Chamber of Digital Commerce

Testimony for the Record

United States Senate Committee on Banking, Housing, and Community Affairs

Hearing *Examining Regulatory Frameworks for Digital Currency and Blockchain*

July 30, 2019

I. Introduction

The Chamber of Digital Commerce (the "Chamber") welcomes the opportunity to submit this testimony for consideration by the Senate Banking Committee (the "Committee") regarding regulatory frameworks impacting digital currencies and blockchain technology. The Chamber is the world's largest blockchain trade association. Our mission is to promote the acceptance and use of digital assets and blockchain technology, and we are supported by a diverse membership that represents the blockchain industry globally.

Through education, advocacy, and close coordination with policymakers, regulatory agencies, and industry across various jurisdictions, our goal is to develop a pro-growth legal environment that fosters innovation, job creation, and investment. We represent the world's leading innovators, operators, and investors in the blockchain ecosystem, including leading edge start-ups, software companies, global IT consultancies, financial institutions, insurance companies, law firms, and investment firms. Consequently, the Chamber and its members have a significant interest in blockchain and distributed ledger technology.

II. Executive Summary

This testimony describes the principles we believe are important to consider when establishing government priorities for blockchain technology; the importance of terminology; and areas of friction related to financial services that we have identified through our many years of work with the industry. Specifically, this document addresses:

- The benefits of blockchain as a technology that creates faster, more efficient, more inclusive systems that, if properly overseen, can create extraordinary opportunities for consumers;
- The need for government support from the federal government and Congress (the states are already capitalizing on the opportunity this technology presents) to ensure that technological advances and associated standards and oversight remain in the United States;
- The existing complex regulation of "spot" markets such as trading platforms and exchanges, and potential solutions;
- The need for clear guidance as to when a digital token is a security triggering the U.S. securities laws as well as solutions to certain consumer protection principles within the securities laws;
- The technological advances blockchain technology brings to anti-money laundering and economic sanctions compliance, and how existing laws inhibit enhanced detection;
- How misunderstandings around what is a "smart contract" are creating a patchwork of inconsistent legislation in the states;
- The lack of accounting standards specific to digital assets such as virtual currencies is limiting the ability of companies to deliver better transparency and obtain necessary regulatory approvals; and
- The current tax treatment that has been criticized broadly due to needed clarification in a number of areas; it is also inhibiting use of virtual currencies as a method of payment.

We thank the Committee for its interest in this important matter and look forward to continued engagement.

III. The Benefits of Blockchain Technology and DLT

Distributed ledger technology is computer software that employs a shared database architecture to maintain multiple, identical copies of an auditable, up-to-date distributed digital record of transactions or data. A blockchain is a specific type of DLT that records transfers of data and organizes them into "blocks" that are stacked or "chained" together chronologically by a cryptographic hash function and confirmed by a consensus mechanism. Advanced blockchains can serve as the foundational protocol upon which many applications can be built - much like how the Internet underpins multiple applications such as e-mail, e-commerce, and business processes.

Characteristics of Blockchain Technology:

- Distributed: Data is shared across nodes rather than being maintained by a central administrator. Each node maintains a copy of the blockchain, making it resilient to localized failures and isolated attacks.

- Consensus Algorithm: A set of rules by which a distributed network reaches agreement to verify a transaction's occurrence and ensures that all nodes have

an identical copy of the ledger of transactions.

- Cryptography: Blockchains use complex mathematical algorithms to secure and validate transactions on the network.

- Immutability and Record Keeping: Once a transaction occurs and is recorded on a blockchain, the hashing and linking functions provide authenticity by showing that items have not been altered.

- Smart Contracts: The ability to link and execute automated smart contracts increases the efficiency of transactions.

Bitcoin was the first iteration of blockchain technology. Bitcoin provided a solution to the operative problems of transferring value in a digital environment – specifically, how to ensure that digital value is not spent twice. Although the solution was beneficial to the promulgation of virtual currencies, its underlying value is in its potential to create transactional efficiencies in transferring value and recording transactions in a secure way in a vast array of industries. This is due, in part, to the manner in which cryptographically-protected information is replicated, shared, and accessed across a network.

At its heart, blockchain is a database technology. As with any database technology, it can be used to create and track digital representations of assets (including natively digital goods). The financial services applications of blockchain include value transfer and the creation of digital tokens[1] representing traditional securities and other traditional financial instruments. It would be too limiting, however, to only consider these applications of the technology and any consideration of blockchain technology must recognize the broad array of uses for tokens as well as assets that can be digitized and transacted in on blockchains, including tangible assets. Simply creating a digital representation of an asset does not change the asset's character or nature, nor should it change the asset's treatment under law.

For more information and detail regarding blockchain technology and legislative solutions, see *Legislators' Toolkit for Blockchain* at https://digitalchamber.org/state-legislators-toolkit/.

IV. Areas in Need of Consideration

The following are areas within the financial services sector that we have identified as requiring attention and/or clarification from government actors to ensure that blockchain technology and DLT can thrive to provide improved products and services to consumers

[1] Digital tokens are transferable units generated within a distributed network that tracks ownership of the units through the application of blockchain technology. CHAMBER OF DIG. COMMERCE, Understanding Digital Tokens: Market Overviews and Proposed Guidelines for Policymakers and Practitioners, https://digitalchamber.org/token-alliance-whitepaper/.

in the United States in a responsible way.

a. Decisive Government Support

The possibilities provided by blockchain technology and its tremendous positive impact for economic advancement have been recognized by policymakers on the federal, state, and multinational levels. Its ability to improve business processes, increase efficiency, and promote transparency in numerous industries is transforming the ways in which companies conduct business and transact. Blockchain is a revolutionary breakthrough, allowing us to create infrastructure towards an "Internet of Value" whereby value can be exchanged as quickly as information.

While technological progress is clear, it does not automatically follow that the United States will establish its preeminence in the blockchain sector. Already, major industrialized nations are making significant advances in promoting and adopting this technology, making a hard run to be the leaders, and obtain the economic benefits, of this industry. If the United States fails to address the outstanding regulatory issues, it risks falling significantly behind other nations who recognize the advantages blockchain brings.

Government agencies within the United States are exploring blockchain technology to streamline federal procurement, for example, and U.S. companies are building systems to streamline operating practices, capture economic efficiencies, and grow the U.S. economy.[2] More needs to be done, however, to coordinate support for this technology in the United States. Laws dating back decades, in some cases 80 years, are proving difficult to apply to this emerging technology and are thus stifling economic growth in this space.

In the twentieth century, the U.S. government realized the tremendous potential of the Internet and took a central role in nourishing, developing, and promoting its creation and widespread adoption. To maintain our technological and economic world leadership, it is imperative that the United States similarly encourage blockchain development or risk falling behind countries that are embracing the technology and exploring its benefits in the private and public sectors. To meet this need, we proposed a National Action Plan for Blockchain to ensure that blockchain technology is encouraged and supported in the United States.[3]

The United States needs two things to remain at the forefront of blockchain developments and promote its innovation and use: 1) provide leadership through strong

---

[2] *See, e.g.,* DEP'T OF HOMELAND SEC., BLOCKCHAIN AND SUITABILITY FOR GOVERNMENT APPLICATIONS (2018), https://www.dhs.gov/sites/default/files/publications/2018_AEP_Blockchain_and_Suitability_for_Government_Applications.pdf; *see also* Steve Delahunty, *Developments and Adoption of Blockchain In the U.S. Federal Government* (Jan. 25, 2018), https://www.forbes.com/sites/forbestechcouncil/2018/01/25/developments-and-adoption-of-blockchain-in-the-u-s-federal-government/#3fb7781d3d99.

[3] CHAMBER OF DIG. COMMERCE, NATIONAL ACTION PLAN FOR BLOCKCHAIN (Feb. 20 2019), https://digitalchamber.org/blockchain-national-action-plan/.

public support and policymakers who are open to and understand the technology; and 2) a coordinated plan to ensure appropriate support and harmonized regulatory approach, where needed.

The U.S. government must explore these opportunities in depth through many means, including conversations with industry leaders and government stakeholders to ensure the United States maintains its competitive advantage in technological development. This engagement could occur through an intergovernmental taskforce, or a regular meetings between the public and private sectors, to discuss the benefits of blockchain technology across industries. An intergovernmental task force will serve to further the U.S. position to promote free enterprise and to develop policy objectives toward promoting industry-led blockchain and economic growth within the United States. This collaboration can also be used to help public officials and regulators remain knowledgeable and informed about the technology.

A cornerstone of any blockchain initiative requires the exploration and understanding of blockchain and DLT. These technologies are often complex and must be properly understood and tested before implementation. We therefore recommend that one result of the Committee's efforts should be to establish an office, or task an existing office, within the Executive branch that coordinates the U.S. Government's blockchain strategy going forward. This office would serve to coordinate agency consideration of blockchain, determine and promote government applications of blockchain that could cut costs for taxpayers, track the government's use of blockchain across agencies, and act as a gateway for industry and government to best understand the laws surrounding blockchain and virtual currencies.[4] Such an office can better develop blockchain-based economic development and activity and coordinate the U.S. government's perspective across agencies. In addition, accelerated government adoption and use, where appropriate, will help the public sector by providing a reference of working examples and best practice implementations. We note that this office would not just consider financial services applications, but all applications that could benefit government, industry, and consumers.

b. Existing Regulation of Spot Markets (Trading Platforms and Exchanges)

The Commodity Futures Trading Commission ("CFTC") has regulatory and enforcement jurisdiction over derivatives of virtual currencies traded in the United States. While it does not have direct oversight jurisdiction over markets or platforms conducting cash or "spot" transactions in virtual currencies, it does maintain after-the-fact enforcement

[4] Several U.S. states have already adopted this approach, as recommended in our Legislator's Toolkit for Blockchain, or developed blockchain task forces or initiatives, including Delaware, Florida, Illinois, New York, North Carolina, Wyoming, and at least 14 states have introduced legislation to do the same.

against fraud and manipulation in those spot markets.[5]

Primary oversight of virtual currency spot market activity – including wallet providers, which are used to store, send, and receive virtual currency, and exchanges – primarily falls under state money transmission laws and federal anti-money laundering ("AML") oversight and enforcement. Currently, 49 states, the District of Columbia, and various U.S. territories each have their own money transmission license requirements,[6] many of which apply to virtual currency-related businesses. Oftentimes, however, it is unclear which or how those requirements apply. Companies are thus subject to significant uncertainty and onerous state-by-state application requirements, fees, examinations, and regulatory oversight in a system that was designed for 20th century business models and services. The various state laws differ in meaningful ways, even on things as fundamental as the definition of a money transmitter, which determines whether companies must file an application and obtain a license.[7]

In addition to state licensing requirements, these companies must also register with the Financial Crimes Enforcement Network ("FinCEN") of the Department of the Treasury as money services businesses ("MSBs") and comply with various federal regulations including recordkeeping, reporting, and development of an anti-money laundering ("AML") program and other requirements.

This patchwork of state and federal regulations is expensive, requiring dedicated personnel to manage the recordkeeping alone, in addition for personnel to maintain AML program compliance obligations and manage each state's and the federal government's on-site examinations, among other things. For blockchain companies, many of which are growing start-ups with seasoned industry executives, this antiquated and inconsistent framework poses a high barrier to entry. The current framework and laws were designed prior to the digital era and are not well-suited for digital companies whose business and service models are inherently global in nature and may not fit the traditional descriptions of "money transmitters." This regulatory regime prevents the introduction of new technologies to advance financial inclusion and the provision of financial services, which blockchain companies enable.

State licensing requirements are primarily focused on consumer protection, the management of the company via background checks and other criteria, and the

---

[5] *Virtual Currencies: The Oversight Role of the U.S. Securities and Exchange Commission and the U.S. Commodity Futures Trading Commission Before the Comm. on Banking, Housing, and Urban Affairs*, 115th Cong. 4 (2018) (statement of J. Christopher Giancarlo, Chairman, Commodity Futures Trading Comm'n). *See also* National Futures Association, Interpretive Notice 9073 – Disclosure Requirements for NFA Members Engaging in Virtual Currency Activities (May 17, 2018), https://www.nfa.futures.org/rulebook/rules.aspx?Section=9&RuleID=9073.

[6] CONFERENCE OF STATE BANK SUPERVISORS, 2017 NMLS MONEY SERVICES BUSINESSES INDUSTRY REPORT (Sept. 2018), https://mortgage.nationwidelicensingsystem.org/about/Reports/2017-NMLS-Money-Services-Businesses-Report.pdf; *see also* Thomas Brown, *50-STATE SURVEY: Money Transmitter Licensing Requirements*, CALIFORNIA ASSEMBLY, https://abnk.assembly.ca.gov/sites/abnk.assembly.ca.gov/files/50%20State%20Survey%20-%20MTL%20Licensing%20Requirements(72986803_4).pdf (last visited February 28, 2019).

[7] CONFERENCE OF STATE BANK SUPERVISORS, *supra* note 12.

solvency of the money transmitter as a custodian of customers' funds. Placing virtual currency and blockchain companies under this regulatory framework is inefficient because it does not take into account broader market oversight including price and market manipulation. This inefficiency may undermine the goals of consumer protection[8] and fair and efficient markets. Indeed, both Chairman Clayton of the Securities and Exchange Commission ("SEC") and Chairman Giancarlo of the CFTC have noted that it may be time to re-evaluate this framework.[9]

In addition, the SEC has jurisdiction over exchanges that offer and sell securities. According to the SEC, "A platform that offers trading in digital asset securities and operates as an "exchange" (as defined by the federal securities laws) must register with the Commission as a national securities exchange or be exempt from registration."[10] A question arises, however, as to when an exchange is selling a digital token that is not a security, and one that is.

The CFTC, FinCEN, SEC, state regulators, and other regulatory bodies all have jurisdiction to oversee various aspects of virtual currency markets. The Chamber believes that there should be a single federal option alternative that recognizes the unique attributes of blockchain technology and digital assets and that pre-empts state money transmitter licensing requirements to avoid duplicative and inefficient regulation. Alternatively, the development of an industry-developed and led self-regulatory organization, empowered by Congress through legislation providing it with enforcement powers, could be an effective vehicle for governance. Either of these options requires a careful balancing of the factors required to achieve meaningful oversight, appropriate sanctions on violators, and encourage robust economic development.

c. The Need for Guidance on Digital Tokens

Many participants in the blockchain industry have developed tokens to enable use of their systems or relied on token sales to fund the development or operation of their blockchain projects. Some of these tokens are widely understood not to be securities under federal securities laws, as is the case with bitcoin and ether. In other instances, however, if the token or method of distribution meet certain criteria, the SEC has found certain tokens to be securities and brought enforcement actions against issuers for violation of securities laws.

The SEC uses the *Howey* Test derived from a U.S. Supreme Court case dating back to

---

[8] SEC Strategic Hub for Innovation and Financial Technology, *Framework for "Investment Contract" Analysis of Digital Assets*, April 3, 2019, https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets.

[9] Jay Clayton and J. Christopher Giancarlo, *Regulators are Looking at Cryptocurrencies,* WALL ST. JOURNAL (Jan. 24, 2018), https://www.wsj.com/articles/regulators-are-looking-at-cryptocurrency-1516836363 ("We would support policy efforts to revisit these frameworks and ensure they are effective and efficient for the digital era.").

[10] SEC Division of Corporation Finance, Division of Investment Management, and Division of Trading and Markets, Statement on Digital Asset Securities Issuance and Trading (Nov. 16, 2018), https://www.sec.gov/news/public-statement/digital-asset-securites-issuuance-and-trading.

1946 to determine whether an investment contract such as a token is a security.[11] The *Howey* Test dates back almost seventy-five years and was not created with the digital age in mind. While the SEC commissioners and staff have made attempts through speeches, testimony, enforcement actions, and other means to signal to market participants what characteristics of a token might make it a security, such guidance is not binding on future agency action. The recent publication of a Framework for "Investment Contract" Analysis of Digital Assets is a helpful checklist for companies to consider in this regard; however, its numerous criteria, without reference to which carry more weight than others if triggered, render the guidance difficult for practitioners to use with confidence. Unfortunately, the No Action Letter published contemporaneously with the Framework was very limited and, arguably, the digital token should not have been considered a security at all.

Innovators need formal guidance, developed with industry input and an understanding of the various token platforms and uses, on the standards and factors that the SEC believes are appropriate for the evaluation of whether a digital token constitutes a security, as well as clear statements that bitcoin, ether, XRP, and similar tokens are not considered, in and of themselves, to be securities. Currently, determinations are made on a case-by-case basis and, for a single token, may change over time as the characteristics of the token change. The lack of clarity around the standards used to determine what constitutes a security is inhibiting development and innovation in the industry and is resulting in the United States falling behind other nations with clearer token guidelines that foster innovation.[12]

In order to provide the certainty companies need to operate in the United States, a digital token definition needs to be established that clearly outlines the criteria for such a token to be deemed a security. Further, certain digital tokens must be explicitly carved out from consideration of a security under securities law. The new definition should include "utility" or use-based tokens that serve a fundamental purpose – as an integral part of a service offering – and, accordingly, should not be considered an investment contract under the *Howey* Test.[13] Many utility token distributions are vital to projects where companies are attempting to create innovative solutions using blockchain, but their fundamental existence is jeopardized by the existing regulatory uncertainty. Creating a clear definition and space for these tokens to exist would not only benefit U.S. innovation, but would serve a dual purpose to address fraudulent activities.

One way to achieve this clarity is through legislation that would spell out these criteria and amend the securities laws as appropriate, and this route may be necessary.

---

[11] *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946); *see* Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO (July 25, 2017), https://www.sec.gov/litigation/investreport/34-81207.pdf.

[12] *See, e.g.,* Leigh Cuen, *Circle Moves Exchange Operations Offshore With New Bermuda Office*, CoinDesk, (July 22, 2019), https://www.coindesk.com/circle-moves-non-us-poloniex-customers-to-new-bermuda-entity.

[13] For more information on "utility tokens," *see* Understanding Digital Tokens: Market Overviews and Proposed Guidelines for Policymakers and Practitioners, https://digitalchamber.org/token-alliance-whitepaper/.

Moreover, the SEC should consider a clearly articulated safe harbor or other exemptive relief concluding that certain digital tokens are not securities. For example, a clear binding statement that bitcoin, ether, and XRP are not securities would go a long way to enabling certain facets of the industry to evolve.

d. Needed Clarifications Concerning Custody of Digital Tokens

With digital tokens, there is no object stored physically; rather records are maintained on an immutable blockchain showing transactions and transfers of ownership that have occurred by sending and receiving tokens via a software wallet using public-private key encryption. The technologies and methods used to maintain ownership and to safeguard these assets are constantly evolving. For example, the application of multi-signature[14] technology bringing added consumer protections to authentic transactions; however, they also bring a layer of complexity to custody requirements for these assets because the keys necessary to execute a transaction may be in multiple physical locations. Public and private keys are analogous to a user name and password where the public key, like a user name, may be viewed by anyone and the private key, like a password, is stored privately and used in conjunction with the public key to access the software. Regulators and policymakers will need to understand the ways in which ownership of these new assets is currently reflected and be mindful of the evolution of the technologies as they consider guidance to market participants on the application of existing regulatory requirements surrounding custody[15] to innovative technologies.

This changing technology is moving faster than regulatory infrastructure and decision-making. Regulated broker dealers and investment advisers, lawyers, independent auditors, and others have spent countless hours at a significant cumulative cost to try to fit rules written for physical and book-entry securities to the blockchain environment. Nevertheless, the market needs more definitive guidance for participants to move forward in light of regulatory and litigation risk.

Any possession or control standards for digital assets need to take into account the technological reality of how these assets are managed, and satisfactory control should focus, for example, on whether the digital asset is properly cryptographically protected and that adequate cybersecurity practices, specific to DLT, are maintained. As the Committee (and the SEC) continues to think through these issues, the Chamber encourages it to be open-minded as to what can constitute possession or control, and for the government to foster a pro-growth environment when interpreting these and

[14] Multisignature, or "multisig" refers to a cryptographic functionality within public key infrastructure that requires more than one private key to complete a transaction. Many companies offer multisig wallets, where, for example, a 2-of-3 multisig wallet would require 2 out of 3 private keys, usually held separately, in order to authorize a transaction.

[15] *See* Reserves and Custody of Securities, 17 C.F.R. § 240.15c3-3 (2018); *see also* Custody of Funds or Securities of Clients by Investment Advisors, 17 C.F.R. § 275.206(4)-2 (2018); *and see also* SEC Division of Trading and Markets and FINRA Office of General Counsel, Joint Staff Statement on Broker-Dealer Custody of Digital Asset Securities (July 8, 2019), https://www.sec.gov/news/public-statement/joint-staff-statement-broker-dealer-custody-digital-asset-securities.

other issues that arise as blockchain technology develops.

e. Enhancement of Anti-money Laundering and Sanctions Compliance

Blockchains provide unprecedented ability to track and trace transactions historically, both by token and by wallet/account. Chamber members Chainalysis and CipherTrace are performing cutting-edge analytics with blockchain technology and helping governments and businesses (including financial institutions) to identify and mitigate risk and enable companies to alert law enforcement. Unlike cross-border wire transfers, blockchains perfectly preserve the provenance of financial transactions and do not suffer from data integrity issues.

Additionally, the Blockchain Alliance, co-founded by the Chamber of Digital Commerce in 2015, is an important medium for sharing information and education between the public and private sector to support law enforcement objectives. With more than 100 members, it continues to serve an important function. Lawmakers should take note of the proactive work being done by this industry to ensure that law enforcement is knowledgeable about the industry and the technology, and that it can achieve its objectives, thus creating an orderly functioning of the marketplace. This work is being utilized by multiple agencies within the government but can be further enhanced to reach and assist more participants.

The ability to trace transactions back through time is a technological advancement and has already provided a boon to law enforcement and its efforts to detect and prosecute criminals. Specifically with respect to Bank Secrecy Act ("BSA") and Office of Foreign Assets Control ("OFAC") compliance obligations, it can support Know Your Customer ("KYC") management in ways that ensure the characteristics of the customer, including beneficial ownership, are well-established on a blockchain. Further, blockchain-enabled KYC, customer due diligence ("CDD"), and transaction monitoring can enhance the Section 314 process – both under Section 314(a)[16] as well as 314(b)[17] (communications between institutions and law enforcement as well as among institutions, respectively) to ensure accurate, comprehensive data. It can also strengthen (real time) auditability of financial transactions between counterparties; facilitate lookbacks given the transparency and immutability of the ledger; and facilitate practical, technology-enabled KYC/CDD efforts, ongoing transaction monitoring, transaction tracking, and auditability/reporting.

Prudential regulators will need to develop publicly available guidance, with industry input, that permits financial institutions to adequately understand first, how they can interact with digital assets and, second, how to understand their customer and the associated transaction that is not so prohibitive that it requires forensics for transactions involving virtual currency that exceed current expectations involving fiat currency transactions and other financial instruments.

[16] 31 C.F.R. § 1010.520.
[17] 31 C.F.R. § 1010.540.

FinCEN and the prudential financial regulators will need to consider how to apply these AML and associated KYC requirements to regulated financial institutions engaging in virtual currency-related activities, and the Chamber urges them to engage with market participants in doing so.

A second area to be considered relates to sanctions compliance. The OFAC designation of two Iran-based individuals and their associated Bitcoin addresses raises a similar question in the context of OFAC sanctions.[18] Sanctions obligations are imposed more broadly than traditional notions of AML because they prohibit transactions or dealings in all property or "interests in" property of a designated person. It is through this extensive authority that OFAC has made clear that U.S. persons cannot transact or deal in the Venezuelan petro.[19]

However, the new guidance with respect to blocking property needs further consideration. For example, if a transaction involving a virtual currency indicates in its transaction history that the specific asset at one point in the past was held by a prohibited Iranian entity (or wallet), must that financial institution block the current transaction? Arguably they should not; however, businesses tend to (and should) take a very cautious approach when it comes to sanctions compliance. This approach, not possible with fiat currency because fiat cannot be traced as directly as some virtual currencies, nevertheless could restrict adoption of these product/service offerings by financial institutions. This and other consequences of OFAC's recent guidance need to be further explored to prevent unintended consequences in a digital environment.

The standards determined around these issues will have a large impact on fungibility in the token market, and ultimately the widespread adoption of tokens as a means of exchange or evidence of value or ownership. The Chamber and the government alike share the goal of preventing illicit finance and bad actors from accessing the financial system. We should strive to achieve these goals in a manner that does not impede the market's development or disincentivize the use of digital tokens and doing this requires industry and regulator cooperation. The Chamber recommends a forum like the Bank Secrecy Act Advisory Group (BSAAG) or similar arrangement to enable a thorough discussion and consideration of these issues.

Finally, technological developments have rendered traditional notions of KYC obsolete and ineffective. These developments can enable the creation of a digital KYC utility that would serve to verify identity of customers across financial institutions, rather than the current approach requiring financial institutions to obtain and verify the name, date of

[18] Press Release, 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.
[19] Exec.Order No. 13,827, 83 Fed. Reg. 12,469 (Mar. 21, 2018).

.

birth, physical address, and telephone number before onboarding a client. For many, these data points no longer authenticate that a customer is who they say they are. A KYC utility could greatly enhance compliance by financial institutions and permit them to elevate more swiftly potential indicia of fraudulent behaviors. As a result, we recommend permitting such a solution, which could require modification to current agency guidance.

f. Multiple State Statutes Addressing Smart Contracts

"Smart contracts" are computer code programmed to execute transactions based on pre-defined conditions that are particularly innovative when used in conjunction with blockchain technology. These can be simple, automated bill pay arrangements, for example, or much more complex transfer systems.[20] The Chamber promotes the use of smart contracts in conjunction with blockchain technology.

Unfortunately, the term "smart contracts" has created confusion as to whether they are in fact "legal contracts" valid under existing legal principles. The answer to this is clear - existing U.S. law, without further revision, supports the formation and enforceability of smart contracts under state law. The Electronic Signatures in Global and National Commerce Act ("ESIGN Act") and the Uniform Electronic Transactions Act ("UETA") provide sufficient legal basis for smart contracts executing terms of a legal contract.

Nevertheless, we are aware of at least nine states that have amended their electronic transaction statutes to specifically recognize "blockchain" and "smart contracts" in this context and four more have introduced legislation attempting to do so. While the Chamber greatly appreciates their pro-active work in promoting blockchain technology, it has unfortunately resulted in multiple states with differing definitions of these terms and different operative language, forming the beginning of a state-by-state patchwork of laws and creating compliance hurdles and confusion for U.S. companies, especially those involved in interstate or global transactions or operations. Additional state legislation, inconsistently drafted, will continue to confuse the marketplace and potentially hinder innovation.[21]

The Chamber recommends establishing a roundtable or briefing on this issue with legal and industry practitioners to fully vet the concerns and legal frameworks to confirm that smart contracts can be valid contracts under existing law and avoid the creation of a state-by-state patchwork of inconsistent laws.

---

[20] *See, e.g., Legal Guidelines for Smart Derivatives Contracts: Introduction*, INT'L SWAPS AND DERIVATIVES ASS'N (Jan. 2019), https://www.isda.org/a/MhgME/Legal-Guidelines-for-Smart-Derivatives-Contracts-Introduction.pdf.

[21] *See also, Guidance Note Regarding the Relation Between the Uniform Electronic Transactions Act and Federal ESIGN Act, Blockchain Technology and 'Smart Contracts'*, UNIF. LAW COMM'N (Mar. 11, 2019), https://www.uniformlaws.org/viewdocument/guidance-note-regarding-the-relatio?CommunityKey=2c04b76c-2b7d-4399-977e-d5876ba7e034&tab=librarydocuments. The Guidance Note provides an overview of the state UETA and federal ESIGN Act regarding blockchain-based smart contracts, concluding that state UETA provisions do not require amendment to enable use of blockchain and smart contracts in electronic transactions and may be detrimental.

g. Need for Accounting Standards

Currently, no authoritative literature exists under accounting principles generally accepted in the United States ("U.S. GAAP") or International Financial Reporting Standards ("IFRS") that specifically addresses accounting treatment for digital assets, including virtual currencies. Although use and acceptance of virtual currencies as a method of payment are not yet widespread globally, the increasing volume of transactions using virtual currencies necessitates the development of accounting guidance addressing the recognition, measurement, presentation, valuation, and disclosure of virtual currencies and related transactions.

Given this lack of clear guidance on accounting standards for virtual currencies, companies have developed a diversity of views on the appropriate accounting treatment. The absence of accounting standards for virtual currencies is a critical issue for companies seeking to invest and innovate in this technology frontier and may hold back economic growth in the United States. The Chamber, therefore, has formally requested that the Financial Accounting Standards Board ("FASB") to consider adding to its standard setting agenda a project to address accounting standards for virtual currencies[22] and we have encouraged the adoption of appropriate International Financial Reporting Standards ("IFRS").[23] That process remains ongoing.

h. Existing Tax Guidance Requires Additional Clarification and Consideration

In 2014, the Internal Revenue Service ("IRS") issued Notice 2014-21 that addressed the tax treatment of "convertible virtual currency" for U.S. tax purposes, finding that convertible virtual currency should be treated as property, not currency.[24] As property, a consumer will realize gain or loss upon a sale or exchange of virtual currency. This means that if a taxpayer uses virtual currency to buy a good or service, such as a cup of coffee, s/he would recognize gain or loss on the use of the virtual currency at that time and must track the original basis (cost) of the virtual currency used for the purchase as well as the ultimate purchase price. The Notice also confirmed that payments made using virtual currency are subject to certain information reporting requirements. For example, if an employee is paid in virtual currency, that amount would have to be

[22] *Agenda Request – Determining the Appropriate Recognition, Measurement, Presentation, and Disclosure for Digital Currencies and Related Transactions*, CHAMBER OF DIG. COMMERCE (June 8, 2017), https://digitalchamber.org/wp-content/uploads/2016/12/Digital-Currency-Agenda-Request_6.7.pdf.

[23] Comments to the IFRS Interpretation Committee Re: Tentative Agenda Decision – Holdings of Cryptocurrencies, CHAMBER OF DIG. COMMERCE (May 15, 2019), http://eifrs.ifrs.org/eifrs/comment_letters/528/528_25561_PaulBrignerChamberofDigitalCommerce_0_ChamberofDigitalCommercelettertoIFRSTADonHoldingsofCryptocurrencies.pdf.

[24] Press Release, Internal Revenue Serv., IRS Virtual Currency Guidance: Virtual Currency Is Treated as Property for U.S. Federal Tax Purposes; General Rules for Property Transactions Apply (Mar. 25, 2014), https://www.irs.gov/newsroom/irs-virtual-currency- guidance.

reported on the employee's Form W-2.

Despite receiving comments and an acknowledged need for additional guidance on its treatment of virtual currencies, the IRS has issued nothing further since 2014 – a situation criticized by the Treasury Inspector General for Tax Administration in a detailed 2016 report.[25] Surprisingly, without issuing further guidance for taxpayers to properly comply, the IRS announced it is now engaging in the beginnings of enforcement actions against over 10,000 taxpayers for failure to follow unclear guidance.[26] Typically agencies are encouraged to issue clear guidance so that affected persons can comply before engaging in enforcement – especially on such a widespread scale.

Comprehensive guidance addressing the tax treatment of virtual currencies and digital securities tokens is sorely needed. This guidance should consider the use of virtual currencies as both a payment mechanism and an investment asset class and should further take into account the rapidly evolving nature of the technology so as not to need frequent re-visiting as the technologies continue to develop. Moreover, the agency should acknowledge that virtual currencies can also be used as a form of payment and, as such, should not incur capital gain/loss treatment and thereby trigger income tax in those circumstances.

V. Conclusion

The Chamber appreciates the consideration of the Committee regarding key financial services principles and areas of friction highlighted in this letter. Ultimately, the U.S. government must publicly recognize the importance of blockchain and establish a framework for enabling and promoting its development. Without this, the United States will not achieve its full benefits and will fall behind other countries who are recognizing this extraordinary opportunity to become a leader in this technology. Through the Chamber's work,[27] we are engaging with stakeholders to address these matters and are pleased to serve as a continued resource.

* * *

[25] Press Release, Treasury Inspector Gen. for Tax Admin., Rising Use of Virtual Currencies Requires IRS to Take Additional Steps to Ensure Taxpayer Compliance (Nov. 8, 2016), https://www.treasury.gov/tigta/press/press_tigta-2016-34.htm.

[26] See Internal Revenue Service, *IRS Has Begun Sending Letters to Virtual Currency Owners Advising Them to Pay Back Taxes, File Amended Returns; Part of Agency's Larger Efforts*, July 26, 2019, https://www.irs.gov/newsroom/irs-has-begun-sending-letters-to-virtual-currency-owners-advising-them-to-pay-back-taxes-file-amended-returns-part-of-agencys-larger-efforts.

[27] A list of our initiatives and working groups is available online, https://digitalchamber.org/initiatives/.