International Franchise Association
52nd Annual Legal Symposium
May 5–7, 2019
Washington, DC

What is Blockchain and Why is it Critical to the Future of Your Domestic and International Business?

Joyce Mazero
Polsinelli
Dallas, Texas

Dan McAvoy
Nixon Peabody LLP
New York, New York

Richard Smith
Wiley Rein LLP
Washington, D.C.

TABLE OF CONTENTS

Page

What is Blockchain and Why is it Critical to the Future of Your Domestic and International Business?

Blockchain technology represents one of the most potentially disruptive innovations in history. With its ability to streamline transactions, especially in the financial sector, and to eliminate the need for intermediaries in favor of public, decentralized systems, blockchain offers an unprecedented opportunity to dramatically improve the efficiency and accuracy of information collection, distribution, and governance.

But as with all emerging technologies, blockchain technology is subject to being overly hyped. Those considering adopting the technology would be well-advised to ignore the somewhat irrational exuberance that has surrounded it over the past year and focus instead on whether the unique advantages to blockchain are suited to the application for which the technology is bring proposed.

This paper seeks to introduce blockchain to franchisors and franchisees. It begins by describing the technology from a practical perspective, offering the reader a non-technical, high-level understanding of what blockchain is and how it works. It then highlights the primary advantages and disadvantages of the use of blockchain systems before focusing specifically on smart contracts and other particularized applications that might be employed by franchisors or franchisees.

I. Blockchain 101

Blockchain is best known as the architecture upon which “cryptocurrencies” and “smart contracts” are based. At its core, blockchain can be defined as a distributed, consensus-based, immutable, chronological ledger of data that relies upon cryptography, game-theory, and computing inefficiencies to ensure its stability and security rather than management by a central authority. That is admittedly a mouthful, so we will take each of those phrases and describe them in turn.

A. Chronological Ledger

In the most simplistic sense, a blockchain is nothing more than a ledger, similar to any other ledger that might be maintained in any more traditional form whenever an accounting is required. Transactions are tracked in a blockchain and ordered chronologically just as they may be in any other ledger system.

One might imagine a home checkbook, where entries are recorded through time as checks are written and deposits are made. Each of those entries, when recorded, contribute to the ledger that sits in the hands of the account owner. As additional transactions are completed, additional entries are recorded within the ledger, and the account owner’s ledger grows. Because the account owner’s act of recording entries in the checkbook is ancillary to the transaction, the account owner may miss entries, or may even make errors in the ledger. The ledger is also susceptible to mischief at the hands of a prankster, or worse, who can simply come behind with a pencil and change the entries after they are made.

At the same time, the account owner's banking institution records transactions in a separate ledger, one created and maintained by the bank. The account owner may, depending on the institution, have rights or access to view the institution's ledger from time to time, but the owner has no ability to change the bank's ledger. Differences will undoubtedly exist between the account owner's ledger and the financial institution's ledger, and those differences may be attributable to error, fraud, mistake, or other causes.

At the end of the day, and in its most basic form, that is blockchain—a simple ledger of transactions evincing transfers of value from one account to another over time.[1]

B. **Distributed**

Unlike the ledgers used as exemplars above, one of the essential features of a blockchain is that it is distributed, meaning that every participant in the blockchain is able to access the same ledger, all at the same time with universal transparency. The private account holder maintains the exact same ledger as all other users, including, in the example above, the financial institution. And in contrast to the traditional, undistributed financial ledger, the blockchain ledger is maintained by all users, regardless of whether they have a vested interest in any particular account. Accordingly, there are no discrepancies between versions of the ledger held by different stakeholders, as there may be in a more traditional form, and no conflict between accountings.

With no conflicts between ledgers, there is no need for a central authority to resolve differences in accountings between, in the example above, the account holder and the financial institution, or even between account owners themselves. Everyone has access to the same ledger in real time.

Blockchains used for private application can be constructed with varying degrees of distribution. Those that allow full distribution to all participants across the entire blockchain are typically referred to as "permissionless" blockchains, whereas those that allow for more limited distribution typically are referred to as "permissioned." Clearly, in applications where privacy is at a premium, a permissioned blockchain is preferred. These types of blockchains often are built to support B2B or other similar exchanges where the primary incentive is to minimize the cost, time, and ease of sharing value or information.[2] But where transparency and trust are necessary, such as in cryptocurrency applications, permissionless blockchains are the norm and are often used for the explicit purpose of creating trust in what might otherwise be a trustless environment.

---

[1] Of course, blockchain can be used for much broader applications than merely providing evidence of transfer. Anything you can put on a spreadsheet, you can put into a blockchain.

[2] Take, for example, a blockchain created for the purpose of supply-chain management. One would expect such an application to be permissioned, so that only those in the supply chain can access and provide inputs, but not entirely distributed. Competing suppliers to a single retailer might be properly excluded from access to the other's inputs as to volume, pricing, and delivery. A permissioned blockchain offers a more nuanced and customizable approach to distribution.

C. **Immutable**

Blockchains are permanent. That is, once a transaction is entered into and accepted for inclusion in the blockchain, the record evidencing that transaction is unalterable. This is typically considered one of primary benefits of a blockchain and is a significant protection that blockchain offers over more traditional ledgers that can be exposed to post-transaction fraud.

Take the example used above of a traditional bank account ledger. That traditional form—whether maintained by the financial institution or by the account holder—is susceptible to being altered after the transaction is recorded. Those alterations may be made knowingly, or accidentally, and be the result of fraud, human error, or other motivation. Not so with transactions recorded in a blockchain. Every transaction, every exchange of value, is recorded permanently in an unalterable state.

The reason for this has to do with the mechanics of how the links in the chain are built. Adding new blocks to the chain—which, depending upon the blockchain architecture, may be referred to as "mining," "establishing proof," or "proof of work" —can be a complex process, and the methodology for doing so varies widely across platforms.[3] But at a high-level, it can be described as ensuring that new blocks are properly validated by a pre-defined process or algorithm before they are added permanently to the chain.

In the most well-known permissionless blockchain—bitcoin—the process occurs as follows: first, as new transactions are being suggested, but before they are recorded, they are distributed in draft to all computers in the network, essentially forming a pool of proposed transactions for potential inclusion in the blockchain. These records include information such as amounts, inputs, outputs, transaction identifiers, and other data. The transactions are digitally signed using asymmetric-key cryptography.

A subset of participants, known as "mining nodes," would then start working on the pool of proposed transactions. A "node" is simply a computer connected to the blockchain, and "mining nodes" are those computers that compete to do the work of creating blocks and adding them to the chain. That process requires the mining node to perform some measure of work before it can create a block and add it to the end of the chain.

In the bitcoin architecture, the mining node is required to successfully solve a mathematical puzzle before it can add a block to the chain. This gating feature protects the blockchain from would-be hackers. The puzzle takes substantial computing power to solve, and the cost associated with marshalling that power acts as an economic disincentive to would-be evil-doers.

To build a block, mining nodes select transactions and validate them, ensuring that the signatures to the transactions are correct and determining by reviewing the shared

[3] Indeed, traditional "mining," an essential feature of the bitcoin architecture, is only one of many means of verification and is now less commonly used in favor of other means of establishing proof.

ledger whether the sender has a balance sufficient to allow the transfer to be completed without overdrawing its account. The selected, validated transactions are placed into a block along with other data such as the digital signature of the current and prior blocks and transactional data. The mining node then competes with all other mining nodes to solve the mathematical puzzle. The winner inserts the puzzle's answer into the block as validation of its victory and earns the right to add that block to the chain. It transmits the new block to all nodes, effectively adding those transactions to the distributed ledger.

The content of each block impacts its digital signature. Accordingly, once a node solves the mathematical puzzle and inserts the answer into the block it has created, the content of that block is finalized, and its digital signature is permanently established. The next block in the chain will be required to include the predecessor's digital signature; thus, because any change in the content of the predecessor's content will alter the predecessor's digital signature and the next block will no longer have the right signature for it, any alteration will break the chain.

In a permissionless ecosystem,[4] because the participants are typically known, trusted, readily identifiable business partners who value speed and efficiency over erecting computational barriers to fraud, the mechanisms used to validate transactions and add them to the chain are typically streamlined and not dependent upon the mining or proof of work mechanisms featured by their permissioned cousins. Rather, these types of blockchains rely on other, less burdensome mechanisms (such as a validation of the hash from the prior block) as a marker for potential fraud. These mechanisms are less robust than in the permissioned ecosystem, but that is a deliberate choice, since (absent a hacking event) the participants are known.

Of course, the immutable feature of a blockchain is not always ideal. Just as valid transactions cannot be changed or voided once recorded, so too, fraudulent and erroneous transactions cannot be corrected or voided. The only allowable correction within a blockchain is to enter a new transaction that reverses the erroneous or fraudulent transaction. That may not be workable, especially in the case of fraud, where one party may be a participant in the fraud, may not consent to a reversing transaction, or may not be found.[5]

---

[4] The architecture of a blockchain and/or its participants is often referred to as an "ecosystem."

[5] A blockchain may also "fork," which is a process by which an architectural change is made within the rules (typically the software) of the particular blockchain that allows for alterations to be made either in the way in which a new block is recognized as valid, or the values associated with individual account holders. In some instances, the fork may result in a split of the blockchain into two strands, one operating under the new rules and one operating under the old. One well-known example of this occurred on the Ethereum blockchain in 2016, when Ethereum forked to return value to investors who had fallen victim to an embedded vulnerability. Following the fork, Ethereum was permanently split into Ethereum and Ethereum Classic.

D. **Consensus-Based**

There is no central authority like a financial institution to police a blockchain. Accordingly, blockchains contain their own policing mechanism to detect invalid blocks and remove them. That mechanism is simple: majority rules.

When a mining node solves the mathematical puzzle, as described above, it transmits its new block to the rest of the nodes to add to the end of the ledger. But with potentially millions of nodes on the network, that transmission can take time, and in the interim, another mining node may have solved a puzzle of its own and attempted to transmit a competing block of its own. When that happens, different blocks could be accepted by different subsets of nodes and different versions of the blockchain could temporarily exist. The temporary issue is resolved when the next block is mined and added to the chain. Because it contains the digital signature of the block it is built from, the chain containing that predecessor block is preferred, and the competing chain is "undone," with all transactions in the losing block unpacked and placed back into the pending queue.

The consensus mechanism not only replaces the need for a central policing authority, but also enhances the security of the blockchain.[6] Because consensus is required to add a new block to a chain, as the scale of a blockchain increases with more and more nodes, the ability of a hacker to illegitimately manufacture consensus declines. But as computing power improves, or as the number of nodes on a blockchain declines or the method of increasing the blocks improves, the possibility of fraud is enhanced.

The same basic tenets control within the permissioned ecosystem. That is, majority still rules, but without the expensive mining or proof-of-work requirement of the permissionless environment, the consensus mechanisms can be computationally streamlined and more efficient.

II. Overall Pros and Cons of Converting to Blockchain-Based Systems

A. **Key Advantages to Blockchain**

There are several key advantages of blockchain technology. First, blockchain networks can offer a level of security that is appealing in today's world of ever-present hacks and data breaches, even if human error remains a risk. This is due to blockchain's decentralized nature and the cryptography used in the digital signatures, which together make blockchain difficult to hack. Relatedly, the immutability of blockchain, and the fact

---

[6] Harkening back to James Surowiecki's 2004 book of the same name, in which he attempted to demonstrate from an economic sociological perspective that large groups can make superior decisions in behavioral economics and other fields, many in the blockchain field refer to this feature as the "Wisdom of the Crowd." See JAMES SUROWIECKI, THE WISDOM OF CROWDS: WHY THE MANY ARE SMARTER THAN THE FEW AND HOW COLLECTIVE WISDOM SHAPES BUSINESS, ECONOMIES, SOCIETIES, AND THE NATIONS (2004).

.

that no party can alter prior blocks, is often seen as a benefit. The immutability of blockchain helps prevent fraud and allows parties to rely on the integrity of the historical blockchain records.

The public, decentralized nature of blockchain is also a benefit for many use cases, and for cryptocurrencies in particular. All participants can access, view and add to the chain, and they are able to instantaneously review the ledger knowing that all other users are seeing the same thing. This creates transparency and allows for simple tracing of the records on a blockchain, which is one of the key benefits for supply chain management, as a user could easily access an audit trail that shows the entire journey of a product and all historical transactions. This can also help users verify authenticity and reduce fraud.

The lack of a central authority and intermediaries is also a benefit of many blockchains. There may be reduced costs and increased efficiencies in eliminating the need for such functionaries to validate transactions and control the ledger, though whether those benefits materialize will depend on how the blockchain network is structured.

B. **Issues to Be Considered or Resolved**

On the other hand, there are some significant hurdles to blockchain adoption and issues that need to be considered or resolved before implementing blockchain within a particular business or industry. Often there is tension between the benefits described above and the issues discussed in this section, and blockchain adopters will often need to make certain trade-offs to establish the structure that works best for each particular use case.

For example, blockchain's promise of heightened security may in some ways be *too* secure. Generally, users on cryptocurrency blockchain networks access the blockchain using a private key. The lack of a central authority means that there is no one to reset or give a user a "hint" to find his or her private key. If the key is lost or stolen, the assets are as well. For cryptocurrency blockchains, the value of decentralization is often paramount, and outweighs the disadvantages of having no way to replace or reset lost or stolen keys. However, for blockchains in many industries outside cryptocurrencies, such as supply chain management, the balance is likely to tip in the other direction.

The choice between a permissioned, private blockchain and a public, permissionless blockchain also has costs and benefits on either side. For a public blockchain, the increased number of users increases security, because every node has a copy of the blockchain, and the greater number means it would be that much more difficult to compromise. But that also diminishes privacy and typically means slower transactions.

Similarly, the benefits of blockchain's immutability mean that there is no way to go in and fix errors on the historical chain. There is no exception for crime, fraud, or simple mistakes. Again, as discussed above, this can be worked around, but not without some tradeoffs in terms of security. The security benefits derived from the mining process come

at a cost as well—it requires a great deal of computing power, meaning there are costs in terms of energy inputs and efficiency. A blockchain network without mining can allow for faster transactions and less energy (and expense). The more difficult the computing problems, the more secure the network will be.

III. Smart Contracts

A. What Are Smart Contracts

Blockchain's utility in a supply chain supporting a franchise system is noteworthy particularly for the use of smart contracts. "Smart contract" is a term from 20 years ago that was originally conceptualized and utilized by Nick Szabo in 1994[7] through the use of Ethereum.[8] He called them "smart" because digitally they were far more functional than inanimate paper-based ancestors. That is, a smart contract is viewed as a set of promises, specified in digital form, including protocols with which the parties perform on the promises.

Smart contracts are computer programs that assume the role of agreements where the terms of such agreement may be pre-programmed with the overall ability to self-enforce and self-execute the terms. A smart contract allows multiple anonymous parties to a given transaction to do business with one another. Smart contracts are autonomous and automatic, eliminating human interference and reducing the potential for human error and increasing a party's access to valuable and timely information.[9]

Computer code is the implementing contractual tool, replicating across multiple nodes of a blockchain benefitting from the security, performance, and immutability offered by the blockchain. A node is an individual device on a blockchain network that carries out a variety of tasks, including maintaining a copy of the blockchain, as well as validating

---

[7] Nick Szabo, *Smart Contracts: Building Blocks for Digital Market* (1996), http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html.

[8] ETHEREUM: BLOCKCHAIN APP PLATFORM, https://www.ethereum.org/ (last visited April 25, 2019). Ethereum is the most prominent public blockchain platform for smart contracts. Jeff Desjardins, *The Power of Smart Contracts on the Blockchain*, VISUAL CAPITALIST, (Oct. 24, 2017), http://www.visualcapitalist.com/smart-contracts-blockchain/. It is a programmable blockchain that allows users to create their own operations. Similar to other blockchains, Ethereum is a peer-to-peer network that utilizes nodes to maintain and update the database. In the Ethereum blockchain, smart contracts are executed through internal codes in a Contract Account. When a transaction is sent to a Contract Account, programs execute and users are able to create new smart contracts by deploying code to the Ethereum blockchain. *What is Ethereum?*, ETHEREUM, http://www.ethdocs.org/en/latest/introduction/what-is-ethereum.html (last visited April 25, 2019)

[9] Michael J. Casey & Pindar Wong, *Global Supply Chains Are About to Get Better, Thanks to Blockchain*, HARVARD BUSINESS REVIEW: INTERNATIONAL BUSINESS (Mar. 13, 2017), https://hbr.org/2017/03/global-supply-chains-are-about-to-get-better-thanks-to-blockchain.

transactions.[10] The node always independently validates transactions, irrespective of what the other nodes conclude.[11]

Given the state of technology today, the input parameters and execution steps of a smart contract will need to be specific and objective. This means the terms of the contract are written directly into lines of code through a series of "if-then" functions.[12] "If" a certain condition is met, "then" the smart contract proceeds to the next coded step in the transaction with the process repeating until all of the necessary if-then conditions are met.[13] The smart contract cannot proceed to the next step until a node confirms and validates that the current transaction satisfies the pending condition.[14]

Smart contracts save valuable time and resources by possessing the ability to be self-enforcing and therefore making policing the contract less burdensome. As adoption of blockchain increases, and more assets are tokenized or go "on chain," smart contracts will likely become increasingly complex and capable of handling more sophisticated transactions. Developers are starting to string together multiple transaction steps to form more complex smart contracts.

Smart contracts are transparent, allowing parties to see every detail of their transactions in an instant. Smart contracts are best suited to execute automatically two types of transactions found in many contracts. These transactions are (i) ensuring the payment of funds upon triggering certain events, and (ii) imposing financial penalties if certain objective conditions are not satisfied.

Smart contracts can also eliminate the so-called procure-to-pay gaps. When a product arrives and is scanned at a warehouse, a smart contract can immediately trigger requests for the required approvals and, once obtained, immediately transfer funds from buyer to seller. Sellers can get paid faster and no longer need to engage in significant collection efforts and buyers can reduce their accounts payable costs. This can positively impact working capital requirements and simplify finance operations for both parties.

On the enforcement side, a smart contract can be programmed to shut off access to an internet-connected asset if a payment is not received. Access to certain content can also be automatically denied if payment is not received. Accordingly, smart contracts are best used for integrating payment with blockchain technology as they arrange payments automatically at the same time as deliveries occur, making the transaction and payment

---

[10] LISK, https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/nodes (last visited April 25, 2019).

[11] *Id.*

[12] Tsui S. Ng, *Blockchain and Beyond: Smart Contracts*, AM. BAR ASS'N: BUS. LAW TODAY (Sept. 19, 2018), https://www.americanbar.org/groups/business_law/publications/blt/2017/09/09_ng.html.

[13] *Id.*

[14] *Id.*

more efficient, transparent, and automated, thereby making it possible to self-monitor terms of agreements, certify transactions, and facilitate or evidence certain transfers of payments.

Franchisors, franchisees, and suppliers would surely appreciate a more transparent and reliable supply chain because finding, negotiating, and enforcing supply contracts can fail to meet even the most humble of expectations, resulting in material harm to the franchise relationship.

Before a compiled smart contract can be executed in a blockchain, parties have to pay a transaction fee for the contract to be added to the chain. In the Ethereum blockchain, contracts are executed on Ethereum Virtual Machine (EVM) and this payment is made by crypto currency known as "gas." The more complex the contract, the more "gas" is required. This is an important gatekeeper.[15]

Companies across various industries have already begun to utilize smart contracts. An Ethereum project called Provenance conducted a six-month pilot that used blockchain technology and smart contracts to successfully track "responsibly-caught fish and key social claims down the chain to export."[16] Projects such as Provenance demonstrate blockchain's success in enhancing visibility in the global supply chain.

French multinational insurance firm AXA is the first major insurance group to utilize smart contracts to offer flight delay insurance.[17] When a customer buys the insurance through the "fizzy" platform, the transaction is recorded on the Ethereum blockchain, thereby connected to global air traffic databases and if a flight is delayed, compensation is triggered automatically.[18]

Slock.It utilizes smart contracts to change the sharing economy through automating payments, sharing, and rentals.[19] Share&Charge uses Slock.It's smart contracts to automate the payment process for renting electric vehicle charging stations.[20]

Smart contracts are also being used for buying and selling real estate. Propy was one of the first companies to do so when a customer purchased an apartment in the

---

[15] *What is the "Gas" in Ethereum?* CRYPTOCOMPARE (July 30, 2015), https://www.cryptocompare.com/coins/guides/what-is-the-gas-in-ethereum/.

[16] *From Shore to Plate: Tracking Tuna on the Blockchain*, PROVENANCE (July 15, 2016), https://www.provenance.org/tracking-tuna-on-the-blockchain.

[17] *AXA Goes Blockchain With Fizzy*, AXA, (Sept. 13, 2017), https://group.axa.com/en/newsroom/news/axa-goes-blockchain-with-fizzy.

[18] *Id.*

[19] *5 Companies Already Brilliantly Using Smart Contracts*, MEDIUM (Mar. 7, 2018), https://medium.com/polyswarm/5-companies-already-brilliantly-using-smart-contracts-ac49f3d5c431.

[20] *Id.*

Ukraine for $60,000.[21] Both parties to the transaction participated in the smart contract, which ensured specific steps were taken to foster fair and legal play despite the challenges of the "across-borders" real estate marketplace.[22]

Wal-Mart is working with IBM and Tsinghua University in Beijing to follow the movement of pork in China within a blockchain. Mining giant BHP is using the technology to track mineral analysis done by outside vendors. Everledger has uploaded identifying data on a million diamonds to a blockchain ledger system to build quality assurance.[23]

B. **Law Applying to Smart Contracts**

There are no federal laws on contracts, and interpretation is dependent on state laws and certain uniform laws and codes that are applied somewhat uniformly across the country. State laws can differ. To have an effective contract, it needs to be legally binding and enforceable in a court. Traditionally courts look to see whether the traditional concepts of offer, acceptance, and consideration are satisfied.[24]

Certain contracts must be in writing and additional formalities are required to be compliant with the U.C.C. and Statute of Frauds.[25] But not all contracts need to be in writing in order to be enforceable. Code-only contracts can be enforceable under various laws governing such contracts such as the UETA—Uniform Electronic Transactions Act,[26] which is accepted in about 47 states and provides, with limited exceptions, that electronic records (including records created by computer programs) and electronic signatures using public key encryption technology are given the same legal effect as written counterparts. UETA goes as far as recognizing electronic agents, which is defined as "a computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part, without review or action by an individual." Under UETA an electronic agent is "capable within the parameters of its programming, of initiating, responding[,] or interacting with other parties or their electronic agents once it has been activated by a party, without further attention of that party," arguably also a recognition of smart contracts.[27]

In a similar manner, the Electronic Signatures Recording Act (E-Sign Act)[28] recognizes the validity of electronic signatures and electronic records in interstate commerce. It also provides that a contract or other record may not be denied legal effect solely because of its formation, creation, or delivery through one or more electronic

---

21 *Id.*

22 *Id.*

23 Casey & Wong, *supra* note 9.

24 Restatement (Second) of Contracts § 1 (1981).

25 U.C.C. § 2-201 (2019).

26 Unif. Elec. Transactions Act §§ 2(5)-2(6) (1999).

27 *Id.*

28 15 U.S.C. § 7001(h) (2019); 15 U.S.C. § 7006(3) (2019).

agents so long as the action of any such electronic agent is legally attributable to the person to be bound.[29]

Some states are expanding the enforceability of smart contracts. In March 2018, Tennessee enacted a new law that recognizes smart contracts and blockchain signatures as legally binding.[30] Tennessee now joins Arizona, Colorado, Delaware, Florida, Nebraska, New York, Nevada, Vermont, and Wyoming[31] in expanding the enforceability of smart contracts.[32]

Senate Bill 1662 acknowledged a signature secured through a blockchain as an electronic signature.[33] It also acknowledged contracts secured through a blockchain as an electronic record.[34] As a result, the electronic signatures and contracts secured through a blockchain have the same legal standing as a traditional contract and signature.[35] Senate Bill 1662 also states "no contract relating to a transaction shall be denied legal effect, validity, or enforceability solely because that contract contains a smart contract term."[36]

Based on all of this, it appears reasonable to believe that courts will look at the smart contract and text contract as a unified contract.[37]

C. Code-Only Versus Complement/Supplement to Traditional Contract

Code can be either the sole manifestation of an agreement between the parties, or a complement to an otherwise traditional text-based contract, and execute certain provisions such as transferring funds. Smart contracts that are created and deployed without enforceable text-based contracts are known as "code-only" contracts in which the contract between the parties is reduced to executable code. Smart contracts used as

---

29 *Id.*

30 Mark Satter, *Blockchain, Smart Contracts Now Legally Binding in Tennessee*, STATESCOOP (Mar. 26, 2018), https://statescoop.com/blockchain-smart-contracts-now-legally-binding-in-tennessee.

31 *Id.*

32 Jonathan Beckham, Alicia Rosenbaum, Marla Sendra, *Smart Contracts Lead the Way to Blockchain Implementation*, THOMAS REUTERS WESTLAW (Mar. 12, 2018), https://www.gtlaw.com/-/media/files/insights/published-articles/2018/03/jonathan-beckhamalicia-rosenbaummaria-sendrathomson-reuters-westlawsmart-contracts-lead-the-way-to-b.pdf. *See also* TENN. CODE. ANN. § 47-10-202 (2018).

33 *Id.*

34 *Id.*

35 *Id.*

36 *Id.*

37 Benjamin Van Adrichem, *Enforceability of Smart Contracts Under the Statute of Frauds*, COL. SCIENCE AND TECHNOLOGY L. REV. (Jan. 31, 2018), http://stlr.org/2018/01/31/enforceability-of-smart-contracts-under-the-statute-of-frauds/?cn-reloaded=1.

vehicles to effectuate certain provisions of traditional text-based contracts are known as "ancillary smart contracts."

As noted above, courts normally look to see whether the traditional concepts of offer, acceptance, and consideration are satisfied. These requirements can be satisfied in a text-based contract and in a smart contract context. Typically, the written contract would be embedded into the smart contract. For example, if flight insurance was purchased to insure against delays, the written contract would determine what certain terms mean (such as "delay") and what certain actions must be taken (such as what premium to pay), and then the actual payment itself can take place via smart contract. The payout would be automatic once the pre-determined delay occurs.

While this is being tested, we are years away from smart contracts being able to be used for subjective decisions, such as whether a condition of best effort or reasonable efforts by a party has been met, or whether an indemnity provision has been triggered and payment should be made.

D. Possible Disruptions in the Use of Smart Contracts

1. Expert Needed to Write and Translate Code

It will be necessary to rely upon and use a trusted technical expert to write and translate computer code so as to capture the parties' agreement in code or confirm that code written by a third party is accurate. This is not done by a lawyer or other non-programmer who would not be able to understand the most basic smart contract.

The text contract could prompt what data to enter into the smart contract, but franchisors and suppliers will still need an expert to test and confirm that the underlying code will actually perform its functions and there are no errors or additional protocols needed. If there is no template, a programmer expert will be needed to create the code itself. This requires more than giving the programmer a legal document to borrow from, and a term sheet on the smart contract may be needed. This means there may be a need for contracts with third-party programming services and insurance may need to be obtained to protect contracting third parties from programmer mistakes (or in instances where the code does not perform as expected). It will also be important to have the parties confirm that the code is written in an acceptable form.

The inability of contracting parties to understand smart contract code will not be a hindrance to parties entering into ancillary code agreements. This is because for many basic functions, text templates can be created and used to indicate what the parameters need to be in order to understand how those parameters will be executed. For example, assume a smart contract function is to extract a late fee from a counter-party's wallet if a defined payment is not received by a specified date. The text template could prompt the parties to enter the amount of the expected payment, the due date, and amount of the late fee. However, a party may want to confirm that the computer code actually would perform the functions specified in the text and that there are no additional conditions or

parameters—especially where the template disclaims any liability arising from accuracy of the code. This review will require a trusted third party with programming expertise.

Where templates do not exist and new code must be developed, there will be a need for the parties to communicate the intent of their agreement to a programmer. Handing a programmer a copy of the legal agreement is inefficient as it would require the programmer to try and decipher a legal document. Parties relying on ancillary smart contracts should also have a separate term sheet of functionality that the smart contract should be able to perform and that can be provided to the programmer.

The parties should also obtain written representations from the programmer that the computer code performs as intended. The result is that for customized arrangements that do not rely on an existing template where new code is to be developed, the parties should enter into a written agreement with the programmer not unlike contracts that the parties would enter into with other service providers of EDI services.

Insurance companies should also create policies to protect the parties from the risk that the computer code does not perform the functions specified in the text of an agreement. Although the parties would also want to review or have third parties review the code, insurance can provide additional protections given that the parties might miss errors when reviewing code. The insurance company would likely conduct its own code audit before agreeing to insure the code.

2. Enforcement of Consumer Smart Contracts

There may be some difficulty with enforcing smart contracts vis-à-vis consumers if proper notice is not given to the consumer. Courts are often hesitant to enforce smart contracts where the consumer was not also provided with an underlying text agreement that included the complete terms.[38]

3. Need for Court-Appointed Experts to Decipher

There may need to be a group of court-appointed experts to help courts decipher smart contracts. Finally, as the validity or performance of smart contracts become increasingly adjudicated, the courts may need a system of court-appointed experts to help them decipher the meaning and intent of the code. Federal and state courts have the authority to retain experts, but rarely exercise authority.[39] This will need to increase.

---

[38] *Nicosia v. Amazon.com Inc.*, 834 F.3d 220 (2d Cir. 2016)

[39] Charles Alan Wright & Arthur R. Miller, *Federal Practice and Procedure*, § 6304 (3d ed. supp. 2011) ("In fact, the exercise of Rule 706 powers is rare under virtually any circumstances. This is, at least in part, owing to the fact that appointing an expert witness increases the burdens of the judge, increases the costs to the parties, and interferes with the adversarial control over the presentation of evidence."); Stephanie Domitrovich, Mara L. Merino & James T. Richardson, *State Trial Judge Use of Court Appointed Experts: Survey Results and Comparisons*, 50 Jurimetrics J. 371, 373–74 (2010).

4. Reliance on Off-Chain Resources

To implement smart contract protocol, reliance on off-chain resources (such as weather information) if performance is based on fluctuating data (e.g., weather dependent) is needed. For example, assume a crop insurance contract is programmed to transfer value to an insured party if the temperature falls below 32 degrees at any point. Three issues are presented. First, smart contacts do not have the ability to pull data from an agreed source. The smart contract will need to receive the temperature data from an agreed source by having it pushed to the smart contract by the off-chain resource. Second, if the data is constantly in flux and since the code is replicated across multiple nodes in the network, different nodes may receive different information even if just a few seconds apart. Third, there will need to be a way to have temperatures across the nodes be validated.

This can be handled by oracles.[40] In this example, the oracle would monitor the daily temperature, determine that the freezing event has occurred, and then push that information to the smart contract. Although oracles present a solution for accessing off-chain resources, this does add another layer of involvement and another point of potential failure. Consider that an oracle might experience a system error and be unable to push out the necessary information, provide erroneous data, or cease doing business. For the same reasons as discussed concerning a programmer, it will be advisable to have a service contract with the oracle and insurance covering those services as well.

5. Conflicts Between Smart Contract and Written Contract

What happens when there is a conflict between the code or smart contract and the written or ancillary contract? While a court would likely look at the text and code as a unified single agreement, issues could arise when the consistency between the traditional text agreement and the code do not align. In the crop insurance example above, the text specifies that the insurance payout will be made if the temperature falls below 32 degrees, while the smart contract triggers the payment if the temperature is equal to or below 32 degrees. The written contract will need to anticipate conflicts by providing which contract prevails and providing for a deemed amendment. The parameters that go into resolving a conflict should also be spelled out in the written contract. For example, whether the code should be treated as a mutually agreed amendment to the written agreement or whether the text of the agreement should prevail.

One approach would be for the parties to use a text-based contract where the parameters that trigger the smart contract execution are visible in the text but also populate the smart contract. In the example, “less than 32 degrees” would not only be seen in the text but would also create a parameter in the smart contract, thereby minimizing the chances of inconsistency.

---

[40] Bisola Asolo, *Blockchain Oracles Explained,* MYCRYPTOPEDIA (Dec. 19, 2018), https://www.mycryptopedia.com/blockchain-oracles-explained/.

6. Ad Hoc Business Actions

What happens when a business person wants to make a subjective decision such as deferring or waiving a condition, or extending the duration or effect of a term which is not provided for in the smart contract? Acting on an ad hoc basis is not an option in a smart contract. This means making decisions like accepting partial performance because of a business decision, or excusing a late fee, would not be easy.

For example, if a customer is late with a payment the vendor can make a real time decision to preserve a customer relationship by waiving the late fee on the payment. If this was reduced to a smart contract, the option not to enforce the agreement on an ad hoc basis likely would not exist. A late payment will result in the automatic extraction of the late fee from the customer account or suspension of access to a software program or an internet-connected device—whatever the smart contract is programmed to do. Therefore, the automated execution provided for by a smart contract would not align with the manner in which many businesses operate in the real world.

7. Complications of Amending or Terminating

There is no simple way to amend or terminate a smart contract. Given that the blockchain is immutable, modifying a smart contract is more complicated than modifying standard software code that does not reside in a blockchain. Flexibility does not lend itself to smart contracts, and amending a smart contract may cause a higher transaction cost to be incurred and increase the likelihood that errors will occur.

Similar challenges exist with respect to terminating a smart contract. If a party discovers an error in an agreement that gives a counterparty more rights than intended, or concludes that fulfilling the obligations would be far more costly than it had expected, a party can engage in or threaten so-called “efficient breach” in a text-based contract (i.e., knowingly breach a contract and paying the resulting damages if it determines that the cost to perform is greater than the damages it would owe). By ceasing performance or threatening to take that step, a party may bring the counter-party back to the table to negotiate an amicable resolution. In a code-only contract, if one party decides not to perform or threatens to withhold performance, there are no “self-help” remedies to get them back to the negotiating table.

E. Risk in Enforcement of Smart Contracts

Theoretically, execution in a blockchain network eliminates the need for intermediary parties to confirm the transaction, leading to self-executing contractual provisions. This also raises significant legal questions in relation to applicable regulation and, therefore, the legal enforceability of smart contracts.

Since smart contracts are prewritten computer codes, how their use works with the traditional “contract” definition and laws of contracts is an open question. This is particularly true where smart contracts are built on permission-less blockchains, which allow for no central controlling authority. Since the point of permission-less blockchains is

to decentralize authority, they might not provide for an arbitrator to resolve any disputes that arise over a contract that is executed automatically. It also remains unclear whether basic contract legal elements, such as capacity and apparent or ostensible authority, would apply. Also at issue is how concepts of offer and acceptance, certainty, and consideration work in this environment. For these reasons, in a business environment supporting a franchise system, the parties would most likely operate in a deliberately permission-only blockchain.

Parties will need to ensure that smart contracts include a dispute resolution provision to reduce uncertainty and provide for a mechanism in the event of a dispute.

1. **Jurisdiction**

Currently, there is no comprehensive or even nascent regulatory framework overseeing blockchain transactions. The non-existent regulatory guidance, coupled with uncertainty over jurisdiction and very few and inconsistent court decisions on jurisdiction, creates an environment among the blockchain user community that feels generally free of law and therefore free of legal enforcement.[41] In this context, users naturally escape any sense of legal norms as the infrastructure itself does not fall under any form of jurisdiction.[42]

For several reasons, blockchain and smart contracts in the supply chain context can be structured in a way to address enforcement and dispute resolution terms. In many blockchain and crypto transactions, the parties are anonymous, which has led to discussion about the enforceability of smart contract blockchain transactions. But smart contract blockchain transactions in supply chains would not be anonymous and would exist in a permissioned network. This removes some of the major issues surrounding jurisdiction and enforceability, and this application of smart contracts and blockchain technology would have the ability to be subject to more typical and traditional jurisdiction and contract law principles. That is, much of the current writing on the concerns over jurisdiction and enforcement are not applicable to properly structured blockchain uses in franchising or a supply chain.

Nevertheless, some questions and issues surrounding enforceability and jurisdiction issues, specifically subject matter jurisdiction, diversity jurisdiction, personal

---

[41] Wulf A. Kaal & Craig Calcaterra, *Blockchain Technology's Distributed Jurisdiction,* WULFKAAL.COM,https://wulfkaal-com.cdn.ampproject.org/v/s/wulfkaal.com/2017/06/20/blockchain-technologys-distributed-jurisdiction/amp/?amp_js_v=0.1&usqp=mq331AQGCAEYASgB#origin=https%3A%2F%2Fwww.google.com&prerenderSize=1&visibilityState=prerender&paddingTop=54&p2r=0&horizontalScrolling=0&csi=1&aoh=15249422445332&viewerUrl=https%3A%2F%2Fwww.google.com%2Famp%2Fs%2Fwulfkaal.com%2F2017%2F06%2F20%2Fblockchain-technologys-distributed-jurisdiction%2Famp%2F&history=1&storage=1&cid=1&cap=swipe%2CnavigateTo%2Ccid%2Cfragment%2CreplaceUrl (last visited April 25, 2019).

[42] *Id.*

jurisdiction, and federal question jurisdiction are present with smart contracts, such as physical presence, domicile/place of business, minimum contacts, and consent. Similarly, enforceability and remedies for breaches of smart contracts is an unanswered and complicated question.

A blockchain has the ability to cross jurisdictional boundaries as the nodes on a blockchain can be located anywhere in the world. This can pose a number of complex jurisdictional issues, which require careful consideration in relation to the relevant contractual relationships. Because smart contracts are prewritten computer codes, how their use aligns with the traditional "contract" definition and laws of contracts is important to address at least in the ancillary contract. The same is the case for basic contract legal elements, such as capacity and apparent or ostensible authority, as well as principles of title.

Identifying the appropriate governing law is essential and, in a decentralized environment, it may again be difficult to identify the applicable rules. Every transaction could potentially fall under the jurisdiction(s) of the location of each and every node in the network. This could result in the blockchain needing to be compliant with an unwieldy number of legal and regulatory regimes. In the event a fraudulent or erroneous transaction is made, pinpointing its location within the blockchain would be challenging.

Accordingly, the smart contract in franchising or a supply chain is likely not best utilized alone as a code-only contract. Rather, as an ancillary contract, the smart contract should have the written contract imbedded into it, facilitating the inclusion of an exclusive governing law and jurisdiction clause, which is essential to ensure that a customer has legal certainty as to the applicable law to determine the rights and obligations of the parties to the agreement and in which court disputes will be heard.

Recently the United States District Court for the Southern District of California denied plaintiff Founder Starcoin, Inc.'s motion for preliminary injunction against defendant Launch Labs, Inc.[43] Although the court did not explicitly state why it had jurisdiction, Founder Starcoin, Inc. argued in its complaint that the United States District Court for the Southern District of California had original jurisdiction under 18 U.S.C. § 1836(c) and 28 U.S.C. § 1331 and supplemental jurisdiction under 28 U.S.C. § 1367(a) because the claims were for breach of contract, trade secret misappropriation, intentional interference with prospective economic advantage, and unfair competition.[44] Founder Starcoin, Inc. also argued venue was proper under 28 U.S.C. § 1391(b)(2) because a substantial part of the event that gave rise to the claims occurred in that district and a substantial part of property at issue is located in that district.[45]

---

[43] *Founder Starcoin, Inc. v. Launch Labs, Inc.*, No. 18-CV-972 JLS (MDD), 2018 WL 3343790 at *15 (S.D. Cal. July 8, 2018).

[44] *Id.*

[45] *Id.*

2. Dispute Resolution

The issues and questions and non-traditional nature of smart contract transactions make a compelling case for customized dispute resolution mechanisms. Since smart contracts are coded for and contemplate potential breaches, it appears that a substantial number of enforcement situations would be contemplated and dealt with through coding for a code-only smart contract or through an embedded traditional contract where the smart contract complements the traditional contract. Using smart contracts as a complement or supplement to a traditional contract is additionally attractive because only the traditional written contract can anticipate the need for subjectivity inherent in almost every business relationship including mistakes, intentions of the parties, and assessing standards of decision-making such as standards of reasonableness, best efforts, and materiality.

One approach to dispute resolution in some blockchains receiving attention is "Distributed Jurisdiction."[46] Here, a system with third-parties and pre-set streamlined rules are applied to resolve disputes.[47]

---

[46] Kaal & Calcaterra, *see supra* note 41.

[47] For example, in the Aragon Network, if a user wants to dispute the execution of a contract, the user must post a bond and submit a brief of their argument (Kaal & Calcaterra, *see supra* note 35). Next, five judges who have also posted a bond are randomly selected from all of the users of the network. After the judges read the briefs, they issue their judgments and a majority decision is needed to determine the dispute's outcome. Judges are rewarded monetarily if they voted with the majority and are punished with the loss of their bond if they did not. In addition, the Aragon Network allows two appeals. If a party disagrees with the initial outcome, the party may appeal by posting a larger bond with their brief. A prediction market is then opened where any user may post a bond and become a judge. Again, briefs are read and all judges issue their judgments with a majority needed to determine the result. Rewards and punishments are then given to judges based on the results. Lastly, after posting a larger bond, a user may make a final appeal to a panel of nine "supreme court" judges who are the most successful judges in the Aragon Network. This is the only form of dispute resolution allowed on the Aragon Network and users are not allowed to opt into different dispute resolution mechanisms. Another example is OpenBazaar. Although OpenBazaar does not use a blockchain, it is a distributed network where all of the parties and transactions are anonymous. As a result of these core elements, OpenBazaar is an appropriate program to compare dispute resolution mechanisms. OpenBazaar is a crypto currency trading platform that uses a "Distributor Jurisdiction" type of dispute resolution mechanism predicated on use of notaries that have different skill sets and permit the parties to a claim to choose notaries, encouraging notaries to continue developing expertise in legal areas. From the beginning of a transaction, users are able to choose whether to involve the notary. If the users do not choose to use the notary, then there are no transaction fees. However, a transaction without notaries increases a user's risk because no arbitration is possible. If the users do choose to use the notary, then the parties can agree to choose a particular pool of notaries with a certain expertise before the contract is signed. The notary's primary job in OpenBazaar is to electronically verify that both parties signed the contract and there are available funds in escrow. Next, after confirming that both parties agree that the terms of the contract have been fulfilled, the notary releases the funds from escrow and sends it

F. **The "Key " — Authenticity and Auditing**

Information provided to the blockchain can only be accepted if it is authenticated. Authentication is provided in the form of an unforgettable digital signature. It is like a physical signature but more secure—allowing someone to prove their identity without enabling someone else to impersonate them in the future. The digital key is required for each interaction. The owner must cryptographically prove ownership of the account and there is no way for anyone else to interfere in this requirement being met. This creates a balance among all participants without regard for security levels of the past.

Because each individual operation or interaction is recorded and archived, auditing is achieved by participating in the blockchain. It allows the participant to replay the input and operations in order to build a framework or model of the transactions. Combined with the authenticity of the participants created for every interaction, strong data systems are built that are not vulnerable to human interference.

G. **Supplier/Vendor Agreements**

Blockchain technology can also transform the traditional, inefficient shipping protocol which is inherent in many systems into a process permitting standardization and transparency, allowing senders and recipients to track their orders in real time. One of the primary documents used in the shipping process is the "Bill of Lading," which specifies the party responsible for a particular obligation in the shipping process at any given point from the time the goods leave the place of origin to the delivery destination.

By incorporating blockchain technology into the shipping process, a record of the Bill of Lading and the shipment's transport and transfer history is maintained and transparently available. When a shipping company signs for a particular shipment of goods, thereby accepting that shipment for future transport, that signature will be recorded to the blockchain. The blockchain possesses the critical transparency necessary for maximized efficiency making that record available anywhere with an appropriate timestamp. The recipient of the shipment can effectively see the information about which company was responsible for transporting the goods at the moment and exactly where they last signed for it.[48]

Shipping agreements are often complex as they may be bundled together or even subcontracted in such a way that the company responsible for the shipment lacks knowledge—including anything about the entity who paid for the shipment or where the target destination lies. Because of the transparency protocol, parties have the ability to see each completed block in the whole chain to successfully identify what issue occurred and how to find the appropriate solution.

---

to the vendor. Lastly, if either party is not satisfied with the transaction, then the notary serves as an arbiter in the dispute.

[48] *Blockchain: The Solution for Transparency in Product Supply Chains*, PROVENANCE (Nov. 21, 2015), https://www.provenance.org/whitepaper.

Blockchain technology has the potential to aid in certification. Currently, a company must place implicit trust in the shipping company to deliver goods safely. The blockchain essentially presents an automated service for the certification of the delivery itself, tamper protection, and certification of the authenticity of a given shipment's contents.

However, the creation, exchange, and use of material things has many potential negative consequences such as environmental damage, exploitative extraction, unsafe work conditions, forgery, and the huge amounts of valuable material wasted at the end of product life.[49] Consider the 50,000 tons of beef found to contain horse DNA.[50]

Provenance is a prototype that uses blockchain technology to enable secure traceability of certifications and other salient information in supply chains. Provenance enables every physical product to come with a digital passport that proves authenticity and origin, creating an auditable record of the journey behind all physical products. The potential benefits for businesses, as well as for society and the environment, are hard to overstate—preventing the sale of fake goods, as well as the problem of double spending on certifications present in current systems.[51]

Guaranteeing the integrity of certificates is a costly process that, despite laborious audits, still struggles to assure validity of the claims being made. Worldwide expansions of certification schemes in regions with levels of higher corruption further endanger credibility.

Blockchain technology operates by consensus, which is a defined convention for how to execute and administer the business logic (e.g., to update the stock of a certain good). The magic of the blockchain and its surrounding incentive structure is that end users can then unambiguously discover the state of the system (e.g., current level of stock or origin of a particular certificate) not from a single particular authority, but rather by independently applying common rules and publishing data openly.[52]

Programs that follow after certification can be used for each production facility including (i) a certification of production capacity for the production of goods; (ii) a description of goods, including a description of the output with additional tags to identify specific attributes like fair trade, fair labor, and organic; and (iii) a production accounting—the registration of created products up to maximum annual capacity, as well as the registration of the sales

The chain of custody records can prevent fraud including counterfeit goods by proving the origins and ownership history of a physical product. For example, a luxury

---

49 *Id*.

50 *Horsemeat Scandal: Dutch Uncover Large-Scale Meat Fraud*, BBC (Apr. 10, 2013), https://www.bbc.com/news/world-europe-22098763.

51 *PROVENANCE*, *see supra* note 48.

52 *Id.*

watchmaker can prove that a watch is authentic reflecting age, repairs, insurance, and valuation via a log on the blockchain that follows the product.[53]

Other examples of blockchain use in the supply chain include Starbucks tracking beans to cup, Alibaba tracking food safety, and Wal-Mart identifying and removing recalled foods. Wal-Mart has also utilized blockchain technology to drastically reduce food tracking times.[54] With the use of blockchain, it now only takes seconds to locate the tracking information when it took days of searching through paperwork before.[55]

Recognized as the "leading enterprise blockchain provider,"[56] IBM's cloud-based IBM Blockchain Platform is helping companies across various industries such as banking, finance, insurance, consumer goods, government, health care, automotive, travel and transportation, and media and entertainment to enhance their visibility and add value to their businesses.[57] In addition, the IBM Blockchain Platform allows users to build on a complete blockchain platform as well as develop and operate the blockchain, all while counting on the highest level of blockchain security available, IBM Z, to protect against insider attacks and malware.[58] Furthermore, IBM and Maersk, a Danish global leader in container logistics, have announced plans to create a joint venture that will use blockchain technology to provide more secure and efficient methods for global trade.[59] After the regulatory approvals are granted, the joint venture's goal "will be to offer a jointly developed 'global trade digitization' platform built on open standards and designed for use by the entire global shipping ecosystem."[60]

---

53 *Id.*

54 John McMahon, *Wal-Mart Leading the Way for Blockchain Based Tracking Systems*, NEWSBTC, (June 6, 2018), https://www.newsbtc.com/2018/06/06/walmart-leading-way-blockchain-based-tracking-systems/.

55 *Id.*

56 Roger Aitken, *IBM Forges Global Joint Venture with Maersk Applying Blockchain to 'Digitize' Global Trade*, FORBES (Jan.16, 2018), https://www.forbes.com/sites/rogeraitken/2018/01/16/ibm-forges-global-joint-venture-with-maersk-applying-blockchain-to-digitize-global-trade/#d5ad178547e8.

57 IBM, https://www.ibm.com/blockchain/solutions (last visited April 25, 2019).

58 *Id.* For additional information on IBM's blockchain services, *see* https://www-01.ibm.com/software/htp/tpf/tpfug/tgf18/TPFUG_2018_MAIN_BlockchainIntro.pdf.

59 Aitken, *see supra* note 56.

60 *Id.*

IV. Capital Raising/Incentive Programs/Legal Constructs

A. Digital Assets

A digital asset is a smart contract, which normally would be blockchain-enabled, representing something of value. This thing of value can be any number of types of assets. A few of the most common types of digital assets include:

- Security tokens, which either mimic or represent an interest in traditional securities, such as stock-like tokens that entitle a holder to an ownership interest in an enterprise with voting and dividend rights, or debt-like tokens that give the holder the right to be repaid principal and interest over time. These may also represent interests in actual property (which may not actually be securities, depending on the circumstances) through a process called tokenization, which is the assignment of a ledger position corresponding to a real asset, creating a separate asset by associating it with something else of value.

- Utility tokens, which are tokens designed to be used to perform a specific function for the holder, which typically will include the ability to purchase goods or services on a platform or platforms that were designed for use with the token. These may include "loyalcoins," which often are initially sold to help build out a platform, but later can be granted to customers for the purchase of goods and services that are available on the platform, similar to rewards points.

- Payment tokens or cryptocurrencies, which solely represent the ability to make payments and are freely-exchangeable for government-issued currency, or fiat currencies. These include the most well-known digital assets, including Bitcoin, Ethereum, and EOS, as well as a subcategory called "stablecoins" that are generally pegged to the value of (but do not represent an interest in) a fiat currency or some other asset.

- Access tokens or identity tokens, which are used to verify the identity of its owner and allow the holder access to a platform that has restrictions on use. For example, an identity token (such as CVC) can be used to retain know-your-customer information so that holders can be pre-verified for making investments or other payments. Others are developing identity tokens to help individuals better own and have access to their own data, such as medical records and usage statistics.

- Hybrid tokens, which combine characteristics of the different types of tokens described above.

Unfortunately, from a U.S. regulatory perspective, there is very little differentiation between these various types of virtual assets, and where there is, regulatory agencies often disagree on where the line is drawn. For example, many virtual assets that the U.S. Securities and Exchange Commission (the "SEC") deem to be securities may be viewed as currencies by the Department of Treasury or state money transmitter authorities, while the U.S. Internal Revenue Service (the "IRS") treats all virtual assets as property even

where all other U.S. regulatory authorities consider them to be currency. Right now, the greatest impediment to mass adoption of virtual assets in the U.S. is the SEC's expansive interpretation of when a digital asset is a security.

1. What is a security?

Under the Securities Act of 1933, as amended (the "Securities Act"), the definition of "security" mostly includes a list of items that people generally think of as securities—stock, bonds, debentures, notes, securities futures, and the like.[61] Even at the time the Securities Act was drafted, legislators knew that certain types of contractual interests (such as interests in a true joint venture, or general partner interests) likely were not securities and that new types of securities might be developed in the future. Accordingly, the definition of "security" includes the deliberately cryptic term "investment contract." When interests in virtual currencies are investment contracts, those interests become securities that are subject to a full array of federal and state securities laws, including restrictions on the ability to transfer the securities absent registration under the Securities Act and state securities laws.[62]

The formative case interpreting what constitutes an investment contract for the purposes of the Securities Act is *SEC v. W. J. Howey Co.*,[63] where the U.S. Supreme Court determined that an investment in an orange grove was actually an investment in a security due to the characteristics of the sale contract. The three original requirements for establishing an investment contract pursuant to what has become known as "the *Howey* Test" were (1) an investment of money, (2) in a common enterprise, (3) with profits solely due to the efforts of others. Accordingly, the contract pursuant to which Mr. Howey picked and sold the oranges for the benefit of his passive investors was a security in addition to being a commercial contract. Over time, there have been numerous other cases determining the boundaries of when these various conditions are met. Some of these cases have modified the prongs of the *Howey* Test themselves, such as a relaxation of the "solely" requirement,[64] or requiring only the expectation of profits rather than actual profits.[65]

Federal courts have reasoned that in determining whether an investment is a security, the form of the investment "should be disregarded for substance and the emphasis should be on economic reality."[66] Indeed, from its inception, the *Howey* Test

---

61 15 U.S.C.A. § 80b-2(a)(18) (West 2019).

62 In addition, certain states explicitly allow a corporation's stock and other traditional securities to be tracked via distributed ledger or to be in the form of a virtual asset. *See, e.g.*, DEL. CODE ANN. tit. 8, § 224 (West 2019) (permitting stock ledgers to be evidenced solely by distributed ledger technology).

63 *S.E.C. v. W. J. Howey Co.*, 328 U.S. 293 (1946).

64 *See S.E.C. v. Glenn W. Turner Enters., Inc.*, 474 F.2d 476, 482 (9th Cir. 1973).

65 *See United Hous. Found., Inc. v. Forman*, 421 U.S. 837, 852 (1975).

66 *Tcherepnin v. Knight*, 389 U.S. 332, 336 (1967).

was intended as a "flexible rather than a static principle, one that is capable of adaptation to meet the countless and variable schemes devised by those who seek the use of the money of others on the promise of profits."[67]

2. The Wild West and the DAO Report

A sale of tokens can offer an attractive alternative to traditional capital raising alternatives such as sales of equity, credit facilities, and issues of convertible notes. In particular, because utility tokens generally do not entitle the holder to any rights to dividends or distributions, and do not give any ownership interest where payments may be made upon the sale of the company, the tokens can be sold without any direct dilution of existing investors. Further, if the tokens are not securities, then there is significantly less regulation in a token sale than in a traditional financing. In concept, purchasers could either use the utility tokens themselves, or resell those tokens over an exchange, with the value of the token potentially increasing either due to (a) token functionality (e.g., tokens that "burn" when used so that supply always decreases), (b) the value of the products or services offered by the platform increasing, or (c) the number of users of the platform increasing while there's a fixed supply of the token, among other things. In many instances, there is no mechanism for helping the generation of any profit, in which case the purchasers likely believe in the potential efficacy of the project and want to support it so that it can create a positive change and solve for a real-world problem.

The early days of token issuances, commonly referred to as ICOs or initial coin offerings, were rife with fraud, lack of adequate disclosure, and slipshod controls, although there were many legitimate and successful ICOs such as Ethereum and Brave that have led to important and innovative businesses. As legitimate companies and entrepreneurs started to take notice of the benefits of digital assets, these largely became more homogenized with the issuers hiring sophisticated legal counsel and advisors and trying to comply with applicable laws to the extent possible. Most practitioners believed that the *Howey* Test was the appropriate way to determine whether a digital asset was a security, although there was no additional guidance on how that test should be applied, which led to a divergence in practices.

In July 2017, the U.S. Securities and Exchange Commission (the "SEC") issued a report (the "DAO Report") confirming that the *Howey* Test was indeed the means to determine whether a virtual asset is a security.[68] The SEC Staff also stated that, under certain circumstances, digital assets may be securities.[69] Based on the analysis set forth

---

67 *Howey*, 328 U.S. at 299.

68 Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO, Exchange Act Release No. 81207 (July 25, 2017), *available at* https://www.sec.gov/litigation/investreport/34-81207.pdf.

69 *Id*. at 10 ("[T]he Commission deems it appropriate and in the public interest to issue this Report in order to stress that the U.S. federal securities law *may* apply to various activities, including distributed ledger technology, *depending on the particular facts and circumstances*, without regard to the form of the organization or technology used to effectuate a particular offer or sale.") (emphasis added).

in the DAO report, as well as the fact that the DAO tokens exhibited a number of characteristics of traditional securities such as ownership of a project and the ability to receive dividends, the issuance of certain types of tokens became much less frequent while the practice of issuing tokens outside of the securities law compliance regime, but generally in compliance with other laws such as anti-money laundering and money controller laws, continued with respect to tokens that were thought to not be securities. Notwithstanding the potentially permissive nature of the language in the DAO report and the actions of the SEC, as well as recent guidance, have made it clear that it views the definition of "security" to be much broader than many securities law practitioners, taking responsibility for investor protection rather than government agencies with more permissive regimes (such as the Federal Trade Commission).

3. The SEC's Current Views

Even after the issuance of the DAO Report, many issuers with actively operating platforms felt that the utility tokens they were offering still were not securities because, among other things, (a) they would be used for payment on the platform and thus look more like currency than securities, (b) there was no 'common enterprise' because ownership of a token for use on a platform doesn't create commonality, and (c) any expectation of profits wasn't through the efforts of others, but rather due to normal market fluctuations as with currencies and interest rates.[70] The legitimate issuers of utility tokens generally tried to comply with laws applicable to the sale of currencies, such as performing know-your-customer and anti-money laundering checks, registering as money transmitters under applicable state laws, and emphasizing the usability of the tokens in marketing materials while trying to avoid setting an expectation that a purchase of the tokens would earn a profit. In addition to raising capital to enhance the services to be provided by the issuer's platform, most platforms require the digital asset to be widely held to ensure the security and development of the platform. Where a platform was not fully functional, sales to U.S. persons generally were made by a simple agreement for future tokens, or SAFT, which would be sold in accordance with private placement rules under the Securities Act and only would convert into freely tradeable tokens once the platform became functional.

Notwithstanding these efforts, the SEC has almost universally labeled sales of utility tokens as offerings of securities. In December 2017, SEC Chairman Jay Clayton stated, "[b]y and large, the structures of initial coin offerings that I have seen promoted involve the offer and sale of securities and directly implicate the securities registration requirements and other investor protection provisions of our federal securities laws."[71] A

---

[70] *See, e.g.,* Patrick E. Gibbs, et al, *Wells Submission of Kik Interactive, Inc. and the Kin Ecosystem Foundation* (Dec. 10, 2018), *available at* https://www.kin.org/wells_response.pdf (making these arguments, among others, in response to the SEC's notice that it would bring an enforcement action in connection with Kin's ICO).

[71] Jay Clayton, Statement on Cryptocurrencies and Initial Coin Offerings (Dec. 11, 2017), https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11.

wave of enforcement actions followed, and the SEC has entered into a number of settlements with issuers in what might be considered "vanilla" initial coin offerings pertaining to illegal offerings and sales of securities.[72] As a general matter, these settlements involved agreements to offer rescission of the offerings (i.e., offering to repurchase the tokens for the delta between the offering price and current price or sale price, as applicable, plus statutory interest) and a requirement to register the tokens under the Securities Exchange Act of 1934, as amended.

In June 2018, William Hinman, the Director of the SEC's Division of Corporate Finance, gave a speech offering a glimmer of hope that certain digital assets might not be viewed as securities by offering a fairly amorphous test to determine whether a digital asset is a security and stating that, at the time, Bitcoin and Ethereum were not securities.[73] He also laid out certain factors that the SEC would look at in determining whether a virtual asset is a security, although these factors were very vague and the actions of the SEC have made it nearly impossible for an issuer of a virtual asset to say with certainty that it is not issuing securities.

As of the writing of this article, the SEC is taking an extraordinarily expansive view of when a virtual asset constitutes a security. There are exactly three situations where the SEC staff has indicated in a nonbinding manner that a virtual asset is not a security—Bitcoin, Ethereum in its present form,[74] and a payment solution token issued by Turnkey Jet, Inc.[75] Under the Turnkey Jet no-action letter, the SEC recommended that it would not enforce a sale of a virtual asset where:

- it would not use any funds from the token sales to develop its platform, network, or app, and each of these will be fully developed and operational at the time any tokens are sold (i.e., the proceeds cannot be used for any purposes that might help the issuer further develop the technological means of effecting a transaction through the token);

---

[72] *See, e.g.*, *Gladius Network*, LLC, Securities Act Release No. 10608, 2019 SEC LEXIS 213 (Feb. 20, 2019), *available at* https://www.sec.gov/litigation/admin/2019/33-10608.pdf; *CarrierEQ, Inc. D/B/A AirFox*, Securities Act Release No. 10575, 2018 SEC LEXIS 3232 (Nov. 16, 2018), *available at* https://www.sec.gov/litigation/admin/2018/33-10575.pdf; *Paragon Coin, Inc.*, Securities Act Release No. 10574, 2018 SEC LEXIS 3231 (Nov. 16, 2018) *available at* https://www.sec.gov/litigation/admin/2018/33-10574.pdf.

[73] William Hinman, Digital Asset Transactions: When Howey Met Gary (Plastic), Remarks at the Yahoo Finance All Markets Summit: Crypto (June 14, 2018), https://www.sec.gov/news/speech/speech-hinman-061418.

[74] *Id.*

[75] Jonathan A. Ingram, Response of the Division of Corporation Finance Re: TurnKey Jet, Inc. (Apr. 3, 2019), https://www.sec.gov/divisions/corpfin/cf-noaction/2019/turnkey-jet-040219-2a1.htm.

- the tokens would be immediately usable for their intended functionality at the time they are sold;

- the tokens cannot be transferred outside the applicable platform (so there is no ability to list the token on an exchange, even if the reason for the exchange is simply to increase the number of nodes or permit third-parties to purchase a means of obtaining services);

- the tokens would be sold pegged to a government-backed (fiat) currency and through its life would remain pegged to that currency;

- any repurchases of tokens would only be at a discount to their fair market value; and

- the token is marketed in a manner emphasizing its functionality and not its nonexistent potential for the increase in market value of the token.

At the same time, the staff released a non-binding complex and opaque multi-pronged test[76] that could be used in determining whether a digital asset is or is not a security. These factors almost exclusively focus on whether there is reliance on the efforts of others; whether the promoter might undertake efforts to promote its own interests to enhance the value of the token; whether there are any elements of the token itself, the platform, or how the token is traded that might lead to a reasonable expectation of profit; and the present functionality of the platform (which was never a component of the *Howey* Test) at the time the virtual asset is sold. Further, it is unclear whether many of the listed factors would weigh in favor of or against the virtual asset being a security.

Notwithstanding this guidance from the SEC, there still are few situations where the SEC has blessed matters relating to virtual assets. As of the time of the writing of this article, there are over 35 applications for registration of virtual asset broker-dealers that are on hold, and hundreds of registration statements and offering circulars that have been filed with or confidentially submitted to the SEC that have yet to be approved or even commented on. Further, while many issuers of digital assets have argued that their tokens are not securities,[77] these arguments largely have fallen on deaf ears, with the balance between investor protection and financial innovation weighing very heavily toward the former.

The SEC has acknowledged that the character of a virtual asset may change over time, and that a virtual asset that has been sold as a security could eventually become something that is not a security, particularly where the platform on which it is used has

---

[76] *Framework for "Investment Contract" Analysis of Digital Assets*, SEC. & EXCH. COMM'N (Apr. 3, 2019), https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets.

[77] Gibbs*, supra* note 70.

been fully built and is decentralized.[78] The SEC, however, has yet to acknowledge that a virtual asset may be or not be a security depending on who is the holder of that virtual asset and what the intended use of the virtual asset is by the holder. There is substantial case law indicating that something can be a security when its owner purchases it for the purpose of turning a profit, while at the same time not being a security when its owner purchases it for its own use under the so-called "risk capital test," such as with respect to timeshares[79] and even franchise agreements.[80]

That said, many franchisors are uniquely positioned to issue or sell digital assets as the franchise business lends itself to compliance with the Turnkey Jet analysis. Franchisors do not need the proceeds of a token sale to build out their platforms as they are already fully-functional operating companies. Much like loyalty points, the platform for spending the digital asset would be fully developed by the time the digital asset is issued. While this type of asset technically would not be pegged to a fiat currency, it largely would be based on fiat currencies and would not be earned for purposes of speculation. Further, this type of asset would be issued solely for its functionality. In many ways, it's an age-old concept being used in a new, innovative manner.

4. Consequences of a Digital Asset Being a Security

Any security that is offered and sold must be registered or exempt from registration under both federal and state securities laws. By far the most common exemption from registration is under Rule 506(b) of Regulation D, which is the traditional private placement of securities to accredited investors without any public advertising or public solicitation.[81] Other common exemptions include Rule 506(c), which permits public advertising and public solicitation but also requires actual verification of accredited investor status,[82] and Regulation S, which involves offshore offerings.[83] There is one key common characteristic between these exemptions—each of them requires the securities issued thereunder to be "restricted securities" that cannot be resold absent another exemption from registration. This inhibits the ability of an issuer to have a compliant private placement of digital assets because it can be difficult, if not impossible, to code a digital asset being listed on an open exchange to prevent resale of the tokens within the U.S. or to U.S. persons. This has pushed many issuers of digital assets completely offshore, with the potential to stifle many innovations within the U.S.

---

78 *Id.*

79 *Cameron v. Outdoor Resorts of Am., Inc.*, 608 F.2d 187 (5th Cir. 1980).

80 *Venture Inv. Co., Inc. v. Schaefer.*, 478 F.2d 156 (10th Cir. 1973) (stopping short of holding that the franchise agreement was a security under federal securities laws due to the presence of actual fraud, but applying the "risk capital" test to infer that it would have been had such a judgment been necessary).

81 17 C.F.R. § 230.506(b) (2019).

82 *Id.* § 230.506(c).

83 *Id.* §§ 230.901–905.

Issuers and holders of virtual assets that are deemed to be securities may be subject to a number of other regulatory regimes. If the token is viewed as an equity security, then it would need to be registered under the Securities Exchange Act of 1934, as amended (the "Exchange Act") if it has more than 2,000 beneficial owners.[84] This would result in the issuer being required to file periodic reports with the SEC, including annual and quarterly reports, and becoming subject to a number of laws applicable to public companies such as the Sarbanes-Oxley Act of 2002.[85] Also, if an issuer holds back a number of its own tokens that are securities and the value of those tokens exceeds 40% of its total assets, it may inadvertently become an investment company, possibly subjecting it to a very restrictive regulatory regime under the Investment Company Act of 1940, as amended.[86]

5. Treatment of Virtual Assets that are not Securities

It is the position of the U.S. Commodity Futures Trading Commission ("CFTC") and the SEC that, for the most part, virtual assets that are not securities generally should be treated as commodities that are subject to CFTC jurisdiction.[87] The definition of "commodity" under the Commodity Exchange Act includes "goods and articles, ... and all services, rights, and interests...in which contracts for future delivery are presently or in the future dealt in."[88] While the CFTC has the power to enforce frauds and other bad acts with respect to all commodities and commodity transactions, it only has the power to regulate derivatives of commodities.[89] There are several Bitcoin and Ethereum futures exchanges that are regulated by the CFTC, and the CFTC has been regulating a number of synthetic instruments relating to cryptocurrencies. In addition, people who manage cryptocurrencies for the benefit of others may be "commodity pool operators" or "commodity trading advisors" that are subject to an additional regulatory regime and oversight by the National Futures Association.

---

[84] Thus far, the SEC appears to have taken the view that utility tokens are indeed equity securities, as many settlements have mandated that the defendant register the tokens under the Exchange Act. *See Airfox*, *Paragon Coin*, *Gladius*, *supra* note 72.

[85] 116 Stat. 745.

[86] *See* 15 U.S.C. § 80a-3(a)(1)(C) (2019).

[87] *See* Jay Clayton, Chairman's Testimony on Virtual Currencies: The Roles of the SEC and CFTC, Testimony Before the U.S. Senate Committee on Banking, Housing, and Urban Affairs (Feb. 6, 2018), https://www.sec.gov/news/testimony/testimony-virtual-currencies-oversight-role-us-securities-and-exchange-commission; Daniel S. Gorfine, Cryptocurrencies—Oversight of New Assets in the Digital Age, Testimony before the U.S. House Committee on Agriculture (July 18, 2018), https://www.cftc.gov/PressRoom/SpeechesTestimony/opagorfine1.

[88] 7 U.S.C. § 1a(9) (2019).

[89] *See* 7 U.S.C.A. § 2(1)(A) (West 2019) (defining the jurisdiction of the CFTC).

The Department of Treasury, as well as state regulators, frequently deem digital assets to be currencies.[90] Accordingly, FinCEN, the enforcement arm of the Department of Treasury, has been investigating a number of cryptocurrency frauds and recently brought its first formal enforcement action.[91] If a virtual asset is deemed to be a currency, it may also be subject to state money transmitter laws, in which case registration may be required in one or more states, depending on the activities of the issuer.

One particularly tricky issue is that some states do not use the *Howey* Test to determine whether a virtual asset is a security, which may lead to lack of harmonization between federal and state regimes. While certain securities that are privately placed are considered to be "covered securities" that preempt the substantive provisions of state securities offering laws,[92] an instrument that is deemed a security for federal law purposes but not state law purposes would not preempt the non-securities law provisions of state law.

6. Other Legal Issues in the U.S. Virtual Asset Framework

The tax treatment of digital assets in the U.S. also has had a chilling effect on their adoption by large businesses. Presently, all virtual assets are taxed as property, no matter the nature of the virtual asset.[93] The character of the gain or loss on the disposition of a virtual asset generally depends on whether it is a capital asset in the hands of the taxpayer.[94] The use of a virtual assets for payment and the sale of virtual assets are all taxable events, severely limiting their utility as a hedging mechanism in the U.S. and for U.S. taxpayers. This is severely different from using fiat currencies as payment, which is nontaxable. This has been exacerbated by the Tax Cuts and Jobs Act of 2017,[95] which eliminated like-kind exchanges for all asset classes other than real property. Further, at the state level, different states classify virtual assets differently, which can lead to confusion on tax returns.

A number of other considerations are paramount when dealing with virtual assets, especially when they do not incorporate personally identifying information. There should be significant focus on know-your-customer, anti-money laundering, and anti-terrorism

---

90 *See*, *e.g.*, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, U.S. TREASURY FINCEN (Mar. 28, 2013), https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering.

91 *FinCEN Penalizes Peer-to-Peer Virtual Currency Exchanger for Violations of Anti-Money Laundering Laws*, U.S. TREASURY FINCEN (Apr. 18, 2019), https://www.fincen.gov/news/news-releases/fincen-penalizes-peer-peer-virtual-currency-exchanger-violations-anti-money.

92 *See* 15 U.S.C.A § 77r (West 2019).

93 *See* I.R.S. Notice 2014-21 (Mar. 25, 2014), *available at* https://www.irs.gov/pub/irs-drop/n-14-21.pdf.

94 *Id.* at 3.

95 131 Stat. 2054.

laws, especially given prevalent historical use of Bitcoin and other cryptocurrencies for illicit purposes. Custody of virtual assets can also be tricky; while the blockchain is decentralized, there is still a central point of access, and consideration should be given to maintenance of the "key" to access the virtual asset in a safe and reliable manner.[96] Custody laws for virtual assets are still developing. For example, while a number of major custody institutions such as Fidelity have developed cryptocurrency custody solutions, there is little to no guidance on how investment managers can comply with the custody rule of the Investment Advisers Act of 1940, as amended,[97] and very few custodians offer solutions for other illiquid virtual assets and virtual assets that may be deemed to be securities. While widely held and traded cryptocurrencies can be reliably valued, there still is little consensus on how to value illiquid virtual assets, and at the time of this writing the "Big Four" accounting firms typically will not do so. Ensuring proper operation of the token and its blockchain are also important; unlike with valuation, the major accounting firms generally do help perform these coding audits. New York also regulates businesses conducting virtual asset activities, requiring them to obtain a "BitLicense" with potentially onerous bonding, insurance, and other requirements. Many international jurisdictions also have similar licensure requirements.

B. **Virtual Assets Internationally**

One of the main advantages of digital assets is their intermutability—they can be used in different jurisdictions and innately change their characteristics without being subject to certain geographical risks, such as local inflation and governmental strife. To the extent the issuer maintains control of the platform, they often can be used to provide uniformity of benefits in circumstances where there may normally be differences in value due to currencies and taxes. There is a wide spectrum of how virtual assets are regulated in different jurisdictions, and which virtual assets are regulated more or less.

For example, Switzerland has become one of the earliest adopters in welcoming innovation that may be accomplished through virtual assets. For example, Zug, located in "Crypto Valley," is the headquarters for a number of blockchain-enabled companies, including the Ethereum Foundation, and became the first municipality in the world to accept Bitcoin as a means of paying taxes. Switzerland's legal structure breaks virtual assets into three categories, which, while they will be considered in a holistic manner, are regulated by existing regulatory regimes:[98]

---

[96] For example, the cryptocurrency exchange QuadrigaCX reportedly lost $137 million of crypto assets when its founder, the only person who knew the key to the exchange's cold storage system, unexpectedly passed away at the age of 30. *See* Gregory Barber, *A Crypto Exchange CEO Dies—With the Only Key to $137 Million*, WIRED (Feb. 5, 2019), https://www.wired.com/story/crypto-exchange-ceo-dies-holding-only-key/.

[97] 17 C.F.R. § 275.206(4)-2 (2019).

[98] *See* Guidelines for Enquiries Regarding the Regulatory Framework for Initial Coin Offerings (ICOs), FINMA, (Feb. 16, 2018), *available at*

- "Payment tokens" that are intended to be used as a means of payment for acquiring goods or services or as a means of money or value transfer.

- "Utility tokens" intended to provide digital access to an application or service via a blockchain-based infrastructure. Utility tokens will not be treated as securities if their "sole purpose is to confer digital access rights to an application or service" and the token can be used in that manner at the point of issue, because in that instance, the token's "underlying function" is to grant access to the platform.[99]

- "Asset tokens" either representing an asset or otherwise having characteristics that look like a traditional debt or equity security.

Other jurisdictions, such as Malta, Gibraltar, and Bermuda, have made great efforts to develop more comprehensive regulatory regimes that balance business-friendliness, innovation and investor protection. Many countries in the EU, such as England, France, and Germany, are taking a measured approach where the government is studying virtual assets in order to create a regulatory framework. While these countries are also determining whether a virtual asset is subject to any existing regulatory regimes on a case-by-case basis, many issuers are still cautiously selling utility tokens in public offerings in these jurisdictions. Other jurisdictions, such as Japan and South Korea, have taken an even more measured approach, banning virtual assets in circumstances that may be more prone to manipulation while still permitting their sale and ownership on a general level.[100] On the other hand, it is illegal to sell or hold many or all cryptocurrencies in the People's Republic of China, Bolivia, and North Korea, among other jurisdictions, and virtual assets may not be used for payment in Russia, Venezuela (other than its government-issued, ostensibly oil-backed cryptocurrency), and some other jurisdictions. Further, most of Canada treats digital assets very similarly to the SEC, which has limited their adoption in that country. That said, the more permissive regimes in many non-U.S. countries could permit adoption of virtual assets in those countries while taking a "wait and see" approach in jurisdictions such as the U.S., further building out its platform and functionality in the interim, which should decrease the chances that a token would be viewed as a security.

C. **Application of Digital Assets to Franchisors and Franchisees**

While the current regulatory environment has had a major chilling effect on the adoption of digital assets by franchisors and franchisees, it is not difficult to see how digital

---

https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?la=en..

99 *Id.* at 5.

100 *See Digital and Digitized Assets: Federal and State Jurisdictional Issues*, AM. BAR ASS'N (Mar. 2019) at 265 *available at* https://www.michaelbest.com/portalresource/ABADerivatives ("[L]ike Japan, [South Korea] generally has moved toward[] legitimizing cryptocurrencies by focusing on targeted regulations in an otherwise permissive regulatory environment.").

assets could be used to augment, and in some ways revolutionize, the franchise industry. Once there is more certainty, virtual assets have the potential to be used for a number of important applications in the business of franchising.

1. Digital Assets as a Means of Raising Capital

Sales of digital assets may become an attractive option for franchisors and franchisees for raising capital. For franchisors, the tokens could become a universal currency that can be used across the franchise platform regardless of jurisdiction. Similar to *TurnKey*, the token could be used as a payment solution that streamlines transactions and eliminates unnecessary expenses. For franchisees, an offering of security tokens could be a means of giving silent partners an economic interest in a group of franchises while eliminating certain investor relations concerns, reducing the need for intermediaries and, in some circumstances, permitting silent partners to resell their investments without lengthy approval processes and in a much more transparent manner.

As noted below, a token sold by a franchisor for capital-raising purposes could be used for a number of other corporate purposes, such as encouraging customer loyalty or providing incentive compensation or performance bonuses. Another potential advantage is that most franchisors already have well-developed platforms where the capital is not needed to build out the platform, but rather for normal working capital purposes or satisfying other existing obligations and the like. This makes it more likely that a virtual asset issued by a franchisor might not be treated as a security under the Securities Act, and is a step in allowing the franchisor to cleanly fall into the *TurnKey* no-action letter.

Recently, some issuers have been conducting initial exchange offerings, or IEOs, where tokens are sold directly onto an exchange and the market determines the initial sale price of the tokens. In IEOs, persons located in countries with questionable legality of the sale of virtual assets simply are not permitted to purchase the tokens, and the tokens by design are limited to being traded on exchanges that will not permit persons from those jurisdictions to access the exchange. While untested, hypothetically this could cause the offering to be outside the jurisdiction of the SEC or other government bodies that place restrictions on the ability to offer or resell utility tokens.

2. Digital Assets to Encourage Brand Loyalty

Digital assets can be developed to mimic loyalty points with additional characteristics built into their smart contracts. A number of solutions are being developed in this area, including permission to exchange points between different platforms so that customers get the benefit of points they actually want while vendors get the benefit of learning about their exact target audience. While the *TurnKey* no-action letter has very limited utility for payment tokens and utility tokens, as noted above, it may swing the door open for the issuance of loyalty coins.

The tax treatment of loyalcoins remains uncertain. While the IRS has issued formal guidance finding that virtual assets are property, loyalcoins look a lot more like traditional loyalty points, which have different tax characteristics and generally are not taxed on use.

3. Digital Assets to Confirm Identity and Subscriptions

While cryptocurrencies are notorious for being anonymous and making it difficult to track bad actors, digital assets can also be coded so that they're specific to an individual or company, or so they can be tracked when sold, such that there's a more reliable way of verifying access than entry through a written password. Further, more information can be stored through a virtual asset than may be permitted otherwise. Another solution being developed is a way to tokenize personally-identifiable information in a way that is GDPR compliant, giving the ability to obtain big data without having any access to impermissible "small data." Further, consumers may be able to sell access to goods or services directly; if the tokens are uniquely identified and give information regarding the characteristics of the holder, it can give franchisors that sell products or services without collecting personally identifiable information a more reliable way to determine actual end-users as opposed to physical coupons or ad clicks.

4. Digital Assets for Risk Management Purposes

Entrepreneurs have been active in developing a number of blockchain-enabled solutions designed to increase efficiencies, and some of these solutions may be useful for any large business. For example, there are many platforms developing methods for trading tokens so that excess electrical power can be transferred from transmitters (which could include businesses with solar panels or off-grid generators) to users. Certain tokens are being designed to solve for inflation in developing countries so that businesses can expand their more desirable markets while minimizing risks that are prevalent in nations that have not completely stabilized, such as election, inflation, and public unrest risks. Franchisors might be able to mitigate certain interjurisdictional risks, or decrease expenses used to pay intermediaries, by permitting use of these types of tokens to purchase products or services.

5. Digital Assets Representing Franchise Interests

Eventually, franchise interests themselves may be able to be represented by virtual assets. A number of terms of a franchise agreement, such as dispute resolution, ownership qualification, background checks, forfeiture, and transfers, could be built into the coding of the token itself. If a franchisor already blockchains its inventory and sales management, this information can be cross-linked to an ownership token ensuring that a franchisee complies with its covenants. Further, this may make it easier to permit subdivision of franchise interests, with certain approved persons controlling the franchise while other economic partners can invest relying on the expertise and ability of the franchisee without being exposed to liability from the franchisor. Further, if the franchise interest is represented by a token, the franchisor could maintain ownership of the actual franchise interest; if the token acts as a proxy, it eliminates the ability to foreclose on a franchise since the franchisor always remains in possession of the franchise.

In the future, it is also quite possible that virtual franchising itself could be enabled through blockchain via digital assets. Certain online sales models and pyramiding business models may lend themselves to the creation of a franchise via the acquisition of

a token without any further effort of the franchisor, with the rules of operating the franchise coded into the token itself, resulting in a forfeiture of the token if there is a material violation of the franchise smart contract. Blockchain's inherent ability to create trust may help manage franchise relationships through a decentralized and impersonal process of which everyone is aware before someone becomes a franchisee.

6. Acceptance of Widely Distributed Cryptocurrencies as Payment

Many companies continue to evaluate adoption of payment via cryptocurrencies. In addition to the legal uncertainties, cryptocurrency values have been quite volatile, which makes them unattractive for payment unless they can readily be converted into fiat currency. That said, accepting payment in cryptocurrency does have some advantages. In addition to opening a company's market to "Bitcoin billionaires," the value of cryptocurrencies may have more certainty than fiat currency in highly inflationary environments, transaction costs may be lower, rebates may become more automated, payment processing may be faster, and it may decrease the likelihood of chargebacks. Because the use of cryptocurrency to purchase goods or services, as well as the conversion of cryptocurrency into fiat currency, is a taxable event, traditional companies that accept cryptocurrencies generally will do so at a premium to account for volatility risk and the taxes that must be paid on subsequent conversion. Further, the value of cryptocurrencies tends to fluctuate much more widely than the fiat currencies of developed countries, and until cryptocurrencies are more widely adopted, they may be subject to increased security risks.

V. Conclusion

In its draft 2018 Interagency Report on blockchain technology, the National Institutes of Technology (NIST) reported that "[t]here is a tendency to overhype and overuse most nascent technology. Many projects will attempt to incorporate the technology, even if it is unnecessary. This stems from the technology being relatively new and not well understood, or the technology being surrounded by misconceptions." Certainly, as the NIST concluded, "[b]lockchain technology has not been immune" to the hype. Indeed, in its introduction even this paper reports that blockchain "technology represents one of the most potentially disruptive innovations in history."

Beyond the hype, however, there can be no mistake that blockchain has enormous potential utility in a variety of applications and in many segments of industry, including for the franchisor/franchisee. Understanding the opportunities, imagining the potential, and recognizing the pitfalls is therefore recommended.