Significant FinCEN Action Against BTC-e, Implications for Virtual Currency Exchangers

By Jason Weinstein and Alan Cohn on July 31, 2017

On July 26, 2017, the Financial Crimes Enforcement Network (FinCEN) of the US Department of the Treasury assessed a civil monetary penalty of $110,003,314 against Canton Business Corporation (BTC-e), one of the largest virtual currency exchanges by volume in the world, and a $12,000,000 penalty against Alexander Vinnik, a Russian national who allegedly controlled, directed, and supervised BTC-e’s operations, finances, and accounts. On the same day, a 21-count criminal indictment against BTC-e and Mr. Vinnick was unsealed, and Mr. Vinnick was arrested in Greece.

This is the second supervisory action that FinCEN has taken against a virtual currency exchanger, and the first against a foreign entity operating as a money services business (MSB) with activities in the United States. FinCEN’s action also imposes the second highest civil monetary penalty assessed against an MSB to date. FinCEN has increasingly brought enforcement actions against MSBs and other non-traditional financial institutions, and similar actions seem likely in the future.

According to FinCEN, BTC-e lacked basic controls to prevent the use of its services for illicit purposes, and as a result, purportedly maintained a customer base of criminals who concealed and laundered proceeds from crimes such as ransomware, fraud, identity theft, tax refund fraud schemes, public corruption, and drug trafficking, none of which BTC-e reported to FinCEN and law enforcement as required.

Specifically, the penalty assessment concluded that BTC-e violated FinCEN’s regulations issued under the Bank Secrecy Act (BSA) applicable to financial institutions by willfully failing to:

1. Register with FinCEN as an MSB
2. Implement an effective anti-money laundering (AML) compliance program
3. Detect suspicious transactions and file suspicious activity reports (SARs)
4. Obtain and retain records relating to transmittals of funds in amounts of $3,000 or more

FinCEN further determined that Mr. Vinnik willfully participated in these BSA violations.
On July 25, 2017, the Securities and Exchange Commission (SEC) issued its first guidance on how it will interpret token issuances or “Initial Coin Offerings” (ICOs) under relevant securities laws.

The headlines—“SEC Finds DAO Tokens are Securities”—come from Release No. 81207, “Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO” (July 25, 2017), in which the SEC determined that the tokens issued in association with the Distributed Autonomous Organization (DAO tokens) in April-May 2016 were securities and explored the various implications of that determination. (See Steptoe’s analysis of this report [here](#).)

However, the real news may be the other document released on July 25, a notice to investors titled “Investor Bulletin: Initial Coin Offerings” (July 25, 2017). In that document, the SEC sets out several areas of concern regarding ICOs—from which the reader can discern the SEC’s initial expectations with respect to ICOs. Much of the guidance is not surprising, but the SEC’s statement paves the way for more certainty for companies considering ICOs.

In a question-and-answer section titled “Some Key Points to Consider When Determining Whether to Participate in an ICO,” the SEC gives recommendations in several pertinent areas, which if rephrased, form important considerations for companies looking to issue tokens through an ICO.

- The SEC will interpret certain ICOs as the offer and sale of securities. (See the DAO Report for an analysis of the DAO tokens.)
- If the tokens issued as part of the ICO can be considered securities, then the virtual coins or tokens must be registered with the SEC, or the sale must be made pursuant to an exemption from registration.
- Companies planning ICOs should carefully review the criteria for exemptions from registration, including the provisions relating to accredited investors and other restrictions involving net worth or income requirements, and should satisfy the criteria for those exemptions for US investors should the token be considered a security.
- The SEC will likely scrutinize representations that particular ICO offerings are exempt from registration.
- Sales of tokens as part of a crowdfunding should adhere to the requirements of the SEC’s crowdfunding regulations (called Regulation Crowdfunding) and other relevant securities laws.
- If the virtual token or coin is a security, “investment professionals and their firms who offer, transact in, or advise on investments” must be licensed or registered in accordance with federal and state securities laws.
- The SEC will scrutinize what it considers to be “jargon-laden pitches, hard sells, and promises of outsized returns.”

The SEC also made recommendations as to what investors should look for in a white paper or other offering document:

- Companies issuing tokens should have “a clear business plan that you can read and that you [can] understand”; the “rights that the token or coin entitles you to should be clearly laid out, often in a white paper or development roadmap”;

...
it should include “how and when you can get your money back in the event you wish to do so,” including whether there
is the right to receive a refund or to resell the token, and “any limitations on your ability to resell the coin or token.”

- The white paper, development roadmap, or other documentation should state “whether the blockchain is open and
  public, whether the code has been published, and whether there has been an independent cybersecurity audit.”

Additionally, the SEC noted a number of concerns regarding ICOs and virtual currencies more generally, including the
following:

- The SEC is concerned that “virtual currency exchanges and other entities holding virtual currencies, virtual tokens or
  coins may be susceptible to fraud, technical glitches, hacks, or malware. Virtual tokens or virtual currency may be
  stolen by hackers.”
- The SEC is concerned that law enforcement faces significant challenges when investigating ICOs, including: tracing
  money, since “traditional financial institutions (such as banks) often are not involved with ICOs or virtual currency
  transactions, making it more difficult to follow the flow of money”; international scope, in that “ICOs and virtual
  currency transactions and users span the globe,” and that “the SEC may be unable to obtain information from persons
  or entities located overseas”; the lack of a central authority that would “collect virtual currency user information”; and
  the inability to freeze or secure virtual currency.

Finally, the SEC highlighted “potential warning signs of investment fraud,” including:

- Guaranteed high investment returns
- Unsolicited offers
- An offering that “sounds too good to be true”
- Unlicensed sellers
- Lack of net worth or income requirements for purchasers of tokens

The SEC will likely issue additional guidance in the months ahead, but these insights drawn from the Investor Bulletin on ICOs
give companies a good sense of some of the SEC’s primary focus issues.
SEC Weighs in on the Distributed Autonomous Organization’s Tokens

By Alan Cohn and Stephen Richer on July 27, 2017

The SEC announced yesterday that “offers and sales of digital assets by ‘virtual’ organizations are subject to the requirements of the federal securities laws.” Although not coming as a surprise, the SEC’s announcement affirms that companies seeking to involve US investors in an initial coin offering (ICO) must register offers and sales with the SEC or else qualify for an exemption.

The SEC chose the token offering by the Distributed Autonomous Organization (DAO) in April-May 2016 as the focus of the study. The DAO was built on top of the Ethereum blockchain by the German unincorporated organization Slock.it, and the success of its token offering ushered in the current wave of ICO activity. Although questions surrounded the DAO offering in terms of its prospective treatment under US securities laws, the DAO made headlines when it suffered an exploitation that led to the loss of $50 million in Ether. Although the SEC found that DAO “may have violated federal securities laws,” it decided against pursuing an enforcement action, choosing instead to use DAO as a demonstrative for future ICOs (“to advise those who would use a Decentralized Autonomous Organization … or other distributed ledger or blockchain-enabled means for capital raising, to take appropriate steps to ensure compliance with the U.S. federal securities laws”).

To reach its conclusion that DAO fell under U.S. securities laws, the SEC applied a traditional four step analysis derived from U.S. case law (most notably SEC v. W.J. Howey Co., 328 U.S. 293, 301 (1946)). Under that analysis, the SEC held that:

1. Foundational principles of the securities laws apply to virtual organizations or capital raising entities making use of distributed ledger technology
2. Investors in The DAO invested money
3. These investors had a reasonable expectation of profits
4. The profits were to be derived from the managerial efforts of others

Accordingly, the DAO should have registered—and entities planning operations similar to the DAO must register—offers and sales of tokens, and they must register as national securities exchanges, unless certain exemptions apply.

The SEC report, together with the Investor Bulletin on ICOs also issued by the SEC, provide the beginning of long-awaited SEC guidance for companies contemplating ICOs. (See Steptoe’s analysis of the SEC Investor Bulletin: Initial Coin Offerings here.) Some companies might pull ICOs out of U.S. markets altogether following the announcement. But others see SEC regulation as an opportunity to gain legitimacy and weed out illegitimate or fly-by-night ICOs. Registration with the SEC is an involved process, but it certainly can be done by ICO companies. San Francisco-based Blockchain Capital raised $10 million a few months ago after registering its token as a security.

The story is still unfolding, but whichever way the companies react, there’s no doubt that the SEC report is an ICO game-changer.
Implications of S. 1241, the Combating Money Laundering, Terrorist Financing, and Counterfeiting Act of 2017

By Alan Cohn and Chelsea Parker on June 23, 2017

Congress has become increasingly interested in the current state of knowledge about potential links between terrorist financing and money laundering. In the House of Representatives, the Financial Services Committee’s Subcommittee on Terrorism and Illicit Finance held a hearing on June 8, 2017, titled “Virtual Currency: Financial Innovation and National Security Implications.” In the Senate, Senator Grassley (R-IA), along with Senators Feinstein (D-CA), Cornyn (R-TX), and Whitehouse (D-RI), recently introduced Senate Bill 1241, titled “Combating Money Laundering, Terrorist Financing, and Counterfeiting Act of 2017.” The bill, which generally aims to strengthen criminal money laundering statutes, is specifically aimed at fighting terrorism and terror finance.

Of particular relevance with respect to S. 1241 are the potential implications of the bill on blockchain and digital currencies. There are three relevant proposed changes:

1. **Inclusion of digital currency in the definition of financial institution and monetary instrument under 31 U.S.C. § 5312(a):** This provision of the Bank Secrecy Act (“BSA”) would be amended to state that “(2) “financial institution” means – […] (K) an issuer, redeemer, or cashier of travelers’ checks, checks, money orders, prepaid access devices, digital currency, or similar instruments, or any digital exchanger or tumbler of digital currency” [changes in bold];

2. **GAO Report:** The bill calls for the Comptroller General to submit a report to Congress on: (1) the impact the amendments would have on law enforcement, the prepaid access industry, and consumers; and (2) the implementation and enforcement of the Treasury Department’s Bank Secrecy Act (“BSA”) regulations (76 Fed. Reg. 45403); and

3. **Homeland Security and Customs and Border Protection (“CBP”) Report:** The bill calls for the Secretary of Homeland Security and the CBP Commissioner to submit a report to Congress on: (1) a strategy to interdict and detect prepaid access devices, digital currencies, and similar instruments at border crossings; and (2) an assessment of the infrastructure needed for this strategy.

Under the BSA, a person or an agent or a bailee of the person who is transporting, will transport, or has transported “monetary instruments” of more than $10,000 at one time to, from, or through the US must file a Report of International Transportation of Currency or Monetary Instruments. Including digital currency in the definition of “monetary instrument” would subject those devices to these anti-money laundering reporting requirements under the BSA, as stated in the bill summary.

The expanded definition of monetary instruments raises numerous logistical and technical questions. Digital currency can be stored in digital wallets, or “hot wallets,” through companies like Coinbase, Xapo, or BitGo, or stored offline in a hardware wallet. In theory, a person always carries their digital currency—or the ability to transact their digital currency—with them, including as they cross a border. This provision effectively requires the declaration of more than $10,000 in digital currency holdings whenever a person or persons jointly filing a declaration cross the border.
The challenge, of course, is that many of today’s financial instruments work this way. If you have online banking access on your phone, or the ability to draw cash off of your credit cards, and this exceeds $10,000, then you are similarly carrying digitally-accessable currency across the border. Moreover, these digital capabilities enable a person to access the overwhelming currency of choice for criminals: Cash.

This challenge is less about virtual currency and more about how to adapt regulatory structures designed for an earlier era to today’s digitally-enabled economy. Singling out virtual currencies at the border doesn’t materially impact the risk of money laundering or terrorism financing. While criminals are using digital currencies like bitcoin, the majority of digital currency activity does not involve illicit activity (See Jonathan Levin of Chainalysis’s Written Testimony). In fact, according to a recent report from the Center for a New American Security (CNAS), “there is no more than anecdotal evidence that terrorist groups have used virtual currencies to support themselves.” The technology does have features that may be attractive to criminals, including enabling low cost, efficient, peer-to-peer transactions, but those features are exactly why the technology may bring huge benefits to myriad industries (e.g., Digital Identity, Smart Contracts, Pharmaceuticals).

At the recent hearing on virtual currencies convened by the House Terrorism and Illicit Finance Subcommittee, the witnesses repeatedly emphasized that criminals and terrorists are mostly using unregulated, overseas exchanges. Due to existing guidance and regulation within the US, US blockchain and digital currency companies are already registering with FinCEN and complying with anti-money laundering (AML) and know your customer (KYC) procedures. This deters criminals from using their services as should the permanence and transparency inherent in blockchain technology. Former Assistant United States Attorney Kathryn Haun suggested the best way to address illicit use of virtual currencies is “more statutory authority to go after the segments of their [unregulated and overseas] businesses that rely upon US companies for support.” In that way, Section 15 of S. 1241, which seeks to strengthen existing laws that allow law enforcement to obtain foreign bank records, is a more impactful step.

Congress should consider the impacts of singling out virtual currency users, the majority of whom are not using virtual currency for illicit purposes. A better and more risk-based approach should strike a balance between discouraging illicit use while still encouraging innovation.
Finding Resiliency in Microgrids

By Alan Cohn, Travis West and Chelsea Parker on May 12, 2017

This is the fifth and final in a series of posts that breaks down our article, “Smart After All: Blockchain, Smart Contracts, Parametric Insurance, and Smart Energy Grids,” recently published in the Georgetown Law Technology Review. We have discussed the enforceability of blockchain-based smart contracts under ESIGN and UETA and a few promising smart contract applications. We will now examine the use of blockchain-based smart contracts for microgrids. You can read the full article here.

Within the energy industry, blockchain-based smart contracts can accelerate the development of smart meters, as we discussed earlier. However, they can also help accelerate the development of microgrids. Blockchain-based smart contracts can provide the tool to give both utilities and customers the levels of efficiency and effectiveness that both strive for, while delivering both the consumer protections and individual choice that stakeholders often advocate.

In the United States, the majority of people receive their electricity from coal and natural gas facilities. These facilities generate power at a central location, which is then transmitted over power lines to the end user. Although this is the dominant model for delivering power in the United States, this model presents specific risks.

For example, centralized power production creates a risk that if a plant goes offline, customers will suffer substantial loss of service. Hurricane Sandy demonstrated this problem in dramatic fashion. The hurricane left 7.9 million people without power in the Mid-Atlantic and New England areas in the immediate wake of landfall. Even a month later, one percent of Jersey Central Power & Light customers remained without power. The crippling effects of the storm demonstrated that an electrical grid relying upon a few central power plants could collapse quickly and need a lengthy rebuild. The fact that multiple storms in the previous year had knocked power out to millions of people on the Eastern Seaboard further confirmed that the electrical grid was vulnerable. For these and other reasons, the centralized grid model has been criticized in recent reports as being outdated and in need of serious upgrade.

Microgrids are a potential supplement to centralized grid systems, but may eventually replace them altogether. Rather than rely exclusively upon a power plant that produces electricity for a region, a microgrid allows residents in the area to better manage local usage and even generate and sell power through solar panels or other alternative energy methods. The residents can use the microgrid to power their own homes or businesses, supplement their power needs from the larger grid—and if they generate extraneous power, residents can sell it either to their neighbors or back to the larger grid. Microgrids provide a backup system in case a storm or terror event disables the centralized grid. In fact, several microgrid participants cited access to a reliable backup as part of the reason that they joined the project. Microgrids may even extend power access to rural and tribal communities.

Blockchain technology is beginning to be deployed in the United States to facilitate microgrids. The most successful example so far is the Park Slope microgrid in Brooklyn, New York, with over 130 buildings participating. Although currently limited in scope, the ultimate goal is to use blockchain-based smart contracts to allow buildings that produce extra energy to sell that energy in an automated fashion to other residents on the microgrid. Blockchain-based smart contracts would be set up in such a way that
when one user produces excess energy, it is automatically sold to another user in the neighborhood, which allows the neighborhood to lessen the amount of energy it draws from the central grid. Facilitating the sale of excess energy produced by one building to a building in need of energy helps reduce the overall strain on the grid, thereby preventing brownouts during times of high-energy consumption. The Park Slope microgrid has already led to reduced energy usage, as well as facilitating a better understanding amongst consumers regarding where the energy originates and how it is made. The emphasis on buying energy as needed forces customers to confront their energy usage and re-evaluate how much they are using.

Adopting blockchain technology in the energy industry poses its own challenges. Strict industry regulation and monopolies make it difficult to implement new technologies even with their likely benefits. For example, as a political subdivision of the state of Arizona, SRP is under different regulations from the Arizona Corporation Commission (“ACC”) than a standard utility company. This regulatory freedom allowed SRP to test and implement its pay-as-you-go smart meters. In this way, co-ops are also strong candidates to begin experimenting with and adopting blockchain-based smart contract technology, in a manner that can ultimately benefit the entire industry.

The energy industry is a promising application for blockchain-based smart contracts. They could increase the efficiency of payment systems and energy transfer while also improving security and resilience. Customers would also have more freedom and information on their energy usage and costs using blockchain-based smart contracts. Microgrids will increase resilience of the energy system, which may become more essential with severe weather patterns or potential terrorist attacks. Blockchain-based smart contracts will also allow people to easily sell or buy more energy depending on their usage at any given time. With fewer regulatory barriers, co-ops may be the best starting place for implementing these new applications within the energy sector, to the overall benefit of the energy industry as it can observe these experiments and take advantage of the technology as it matures.
Rethinking the Energy Industry with Smart Meters

This is the forth in a series of posts that breaks down our article, “Smart After All: Blockchain, Smart Contracts, Parametric Insurance, and Smart Energy Grids,” recently published in the Georgetown Law Technology Review. We previously discussed the enforceability of blockchain-based smart contracts under ESIGN and UETA and the application of blockchain-based smart contracts for simple insurance contracts and parametric insurance. We will now examine the use of blockchain-based smart contracts in the energy industry, specifically for smart meters. You can read the full article here.

The energy industry is actively examining new models and mechanisms for delivering service to customers. Likewise, customers themselves are looking for new ways to purchase energy and to understand the origins of the energy they purchase. Blockchain-based smart contracts can provide a new, more secure basis for smart meters and, in fact, can take advantage of blockchain’s currency foundations to automate payments as well.

Retail energy provides power to customers through energy lines. The electric utility tracks a customer’s power consumption through a meter installed at the customer’s home. At the end of the billing cycle, a customer is sent a bill for their past month’s consumption.

Although this process is well understood by all parties involved, it has several drawbacks. First, by receiving a bill only once a month, it is difficult for customers to obtain immediate feedback on their energy usage. On a hot day, a customer may know that their usage will be higher, but they would not have a way of knowing exactly how much more energy they used that day compared to a regular day. For instance, they may know that keeping the house at 73 degrees will be expensive but not how much more expensive relative to keeping it at 75 degrees. This limits the ability of a household to adjust its usage on a less-than-monthly basis. If a homeowner wants to balance their comfort with low heating and cooling costs, having access to this more granular level of detail will enable them make the best decision. Second, the process relies on customers being able to provide forms of identification and credit, which may be difficult for certain populations, like students and households without bank accounts. Many utilities require either a Social Security number or two forms of identification, including one with a photo. Even if the potential customers do have those forms of identification, they may lack access to banks or credit cards that a utility requires.

In response, some utility companies have begun to use smart meters, which are electrical meters that wirelessly send meter readings to the utility company. This allows the company to provide a more accurate and up-to-date bill while also freeing the company from needing to send inspectors out every month to read the meters.

Smart meters can go a step further, however, to allow customers to pay as they go rather than rely on monthly assessments and the credit requirements. For example, Arizona’s Salt River Project Agricultural Improvement and Power District (“SRP”) implemented a pay as you go smart meter system, M-Power, which is currently one of the largest pre-paid energy programs in the United States. Under M-Power, SRP installs smart meters in customers’ homes and allows them to use pre-paid smart cards to
purchase energy. These cards can be re-loaded at pay centers across the Phoenix metro area, which includes centers that are open 24 hours a day. This system gives customers more control and flexibility over their energy bill, which is particularly beneficial for those with tight budgets, such as lower-income families or students. Customers are also more aware of their energy usage, resulting in a twelve percent reduction in electricity use of M-Power customers. With high satisfaction ratings, SRP’s customer base has also expanded from those needing more flexibility than a monthly electricity bill to include customers interested in measuring their energy use or wanting to reduce their energy use.

Blockchain-based smart contracts could build further on the pay-as-you-go smart meter concept. For example, blockchain-based smart contracts can resolve some security concerns and allow for quicker payments. A recent report noted that smart-meters are woefully insecure, using outdated encryption protocols that can be easily brute-forced. Some customers are also unable to reload their payment cards without visiting a separate payment machine, which can pose a problem if their energy runs out in the middle of the night and no pay centers are open. Finally, some consumers have protested that smart meters inaccurately measure their consumption and overcharge them. By contrast, blockchain-based device authentication tools can augment the security of smart meters on a blockchain-based system.

Blockchain-based smart contracts can also enhance payment processes for smart meters. Instead of relying upon payment cards that must be reloaded at a separate location, with blockchain-based smart contracts paired with smart meters, customers can arrange payments on their phones using blockchain-based smart contracts that execute when their remaining electrical power drops below a certain amount of time left. This makes it easier for customers to pay than the current system, which often requires going to a separate physical location to add to one’s balance. Blockchain-based smart contracts could also be structured so that when an external weather reporting site indicates that the next week will be particularly cold or hot, the contract would automatically add more money to the consumer’s balance to account for the expected higher usage. For some users, the assurance of knowing that they will not need to frantically add to their balance during the middle of a snowstorm or heat wave is worth paying earlier than necessary. The consumer would also benefit from having multiple smart contracts execute during what would have been a traditional monthly billing cycle. The consumer would have more immediate feedback about their energy usage and could adjust in real-time or based on pre-programmed parameters if necessary.

As noted above, blockchain technology also offers benefits of greater transparency for all participants, as well as a greater sense that rules cannot be changed unilaterally. As a result, a blockchain solution can address questions concerning overbilling. With a blockchain-based system, consumers would have direct access to an immutable record of their usage, which could be compared to historical usage or the average usage of neighbors. A user who suspects they were either overcharged or perhaps had their smart meter hacked would be able to compare their usage on an extremely granular level to the usage of their neighbors to demonstrate errors. These benefits may allow companies to reach new markets of people looking for more flexibility or who have difficulty with the traditional requirements.
New Models of Insurance: Parametric Insurance

By Alan Cohn, Travis West and Chelsea Parker on May 9, 2017

This is the third in a series of posts that breaks down our article, “Smart After All: Blockchain, Smart Contracts, Parametric Insurance, and Smart Energy Grids,” recently published in the Georgetown Law Technology Review. We previously discussed the enforceability of blockchain-based smart contracts under ESIGN and UETA and the application of blockchain-based smart contracts for simple insurance contracts. We will now examine the use of blockchain-based smart contracts for parametric insurance. You can read the full article here.

As discussed in our last post, life insurance and final expense insurance are good examples of simple “if-then” arrangements that can be digitized into blockchain-based smart contracts in relatively straightforward ways. But could other types of insurance that are currently reliant on more subjective factors be restructured into products with more firmly defined parameters, enabling their digitization and administration through blockchain’s transparent processes? Parametric insurance policies offer such potential. By pairing parametric insurance with blockchain-based smart contracts, insurers can reinvent the manner in which classes of insurance are offered.

Parametric insurance is a form of insurance where the payouts are determined not through a claims adjuster surveying the damage, but based on objective measures, such as the magnitude of a weather event. It is most often used for insurance for natural catastrophes, such as tornadoes or hurricanes, where individualized policies based on specific damage would be difficult and costly to administer but a standardized payout based on proxies, such as the severity of the storm, would suffice. Parametric insurance is preferable to other forms of insurance when a quick payout is necessary, such as when a country suffers a hurricane and needs to quickly obtain money to begin rebuilding and pay emergency workers. Parametric insurance can lower the time of payment from months to two weeks, which can help jumpstart the rebuilding process.

The key to parametric insurance is finding objective indicators that can serve as an effective proxy for the type of loss being covered. The benefit to doing so is that once effective proxies are identified, policies that would need to be adjusted qualitatively could instead be reduced to simpler “if-then” statements. For example, by relying upon objective markers, such as storm intensity, wind speed, or amount of rain, there is no need for individualized adjustment of claims. After a hurricane damages an area, an oracle can pull data from a third-party site, such as the National Weather Service, to determine objective measures, such as the strength of the storm, and then make a payment based on that data. While individual losses may be greater or less than the specified payment amount, the insurer gains certainty in loss forecasting and the policyholder gains speed in payment. Both parties benefit from the automation of the process and the reduction in frictional costs.

Parameterizing current forms of insurance based on proxies for loss and coding these policies onto blockchain-based smart contracts can fundamentally alter insurance offerings by (1) lowering transactional costs of simple policies to allow for lower-premium policies to be profitably administered and (2) opening new markets for insurance products since locally-based claims adjustors or other local trusted agents would no longer be necessary to effectively administer the policy. Although some costs are difficult to manage, studies have found that for property and casualty insurance, management and contract administration is the
largest driver of cost variance. Indeed, a study by McKinsey & Company concluded that for property and casualty insurance over eighty percent of the cost variance was attributed to management factors, not to the underlying product. It is estimated that improving IT efforts alone could reduce costs by twenty to forty percent, with business complexity and performance management being other large drivers of cost variance.

Moving to parametric blockchain-based smart contracts has the benefit of addressing IT improvement, business complexity, and performance management, while gaining transparency and trust. Blockchain technology can be implemented without having to discard current IT systems, as a blockchain-based platform can be added on top of an existing IT system. Commercial blockchain platforms are already available through several cloud services providers (e.g., Microsoft Azure). Parameterizing current policy structures drastically reduces business complexity, and its standardization of payouts and parameters allows for much more bounded modeling of potential loss events and amounts. Finally, blockchain-based smart contracts can be administered through oracles and monitored in real-time through analytic software examining the permanent blockchain record of transactions and loss occurrences. Fewer local agents would be necessary, and the use of oracles could replace the need to rely on the reports of adjusters on the ground.

As a result of the reduction in frictional costs, policies that were previously unprofitable because of low margins—due to the low premiums or high administration costs—could become profitable areas for new products. For example, companies could profitably insure extremely low premium and low payout events through no-fault parametric policies, where the payouts are determined based on readings from sensors installed in the cars to monitor damage, pattern of driving before the incident, violation of local traffic laws, or other factors. Homeowners could have parametric insurance for incidents such as fires in their homes where a smart fire alarm and smart home sensors could identify the source of a fire, the resulting damage, and potentially its cause.

Moreover, the agricultural industry lends itself to the use of parametric, blockchain-based smart contract insurance. Touting the numerous potential benefits of parametric insurance to improve the welfare of smallholder farmers, increase resilience, and eliminate the need to verify losses, numerous organizations have piloted index insurance programs all over the world, particularly in developing countries. However, the ability to reach smallholder farmers to make sure they can access and understand the insurance contracts currently limits scalability. Rural areas with poor infrastructure may be hard to reach with traditional methods.

The ability to market and administer blockchain-based smart contract-enabled parametric insurance policies solely through internet-connected smartphones can aid in reaching underserved populations. For example, a smartphone-based system, potentially modeled after Kenya’s M-Pesa, could be a good solution. M-Pesa is a mobile payment system that allows people to send and receive money using their cellphone. Since 2007, the technology has taken off with at least one individual in ninety-six percent of Kenyan households using it. Indeed, seventy-five percent of the unbanked population in Kenya uses M-Pesa. Elsewhere in Africa, BitPesa is using the Bitcoin blockchain to bring the M-Pesa model to other African countries and to cross-border transactions.
In sum, parametric, blockchain-based smart contracts represent not only an opportunity to digitize existing insurance products to realize efficiencies, but also open potentially untapped markets for insurance products using the benefits of newly-developed technology.
Efficiency Gains in the Insurance Industry

By Alan Cohn, Travis West and Chelsea Parker on May 8, 2017

This is the second in a series of posts that breaks down our article, “Smart After All: Blockchain, Smart Contracts, Parametric Insurance, and Smart Energy Grids,” recently published in the Georgetown Law Technology Review. We previously discussed the enforceability of blockchain-based smart contracts under ESIGN and UETA and will now look at the application of blockchain-based smart contracts for simple insurance contracts. You can read the full article here.

Even though basic insurance contracts can often be boiled down to an agreement to make payment upon the occurrence of a discrete event, administration can quickly become complex. Claims adjusters are needed to assess a claim and its validity and disagreements can arise if parties later disagree about the interpretation of the terms or relied on representations outside of the policy. In addition, parties are often mistrustful of one another because of the potential for fraud, abuse, or denial of claims. In either event, insurance companies incur costs administering even the simplest of contracts, and those costs are often passed along to consumers in the form of higher premiums. However, reducing basic insurance contracts to “if-then” statements and digitizing administration would reduce the cost of administering these products and help overcome challenges of trust and transparency.

Efficiency Gains in Current Insurance Contracts: Life Insurance and Final Expense Policies

Some of the simplest “if-then” types of insurance policies are individual life insurance and final expense policies. Life insurance contracts pay out upon the policyholder’s death. Although this process is normally easy for the survivors to carry out problems can arise in multiple ways. For example, the policyholder may hold multiple life insurance policies, the beneficiary may not know about the policy, or the beneficiary may misplace the paperwork for the policy. As a result, inefficiencies and increased administration costs can arise without any malfeasance or ill-will from any party.

Blockchain-based smart contracts can remedy many of these problems. For example, rather than maintaining only a written insurance contract, a blockchain-based smart contract is digitally instantiated and recorded to the blockchain’s immutable ledger. Rather than relying upon the policyholder to retain the policy (making the policy subject to loss through misplacement or destruction by fire, flood, or similar occurrences), the policy would be recorded on the blockchain and its terms would be available at any time for the insurer, the policyholder, and the beneficiary to review. Rather than relying upon a beneficiary to notify the insurance company, a blockchain-based smart contract can be constructed to rely on oracles set to monitor specific sources of information about individual deaths. The transparency of the blockchain and the fact that its rules are not administered by any single participant in the process can allow purchasers to rely on digital instantiation and administration.

Digitization has already enabled portions of this process. The United States government maintains the Social Security Death Master File, which tracks when a person with a Social Security number dies. Although this is not a perfect record and has in many instances been subject to legitimate criticism for its accuracy, an oracle could monitor this file for policyholders, and upon the death of a policyholder trigger contract execution. Currently, the Master File is only updated once a week and a person’s death must be reported to the Social Security Administration for it to be filed. For that reason, oracles could also monitor other
digitally-available sources of information, such as social media, in order to provide further assurances before the final execution of the contract. Indeed, some organizations are already experimenting with peer-to-peer unemployment insurance smart contracts based on LinkedIn data.

A similar application for blockchain-based smart contracts in insurance is final expenses insurance. Final expenses insurance is a form of insurance where a fixed sum is paid out upon a person’s death to help cover funeral costs. For some cultures, it is essential to have a proper funeral or perform funeral traditions. However, families are often unable to pay for an unexpected funeral or even the funeral of an elderly family member. A blockchain-based smart contract could be set up using the same sources as a life insurance smart contract and perform the same function. Indeed, contracts could even be purchased by family members in other countries, with agreed-upon oracles and specified mechanisms of digital payment, such as direct payment to funeral providers, rather than reliance upon local reporting and paper checks.

**Smart Contracts, Insurance, UETA, and ESIGN**

In our last post, we argued that blockchain-based smart contracts are enforceable under UETA and ESIGN. Specifically with respect to insurance contracts, however, these types of digital contracts are also the exact types of contracts that Congress wanted to protect under ESIGN. Insurance contracts are specifically included in the statute (6 15 U.S.C. § 7001(i)-(j)). ESIGN, as part of its consumer protection provisions, prohibits the cancellation of life insurance policies through electronic means. This protection reflects the special status of life insurance as providing for one’s family after death, which has led states to protect life insurance proceeds in other ways. UETA does not have a similar protection, but many states have implemented similar exemptions (e.g., N.C. GEN. STAT. § 66-313(e)(3)). These limitations restrict the kinds of smart contracts that can be created for insurance products.

In order to take advantage of UETA and ESIGN, a blockchain-based smart contract for life insurance would not be able to cancel a policyholder’s policy upon non-payment of the premium. Instead, the cancellation notice would need to be sent via physical form. Cancellation of blockchain-based smart contract-driven life insurance policies for non-payment may be an area for further development of legal guidance under UETA and ESIGN. In addition, smart contracts need to be worded carefully to ensure that policyholders do not use them as a substitute for a will, as ESIGN and UETA would not ensure that they are valid.
The Enforceability of Smart Contracts

By Alan Cohn, Travis West and Chelsea Parker on May 4, 2017

This is the first in a series of posts that breaks down our article, “Smart After All: Blockchain, Smart Contracts, Parametric Insurance, and Smart Energy Grids,” recently published in the Georgetown Law Technology Review. First, we will discuss the enforceability of blockchain-based smart contracts followed by four use cases: simple insurance contracts, parametric insurance, smart meters, and microgrids. You can read the full article here.

Smart contracts have the potential to impact a range of industries, and some are even calling 2017 “The Year of Smart Contracts.” Smart contracts can be used not only to automate existing processes, but also to create new industries and reach new markets. By providing a digital platform for coding “if-then” statements, providing a secure and resilient environment for value transactions, and preserving a detailed and immutable transaction history, the blockchain provides an ideal platform for smart contracts.

With companies and industries continuing to explore new blockchain-based smart contract applications, it is important to establish their enforceability.

Numerous questions have already been raised as to whether a contract on the blockchain is binding and enforceable. Vermont, for instance, has made multiple attempts to pass a law that would make blockchain evidence self-authenticating, and has finally succeeded in enacting one. Arizona recently passed a law clarifying that signatures obtained through blockchain technology are valid electronic signatures. We believe that the federal Electronic Signatures in Global and National Commerce Act (“ESIGN”) and state laws modeled on the Uniform Electronic Transaction Act (“UETA”) provide sufficient legal foundation for blockchain-based smart contracts to be enforced under current law.

Development of UETA and ESIGN

In the early days of the internet, states enacted a patchwork of laws designed to balance the needs of online commerce with protections of consumers and businesses. In response to the often-contradictory state laws, the National Conference of Commissioners on Uniform State Laws (“NCCUSL”) drafted UETA to provide a model law to harmonize the rules governing electronic commerce transactions. Currently, forty-seven states, along with the District of Columbia and the U.S. Virgin Islands, have enacted some form of UETA.

Despite the UETA’s purpose of providing a standard national code governing electronic commerce transactions, states inconsistently implemented UETA by changing several provisions to protect consumers or reflect their own state laws. Businesses, again facing the challenge of needing to comply with multiple inconsistent state laws, pushed for a new law to standardize the equivalence between electronic signatures and other forms of signatures on a national level.

Congress responded by passing ESIGN, which, while mirroring UETA in many ways, diverged in some others, including consumer consent requirements. However, Congress included a pre-emption provision that gives states the option to choose...
between ESIGN compliance or UETA adoption. Congress specified that states could preempt ESIGN with their own laws, so long as those laws were either UETA or did not conflict with ESIGN. This reflected the desire that states either follow ESIGN or adopt UETA. In this way, the preemption provision ensures that either ESIGN or UETA governs electronic transactions.

**Common Provisions of UETA and ESIGN**

UETA and ESIGN share several features. First, both guarantee that a signature or record will not be held legally ineffective because it is in electronic form. Second, both clarify that any law that requires a record to be in writing will be satisfied by an electronic record. Finally, an electronic signature is held to be the equivalent of a written signature for any law that requires a signature. Collectively, these provisions ensure that electronic records and signatures carry the same legal authority as physical documents and signatures.

These provisions also recognize the notion that consent can be granted by electronic means. UETA requires that both parties agree to “conduct transactions by electronic means,” which can be “determined from the context and surrounding circumstances, including the parties’ conduct.” ESIGN and UETA also have sections relating to the retention and accessibility of any electronic records. Both acts require that an electronic record be producible and accurately reflect the final form that the parties agreed upon.

Overall, the effect of UETA and ESIGN is to allow digital signatures to have the same effect as a physical signature. Congress wanted to allow businesses to benefit from the efficiency of transmitting and signing documents electronically and to free businesses from being required to keep a warehouse full of contracts. Although it is difficult to imagine now, the Congressional Record is replete with the concern that electronic signatures would somehow be less valid than physical signatures unless Congress acted. The courts have interpreted both the UETA and ESIGN in a way to help facilitate digital transactions, which has allowed the digital economy to grow. Indeed, UETA and ESIGN have allowed credit card applications, loan applications, and other transactions to be performed online while still being enforceable.

**How Do UETA and ESIGN Apply to Blockchain-Based Smart Contracts**

The key to the applicability of UETA and ESIGN to blockchain-based smart contracts is the cryptographic key with which blockchain-based smart contracts are signed and acknowledged. From our perspective, asymmetric key encryption falls squarely within the both the language and intent of ESIGN and UETA as an “electronic signature.”

In short, one way for a party to express agreement with the terms of a blockchain-based smart contract is to provide its digital signature utilizing a cryptographic key. This signature, expressed using the blockchain's asymmetric key encryption, is similar to the initial digital signatures that early forms of UETA envisioned. UETA defined “electronic signature” as “an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.” An electronic signature therefore has two components: the signature, in whatever form it is, and the intent to sign.
Courts have interpreted the requirement for the signature and the intent to sign broadly. For example, courts have found that typing “Thanks” plus the sender’s name in an email constitutes a signature. The court in that case noted that the plaintiff manually typed her name, as opposed to having a default signature automatically attached by her email program. This is a low bar to set to allow UETA to enforce the contract.

By contrast, parties using blockchain-based smart contracts would negotiate terms and then each party would need to use their cryptographic key, unique to them, to sign off on the contract. The cryptographic key would be either a “symbol or process attached to or logically associated with a record,” and the deliberate signing off would demonstrate each party’s “intent to sign the record.” Regardless of the specific contract terms, the fact that a blockchain-based smart contract can require the participants to sign the contract through the cryptographic key should assure courts that a blockchain-based smart contract is a legally-binding agreement under UETA and ESIGN.

Moreover, a blockchain-based smart contract can prevent some of those factual challenges because the cryptographic nature of the signature for a blockchain-based smart contract can more effectively establish a person’s identity. In a case arising out of Louisiana, a court upheld the applicability of Louisiana’s version of UETA to automobile insurance contracts but held that a genuine issue of fact existed over whether the plaintiff had actually signed the insurance waiver (Bonck v. White, 2012-1522 (La. App. 4th Cir. Apr. 24, 2013); 115 So. 3d 651, 655). The insurance company insisted that she had, but she pointed out that the waiver was signed four days after she met with the insurance agent to apply for insurance. Due to this conflict, the case needed to go back to the trial court for further proceedings. This is not an uncommon issue, as similar cases have arisen in other jurisdictions. These kinds of disputes often boil down to which side can muster enough evidence that the proper person signed the contract or create enough doubt to go to trial, where a jury could be swayed by other concerns.

A blockchain-based smart contract, by contrast, needs to be signed by each party using a cryptographic key that only each party has access to. This cryptographic key is a much more reliable identifier, as it is nearly impossible for someone to forge the key. A third party can see that signature and immediately know who signed it, preventing many disputes about the authenticity of a signature. A party may argue that its cryptographic key was stolen, but the key is unlikely to be stolen because the benefits of stealing the key for an insurance contract or other type of blockchain-based smart contracts are small. In the case of an insurance contract, the beneficiary could not be changed without needing a new smart contract, and the smart contract would ensure that the premium is being paid, which lessens the chance a party could enter into a fraudulent contract. Instead, the cryptographic signing would function much like having witnesses observe the signing of a will. It would create a high barrier to overcome and reduce costs of enforcement because fewer parties would be willing to go to court to contest that they signed a contract with such strong evidence.
Insurance with Assurance

By Jason Weinstein on December 9, 2016

In the last installment of our five-part blockchain series, we focus on the insurance industry. Insurance and reinsurance companies are actively exploring and developing applications for blockchain technology. And for good reason – distributed ledger technology has the potential to revolutionize the way insurance companies operate and engage with their policyholders and to open a window into new products and new markets.

At the retail level, the blockchain promises to benefit both the consumer and insurer by simplifying the claims process, increasing efficiency of underwriting and claims handling, improving risk management, and reducing operational costs. The blockchain will help ensure the security of private or confidential information, improve auditability and transparency, and increase effectiveness in fraud detection. These enhancements will also help lead to an improved customer experience.

At the wholesale level, blockchain technology can help streamline and enable new mechanisms for funds and risk transfer among institutions, with enhanced accountability and certainty around transactions.

Automating processes, including through the use of smart contracts, will also enable the development of new types of insurance products and the service of new markets, including products and underwriting processes tailored to emerging markets and to the Internet of Things. Indeed, according to Lloyd’s 360° Risk Insight Report, the potential market for microinsurance in developing economies could be 1.5-3 billion policies.

Numerous insurance and reinsurance companies around the world are already exploring the use of the technology. In October, Aegon, Allianz, Munich Re, Swiss Re and Zurich formed B3i, the Blockchain Insurance Industry Initiative, to explore the use of distributed ledger technology, emphasizing its potential to provide clients with “faster, more convenient and secure services.” Among other things, companies are experimenting with the use of smart contracts for unemployment insurance and disaster relief claims.

While the possible applications of blockchain technology are endless, one common potential obstacle to these applications is regulation. So engaging with regulators and policymakers, both in the US and abroad, is critical. Insurers are subject to increasingly complex and prescriptive regulations and standards. In addition, companies should be prepared for the legal issues surrounding the creation, execution, and enforcement of smart contracts. How will regulators respond to this new technology? Are new laws and regulations required for smart contracts, or do they mesh with existing legal regimes? As we have written in this space before, for any industry, a legal strategy is a critical part of an overall strategy for adopting blockchain technology. This industry is no exception. Insurers and reinsurers know better than most companies how to assess risk and opportunity – and if the legal risks are addressed appropriately, the business opportunities presented by the blockchain could be extraordinary.
Taking Control of Your Identity

By Alan Cohn on December 6, 2016

One of the most intriguing uses of the blockchain may be the enhancement of identity solutions.

As we know, the blockchain offers enhancements over current mechanisms for creating and storing digital identities, such as security and resilience built in by design, a greater ability to control the uses of encrypted information, and the ability to provide standardization across a range of legacy IT systems. But what does this actually mean for identity applications in different industries?

A lot, actually. Identity validation for internet applications is a persistent problem. As the New Yorker cartoon famously says, “On the Internet, nobody knows you’re a dog.” Yet as we have seen, the use of fraudulent identity on the internet leads to mistrust in electronic transactions, a mistrust of the identity of individuals and organizations posting materials to social media, crowdsourced reviewing applications, and other sites, and an inability to take forward applications such as internet polling and voting.

The Obama Administration’s “National Strategy for Trusted Identities in Cyberspace” (April 2011) sets our four guiding principles for digital identity solutions. They must be:

- Privacy-enhancing and voluntary
- Secure and resilient
- Interoperable
- Cost-effective and easy to use

Blockchain-based identity solutions meet all of these criteria. While being secure, resilient, and interoperable, because of the individual control over identity, they are also privacy-enhancing and voluntary; and blockchain companies are making them cost-effective and easy to use.

Beyond just internet applications, how would blockchain-based identity solutions approach harder challenges? One emerging challenge is the ability to authenticate devices on the Internet of Things. Blockchain-based identity applications are ideal for this application. Identity solutions that enable identity to be transacted securely and privately by individuals can do the same for machines, and given the “fat layer” of the blockchain (meaning that most of the computing power and programming needs are in the blockchain itself, not in the application) IoT devices can authenticate identity at low cost and low computing burden. Indeed, the U.S. Department of Homeland Security gave a research and development grant to a blockchain infrastructure and consulting company in early 2016 to explore exactly this application.

Private transactions are one thing, but how about interacting with the government? Blockchain-based identity applications offer advantages here as well. First and foremost, because individuals hold their own identity information, identity can be validated through blockchain applications without the government holding vast stores of identifying information. Instead, the government
can specify through regulations or other requirements what identity information it needs to validate in order to permit certain uses, such as entering a government building or applying for a license or permit. The individual then enters into a voluntary identity transaction, agreeing to reveal the required identity information and/or have that information validated against other sources in exchange for the benefit or service (or not). The government receives the assurances it needs concerning an individual’s identity, while the individual keeps control of his or her information.

So what needs to change in order to enable this functionality? Arguably, it’s not wholesale changes to laws and regulations, but rather interpreting guidance concerning the applications of statutes such as the Privacy Act of 1974, the E-Government Act of 2002, and the Electronic Signatures in Global and National (ESIGN) Commerce Act of 2000. It’s also the construction of government systems for effectively interacting with blockchain-based identity solutions.
After eight months, an update on the Blockchain Alliance

By Alan Cohn and Jason Weinstein on July 26, 2016

The Blockchain Alliance was announced last October. Since then it has grown from about 20 to over 50 members, including digital currency companies, law enforcement groups, and regulatory bodies from all over the world. But what has it been up to?

Last October, Coin Center and the Chamber of Digital Commerce announced that they had teamed up with our firm, Steptoe & Johnson LLP, to create the Blockchain Alliance, a coalition of industry members and government agencies focused on improving dialogue and engagement between the private and public sectors on digital currencies and blockchain technology. The Blockchain Alliance is a resource for the blockchain community to understand the interests and concerns of government agencies regarding the technology and its applications. At the same time, it’s a resource for law enforcement and regulators, a forum where they can feel comfortable asking technical questions to some of the brightest minds in the Bitcoin and blockchain space.

The basic idea is that by educating law enforcement directly about this technology, we can reduce their fear or anxiety about it, and make them less likely to overreact to it. That in turn makes it less likely that lawmakers will overreact as well. And of course it’s helpful for industry to hear about what law enforcement is worried about in terms of the use of the technology for illegal purposes.

That’s what happened in the early days of the Internet—the nascent commercial Internet was used primarily by criminals and pornographers. So about 20 years ago, law enforcement agencies got help from Internet companies to learn how the technology worked, so they could improve their capacity to go after criminals who misused that technology to facilitate their crimes. That effort went a long way toward dialing down concerns about the Internet.

Through the Blockchain Alliance, we’re trying to do the same thing for digital currencies and the blockchain. The critical difference is that this time, the industry reached out to law enforcement, not the other way around. The Blockchain Alliance was created by industry, and it’s our member companies and organizations that deserve the credit for their vision in recognizing why this is so important for the ecosystem, and for their determination in making it a reality.

As Coin Center’s Jerry Brito said at the time of our launch, one goal of the Blockchain Alliance was “to ensure that the capacity of Bitcoin and the blockchain to benefit so many is not overshadowed by the potential for misuse by a few. Working together, we can promote an approach to enforcement and regulation that supports, rather than stifles, innovation.”

So what have we been doing to further these goals?

Among other things, we’ve engaged in an extensive education campaign to help improve the depth and breadth of knowledge among US and foreign law enforcement officials and regulators. That education campaign has included a series of webinar-style information sessions, with a curriculum focused on the areas where the law enforcement and regulatory agencies said they most wanted the education, and with the content provided by the industry members. We’ve done four of these sessions to date, with
many more to follow, but so far we’ve already reached nearly 500 law enforcement officials and regulators in well over a dozen countries.

We’ve also established an open and productive dialogue between industry and government agencies about trends in criminal misuse of this technology and other issues of concern. That dialogue has been substantively beneficial to both sides. But it has also been beneficial on another level, because it has gone a long way toward building trust and credibility. That’s important so we can help ensure that when law enforcement goes after criminals misusing this technology, they don’t paint the companies with the same brush as the criminals. The engagement between the private and public sectors through the Alliance is going a long way toward demonstrating that the companies in this space are not just good companies, but good corporate citizens.

When we launched last fall, we had about 15 industry members and 6 U.S. federal government participants. In the approximately 8 months we’ve been in operation, we’ve grown by leaps and bounds. We now have over 25 companies and industry groups as members. And we now have participants from 25 law enforcement and regulatory bodies around the world, including both the criminal and national security-related components of the U.S. Department of Justice, as well as the FBI, U.S. Marshals Service, U.S. Secret Service, U.S. Immigration and Customs Enforcement/Homeland Security Investigations, U.S. Customs and Border Protection, Internal Revenue Service, Food and Drug Administration, U.S. Postal Inspection Service, SEC, CFTC, FinCEN, the Attorney General’s Offices of California and Texas, and the Manhattan DA’s Office. Internationally, we have key partnerships with Europol and Interpol as well as the Australian Federal Police and the Commonwealth Secretariat.

And we’re really just getting started.

We’re proud to be working with so many great industry partners in this effort. By educating law enforcement agencies and regulators around the world about digital currencies and the blockchain, and by reducing their fear and anxiety about this technology, we will go a long way toward creating an environment where innovation can flourish and where the full potential of this technology can be realized. To learn more about the Blockchain Alliance and its member companies, please visit www.blockchainalliance.org.
Are Bitcoin and Other Digital Currencies Securities?

By Jason Weinstein and Alan Cohn on February 12, 2016

Anyone who has tried to explain bitcoin around their kitchen table knows that it is not easy to put your finger on what exactly the technology is. Because of their innovative nature, digital currencies don’t have obvious analogs or fit easily into existing categories. Bitcoin is part currency, part digital payment system, and part immutable ledger.

This confusion is not merely academic. How digital currencies are defined determines how they are regulated. For instance, the Internal Revenue Service (IRS) determined that bitcoin is a form of property, not currency, for tax purposes. The Commodity Futures Trading Commission (CFTC) labeled bitcoin a commodity. Could the Securities and Exchange Commission (SEC) decide that bitcoin is a form of security?

Coin Center recently released a thorough and thoughtful report examining this question and proposing guidelines for determining when a digital currency should be treated as a security.

The guide, a “Framework for Securities Regulation of Cryptocurrencies,” draws on the Supreme Court’s famous Howey test. SEC v. W.J. Howey Co. held that an investment contract—for the purposes of securities regulation—is a “contract, transaction or scheme whereby a person [1] invests his money [2] in a common enterprise and [3] is led to expect profits [4] solely from the efforts of the promoter or a third party.” The report’s framework identifies seven key variables that distinguish different digital currencies and maps them onto the four factors of the Howey test. A recent Coin Center blog post identified “seven key variables that might differ from one cryptocurrency to another:

- Scarcity (what are the economics of the coin’s supply?)
- Distribution (how do new coins reach users?)
- Consensus (how does the network agree on supply and transaction history?)
- Permissions (what does possession of the coin allow the user to do?)
- Decentralization (how centralized is the network and developer community?)
- Profit-Development Linkage (how linked are developer profits to coin sales?)
- Transparency (how transparent is the network and developer community?)"

Different variables map onto different factors of the Howey test. For example, the distribution variable maps onto the “invests his money” factor of the test—if coins are purchased, instead of mined competitively, the cryptocurrency starts to look more like a traditional security.

The framework concludes that several types of digital currencies do not fit the definition of a security. First, highly-decentralized cryptocurrencies, including bitcoin, do not have a third-party promoter that investors rely on. Sidechain projects have no expectation of profit because the value of a sidechain coin is pegged to pre-existing bitcoins. Similarly, platforms that create and use tokens for a particular use or application, such as Ethereum, do not create an expectation of profit. Finally, cryptocurrencies
distributed through competitive mining or similar processes do not involve the investment of money, and should not be treated as securities.

On the other hand, securities regulation may be appropriate where a digital currency is distributed through pre-sales from a small and non-diverse developer group. Oversight is particularly important where the cryptocurrency is not transparent, because the trust of investors is based mostly on a promoter’s actions. Permissioned ledgers are also a better fit for the Howey test because the central authority may play the role of a third-party promoter.

Coin Center believes this approach aligns with the purpose of the securities laws and would lead to positive policy outcomes. The proposal would protect investors by regulating the cryptocurrencies that pose the greatest risk, while avoiding unnecessary regulation on relatively safer options.

With a framework instead of a bright-line rule, it won’t always be clear whether a cryptocurrency is a security or not. Still, Coin Center has articulated a comprehensive view of how digital currencies interact with securities laws, which will be useful as federal and state regulators think about how to approach bitcoin and other digital currencies.