Decentralized finance: Ready for its "close-up"?

Lewis Cohen, Angela Angelovska-Wilson & Greg Strong
DLx Law

Unstoppable code

Smart contract code deployed to a functioning blockchain network is unstoppable. Decentralized finance ("**DeFi**") protocols are suites of smart contracts – executable code accessible to anyone with the technical and practical capability to interact with that code – that allow users to transact value with others over the Internet with deterministic certainty yet without the need for one or more intermediaries. So long as the blockchain networks on which these smart contracts are deployed remain operational, the related DeFi protocols will be accessible.

There was more than the equivalent of US$92 billion of total value in digital assets "locked" in (*i.e.*, committed to) DeFi protocols as of September 16, 2021.[1] That amount of value, combined with the ability of users to conduct financial transactions pseudonymously without identification by an intermediary, is prompting regulators around the world to scrutinize the DeFi space. A global effort is under way to bring DeFi within (or at least closer to) the regulatory frameworks that apply to traditional finance. Whether and how can this be achieved in the context of unstoppable code remains very much an open question.

While the execution of blockchain-based smart contract code may be unstoppable, the individuals and businesses who develop the code and provide user-friendly access to that code are not. Our traditional regulatory frameworks focus on people – typically issuers and intermediaries – and there is a movement to bring those that develop, provide access to, or benefit economically from the operation of, the smart contracts comprising DeFi protocols within those existing regulatory definitions.

The development of DeFi forces regulators and market participants alike to confront some challenging questions: When should an individual or entity involved in developing smart contracts for DeFi protocols be held responsible for the outcomes of that code, especially when vulnerabilities in the code (leading to exploits and financial loss) are exposed? Should developers of the smart contracts or those who financed the development and who benefit economically through the ownership of related digital assets be required to take responsibility for the regulatory compliance of the protocols? What about a person or entity that simply provides access to such protocols through a website or application? Should regulators attempt to shoehorn developers and others into existing regulatory definitions that may not really fit in order to bring them within the ambit of existing regulatory frameworks, particularly when DeFi protocols are designed to eliminate traditional intermediaries? Alternatively, should brand-new regulatory frameworks be developed to meet the challenge of DeFi? These tricky questions are illustrative of the challenges in regulating actors contributing to DeFi as issuers or intermediaries.

Many now agree that DeFi needs regulation to evolve and grow. Not all current or future users of DeFi protocols will be sophisticated enough to fully evaluate the underlying smart contract code for themselves and will rely on others for this work. It is not hard to see that these users should benefit from protections. In addition, open peer-to-peer ("**P2P**") protocols allowing pseudonymous access can readily be used by bad actors for nefarious purposes, something that concerns all of us. That said, policymakers will need to be creative in approaching these developments. Yesterday's regulatory solutions will not be sufficient to address today's technologies. Efforts to encourage the development of regulation that is tailored to the unique nature of this technology to foster responsible growth and development must be encouraged. New approaches to regulation will provide more effective protection for the users of DeFi as well as clarity to actors contributing to these protocols with respect to their regulatory responsibilities.

Regulation of issuers and intermediaries

Regulation in the traditional finance world focuses on issuers and intermediaries. Our securities laws regulate issuers of securities and securities intermediaries that facilitate securities transactions. Our commodities laws regulate intermediaries that facilitate transactions in commodity derivatives and entities that offer commodity derivative contracts. Our financial regulatory laws, such as the Bank Secrecy Act (the "**BSA**"), apply to financial institutions broadly and require transaction monitoring, reporting, and recordkeeping in a variety of contexts. All of these frameworks are implicated by developments in DeFi.

Securities laws

Our securities laws regulate issuers of securities and intermediaries involved in securities transactions. Issuers of securities are generally required to disclose important information about the securities they intend to sell and their financial condition such that prospective investors can make informed investment decisions.[2] This information must be accurate and complete.[3] The level of detail required depends on whether the offering is registered and sold publicly[4] or whether it is exempt from registration and sold to limited numbers of persons or limited in size.[5] In addition to the disclosure requirements in connection with the initial sale of securities, issuers of public securities with 300 or more shareholders, and issuers with more than US$10 million in assets with securities held by more than 500 owners, must file annual and other periodic reports as well.[6]

Our securities laws also regulate intermediaries such as broker-dealers, transfer agents, clearing agencies, national securities exchanges, and investment advisors. Generally, each of these intermediaries must register with the Securities and Exchange Commission (the "**SEC**") and comply with the laws and regulations applicable to their activities as intermediaries.[7] The obligation of an entity to register with the SEC as one of the above-listed intermediaries is triggered by engaging in the regulated activity with respect to securities. For example, whether the assets that are being brokered are securities will determine whether registration as a broker-dealer is required.

Commodities laws

The Commodities Exchange Act (the "**CEA**") and related regulations regulate the trading of commodity derivatives.[8] One important component of this regulatory scheme is the registration and oversight of intermediaries who act on behalf of others in connection with commodity derivatives. There are a variety of intermediaries regulated under the CEA, including Commodity Pool Operators, Commodity Trading Advisors, Futures Commission Merchants, Introducing Brokers, Major Swap Participants, and Swap Dealers.[9] In addition, the

CEA generally requires that many commodity derivatives be traded on a designated contract market ("**DCM**").[10] DCMs are also licensed and regulated by the CFTC and allow the CFTC to oversee transactions in commodity derivatives available to retail market participants.[11]

The BSA

The BSA mandates that "financial institutions,"[12] intermediaries who act on behalf of others in connection with financial transactions, collect and retain information about their customers and their transactions, and share that information with the Financial Crimes Enforcement Network ("**FinCEN**"). The BSA and its implementing regulations require the registration of a money services business ("**MSB**") within 180 days of beginning operations and the renewal of such registration every two years,[13] and require an MSB to develop, implement, and maintain an effective written anti-money laundering ("**AML**") program that is reasonably designed to prevent the MSB from being used to facilitate money laundering and the financing of terrorist activities.[14] An MSB is required to implement a written AML program that, at a minimum: (a) incorporates policies, procedures and internal controls reasonably designed to assure ongoing compliance; (b) designates an individual responsible to assure day-to-day compliance with the program and BSA requirements; (c) provides training for appropriate personnel, including training in the detection of suspicious transactions; and (d) provides for independent review to monitor and maintain an adequate program.[15]

In particular, when money transmitters process transactions that involve a "transmittal of funds,"[16] the Funds Travel Rule[17] applies to those transactions. Under the regulatory framework established under the BSA, a transmittal of funds is initiated by a "transmittal order," which is an instruction to pay funds to a recipient. The Funds Travel Rule requires that each of the financial institutions in a chain of transmittal orders involved in a transmittal of funds of US$3,000 or more originated by customers and non-customers maintain accurate records relating to the funds transfer and verify the identity of non-customers originating funds transfers.[18] The information required to be maintained depends on the role of the financial institution in the payment chain, *i.e.*, originator, intermediary, or beneficiary institution.[19] Financial institutions acting as originator or intermediary financial institutions must cause the information to "travel" to the next financial institution.[20]

FinCEN 2019 Guidance

On May 9, 2019, FinCEN, a division of the U.S. Treasury Department, issued guidance entitled "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies" (the "**Guidance**").[21] FinCEN is the arm of the Treasury Department responsible in the first instance for enforcing the U.S. federal laws and regulations relating to the transmission of money, including the BSA, frequently working in conjunction with other federal agencies and bureaus, including the Federal Bureau of Investigation and the National Security Agency. The Guidance was designed to consolidate current regulations, administrative rulings, and earlier guidance related to MSBs, with a focus on money transmission involving convertible virtual currency ("**CVC**").

While the Guidance touches on a number of different areas, two key areas include: (1) how the Funds Travel Rule applies to certain transactions involving CVCs and whether any such transactions trigger regulatory obligations under U.S. federal law for any participants who may be considered "money transmitters"; and (2) the application of relevant U.S. laws and regulations with respect to "decentralized" systems.[22] With respect to the former, the Guidance indicates that the Funds Travel Rule applies to transactions in CVCs.[23] Accordingly, any intermediary financial institution involved in the transmission of funds must provide certain information to the receiving financial institution, but they have no duty

to obtain information not provided by the transmitter's financial institution or the preceding financial institution.[24] The recipient's financial institution must receive, evaluate, and store the information received from the transmitter's financial institution or the intermediary financial institution.[25]

The key question is whether there are intermediaries in a given transaction that meet the definition of financial institution and are subject to the Funds Travel Rule. In the context of centralized intermediaries, the analysis is straightforward. In the context of automated transactions in decentralized systems, it is more difficult to identify an intermediary to hold responsible for compliance. The Guidance addresses the responsibility of developers/contributors to decentralized systems.[26] Under Section 5.2.2 of the Guidance, decentralized application ("**DApp**") developers are not regulated as money transmitters for "the mere act of creating the application, even if the purpose of the DApp is to issue a CVC or otherwise facilitate financial activities denominated in CVC," but they may be regulated as money transmitters if they "use" or "deploy" it "to engage in money transmission."[27] The Guidance is explicit about the application to decentralized systems and makes multiple references to unincorporated organizations coming within the ambit of the BSA in reference to decentralized systems. The Guidance goes on to specifically address DApps in the discussion of business models involving CVC money transmission, reiterating that the same rules apply there as well.[28]

DeFi contributors as issuers or intermediaries

Increasingly, regulators have sought to shoehorn DeFi participants into the existing regulatory frameworks described above by branding them intermediaries. This is true with respect to U.S. securities, commodities, and financial regulatory laws.

FATF virtual asset guidance

The issue of information reporting in connection with virtual asset transfers is at center stage internationally. In the Fall of 2018, the Financial Action Task Force ("**FATF**"), a multi-governmental organization that sets global standards related to AML, proposed amended Recommendation 15, which addresses new technologies to clarify how the FATF standards apply to activities or operations involving virtual assets.[29] Subsequently, FATF released an Interpretive Note to Recommendation 15.[30] Paragraph 7(b) of the Interpretive Note seeks to impose a corollary to the Funds Travel Rule on Virtual Asset Service Providers ("**VASPs**") processing virtual asset transfers.[31] The Interpretive Note was finalized in June 2019 following private sector consultations.[32]

More recently, FATF released new proposed updated guidance regarding virtual assets and VASPs, which is currently open for comment (the "**Updated FATF Guidance**").[33] A VASP "is any natural or legal person who is not covered elsewhere under the Recommendations and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

i. Exchange between virtual assets and fiat currencies;
ii. Exchange between one or more forms of virtual assets;
iii. Transfer of virtual assets;
iv. Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and
v. Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset."[34]

Notably, the Updated FATF Guidance seeks to make clear that the definitions of "Virtual Asset" and "VASP" are expansive[35] and interprets the definition of a VASP to include "a

central party with some measure of involvement" with a DApp.[36] This involvement could include "creating and launching an asset, setting parameters (for the operation of the Dapp), holding an administrative "key" or collecting fees."[37] This broad interpretation would potentially bring a variety of DeFi participants within the definition of a VASP and subject them to compliance with anti-money laundering and counter-terrorism financing ("**AML/CFT**") laws in jurisdictions that implement this interpretation of the VASP definition.

The Updated FATF Guidance also clearly recognizes that a DApp itself is not a VASP as the standards do not apply to underlying software or technology.[38] In fact, "the FATF standards are intended to be technology neutral."[39] This position underscores the idea that code deployed to a functional blockchain network is unstoppable – it is immutable and is not something that can practically be regulated. Instead, FATF and other regulators have sought to expand the scope of existing definitions, such as VASP, in order to fill perceived regulatory gaps by bringing certain participants in DApps within the ambit of existing regulatory regimes.

The Updated FATF Guidance is also clear that it does not seek to regulate users of virtual assets as VASPs.[40] Instead, the focus is on VASPs as facilitators of certain virtual asset activities.

FinCEN "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets"

In December 2020, FinCEN published a notice of proposed rulemaking regarding "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets" (the "**NPRM**").[41] The stated objective of the NPRM was to aid law enforcement in the reduction of the illicit use[42] of CVC held in "unhosted wallets" or in wallets hosted in a jurisdiction identified by FinCEN. Initially, the comment period for the 72-page NPRM was 15 days. That comment period was later extended and there has not yet been a final rulemaking following the NPRM and the close of the comment period.

Despite the fact that the NPRM has not moved to final rulemaking, the NPRM was certainly designed to bring transactions in CVCs squarely within the regulatory ambit of the BSA. It would do so by imposing strict reporting and recordkeeping requirements on financial institutions, primarily aimed at centralized CVC exchanges, with respect to CVC transactions in an attempt to promote law enforcement. By requiring financial institutions to know the "[t]he name and physical address of each counterparty to the transaction of the financial institution's customer, as well as other counterparty information the Secretary may prescribe as mandatory on the reporting form for transactions subject to reporting pursuant to § 1010.316(b),"[43] the proposed rules would ostensibly allow for the identification of unhosted wallet users who choose to transact with financial institutions that would be subject to the rules.

In addition to the practical and technological compliance difficulties presented, the proposed strict recordkeeping requirements with respect to transfers of CVCs go beyond the more flexible rules currently applicable to transfers of dollars or other fiat currencies by customers of financial institutions. If the NPRM is finalized in current form, financial institutions may determine that doing business with unhosted wallets is not worth the added compliance expense. This would result in unhosted wallet activity remaining outside of financial institutions subject to the BSA and related regulations, exactly the opposite of what the NPRM is attempting to accomplish.

If finalized, these rules might also encourage users of digital assets to turn to alternatives. DeFi protocols, including "smart contract"-based P2P exchange tools, that are not owned or

controlled by any one or more identifiable persons or businesses are the likely alternative. An increase in the use of non-regulated storage solutions and P2P exchange services would cause law enforcement to lose access to information generated by centralized and regulated exchange platforms, the primary target of the NPRM and one of law enforcement's most valuable partners. CVC that remains on self-hosted wallets and transacted only in decentralized protocols is much more difficult to track and regulate absent new laws or regulations, or new interpretations of our laws and regulations. Accordingly, the struggle to regulate DeFi protocols is taking center stage.

Finally, the NPRM defines CVC broadly and does not account for the fact that CVCs are often used for purposes other than payment, such as being staked to contribute to securing a proof of stake network. To foster the use and benefits of blockchain technology and CVCs, proposed regulations that treat transactions in CVCs that are used for multiple purposes, not all of which involve payments or transfers of value, more strictly than transactions in fiat currency, which is only used for one purpose, should be re-examined.

Report of the Attorney General

A report prepared by the Cyber-Digital Task Force of the Office of the Deputy Attorney General highlighted the distinction between centralized and P2P exchanges and indicated that P2P exchanges are still subject to AML/CFT compliance:[44]

> "[U]nlike centralized virtual asset exchanges, P2P exchange platforms may operate without an intermediary that will accept and transmit virtual assets in exchange for fiat or another type of virtual asset, or that will collect customer identification information. Individual exchangers—as well as platforms and websites—that fail to collect and maintain customer or transactional data or maintain an effective AML/CFT program may be subject to civil and criminal penalties."[45]

The Cyber-Digital Task Force Report indicates that platforms or websites that fail to collect certain information may be violating the law and subject to penalties.

The Cyber-Digital Task Force Report highlights a focus on sanctions compliance with respect to digital assets. Using digital assets to hide financial transactions for the purpose of avoiding sanctions is identified as an illicit use of digital assets in the Report.[46] U.S. persons and persons otherwise subject to the jurisdiction of the Office of Foreign Assets Control of the Treasury Department "are responsible for ensuring that they do not engage in transactions prohibited by OFAC sanctions (such as dealings with blocked persons or property) or in otherwise-prohibited trade or investment-related transactions. Prohibited transactions generally also include those that evade or avoid, have the purpose of evading or avoiding, cause a violation of, or attempt to violate prohibitions imposed by OFAC under various sanctions authorities."[47]

SEC Guidance

The SEC has also sought to bring activity involving digital assets and DeFi within its regulatory ambit. The primary focus in this effort is investor protection and ensuring that this public policy goal is being achieved in the context of blockchain and digital assets. In the view of new SEC Chair Gary Gensler, "Right now, we just don't have enough investor protection in crypto. Frankly, at this time, it's more like the Wild West."[48]

In fact, the SEC was one of the first regulators to bring an action holding a developer of a decentralized exchange responsible for violating the securities laws.[49] In November of 2018, the SEC settled an enforcement action involving EtherDelta, a protocol for the P2P exchange of digital tokens that was billed as "decentralized."[50] The SEC entered into a

consent order with Zachary Coburn, an individual and the founder of EtherDelta, to resolve the investigation.[51] The order alleged that EtherDelta was an unregistered exchange because at least some of the tokens traded on EtherDelta were unregistered securities.[52] In addition, Coburn was alleged to have caused the EtherDelta "trading system" to violate certain provisions of the Exchange Act. Coburn caused these violations by: creating EtherDelta; coding and deploying the smart contract; having exclusive control over administrative keys to the EtherDelta smart contract (allowing him to change the fees charged for exchanges); and promoting EtherDelta on Twitter and Reddit.[53] The SEC deemed Coburn responsible for this P2P protocol given his significant involvement in the protocol.

A necessary element of securities law jurisdiction is activity involving an asset that meets the definition of a security. Activity that does not involve a security is not subject to the jurisdiction of the SEC. In the Coburn Order, the SEC did not specifically identify the asset(s) trading on EtherDelta that they determined were securities, and which would trigger a requirement to register as an exchange or operate within an applicable exemption from such registration.[54] In addition to the Coburn Order, the SEC has taken action against a variety of other intermediaries for failing to register as required when engaging in activities involving digital assets, or transactions in digital assets, deemed by the SEC to be securities.[55] In each of these cases, the SEC has declined to specifically identify the digital asset, or transaction in digital asset, that constituted the security triggering an obligation to register as a securities intermediary.[56]

Recent statements from newly appointed SEC Chair Gary Gensler take a similar tack, indicating a view that many tokens (digital assets) may be securities and that an exchange that facilitates the trading of lots of digital assets is probabilistically engaging in unregistered exchange activity.[57] In other words, rather than telling those engaging with digital assets when they believe specific assets are securities, the key in determining whether regulatory obligations are triggered for intermediaries pursuant to our securities laws, the regulator is instead telling those facilitating transactions in digital assets to do their own research and, if they engage in a lot of activity, they should assume that at least some of it will involve digital assets the SEC believes are securities.

At the same time, the SEC is warning digital asset market participants that they believe many digital assets should be treated as securities.[58] "Make no mistake: It doesn't matter whether it's a stock token, a stable value token backed by securities, or any other virtual product that provides synthetic exposure to underlying securities. These products are subject to the securities laws and must work within our securities regime."[59]

Chair Gensler has also addressed DeFi in recent statements as well, noting that:

> "The American public is buying, selling, and lending crypto on these trading, lending, and DeFi platforms, and there are significant gaps in investor protection.
>
> Make no mistake: To the extent that there are securities on these trading platforms, under our laws they have to register with the Commission unless they meet an exemption.
>
> Make no mistake: If a lending platform is offering securities, it also falls into SEC jurisdiction."[60]

The SEC has recognized that there are regulatory gaps when it comes to digital assets, and has expressed a desire to help fill those gaps.[61] While it remains to be seen whether the SEC will bring actions with respect to DeFi platforms, it certainly seems that they will attempt to bring as many digital assets and digital asset transactions as possible within the definition of security in order to assert jurisdiction over the issuers of those assets as well as the intermediaries facilitating transactions in those assets in order to fill any regulatory gaps.

CFTC

The CFTC has expressed similar concerns with respect to commodity derivatives activity involving digital assets occurring outside its regulatory framework. In a June 2021 speech, then Commissioner Daniel Berkovitz[62] expressed concerns about DeFi cutting out traditional intermediaries that are relied upon to provide important services, stability, and safety to our financial markets by virtue of their regulated status.[63] Eliminating those intermediaries in favor of P2P markets also eliminates the important benefits and protections that intermediaries provide to market participants.[64] Commissioner Berkovitz goes on to indicate that unlicensed DeFi markets for derivative instruments are illegal under the CEA, as those instruments are generally required to be traded on a DCM or a swap execution facility ("**SEF**").[65] He notes that DeFi markets, platforms, or websites are not registered as DCMs or SEFs and that there is no exception from registration for smart contracts or digital assets.[66] Accordingly, we may see increased regulatory scrutiny of blockchain-based systems that facilitate transactions in digital assets that could be deemed commodity derivatives.

Responses from DeFi

Aave and Compound Finance are two of the DeFi industry's best-known permissionless liquidity protocols. Aave is an open-source and non-custodial liquidity protocol for earning interest on deposits and borrowing assets,[67] while Compound is an algorithmic, autonomous interest rate protocol built for developers in order to unlock a universe of open financial applications.[68] Fundamentally, both protocols allow individuals to lend or borrow digital assets with lenders, or liquidity providers, earning interest on the assets they provide or paying interest on assets borrowed. The returns generated by DeFi protocols like Aave and Compound have sparked institutional interest, but financial institutions need to comply with AML, know-your-customer ("**KYC**"), and know-your-transaction rules and regulations. To address this, both Aave and Compound Finance have launched permissioned versions of their protocols to allow institutional participation in a controlled environment with known participants.

Aave Arc

Aave Arc is a new, permissioned protocol being designed by Aave specifically for institutional investors.[69] By completing a required KYC process, large corporations and financial clients will be able to utilize the Aave protocol while also complying with applicable laws and regulations.[70] In order to ensure compliance, these permissioned pools will be separated from Aave's other deployments, and be inaccessible to non-qualified participants.[71] Furthermore, Aave Arc will include a "whitelisting layer" onto its smart contracts to ensure that only those institutions that have successfully completed the KYC verification can access the permissioned protocol.[72] Initially, only four assets – Bitcoin, Ether, Aave, and USDC – will be supported by the protocol.[73]

With the exception of the KYC requirement and the whitelisting or blacklisting by Fireblocks, effectively acting as gatekeepers, Aave Arc seems to mimic the experience offered by Aave, the permissionless version of the protocol. The distinction, of course, is security – liquidity providers are known and traceable, as opposed to the pseudonymous users of Aave. Another distinction is that only four assets will initially be available in these segregated pools.

Compound Treasury

Compound Labs, creators of the Compound Finance protocol, launched a similar protocol called Compound Treasury at the end of June 2021.[74] In addition to compliance, Treasury was designed to make the customer experience simple by removing protocol complexity

such as private key management, crypto-to-fiat conversion, and interest rate volatility.[75] Businesses can wire U.S. dollars to their Compound Treasury Account, which will then be converted into USDC and deployed onto the protocol. They will be able to earn a guaranteed fixed rate of interest on such deployed assets and are free to withdraw their funds at any time.[76] Like Aave Arc, this product is permissioned such that institutions will have to register in order to use the protocol.[77]

Treasury users seemingly never directly interact with the protocol. Instead, they simply provide fiat, which is then converted to USDC stablecoins and deployed onto the platform. Compound Finance, the permissionless protocol, allows users to directly contribute ERC-20 tokens to liquidity pools and users are constantly chasing pools with the highest returns, a tactic known as yield farming. By limiting the investment to USDC stablecoins and guaranteeing a return, most of the risk is removed.[78] Treasury "users" have a much different experience than the users of Compound Finance.

These permissioned protocols designed to provide institutional access to quasi-DeFi show that developers can build KYC into these protocols when desired. The idea of KYC is in conflict with the concept of DeFi, which is built on an ethos that values privacy and enabling composable P2P pseudonymous transactions. However, these permissioned protocols are likely a recognition of the fact that regulated institutional market participants can only engage with protocols that have the compliance features necessary to allow them to meet their regulatory obligations. They signal a new direction for DeFi in which certain aspects of DeFi protocols are made available on a permissioned basis in order to foster regulatory compliance and truly open and permissionless DeFi protocols continue to exist as unstoppable code.

DeFi and permissioning

A dual regulatory system that allows open access to DeFi's "unstoppable code" for those individuals and businesses that have the means and ability to use these protocols, complemented by permissioned access points to these protocols for others, could have significant benefits.[79] Such an approach would allow for regulated access to rapid technological developments occurring in the DeFi space. It would also acknowledge the reality that, as long as access to the Internet is available, the blockchain-based smart contract code underlying these protocols will be accessible to anyone with the necessary technical ability on a permissionless and anonymous basis. Regulators should seize this opportunity to work with DeFi participants to encourage ongoing innovation and to strike a balance between preserving the autonomous nature and spirit of DeFi while also establishing regulated access points to these protocols, where appropriate (for example, for commercial grade transactions or by fiduciaries acting on behalf of third parties). These permissioned access points can serve as regulated intermediaries responsible for compliance with securities, commodities, or financial regulatory laws, as applicable, depending on the type of assets transacted using the protocol.

In such a dual track system, regulators would have less of a need to expand intermediary definitions to fill regulatory gaps. For instance, we would not need to treat digital assets as securities to bring secondary transactions within our securities law regulatory framework. This would be more consistent with the application of the *Howey* test to determine when a digital asset is initially sold in an investment contract scheme.[80] The *Howey* test is a facts-and-circumstances-dependent test that has been applied in the context of initial sales and requires a variety of elements to be present in order for a particular scheme to be deemed an investment contract.[81] However, when a digital asset initially sold in an investment contract

is resold in a secondary transaction, the *Howey* test is difficult to apply and more difficult still to satisfy. The object of the initial investment scheme is very rarely a security in and of itself. This may be why, in all the actions taken to date against intermediaries whose securities law obligations are only triggered by secondary transactions in digital assets, the particular assets believed to be securities have not been identified.[82]

Rather than continuing down this path of confusion with respect to both centralized and decentralized platforms, establishing regulated access points to DeFi protocols could bring a portion of the related activity with respect to these assets within the regulatory perimeter from both a KYC/AML perspective and from the perspective of protecting those that transact using these permissioned access points. The U.S. also maintains robust federal- and state-level consumer protection laws that have been flexibly applied to address a wide variety of consumer issues, from deceptive marketing of drugs to unfair and deceptive practices with respect to residential mortgage-backed securities to deceptive statements in connection with credit ratings. Consumer protection frameworks in the U.S. provide ample regulatory authority to protect purchasers of digital assets that can be used to access blockchain-based services, contribute to the security of blockchain networks, or transfer value.

Regulation of permissioned access points from a financial regulatory and consumer protection perspective can be greatly enhanced by leveraging rich and highly granular data availability associated with blockchain ledgers – much more than is available in the world of traditional finance. Rather than relying on the after-the-fact oversight conducted in traditional finance, regulators engaging with DeFi (both permissioned and open access) can tap into the vast pools of real-time data generated by blockchain networks. Coupling this data with blockchain analytics means that regulators have an unprecedented ability to monitor transactions and information, which may be helpful with respect to identifying concerning activity in both permissioned and open DeFi protocols. Utilizing these tools to monitor transaction activity may provide the foundation for a new regulatory approach to blockchain-based transactions that does not necessarily rely on inefficient manual oversight of, or highly fallible self-reporting by, regulated intermediaries. This would be especially valuable with respect to those choosing to use open access DeFi protocols, while permissioned access points could be regulated as intermediaries, combining traditional and blockchain-based oversight.

This dual system could allow for DeFi to continue to grow and develop for the benefit of the future of finance. Regulators should work with DeFi builders and market participants towards an optimal regulatory solution that allows for continued growth and innovation, while providing meaningful protections to all stakeholders.

* * *

Endnotes

1. https://defipulse.com/.
2. 15 U.S.C. § 77j.
3. 15 U.S.C. § 78j.
4. 15 U.S.C. § 77e(a) and (c).
5. 15 U.S.C. § 77d. Exemptions from registration include Regulation D, Regulation A, Regulation CF, and the intrastate offering exemption.
6. 15 U.S.C. § 78l.
7. For example, broker-dealers must register with the SEC pursuant to 15 U.S.C. § 78o.

8. 7 U.S.C. § 1.
9. *See*, *e.g.*, https://www.cftc.gov/IndustryOversight/Intermediaries/index.htm.
10. *See*, *e.g.*, CEA § 4(a).
11. Transactions in commodity derivatives by eligible contract participants are not required to take place on a DCM. Eligible contract participants are generally highly sophisticated and well-capitalized entities or individuals. *See* 7 U.S.C. § 1a(18). Retail market participants may also be referred to as non-eligible contract participants.
12. "Financial institution" is a broad category of business offering financial services. 31 U.S.C. § 5321(a).
13. 31 U.S.C. § 5330 and 31 C.F.R. § 1022.380(b)(2).
14. 31 U.S.C. §§ 5318(a)(2) and (h); 31 C.F.R. § 1022.210(a).
15. 31 U.S.C. §§ 5318(a)(2) and (h)(1); 31 C.F.R. §§ 1022.210(c) and (d).
16. 31 C.F.R. § 1010.100(ddd).
17. 31 C.F.R. § 1010.410(f).
18. *Id*.
19. *Id*.
20. 31 C.F.R. §§ 1010.410(e) (funds transfer recordkeeping for BSA financial institutions and other banks) and 1010.410(f) (the Travel Rule).
21. *See* Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies (https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf). FinCEN first addressed rule-making authority over virtual currency in March 2013, clarifying that it would regulate transmitters of virtual currency in the same manner as transmitters of fiat currency. Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001 (Mar. 18, 2013) (the "**2013 Guidance**"). Since issuing the 2013 Guidance, FinCEN has issued other Guidance and rulings on virtual currency that further inform the application of existing money transmission regulations: Application of FinCEN's Regulations to Virtual Currency Software Development and Certain Investment Activity, FIN-2014-R002 (Jan. 30, 2014) (the "**2014 Software and Investment Guidance**"); Application of FinCEN's Regulations to Virtual Currency Mining Operations, FIN-2014-R001 (Jan. 30, 2014) (the "**2014 Mining Guidance**"); and Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Payment System, FIN-2014-R012 (Oct. 27, 2014) (the "**2014 Payment System Ruling**").
22. *Id*.
23. *Id*.
24. *Id*.
25. *Id*.
26. *Id*.
27. *Id*.
28. *Id*.
29. *See Recommendation 15*, Financial Action Task Force.
30. *See Interpretive Note to Recommendation 15* (INR. 15), Financial Action Task Force (June 2019).
31. *See Interpretive Note to Recommendation 15* (INR. 15), Financial Action Task Force (June 2019).
32. *See Interpretive Note to Recommendation 15* (INR. 15), Financial Action Task Force (June 2019).

33. *See Draft Updated Guidance for a Risk-Based Approach to Virtual Assets and VASPs*, Financial Action Task Force (March 2021).
34. *Id*. at paragraph 47.
35. *Id*. at paragraph 76.
36. *Id*. at paragraph 56.
37. *Id*.
38. *Id*. at paragraph 57.
39. *Id*. at paragraph 68.
40. *Id*. at paragraph 70.
41. *See* "*Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets*", Financial Crimes Enforcement Network, 85 FR 83840 (Dec. 23, 2020), available at: https://www.federalregister.gov/documents/2020/12/23/2020-28437/requirements-for-certain-transactions-involving-convertible-virtual-currency-or-digital-assets.
42. The term "illicit use," for purposes of this chapter, refers to any unlawful use of CVCs or other monetary instruments, including for money laundering, terrorist finance, ransomware or other criminal activity.
43. Proposed 31 C.F.R. § 1010.410(g)(1)(vii).
44. *See* "*Report of the Attorney General's Cyber-Digital Task Force*" (the "**Cyber-Digital Task Force Report**"), available at: https://www.justice.gov/ag/page/file/1326061/download.
45. Cyber-Digital Task Force Report at p. 38. Where the exchange platform is a decentralized computer protocol rather than a business or individual, there may be no one to collect information or to maintain transaction records, nor anyone to prosecute for not doing so.
46. *Id*. at 26.
47. *Id*. at 26.
48. *Remarks Before the Aspen Security Forum* (the "**Aspen Speech**"), SEC Chair Gary Gensler (Aug. 3, 2021).
49. *In the Matter of Zachary Coburn* (Securities Exchange Act Rel. No. 84553) (Nov. 8, 2018) (the "**Coburn Order**").
50. *Id*.
51. *Id*.
52. *Id*.
53. *Id*.
54. *Id*.
55. *See*, *e.g.*, the Coburn Order; *In the Matter of TokenLot, LLC, Lenny Kugel, and Eli L. Lewitt* (Securities Act Rel. No. 10543, Exchange Act Rel. No. 84075, Investment Company Act Rel. No. 33221) (Sept. 11, 2018); *In the Matter of ICO Rating* (Securities Act Rel. No. 10673) (Aug. 20, 2019); *In the Matter of Blotics LTD. f/d/b/a Coinschedule LTD.* (Securities Act Rel. No. 109546) (July 14, 2021); *In the Matter of Poloniex* (Exchange Act Rel. No. 92607) (Aug. 9, 2021).
56. The only SEC enforcement actions with respect to digital assets in which they allege a digital asset is a security are those actions against "issuers" for failure to register a specific asset as a security. In contrast to those matters, the enforcement actions against intermediaries for failure to register do not identify the digital assets that the SEC believes are securities and that trigger the registration obligation.
57. *See* the Aspen Speech, *supra* note 47.
58. *Id*.
59. *Id*.

60. *Id*.
61. *Id*.
62. *Keynote Address of Commissioner Dan M. Berkovitz Before FIA and SIFMA-AMG*, *Asset Management Derivatives Forum 2021* (the "**FIA Speech**"), CFTC Commissioner Dan M. Berkovitz (June 8, 2021).
63. *Id*.
64. *Id*.
65. *Id*.
66. *Id*.
67. https://aave.com.
68. https://compound.finance.
69. Kofi Ansah, *Aave Set to Unveil Permissioned DeFi for Financial Institutions in July*, Coinspeaker (July 5, 2021), https://www.coinspeaker.com/aave-permissioned-defi-institutions/.
70. Sarah Tran, *Aave Pro to Launch in July for Institutional Access to DeFi Markets*, FXStreet (July 6, 2021), https://www.fxstreet.com/cryptocurrencies/news/aave-pro-to-launch-in-july-for-institutional-access-to-defi-markets-202107060509.
71. Ansah, *supra* note 3.
72. Ansah, *supra* note 3.
73. Sean Dickens, *Aave to Debut Institutional DeFi Lending via Aave Pro*, Yahoo!: News (July 7, 2021), https://news.yahoo.com/aave-debut-institutional-defi-lending-154914554.html.
74. https://compound.finance/treasury.
75. Calvin Liu, *Announcing Compound Treasury, for Businesses & Institutions*, Medium (June 28, 2021), https://medium.com/compound-finance/announcing-compound-treasury-for-businesses-institutions-83d4484fb82e.
76. Aisshwarya Tiwari, *Compound (COMP)Unveils Institutional-Grade DeFi Product Compound Treasury*, BTCManager (June 29, 2021), https://medium.com/compound-finance/announcing-compound-treasury-for-businesses-institutions-83d4484fb82e.
77. Sergio Goschenko, *Compound Launches Treasury to Introduce Institutions to DeFi*, Bitcoin.Com: News (July 7, 2021), https://news.bitcoin.com/compound-launches-treasury-to-introduce-institutions-to-defi/.
78. Brady Dale, *Compound Labs Launches "Treasury" to Get Big Firms Reaping DeFi Yields*, CoinDesk (June 28, 2021), https://www.coindesk.com/compound-labs-launches-treasury-to-get-big-firms-reaping-defi-yields.
79. *See* Alex Lipton and Lewis Cohen, "*DeFi: a pathway forward*", IFLR (Sept. 9, 2021), https://www.iflr.com/article/b1thnhzpsrjkqf/defi-a-pathway-forward.
80. *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946).
81. *Id*.
82. *Supra*, note 55.

Lewis Cohen
Tel: +1 202 754 2012 / Email: lewis.cohen@dlxlaw.com

Lewis provides in-depth legal counsel to startups, major enterprises, and governmental entities on a broad range of matters involving the use of blockchain, cryptocurrencies and other disruptive technologies. He is passionate about the ability of innovative technologies to change the way businesses and individuals work together, and is a major advocate for the potential of emerging technologies to benefit and transform industries around the globe. Lewis has more than 20 years of experience in traditional capital markets and finance and is a frequent public speaker on the topic of blockchain and distributed ledger technology. Lewis is also recognized by *Chambers Global* as one of only three lawyers in "Band 1" for Legal: Blockchain & Cryptocurrencies – USA.

Angela Angelovska-Wilson
Tel: +1 202 365 1448 / Email: angela@dlxlaw.com

Angela is an early distributed ledger technology adopter and a leading authority in the evolving global legal and regulatory landscape surrounding distributed ledger technology and smart contracts. Prior to co-founding DLx Law, Angela served as the Chief Legal & Compliance Officer of Digital Asset and was part of the founding team. Prior to joining Digital Asset, Angela was a partner at Reed Smith where she regularly advised clients on the implementation of new technologies to finance and the complex regulatory schemes involved in the development, creation, marketing, sale and servicing of various financial services and products. Before Reed Smith, Angela spent most of her career in various roles at Latham & Watkins, where she was recognized by *The Legal 500 US* among the top finance attorneys in the U.S.

Greg Strong
Tel: +1 302 766 5535 / Email: greg.strong@dlxlaw.com

Greg advises clients on compliance with securities laws, commodities laws, and other laws and regulations that may apply to activities involving blockchain and digital assets. He has successfully represented clients before the Securities and Exchange Commission, and various other regulators. In addition, he has worked on a variety of cutting-edge transactions involving digital assets.

Prior to joining DLx Law, Greg was a Deputy Attorney General in the Delaware Department of Justice from 2003 to 2018. During that time, Greg served as the Director of Investor Protection for the State of Delaware for three years and was responsible for administering and enforcing Delaware securities laws. Greg also served as the Director of the Consumer Protection Unit for three years.

DLx Law

4913 43rd St. NW, Washington, D.C. 20016 / 114 East 25th Street, New York, NY 10010 /
1007 N. Orange Street, Wilmington, DE 19801, USA
Tel: +1 212 994 6845 / URL: www.dlxlaw.com