the same level of prevention in a blockchain-based financial ecosystem, given that blockchain-based financial crimes along with those originating from traditional financial services could persist in tandem.

[34] FINANCIAL ACTION TASK FORCE, VIRTUAL CURRENCIES: KEY DEFINITIONS AND POTENTIAL AML/CFT RISKS (June 2014), http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

First, blockchain technology can preclude intermediaries from transactions between crypto assets. As discussed above, users are able to transact on a peer-to-peer basis, which need not adhere to AML/CFT/KYC regulations and could enable criminal conduct. In relation to this point, FATF has pointed out that "[l]aw enforcement cannot target one central location or entity (administrator) for investigative or asset seizure purposes,"[35] and "[d]ecentralised convertible virtual currencies allowing anonymous person-to-person transactions may seem to exist in a digital universe entirely outside the reach of any particular country."[36]

Second, sophisticated anonymization technologies and others that obfuscate the tracing of transactions are evolving. For peer-to-peer transactions, regulators must directly prohibit individual users from conducting financial transactions on the blockchain for unlawful purposes. However, enforcement of regulations upon individual users would be limited with respect to policing capacity. And moreover, individual users could utilize sophisticated technologies that anonymize users or hide the linkage between transactions within a blockchain-based system, which would further complicate enforcement actions toward individual users and render them more costly. For example, various privacy-enhancing technologies including but not limited to signature aggregation,[37] zk-SNARKs,[38] and Mixing[39] are in development. In addition, Lightning Network, a layer-2 technology for Bitcoin, applies onion routing to hide linkages between senders and receivers of a transaction from the public.[40] Such technologies have already been deployed in various projects.[41] Despite

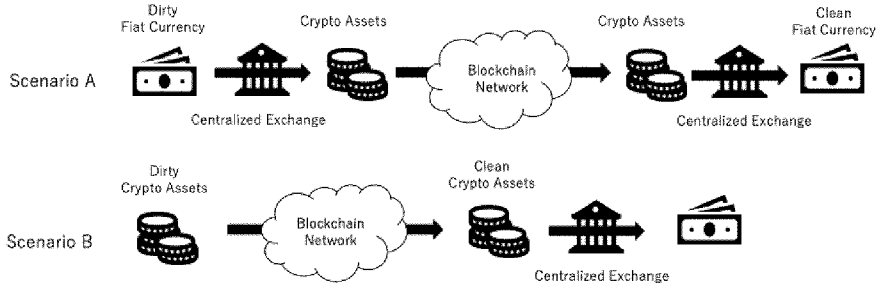
---

[35] *Id.*
[36] *Id.*
[37] A ring signatures is a type of digital signature that provides a high degree of anonymity by obscuring the original sender's outputs from a public address through incorporation of several "decoy signatures." *See Ring Signature*, MONEROPEDIA, https://web.getmonero.org/resources/moneropedia/ringsignatures.html (last visited Nov. 1, 2019).
[38] Zero-knowledge proofs are a method of interaction between individuals or computer systems by which one user can prove to another that they know a said value, without divulging what that value is. *See What are zk-SNARKs?*, ZCASH, https://z.cash/technology/zksnarks.html (last visited Nov. 1, 2019).
[39] Evan Duffield & Daniel Diaz, *Dash: A Payments-Focused Cryptocurrency*, DASH, https://github.com/dashpay/dash/wiki/Whitepaper (last visited Nov. 1, 2019).
[40] The technical standard for Lightning Network deploys onion routing to enhance privacy. *See* BOLT #4: ONION ROUTING PROTOCOL, LIGHTNING NETWORK, https://github.com/lightningnetwork/lightning-rfc/blob/master/04-onion-routing.md (last visited Nov. 1, 2019).
[41] *See, e.g.*, Gary Basin, *The State of Decentralized Exchange*, HACKER NOON (June 21, 2018), https://hackernoon.com/the-state-of-decentralized-exchanges-235064446ab0; MONEROPEDIA, *supra* note 40; ZCASH, *supra* note 38.

the projects' limited market share,[42] their network participants already have the ability to hide their information, and even Bitcoin is subject to greater anonymity via the aforementioned developments. FATF points out that they "may allow greater anonymity than traditional non-cash payment methods. Virtual currency systems can be traded on the Internet, are generally characterised by non-face-to-face customer relationships, and may permit anonymous funding (cash funding or third-party funding through virtual exchangers that do not properly identify the funding source)."[43] It should be noted that many works regarding techniques to de-anonymize and/or de-link transactions,[44] as well as several AML/CFT solutions for blockchain, are available,[45] although we cannot attest to their efficacy.

Third, financial regulators can neither stop the decentralized network that facilitates financial transactions nor modify the transactional record. In the current financial system, when a regulator finds unlawful transactions, it can order suspension of the service or, in cooperation with financial intermediaries, can cancel or reverse the transaction; however, in a blockchain-based financial ecosystem, even if a regulator succeeds in finding unlawful activity, it is highly difficult to forcefully address.

Fig 1. Scenarios of money laundering through a blockchain network



[42] Möser explains: "Privacy-enhancing technologies ("PETS") face low adoption due to the constraints they place on performance. Mixing, for example, places additional stress on the blockchain. Cryptographically sophisticated techniques have the greatest impact on performance. PETS also add significant complexity to cryptocurrencies which limits adoption. For various reasons, there is competition among PETS. This is perhaps an opportunity for regulators as it narrows the anonymity set of any given PETS. Regulatory pressure also may act as a disincentive to adopt PETS to begin with." *See* Malte Möser, *Cryptocurrency privacy: research-based guidelines for protocol designers* (Jan. 29, 2018), https://www.youtube.com/watch?v=qpn9ICem5wk&feature=youtu.be0.

[43] FINANCIAL ACTION TASK FORCE, *supra* note 34.

[44] We found several empirical analyses including Malte Möser et al., *An Empirical Analysis of Traceability in the Monero Blockchain* (Apr. 2018), https://arxiv.org/pdf/1704.04299; George Kappos et al., *An Empirical Analysis of Anonymity in Zcash* (Aug. 2018), https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-kappos.pdf.

[45] Examples of service providers include (but are not limited to) Blockchain Intelligence, Chainalysis, and CipherTrace.

3.1.3.2 Current efforts in financial crime prevention

FATF recommendations and domestic regulations

With regard to crypto assets-related activities, key jurisdictions and international organizations including FATF have been working on regulation mainly focusing on intermediaries such as crypto assets exchanges as entry and exit points for crypto assets markets.

For example, FATF "requires countries to ensure that convertible VC exchangers which act as nodes where convertible VC activities intersect with the regulated fiat currency financial system are subject to adequate regulation and supervision. Countries should consider amending legacy legal frameworks, as needed, to authorize effective AML/CFT regulation of decentralized VC payment mechanisms."[46]

As discussed in the previous section, regulation on crypto assets-related businesses as gatekeepers is important to prevent money laundering through blockchain networks. And it should be implemented in all jurisdictions including those with emerging markets because a gap within just one jurisdiction could greatly reduce the effectiveness of the efforts by the rest of the regulatory community.[47] For now, however, regulatory approaches vary between countries and can cause regulatory arbitrage. FATF has conducted a stock take to identify the different regulatory approaches among its member jurisdictions.[48] The results are summarized in the following table:

Table 2. Current regulatory approaches for crypto assets-related activities

Measures Currently Applied	Countries
Prohibition (on issue / use / dealing / settling of virtual currencies/crypto assets)	China, India, Indonesia
Regulation of intermediaries / exchanges and others (using new or existing AML/CFT regulation)	Australia, France, Germany, Italy, Japan, Switzerland, United States

[46] FINANCIAL ACTION TASK FORCE, VIRTUAL CURRENCIES: GUIDANCE FOR A RISK-BASED APPROACH (June 2015), http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf.

[47] Paech, *supra* note 31.

[48] FINANCIAL ACTION TASK FORCE, FATF REPORT TO THE G20 FINANCE MINISTERS AND CENTRAL BANK GOVERNORS (July 2018), https://www.fatf-gafi.org/media/fatf/documents/reports/FATF-Report-G20-FM-CBG-July-2018.pdf.

Suspicious transaction reporting only	Argentina, South Africa
Preparing laws or regulations	Brazil, Canada, EU, Mexico, Russia, Saudi Arabia, South Korea, Turkey, UK

Afterwards, FATF revised its recommendations, stating "countries should ensure that virtual asset service providers are regulated for AML/CFT purposes, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations."[49] It also provided an Interpretive Note on a related section of recommendations in February 2019.[50] In the regulatory community, the challenge is ongoing to ensure a sufficient level of oversight globally. FATF thus emphasized that it "encourages appropriate and consistent safeguards for activities in this space that reduce the potential for regulatory and legal arbitrage globally as a result of inadequate or non-regulation and supervision in many jurisdictions. All jurisdictions should urgently take legal and practical steps to prevent the misuse of virtual assets."[51]

Beyond complexities in globally consistent implementation of regulations, it is also notable that even in the countries that have already imposed regulations on crypto assets exchanges domestically, regulated exchanges are still struggling to comply properly. For example, Japan's financial regulator recently published a report explaining that most regulated crypto assets exchanges fail to establish the necessary capacity to conduct AML measures and meet regulatory requirements.[52] This shows that regulation of centralized crypto assets exchanges in practice is troublesome with respect to ensuring compliance and effectively preventing criminal activities. Currently, FATF is working to elaborate on how revised requirements should be applied in relation to crypto assets.[53]

---

[49] *See* FINANCIAL ACTION TASK FORCE, *supra* note 11.

[50] FINANCIAL ACTION TASK FORCE, PUBLIC STATEMENT – MITIGATING RISKS FROM VIRTUAL ASSETS (Feb. 22, 2019), http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets-interpretive-note.html.

[51] FINANCIAL ACTION TASK FORCE, FATF REPORT TO G20 LEADERS' SUMMIT (Nov. 2018), http://www.fatf-gafi.org/media/fatf/documents/reports/Report-G20-Leaders-Summit-Nov-2018.pdf.

[52] FINANCIAL SERVICES AGENCY, 仮想通貨交換業者等の検査・モニタリング 中間とりまとめ (Aug. 10, 2018), https://www.fsa.go.jp/news/30/virtual_currency/20180810-2.pdf.

[53] FINANCIAL ACTION TASK FORCE, REGULATION OF VIRTUAL ASSETS (Oct. 19, 2018), http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets.html.

In addition, it is worth noting that the above efforts focus on the regulation of intermediaries, while peer-to-peer transactions described in Scenario B of Figure 1 fall outside of the regulatory perimeter. Since tactical and competent illegal players can deploy sophisticated decentralization and anonymization tools[54] in a blockchain-based financial ecosystem, regulatory enforcement in turn would need to evolve.[55] In fact, FATF pointed out that "[g]iven the compliance and law enforcement challenges presented by decentralized convertible VC [virtual currencies], financial institutions, DNFBP, developers, investors, and other actors in the VC space should seek to develop technology-based solutions that will improve compliance."[56] Paech echoed the assertion by stating that "although there certainly seems to be a significant problem, no suitable solution has as yet been found."[57] Thus, it is necessary to take further actions to address risks associated with financial activities on blockchains.

One notable example of such action on the enforcement side is the US Treasury Department Office of Foreign Asset Control's ("OFAC") addition of two Bitcoin addresses to its sanctions list for the first time.[58] OFAC explained that these addresses are associated with malicious Iranian cyber actors. In its document. it reiterated that "[a]s a result of today's action, all property and interests in property of the designated persons that are in the possession or control of U.S. persons or within or transiting the United States are blocked, and U.S. persons generally are prohibited from dealing with them." An OFAC official called on digital currency industry and international counterparts to make further efforts.[59] It remains to be seen how effective such measures prove in practice.

Current situation with respect to financial crimes deploying blockchain-based financial services

As far as we know, at present there is no comprehensive statistical analysis of criminal activities utilizing blockchain and related services (from

---

[54] Blake Schmidt, *The Criminal Underworld Is Dropping Bitcoin for Another Currency*, BLOOMBERG (Aug. 26, 2018), https://www.bloomberg.com/news/articles/2018-08-26/these-crypto-tycoons-are-about-to-learn-how-rich-they-really-are.

[55] Kieran Corcoran, *Law enforcement has a massive problem with these 3 cryptocurrencies*, BUSINESS INSIDER (Feb. 26, 2018), https://www.businessinsider.com/law-enforcement-problems-with-monero-zcash-dash-cryptocurrencies-2018-2?r=UK&IR=T.

[56] FINANCIAL ACTION TASK FORCE, *supra* note 34.

[57] Paech, *supra* note 31.

[58] Press Release, Office of Foreign Assets Control, Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses (Nov. 28, 2018), https://home.treasury.gov/news/press-releases/sm556.

[59] *See* Under Secretary Sigal Mandelker's remarks at the ABA Financial Crimes Enforcement Conference on Dec. 3, 2018, available at https://home.treasury.gov/index.php/news/press-releases/sm563.

a trusted source). However, national authorities and private research companies occasionally report their relevant findings on an ad hoc basis. Some examples are shown in the following table:

Table 3. Examples of recent publications and explanations regarding AML/CFT issues related to crypto assets

Reports / Publisher	Year	Explanation of Criminal Activities
FinCEN (US)[60]	2018	Director revealed at a Chicago conference that FinCEN receives more than 1,500 cryptocurrency-related reports monthly from financial institutions related to cryptocurrency.
European Parliament (EU)[61]	2018	A former Europol director stated that cryptocurrencies comprise approximately EUR 3-4 billion, or three to four percent, of illicit proceeds laundered through Europe annually.[62] Law enforcement officials across Europe are identifying an increasing number of money laundering cases involving the use of cryptocurrencies.
CipherTrace Cryptocurrency Intelligence[63]	2018	A quantitative analysis of all transactions on top-20 cryptocurrency exchanges globally revealed that 97% of direct Bitcoin payments from identifiable criminal sources were received via unregulated cryptocurrency exchanges.

These reports indicate that financial criminals are open to adopting new technologies while enforcement of regulations has lagged.

---

[60] Kenneth A. Blanco, Director of FinCEN, Prepared Remarks Delivered at the 2018 Chicago-Kent Block (Legal) Tech Conference (Aug. 9, 2018), https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-2018-chicago-kent-block.

[61] POLICY DEPARTMENT FOR CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS, DIRECTORATE GENERAL FOR INTERNAL POLICIES, EUROPEAN PARLIAMENT, VIRTUAL CURRENCIES AND TERRORIST FINANCING: ASSESSING THE RISKS AND EVALUATING RESPONSES (May 2018), http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf.

[62] Shiroma Silva, *Criminals hide "billions" in crypto-cash – Europol*, BBC NEWS (Feb. 12, 2018), http://www.bbc.co.uk/news/technology-43025787.

[63] *2018 Q3 Cryptocurrency Anti-Money Laundering Report*, CIPHERTRACE (2018), https://ciphertrace.com/crypto-aml-report-2018q3.pdf.

In a more concrete example, hacking incidents suffered by centralized exchanges gives us a clearer picture of the current situation.[64] In January 2018, Coincheck—one of Japan's largest crypto assets exchanges—was hacked, and $5 million worth of cryptocurrencies was stolen.[65] In the same year another hacking incident hit crypto exchange Zaif, which lost $0.5 million worth of cryptocurrencies.[66] In response, Japanese authorities and so-called "white hat hackers" attempted to trace the stolen cryptocurrency to identify the hacker(s); however, they ultimately failed.[67] The Coincheck and Zaif cases demonstrate that even in the presence of a centralized intermediary and absence of sophisticated privacy-enhancing technologies, illegal actors still can hide their identities and launder money.[68]

Recently we have witnessed the emergence of potentially scalable blockchain-based financial services including global stablecoins, which could pose even more serious risks.[69] Hence it is important for regulators to consider carefully and with haste the latest developments in the space before they become widely available to illegal players.

CONCLUSION TO PART I

Technical characteristics of blockchain-based networks including globalization, decentralization, autonomization, pseudonymization & anonymization, tamper-resistance, and openness render high cost or impossible any orthodox enforcement of regulation. Thus, regulators must find ways to overcome technical limitations on regulability.

Although risks are material in the area of financial crime prevention, regulators in many countries have appeared to avoid taking forceful

---

[64] Criminals have hacked exchanges to steal crypto assets for the purpose of exchanging them for other forms of value such as fiat currency or physical goods. In so doing, they launder the stolen crypto assets in a way similar to how financial criminals launder "dirty" money. On the opposite end, financial regulators and police agencies must identify the hacker(s) before completion of laundering. Thus, hacking of crypto asset exchanges is connected to AML/CFT, although hacking itself is a cybersecurity issue.

[65] Darryn Pollock, *Story of Coincheck: How to Rebound After the 'Biggest Theft in the History of the World'*, COINTELEGRAPH (Apr. 3, 2018), https://cointelegraph.com/news/story-of-coincheck-how-to-rebound-after-the-biggest-theft-in-the-history-of-the-world.

[66] Wolfie Zhao, *Crypto Exchange Zaif Hacked In $60 Million Bitcoin Theft*, COINDESK (Sept. 20, 2018), https://www.coindesk.com/crypto-exchange-zaif-hacked-in-60-million-6000-bitcoin-theft.

[67] NEM Official (Editors), *Coincheck Hack Update: Removal of Mosaic Tagging System*, MEDIUM (Mar. 19, 2018), https://medium.com/nemofficial/coincheck-hack-update-removal-of-mosaic-tagging-system-18b4157ff060.

[68] Zhao, *supra* note 66.

[69] G7 CHAIR, CHAIR'S SUMMARY: G7 FINANCE MINISTERS AND CENTRAL BANK GOVERNORS' MEETING (July 2019), https://www.banque-france.fr/sites/default/files/media/2019/08/02/g7_chairs_summary_vff_en.pdf.

measures with the exception of a few occasions[70] and have opted for a light touch policy approach.[71] As aforementioned, challenges for the regulators are predicated not solely on technical issues of regulability, but also on the choice/balance between seemingly competing values—the option to address market failures with more policy actions, and the need for innovation with less intervention in the midst of uncertain future trajectories.

In general, we call the process of resolving competing values "politics." Thus, we should seek an optimal way to handle politics when establishing a governance mechanism for a blockchain-based financial ecosystem. In Part II of this paper, we will aim: (1) to show an approach to overcome the issue of regulability in a blockchain-based financial ecosystem, especially focusing on prevention of financial crimes; (2) to propose a governance mechanism that appropriately handles the politics of competing values that would exist in a blockchain-based financial ecosystem.

Without overcoming the technical limitations of regulability, attempts to regulate a blockchain-based financial ecosystem would be infeasible; thus, we first must consider how to overcome such limitations. We do not necessarily stick to the assumption that regulators alone can provide regulatory functions. Rather, we believe it is essential to give consideration to broader possibilities. Then, with a practical mechanism for achieving regulatory goals in hand, we should consider how to deal with politics related to competing values in the ecosystem, including matters of control.

Part II of this paper will be devoted to lessons from Internet governance as reference points, in light of extant and looming parallels.

---

[70] For example, the Chinese government banned ICOs in China. *See* THE PEOPLE'S BANK OF CHINA, *中国人民银行 中央网信办 工业和信息化部 工商总局 银监会 证监会 保监会关于防范代币发行融资风险的公告* (Sept. 4, 2017), http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/3374222/index.html.

[71] For example, in a number of countries, regulators have established "regulatory sandboxes," allowing businesses to test innovative propositions in the market with real consumers. *See* FINANCIAL CONDUCT AUTHORITY, REGULATORY SANDBOX, https://www.fca.org.uk/firms/regulatory-sandbox (last visited Nov. 1, 2019).