Skadden

The Distributed Ledger

Blockchain, Digital Assets and Smart Contracts

New York Launches Suite of BitLicense Initiatives

On June 24, 2020, the New York State Department of Financial Services (DFS) announced a set of policies and proposals to clarify and streamline the regulatory landscape for virtual currency entities doing business within the state. These initiatives all relate to the licensing framework DFS established in June 2015 in anticipation of a proliferation of blockchain technology and virtual currencies, 23 NYCRR Part 200 (the 2015 Licensing Regime). The licensure and compliance requirements imposed by the 2015 Licensing Regime caused the BitLicense — the business license issued by DFS under the 2015 Licensing Regime permitting companies to engage in virtual currency activities — to be viewed as an indication of quality and security. At the same time, the standards and procedures under the 2015 Licensing Regime have been widely criticized as expensive, time-consuming and onerous, and have caused a number of virtual currency business to cease either their operations or plans to operate within New York.

The initiatives, launched under the direction of DFS Superintendent Linda A. Lacewell, are intended to address what DFS acknowledged was the "actual or perceived hurdles in obtaining a BitLicense."[1] The June 2020 announcement aimed to foster New York's virtual currency industry in three ways:

1. **Proposed Conditional Licensing Framework and SUNY Partnership.** DFS proposed a conditional licensing framework that lowers the barrier to entry for new virtual currency entities. It further announced a partnership with the State University of New York (SUNY) to facilitate that process.
2. **Final Guidance on Listing New Coins.** DFS issued final guidance for listing new virtual currency coins.
3. **Procedural Changes for BitLicense Applications.** DFS instituted procedural changes to the existing application process.

Superintendent Lacewell stated that the goal of the June 2020 initiatives is for virtual currency companies "to innovate and germinate and incubate and grow right here in the state of New York."[2]

[1] N.Y. Dep't of Fin. Servs., "Request for Comments on a Proposed Framework for a Conditional BitLicense" (2020).

[2] Jon Hill, "NY Looks To Push BitLicense Program at 5-Year Mark," Law360 (June 24, 2020).

Proposed Conditional Licensing Framework and SUNY Partnership

DFS is seeking comments from interested parties and the general public on its proposed framework for conditional BitLicenses by August 10, 2020.[3] This proposal contemplates that entities seeking to conduct virtual currency business in New York (Applicants) would be sponsored by BitLicensees or New York limited purpose trust charters authorized to engage in virtual currency business (Sponsors). Upon approval by DFS, an Applicant would receive a conditional BitLicense and could begin operating with the support of its Sponsor, which could include structural, capital, systems, personnel or other forms of support. Over time, a conditional BitLicensee would be able to seek and obtain its own full BitLicense.

To pursue a conditional BitLicense, an Applicant would first identify a specific Sponsor and enter into, or at least draft, a service level or similar agreement. The Applicant would then notify DFS of its Sponsor, provide a copy of the service level agreement, and submit certain documents and information tied to the type of business the Applicant intends to pursue and the risks particular to that business. When and if the Applicant clears substantive review by DFS of its application package, it would enter into a supervisory agreement with DFS. That agreement would outline the scope of business activities permitted for the Applicant, the responsibilities and liabilities of the Sponsor with respect to the Applicant, and the ongoing DFS oversight and compliance requirements for the Applicant. DFS would then issue the Applicant a conditional BitLicense subject to the supervisory agreement.

DFS also executed a memorandum of understanding (MOU) with SUNY on June 18, 2020, under which SUNY BLOCK will be created "to support the establishment and launch of virtual currency-related businesses ... in connection with DFS's conditional licensing framework."[4] Once created, SUNY BLOCK will be fully authorized by DFS to conduct virtual currency business activity through either a BitLicense or the limited purpose trust charter regime. SUNY BLOCK could then act as a Sponsor for conditional BitLicensees in the above-described conditional licensing framework.

If established as contemplated by the MOU, SUNY BLOCK would mitigate concerns that BitLicense holders could wield undue power over prospective Applicants for conditional BitLicenses. As of publication, there are 25 BitLicensees, each of which is a business enterprise or trust.[5] Instead of relying on potential strategic competitors to act as a Sponsor, prospective Applicants can turn to SUNY BLOCK, which is intended to support students and alumni as well as entities from the broader New York community.

Questions remain, however, regarding how SUNY BLOCK would handle conflicts of interest between Applicants and conditional BitLicensees that it sponsors, as well as whether and to what extent DFS should regulate the relationship between Sponsors and conditional BitLicensees.

Final Guidance on Listing New Coins

The June 2020 announcement also included final guidance regarding the adoption or listing of virtual currencies.[6] This final guidance incorporates feedback DFS had received after previously making the proposed policies available for public notice and comment on December 11, 2019. The final guidance is directed to two specific policies: (1) the General Framework for the Creation of a Virtual Currency Entity's Coin-Listing Policy (the Self-Certification Policy), and (2) the General Framework for Greenlisting Coins (the Greenlist Policy). Together, these policies allow BitLicensees to list additional types of virtual currencies, beyond what DFS had approved in their initial applications to DFS, without the administrative delay of seeking and obtaining case-by-case authorization from DFS.

The Self-Certification Policy allows a BitLicensee to create an internal virtual currency-listing policy through which it can self-certify the use of new virtual currencies (in addition to those permitted under the Greenlist Policy) without obtaining case-by-case approval from DFS. Prior to listing new virtual currencies through an internal coin-listing policy, a BitLicensee must obtain DFS approval that the policy meets certain criteria to protect consumer welfare. DFS requires that the policy be "tailored to the [BitLicensee's] specific business model, operations, customers and counterparties, geographies of operations, and service providers; and to the use, purpose, and specific features of coins being considered."[7] Moreover, the policy must demonstrate certain attributes (detailed by DFS) pertaining to governance, risk assessment and ongoing monitoring procedures. The Self-Certification Policy does not modify prior prohibitions on the listing of any virtual currencies that "facilitate the obfuscation or concealment" of anyone's identity or virtual currencies that are "designed or substantially used to circumvent laws and regulations."[8] DFS uses privacy coins and gambling coins as examples of virtual currencies that are still prohibited due to those rules.

[3] N.Y. Dep't of Fin. Servs., "Request for Comments on a Proposed Framework for a Conditional BitLicense" (2020).

[4] "Memorandum of Understanding between the New York State Department of Financial Services and The State University of New York" (June 18, 2020).

[5] N.Y. Dep't of Fin. Servs., "Regulated Entities" (updated June 19, 2020).

[6] N.Y. Dep't of Fin. Servs., "Guidance Regarding Adoption or Listing of Virtual Currencies" (2020).

[7] *Id.*

[8] *Id.*

Under the Greenlist Policy, DFS will maintain a public record of any virtual currency that BitLicensees are preauthorized to list without case-by-case approval from DFS (the Greenlist), subject to any usage restrictions imposed by DFS. There are two mechanisms through which a virtual currency can appear on the Greenlist. DFS may exercise its discretion to include any virtual currency on the Greenlist. Alternatively, if at least three separate and unrelated BitLicensees use the Self-Certification Policy to list the same virtual currency for the same use, that virtual currency will appear on the Greenlist (limited to that use) after a six-month waiting period. As of publication, the Greenlist permits the listing and custody of Bitcoin, Bitcoin Cash, Ethereum, Gemini Dollar, Litecoin, PAX Gold and Paxos Standard.[9] Additionally, Ethereum Classic and Ripple are permitted for custody only.[10]

To maintain compliance with DFS requirements, all BitLicensees must disclose to customers whether each virtual currency they offer for use is authorized through the Self-Certification Policy, the Greenlist Policy, or the standard case-by-case DFS approval process. Additionally, although the Self-Certification Policy and Greenlist Policy allow BitLicensees to list virtual currencies without specific DFS approval, they nonetheless must provide DFS with notice so that DFS may provide proper oversight and regulation.

Procedural Changes for BitLicense Applications

Two procedural changes to the BitLicense application process, designed to enhance both the efficiency and rapidity of BitLicense application processing, were also part of the June 2020 announcement: (1) the substantive review limit and (2) the deficiency letter limit.[11]

Under the substantive review limit, DFS will now only allocate resources to provide substantive review of BitLicense applications that are facially complete. Previously, DFS would begin substantive review for applications regardless of whether they were facially complete; doing so consumed DFS time and resources when partial applications were reviewed by DFS but never completed by the applicant. A BitLicense application will be deemed facially complete when every document has been filled out in the online application system (the Nationwide Multistate Licensing System & Registry) and submitted either to that system or to DFS directly, as set forth in the online checklist of BitLicense application requirements. If a BitLicense application is characterized as facially complete but substantive review reveals a deficiency with respect to the checklist requirements, the review will be suspended unless and until the applicant remedies the deficiency.

Under the deficiency letter limit, DFS has established a "three strike rule," where DFS has the discretion to deny a BitLicense application for failing to remedy a specific deficiency three times. DFS will send an applicant deficiency letters if, during the substantive review process, it identifies any issues that prevent the application from being approved. Each deficiency letter will include a return date by which a complete response is due, and DFS will be available prior to that return date to answer applicant questions about the deficiency. If DFS sends an applicant three deficiency letters about the same requirement, or set of requirements, and that requirement is not satisfied by the return date of the third letter, DFS may elect to deny the BitLicense application. The goal of this policy is to conserve DFS resources, thereby allowing quicker reviews of other applications.

US v. Gratkowski: Bitcoin Blockchain and the Expectation of Privacy

In a first-of-its-kind ruling at the intersection of cryptocurrency and constitutional privacy rights, the U.S. Court of Appeals for the Fifth Circuit ruled in *U.S. v. Gratkowski*[12] that Bitcoin holders have no reasonable expectation of privacy in their public keys on the Bitcoin blockchain.

Background

Like most blockchain-based networks, the Bitcoin blockchain uses public-key cryptography that relies on a pair of cryptographic keys: a private key that is kept confidential and a public key that is visible on the blockchain. These keys are comprised of a random series of letters and numbers. This system helps ensure the authenticity and integrity of a transaction message, as each individual transacting on the network is associated with at least one public key address. (Users could, of course, have multiple addresses representing multiple accounts.)

In order to transact in Bitcoin, users must download a wallet that either holds the Bitcoin or generates a private-public key pair. For each transaction, the Bitcoin blockchain records the amount transferred, public address of the sender and public address of the receiver. It is not possible to link an individual to a public key without additional information such as from a wallet provider, or, in some cases, by analyzing the transaction itself.

[9] N.Y. Dep't of Fin. Servs., "Virtual Currencies: Greenlist" (updated June 19, 2020).

[10] *Id.*

[11] N.Y. Dep't of Fin. Servs., "Notice of Virtual Currency Business Activity License Application Procedures" (2020).

[12] Case No. 19-50492 (5th Cir. June 30, 2020).

The *Gratkowski* Decision

In *Gratkowski*, federal agents analyzed the public Bitcoin addresses associated with a website selling child pornography and then subpoenaed the wallet provider, Coinbase, for all information on its customers who had sent Bitcoin to those addresses. In response, Coinbase identified Richard Gratkowski. In a search of Gratkowski's home, the agents subsequently found a hard drive containing child pornography, and Gratkowski admitted to making the illegal payments. Gratkowski moved to suppress the evidence from that search, claiming that both the blockchain analysis and the subpoena to Coinbase violated his Fourth Amendment rights against unreasonable searches and seizures.

Relying upon *Carpenter v. U.S.* (2018), in which the U.S. Supreme Court held that individuals held a right to privacy in their cell-site location information (CSLI), Gratkowski argued that his Bitcoin information should be subject to the same protections. The Fifth Circuit rejected this position, distinguishing CSLI from the Bitcoin information at issue on the grounds that (1) CSLI provides a full account of the phone owner's whereabouts and activities, supplying an "intimate window into a person's life," and (2) CSLI is not "voluntarily" shared because location logs are kept without any affirmative act on the user's part — if the phone is on, it is transmitting CSLI to a third party.

The court instead analogized Bitcoin public addresses to bank records and telephone call logs, neither of which are subject to Fourth Amendment protections because they are voluntarily disclosed to third parties (*e.g.*, bank employees and the telephone company). In doing so, the court relied on the Supreme Court's decision in *U.S. v. Miller* (1976), which held that bank records were "negotiable instruments" rather than confidential communications, and thus individuals had no expectation of privacy in them. The Court also relied on *Smith v. Maryland* (1979), in which it applied the "third party doctrine" to telephone call logs and concluded that individuals had no expectation of privacy because they were aware the telephone company was tracking the numbers that they dialed.

The Fifth Circuit reasoned that since the Bitcoin blockchain is public, users do not have an expectation of privacy in the addresses shared on the chain. The court left open the possibility that if Bitcoin were to become an inescapable part of daily life akin to cellphones, Bitcoin information may one day be afforded CSLI-like protections under the Fourth Amendment.

Likewise, the court found no expectation of privacy in Gratkowski's Coinbase transactions. Gratkowski elected to use Coinbase's services and provide the company with personal information. The court emphasized that sophisticated users can choose to transact directly with each other on the Bitcoin blockchain without using a third-party wallet provider and thus gain more privacy in their Bitcoin transactions. Coinbase users are therefore choosing to accept the trade-off of reduced privacy for the ease of transacting that comes with the use of a third-party intermediary, the court determined.

Key Takeaways

Because *Gratkowski* is the first federal appellate court to address these novel issues, the possibility remains that other circuit courts may reach different conclusions. This could tee up the questions raised in *Gratkowski* for the Supreme Court to address. Moreover, as the *Gratkowski* court itself acknowledged, its ruling may be time-limited in nature, particularly if the understandings and experiences of Bitcoin users evolve as the technology achieves further adoption. On this score, the decision could affect Bitcoin users' conduct, as more individuals seek ways to transact without third-party intermediaries in order to preserve their expectations of privacy.

Finally, although the *Gratkowski* court concluded that Bitcoin users have no Fourth Amendment expectation of privacy in their on-chain records, it remains to be seen whether public keys constitute personal data for civil privacy purposes under statutes like the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act. Indeed, the French data protection authority, "Commission Nationale de l'Informatique et des Libertés," has suggested that public keys are "personal data" under the GDPR.[13] A report commissioned by the European Parliament suggested a similar approach.[14]

We expect that the third-party doctrine will continue to evolve in the distributed ledger context, particularly as the technology becomes more pervasive and as more personal data is passively collected from users without those users affirmatively providing it. As the first word on these matters, *Gratkowski* will hardly be the last.

OCC Interpretive Letter Confirms National Bank Authority To Provide Cryptocurrency Custody Services

On July 22, 2020, the Office of the Comptroller of the Currency (OCC) issued a release[15] confirming the authority of national banks and federal savings associations to provide cryptocurrency custody services. Determining that these services fall well within

[13] Commission Nationale de l'Informatique et des Libertés, "Blockchain and the GDPR: Solutions for a Responsible Use of the Blockchain in the Context of Personal Data" (Nov. 6, 2018).

[14] European Parliamentary Research Service, "Blockchain and the General Data Protection Regulation: Can Distributed Ledgers Be Squared With European Data Protection Law?" (July 2019)

[15] *See* OCC Interpretive Letter No. 1170 (July 22, 2020) (hereinafter "Interpretive Letter 1170") (Authority of a National Bank To Provide Cryptocurrency Custody Services for Customers).

national banks' "longstanding authorities to engage in safekeeping and custody activities,"[16] the OCC concluded that a national bank may permissibly engage in the provision of cryptocurrency custody services on behalf of its customers, including by holding the unique cryptographic keys associated with cryptocurrency. Notably, the OCC describes cryptocurrency custody services as merely "a modern form of traditional bank activities related to custody services."[17] This release is the latest among a flurry of recent releases by OCC that have focused on "modernizing" the bank regulatory framework under the leadership of the new acting comptroller of the currency, Brian Brooks.

The interpretive letter, written by OCC Chief Counsel Jonathan Gould, reflects the OCC's position that custody of a cryptocurrency asset is a necessary regulatory innovation for the banking sector in light of recent technology developments. The OCC preemptively defends the authority for national banks to engage in such activity by stating that national banks have long provided safekeeping and custody services of both physical objects and electronic assets. Further, "as the banking industry entered the digital age, the OCC recognized the permissibility of electronic safekeeping activities."[18] The OCC cited prior interpretive letters authorizing national banks to provide similar services with respect to other electronic assets, including escrow encryption keys, file retrieval activities and secure web-based document storage.[19]

The OCC notes that custody for cryptocurrencies will, more often than not, mean that the bank is actually taking possession of the cryptographic access keys to that unit of cryptocurrency. As the OCC states, "[a] bank that provides custody for cryptocurrency in a non-fiduciary capacity would essentially provide safekeeping for the cryptographic key that allows for control and transfer of the customer's cryptocurrency."[20]

Interestingly, the letter goes on to suggest that broader applicability may be possible. The OCC includes a note that "crypto custody services may extend beyond passively holding 'keys.'"[21] The OCC notes that a bank may provide "related" custodial services and provides, in a footnote, a list of examples of ways of facilitating a customer's cryptocurrency and fiat currency exchange transactions, transaction settlement, trade execution, record keeping, valuation, tax services, reporting or other appropriate services.[22] Additionally, the OCC includes a reference to OCC regulations that "explicitly authorize national banks to perform, provide or deliver through electronic means and facilities any activities that they are otherwise authorized to perform."[23]

The letter "reaffirms the OCC's position that national banks may provide permissible banking services to any lawful business they choose, including cryptocurrency businesses, so long as they effectively manage the risks and comply with applicable law."[24] As with all activities performed by national banks, cryptocurrency activities must be conducted in a safe and sound manner. The OCC will require its supervised institutions to establish adequate systems for identifying, measuring, monitoring and controlling the risks of such activities, and to implement internal controls. As with any new asset or product, the bank will be expected to develop sufficient and ongoing training, and to have robust compliance and management information systems governing cryptocurrency custody services. The OCC also require all custody activities to include dual controls, segregation of duties and accounting controls.

A bank will not be required to seek formal OCC approval to engage in cryptocurrency custody activities. The OCC recognizes that, as the financial markets are increasingly digitized, the need will increase for banks and other service providers to leverage new technology and innovative ways to serve their customers' needs. Importantly, however, the letter highlights the expectation of the OCC that a national bank will consult its OCC supervisors "as appropriate" prior to engaging in such activities.[25]

Acting Comptroller Brooks has stated that one of the priorities of the agency is to build upon responsible innovation to help the banking system keep up with changes in the way American consumers and businesses manage their finances.[26] Mr. Brooks, the former chief legal officer at cryptocurrency exchange Coinbase, took over as acting comptroller on May 29, 2020, and quickly focused his attention on banking innovation. On June 4, 2020 — less than a week after Mr. Brooks assumed his new role — the OCC published an advance notice of proposed rulemaking (ANPR)[27] concerning the regulation of digital activities in banking, and in particular those activities involving cryptocurrency and distributed ledger technology. Consistent with his stated

[16] *Id.* at 7.

[17] *Id.* at 6.

[18] *Id.*

[19] *Id.* at 6-7.

[20] *Id.* at 6.

[21] *See* OCC News Release 2020-98, "Federally Chartered Banks and Thrifts May Provide Custody Services for Crypto Assets" (July 22, 2020).

[22] Interpretive Letter No. 1170 at 8, FN 39.

[23] *Id.* at 8.

[24] *Id.* at 1.

[25] *Id.* at 10.

[26] OCC News Release 2020-69, "Brian P. Brooks Statement on Becoming Acting Comptroller of the Currency" (May 29, 2020) (quoting Acting Comptroller Brooks' belief that "the OCC can build on its foundation of innovation to provide banks and thrifts the regulatory certainty, the flexible framework, and oversight that allows them to evolve and capitalize on technology and innovation to deliver better products and services, to operate more efficiently, and to reduce risk in the system").

[27] *See* "A National Bank and Federal Savings Association Digital Activities" (June 4, 2020).

priorities, the ANPR established that the OCC is in the midst of an active review of regulations focused on the modernization of such activities. It requested public comment on the ways in which digital activities are currently being used in banking, in order "to ensure that its regulations continue to evolve with developments in the industry."[28] The public comment period for this ANPR ends on August 3, 2020.

In connection with the most recent opinion on custody activities, Mr. Brooks stated that "from safe-deposit boxes to virtual vaults, we must ensure banks can meet the financial services needs of their customers today. ... This opinion clarifies that banks can continue satisfying their customers' needs for safeguarding their most valuable assets, which today for tens of millions of Americans includes cryptocurrency."[29]

Kentucky Establishes Blockchain Technology Working Group

Kentucky is the latest state to launch a formal exploration of the application of blockchain technology to government functions and other sectors. A new state law[30] that went into effect on July 15, 2020, establishes the Blockchain Technology Working Group and tasks it with evaluating how blockchain can be used to improve — and increase the security of — Kentucky's critical infrastructure. The Kentucky initiative is yet another example of how various states are looking to position themselves as blockchain-friendly to both start-ups and more established companies working in this space.

Background

The Blockchain Technology Working Group — to be comprised of nine members, three of whom are ex officio members — will explore the application of blockchain technology to various sectors including, but not limited to, government, emergency services, public utilities and telecommunications. The working group, chaired by the chief information officer for the Commonwealth Office of Technology, includes representatives from the state Office of Homeland Security and the state Public Service Commission.

Estimated to cost the state $400,000 annually,[31] the working group is expected to report to Gov. Andy Beshear and the Legislative Research Commission at the end of each calendar year. The group will provide a priority list of critical state infrastructure that could benefit from blockchain technology, a determination of the feasibility of implementing blockchain and an associated cost-benefit analysis.

As with other state laws related to blockchain technology, a key component of the Kentucky law is how certain key terms are defined. The Kentucky law defines "blockchain technology" as "shared or distributed data structures or digital ledgers used in peer-to-peer networks that store digital transactions, verify and secure transactions cryptographically, and allow automated self-execution of smart contracts." It defines "smart contract" as "a computerized transaction protocol that self-executes the terms of a contract and that is integrated into the blockchain program architecture." The definition of "smart contract" may create some uninvited ambiguity given that many smart contracts only execute very discrete terms of a contract.

The definitions applied by Kentucky are also somewhat more limited than those applied by states taking a more expansive view of this area. For example, Wyoming, which has sought to position itself as a leading crypto-friendly state, has created a broad structure of cryptocurrency law, including defining digital assets as property.[32] Kentucky will likely have to evolve its definitions, and thus provide more guidance, as it builds its understanding of what blockchain technology implementation looks like in the state.

Key Takeaways

Kentucky joins a growing number of states seeking to embrace and explore how blockchain technology can streamline government processes and shape the delivery of critical services. Although some assert these laws are primarily marketing mechanisms to attract blockchain companies, legislatures across the United States are studying the costs, benefits and applications of distributed ledger technology, we expect its application in government to become more common over time. Until then, it remains to be seen what the practical outcome of the Kentucky legislation will be for blockchain companies. Interestingly, the Kentucky law does not purport to address the complex issues of cryptocurrency and the use of digital assets for financial transactions. Indeed, the newly formed working group omits the state departments dealing with financial services.

[28] "*Id.* at 1.

[29] OCC News Release 2020-98, "Federally Chartered Banks and Thrifts May Provide Custody Services for Crypto Assets" (July 22, 2020).

[30] §42.747.

[31] Legislative Research Commission, Commonwealth of Kentucky Fiscal Note Statement (2020).

[32] 2019 Wy. SF 125.

Other states racing to be a trailblazer in blockchain implementation include:

- Wyoming, which in enacting more than a dozen blockchain-enabling laws has established itself as the "Delaware of digital asset law";[33]
- Illinois, which continues to explore implementation of blockchain technology across government agencies through the Illinois Blockchain Initiative;
- Florida, which has established a Blockchain Task Force as part of the Department of Financial Services to develop a master plan to deploy blockchain across state functions; and
- Virginia, which is exploring how blockchain can be used to secure its state election results and voter records.

[33] Caitlin Long, "What Do Wyoming's 13 New Blockchain Laws Mean?" Forbes (Mar. 4, 2019).

Contacts

Alexander C. Drylewski
Partner / New York
212.735.2129
alexander.drylewski@skadden.com

Eytan J. Fisch
Partner / Washington, D.C.
202.371.7314
eytan.fisch@skadden.com

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

Skadden, Arps, Slate, Meagher & Flom LLP
One Manhattan West
New York, NY 10001
212.735.3000

skadden.com