

Humpty Dumpty Sat on the Wall: Cryptocurrency, Money Laundering, and Smart Contracts all Might Take a Great Fall

Speakers:

Daniel B. Garrie, Esq., Co-founder, Law & Forensics; Mediator, Arbitrator, and eDiscovery Special Master, JAMS

David A. Cass, Senior Partner, Law & Forensics, Adjunct Faculty Harvard & Rutgers Law

Steve Pearlman, US Chief Compliance Officer, Revolut Technologies

(c) 2021 Lexeprint Inc. All Rights Reserved

Speakers



Daniel B. Garrie, Esq.
Co- founder, Law & Forensics
Mediator, Arbitrator, and eDiscovery
Special Master, JAMS



David A. Cass
Senior Partner, Law & Forensics
Adjunct Faculty Harvard & Rutgers
Law



Steve Pearlman
US Chief Compliance Officer
Revolut Technologies

(c) 2021 Lexeprint Inc. All Rights Reserved

Disclaimer

This is not legal advice nor should it be considered legal advice.

This presentation and the comments contained therein represent only the personal views of the participants, and do not reflect those of their employers or clients.

This presentation is offered for educational and informational uses only.

(c) 2021 Lexeprint Inc. All Rights Reserved



A Primer on Money Laundering with Cryptocurrency

(c) 2021 Lexeprint Inc. All Rights Reserved

This Photo by Unknown Author is licensed under CC BY

A Primer on Money Laundering with Cryptocurrency

Three key stages:

- Placement
- Layering
- Integration



This Photo by Unknown Author is licensed under CC BY-SA

(c) 2021 Lexeprint Inc. All Rights Reserved

Placement

- The placement stage is the taking of illicit funds and moving it into the financial ecosystem. This is like an exchange - Ransomware, Drugs, Weapons, Passports
- As this is considered the riskiest stage of money laundering, this risk increases the distinctive traits of the crypto economy, making it more attractive to money launderers.



(c) 2021 Lexeprint Inc. All Rights Reserved

Layering: Hide Where the Money Came From

- Mixers/Tumblers - Cryptocurrency Mixing (Tumblers) – take a user's crypto and mix their crypto with other user's crypto currency by sending it through a series of different addresses and then recombining them to give a "clean" appearance
- Third-party wallets
- Chain hopping: This is a common method of layering with cryptocurrencies, that makes the origins of transactions nearly impossible to trace.
- Alt-coins: This is where the "best-known cryptocurrencies are exchanged for "alt-coins", or less well-known cryptocurrencies, which can only be purchased at advanced exchanges using other forms of cryptocurrency and not cash."
- Gambling sites -- Dual purpose in integration as well
- Governments



(c) 2021 Lexeprint Inc. All Rights Reserved

Integration – Using the Funds to Buy Legitimate Assets

- Using P2P payment networks in other countries with more lax security controls than those in the U.S.
- Crypto P2P Networks – A lot of them are based in countries with less or limited enforcement or less stringent AML regulations. Convert crypto to fiat to purchase other goods.
- Gambling sites – Several accept crypto in exchange for chips and allow the user to cash out in fiat.



(c) 2021 Lexeprint Inc. All Rights Reserved

Integration - "Clean Money"

- Property
- NFTs
- Cashing out in fiat
- Crypto ATMs – Allow the purchase of crypto with credit/debit cards. Some even accept cash for immediate exchange into cryptocurrency. It can be hard to do KYC with these machines depending on what country they are in.
- Paying bills etc.



(c) 2021 Lexeprint Inc. All Rights Reserved



Regulators

(c) 2021 Lexeprint Inc. All Rights Reserved

This Photo by Unknown Author is licensed under CC BY-SA

Regulatory Landscape

- There is no one regulator for crypto in the U.S – State and Federal
- There are many regulators with different definitions
- The U.S Treasury's view as a virtual decentralized currency - not legal tender. If you process it, it may be considered a money transmitter subject to FinCEN requirements
- IRS defined as property – capital gains
- CFTC defined Bitcoin as a commodity



(c) 2021 Lexeprint Inc. All Rights Reserved

Public Policy

- Ensure financial stability
- Protect investors against fraud and other threats
- Ensure the integrity of markets
- General goal of public policy frameworks includes guarding against illicit activities



(c) 2021 Lexeprint Inc. All Rights Reserved

AML Regulations - The Impact of Crypto

- Financial Action Task Force (FATF) published its guidance for virtual assets and virtual asset service providers (VASP).
- Monitory Authority of Singapore (MAS)'s Payment Services Act & proposed another set of regulations
- EU AML Directive 5
- Financial Crimes Enforcement Network (FinCEN) & State requirements such as BitLicense



(c) 2021 Lexeprint Inc. All Rights Reserved



Lawyers

(c) 2021 Lexeprint Inc. All Rights Reserved

This Photo by Unknown Author is licensed under CC BY-NC-ND

Counterparty Risk

- Hit innocent person because you got the bad actor wrong.
- SEC – Bitcoin assets or tokens may be defined as a security
  - 75 enforcement actions to date
- State and municipality approaches vary i.e: Wyoming – Special Purpose Depository Institution



(c) 2021 Lexeprint Inc. All Rights Reserved

Other Legal Risks

- Privacy Risks
- GDPR and CCPA requirements potentially conflict with Append Only ledgers



(c) 2021 Lexeprint Inc. All Rights Reserved



Law Enforcement

(c) 2021 Lexeprint Inc. All Rights Reserved

This Photo by Unknown Author is licensed under CC BY-ND

"WILD WEST" Crypto economy

- SEC's Chairman, Gary Gensler noted that they will "police cryptocurrency markets to the maximum extent possible." However, he describes the current level of protection for investors in crypto as the "wild west."
- The Chairman continues to call on Congress to approve the 'agency with more authority and resources to regulate the sector.'
- As there is no single regulator overseeing crypto exchanges or brokers, scams and the market value of the asset class has drastically increased.



(c) 2021 Lexeprint Inc. All Rights Reserved



Smart Contracts: The Good, the Bad and the Ugly

(c) 2021 Lexeprint Inc. All Rights Reserved

The Good

- Transformative for the industry
- Faster transactions
- Little or no intermediaries required



(c) 2021 Lexeprint Inc. All Rights Reserved

The Bad

- Poor coding or limited understanding of how the code is implemented
- Risk of security breaches
- Improper administration
- Lack of a governance or control process



(c) 2021 Lexeprint Inc. All Rights Reserved

The Ugly

Small – lose some money

Medium – lose all your money

Big – lose it all and pay lawyers!



(c) 2021 Lexeprint Inc. All Rights Reserved

Smart Contracts in the Future

- FUBAR (Fouled Up Beyond All Recognition/Recovery/Reason/Any Repair)
- Finance Smart Chain has many Fubar Defi smart contracts.
  - Those that are “food” plus “Swap” are mostly Fubar.
- Example:
  - Pancake Swap -- https://decrypt.co/61431/pancakeswap-hacked



This Photo by Unknown Author is licensed under CC BY-NC-ND

(c) 2021 Lexeprint Inc. All Rights Reserved

The TAKE-AWAY

- While cryptocurrency has an ever growing potential to change the financial system for the better, financial risks will continue to increase.
- Threat actors will continue to create new ways to take advantage of the crypto economy's weaknesses and legal gaps.
- To effectively manage the growing risks of businesses that relate to cryptocurrency, anti-money laundering and compliance professionals should become familiar with the unique traits of cryptocurrency and how threat actors can utilize these traits.

(c) 2021 Lexeprint Inc. All Rights Reserved

This Photo by Unknown Author is licensed under CC BY-NC-ND

Contact Us



Daniel B. Garrie
Email: daniel@lawandforensics.com
Phone: 855-529-2466
URL: www.lawandforensics.com



David Cass
Email: davidcassciso@gmail.com
URL: https://www.newyorkfed.org/



Steve Pearlman
Email: steve.pearlman@revolut.com

(c) 2021 Lexeprint Inc. All Rights Reserved



Daniel B. Garrie, Esq.
Law & Forensics – Co-founder
JAMS – Mediator, Arbitrator, eDiscovery Special Master
Contact:
W: (855) 529-2466
E: daniel@lawandforensics.com
URL: www.lawandforensics.com

B.A., Computer Science, Brandeis Uni.
M.A., Computer Science Brandies Uni.
J.D., Rutgers School of Law

Daniel Garrie is the Co-Founder of Law & Forensics LLC, Head of Computer Forensics and Cyber Security Practice Groups and has been a dominant voice in the computer forensic and cybersecurity space for over 20 years. Prior to Daniel's legal career, he successfully built and sold several technology start-up companies. Since co-founding Law & Forensics LLC in 2008, Daniel has built it into one of the leading boutique cybersecurity forensic engineering firms in the industry. Daniel has both a Bachelor's and a Master's Degree in computer science from Brandeis University, as well as a J.D. degree from Rutgers Law School. Daniel has led forensic teams in some of the most visible and sensitive cyber incidents in the United States. In particular, Daniel recently located and recovered deleted files in both private and public cloud computing environments using his patented software, Forensic Scan. This investigation took less than forty-eight hours to clean and recover the data from the servers of a cloud-hosting provider that was compromised by a malicious cyber-attack. Thanks to the Forensic Scan technology, that Daniel co-invented and patented (US9990498B2 and US9990497B2), and his own expertise, Daniel and his team was able to identify the source of the breach and remediate the problem in record time.

Daniel regularly testifies as an e-discovery, cybersecurity and computer forensic expert witness, authoring forensic expert reports on multi-million-dollar disputes. His ability to perform complex investigations and effectively communicate the results to a jury has made him one of the most sought-after experts in the country. His testimony has been pivotal in a number of cases, including one involving the embezzlement of millions of dollars from a large non-profit. Daniel was able to perform a thorough analysis of the alleged embezzlers' phone and computer, despite the embezzlers' attempts to wipe them, and identify concrete evidence of the embezzlement to a jury. Since 2008, Daniel has served as a Neutral and Special Master and in 2016, he joined JAMS as one of the organization's youngest Neutrals. At JAMS, Daniel serves as an Arbitrator, Forensic Neutral, and technical Special Master with a focus on cybersecurity, cyrptocurrency, and complex software and technology related disputes. Some of the major cases for which he has served as an e-discovery special master, or forensic neutral include: *Hougan vs. City of Newport Beach, No. 30-2012-00582855* (Super. Ct. Cal. 2014)*; Small v. University Medical Center of Southern Nevada, 2014 WL 4079507*(D. Nev. 2014)*; C.D.S. Inc. v. Zelter and Amazon Web Services, Inc.*, (S.D.N.Y. 2016); *Jawbone, Inc. v. Fitbit Inc.* et al (Super. Cal., S.F. County 2018). In addition to his vast litigious experience, Daniel is well-published in the cybersecurity space, Editor-in-Chief of the Journal of Law & Cyberwarfare, author of more than 200 articles and books including, "Understanding Software, the Internet, Mobile Computing, and the Cloud. A guide for Judges", published by the Federal Judicial Center. He has been recognized by several United States Supreme Court Justices for his legal scholarship and is a trusted source and a thought leader for cybersecurity articles and opinions, being cited over 500 times to date.

(c) 2021 Lexeprint Inc. All Rights Reserved



David Cass
Law and Forensics Senior Partner
Contact:
E: david@lawandforensics.com
URL: www.lawandforensics.com

LAW & FORENSICS
A Global Legal Engineering Firm

Mr. Cass recently joined Law and Forensics as a Senior Partner. He leads the Crypto & Digital Banking Practice and is a key member of the Cybersecurity & Privacy practice. Prior to joining, David served as a regulator. He was the Vice President for Cyber & IT Risk for the Federal Reserve Bank of New York. David specialized in large institution supervision, Fin-Tech, AI/ML, and cryptocurrencies. Prior to this role, David served as the Chief Information Security Officer for IBM. He had global responsibility for all aspects of security practices, processes, and policies across the IBM Cloud SaaS business unit.

Previously David served as the SVP & Chief Information Security Officer for Elsevier, where he led an organization of experienced legal, risk and security professionals that provided data protection, privacy, security, and risk management guidance on a global basis for Elsevier.

David has extensive experience in IT security, risk assessment, risk management, business continuity and disaster recovery, developing security policies and procedures. He has played a key role in leading and building corporate risk & governance and information security organizations in the financial sector. As the Senior Director of Information Security Risk and Governance for Freddie Mac, David rebuilt the risk and governance function and developed a team to provide risk assessments, methodologies, tools, services, and training to improve the organization's capabilities and maturity. Prior to that he was Vice President of Risk Management for JPMorgan Chase and was responsible for providing an accurate assessment of the current risk management state, contributing to the future direction of risk management, continuity and disaster recovery capabilities for the organization.

David has a MSE from the University of Pennsylvania, and a MBA from MIT. He is adjunct faculty for Rutgers Law School and Harvard. He is also a frequent speaker at high profile industry conferences and served on several boards.

(c) 2021 Lexeprint Inc. All Rights Reserved



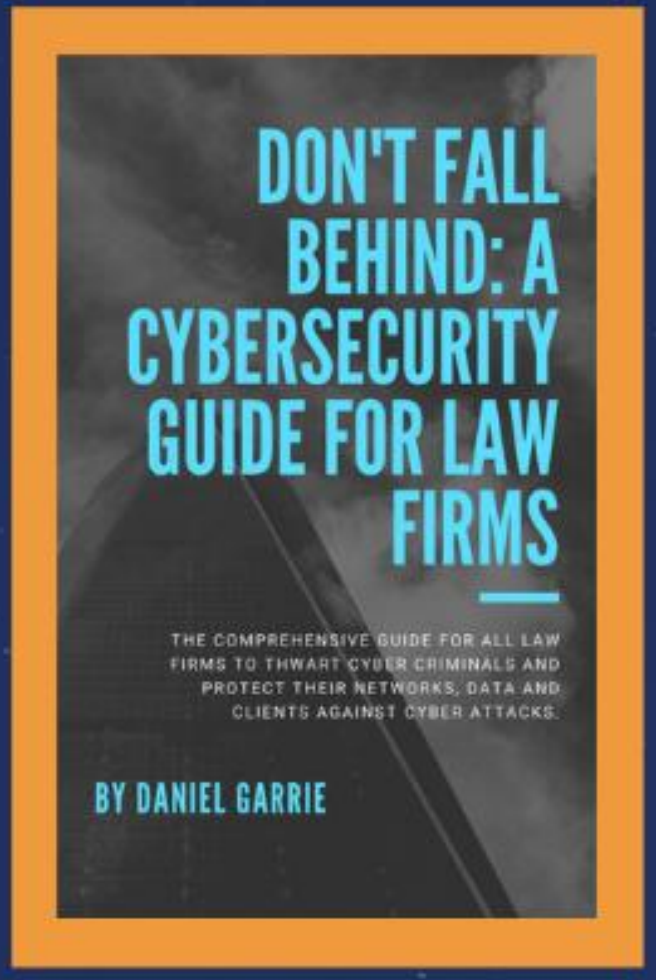
Steve Pearlman
US Chief Compliance Officer
Revolut Technologies
Contact:
E: steve.pearlman@revolut.com

Steve Pearlman is the US Chief Compliance Officer for Revolut Technologies which offers a technology platform in the US that allows customers access to banking, payment and crypto services. Steve is an experienced compliance executive and attorney with over 25 years' experience in Fintech, banking and consumer compliance having had senior compliance roles at E*TRADE and Freddie Mac and served as a compliance consultant.

Prior to joining Revolut as US Chief Compliance Officer in early 2021, Steve was the Chief Compliance Officer at E*TRADE Bank, a national bank with over $50 Billion in assets and E*TRADE Savings Bank, a national bank subsidiary of E*TRADE Bank. He has also served as a Senior Director at Treliant Risk Advisors, Deputy Chief Compliance Officer for Freddie Mac and Director of Compliance at Capital One. He holds a Bachelor of Arts from Duke University, Juris Doctor from University of Michigan School of Law and is a Certified Regulatory Compliance Manager (CRCM).

(c) 2021 Lexeprint Inc. All Rights Reserved

A CYBERSECURITY GUIDE FOR LAW FIRMS



"NO ONE IS IMMUNE TO A CYBERSECURITY INCIDENT. EVERY INDUSTRY AND BUSINESS SECTOR—INCLUDING THE LEGAL PROFESSION—IS A TARGET FOR HACKERS AND CYBER CRIMINALS. AS EARLY AS 2009, THE FBI FLAGGED THE LEGAL INDUSTRY AS A GROUP THAT WAS VULNERABLE TO CYBER ATTACKS, ISSUING AN ADVISORY THAT HACKERS WERE INCREASINGLY TARGETING LAW FIRMS."



AVAILABLE ON:

amazonkindle AND PAPERBACK!

Buy Now

(c) 2021 Lexeprint Inc. All Rights Reserved

Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

FinCEN's New Adviser Aims To Crack Down On Crypto Crime

By **Al Barbarino**

Law360 (July 29, 2021, 8:23 PM EDT) -- Michele Korver's career has led her into the deepest parts of the criminal underworld, hunting criminals who use digital currencies to finance their misdeeds.



Michele Korver

But as debate rages over the regulation of digital assets, there are no hard feelings regarding crypto from Korver, who became the Financial Crimes Enforcement Network's first-ever chief digital currency adviser **earlier this month**.

"To me, it's just another means of payment or value transfer that's developed over time, just like any financial technology," said Korver, a longtime government attorney and adviser focused on digital assets. "It's something that exists in the financial ecosystem that we focus on in the same way that we do any other means of payment or value transfer."

In fact, Korver said she finds the digital assets space and related technological innovations cool and interesting. And as part of her work tracking down illicit activity, crypto can in some cases be easier to trace than cash, she noted.

In her most recent role as the U.S. Department of Justice's digital currency counsel, Korver advised government attorneys, federal agents and the U.S. Department of the Treasury on prosecutorial strategies, crypto seizure and forfeiture policy.

Prior to that, her experience includes 10 years as an assistant U.S. attorney in Colorado, where as a lead prosecutor she helped bring down the so-called ItalianMafiaBrussels, a drug trafficking organization that exclusively accepted bitcoin as payment.

In an interview with Law360, Korver talked about her goals for her latest endeavor, the role that crypto is currently playing in criminal activity, and what she and the broader regulatory community can do to keep it in check.

This interview has been edited for length and clarity.

Your new role is as FinCEN's first-ever digital currency adviser. Why do you think this position was created and is needed now?

FinCEN has always been ahead of the curve when it comes to the regulation of value transfers, payments and entities providing financial services, even in these new technologies such as blockchain or distributed ledger technology. As early as 2011, just a couple of years following the launch of the first decentralized cryptocurrency, bitcoin, FinCEN published their regulation broadly defining money transmission. In 2013, and again in 2019, FinCEN issued guidance following that regulation that applies directly to convertible virtual currency activities and business models.

The team is growing to match the increase in activity involving cryptocurrency as well as the number of covered entities that are providing these CVC money transmission services as the technology continues to develop, particularly in the financial ecosystem.

What are your key responsibilities and goals?

My role is in the office of the director, advising FinCEN acting Director Michael Mosier and Deputy Director AnnaLou Tirol and leading the work with internal and external partners on strategic and innovative solutions that help prevent and mitigate illicit financial practices. The role includes work across all of FinCEN's respective divisions, whether advising on civil enforcement actions or assisting the policy division on legislative proposals or rulemaking. Externally, I'll be representing FinCEN at interagency meetings or working groups engaging with the private industry, including through our FinCEN Exchange events and Innovation Hours.

My goals are the same as the agency's goals: to understand the methods, products and services that can be used for money laundering, terrorist financing and illicit finance. For me specifically, I'll be assisting FinCEN with its responsibilities for enforcing the Bank Secrecy Act as it relates to CVCs, digital currencies and blockchain technologies. That includes ensuring compliance among those who provide financial services involving crypto or who serve as financial gatekeepers of these types of products and activities.

What are you looking forward to most?

I'm looking forward to working at an agency that approaches things from a different angle than we did when I was a prosecutor at the DOJ. I like to change things up, and I'm also looking forward to seeing what the changes are going to be in the industry, because I love to tackle new projects and to think creatively outside the box. It'll be interesting to see, as the technology very quickly changes in this area, how we adapt to meet our goals.

Do you think the mainstream adoption of crypto by banks and payment companies is positive or negative from a crime-detection standpoint?

To me, it's just another means of payment value transfer that's developed over time, just like any financial technology. It's funny, I date myself sometimes when I think about what everybody must have thought when the Diners Club card came out. [*Laughs*] But financial technologies evolve over time, and the innovation of money payments and value transfer will continue. The criminal use of the financial ecosystem will always exist, too. The government agencies tasked with protecting our financial system and citizens can address these issues through appropriate regulations, as well as through civil and criminal enforcement of law as appropriate.

Personally, I've worked in this space for a long time, and I think these emerging technologies are cool and interesting. From my position in the government, it's something that exists in the financial ecosystem that we focus on in the same way that we do any other means of payment or value transfer.

There's been much debate lately among lawmakers and other stakeholders over the regulation of crypto. What do you make

of it?

These kinds of letters and legislative proposals and calls to action in the crypto space are nothing new. I've been seeing this stuff all the way back to, I want to say 2017, when I actually got hired by [the DOJ] in the Money Laundering and Asset Recovery Section [as its first full-time adviser on crypto-related prosecutions and forfeitures]. There's been a steady flow of these types of requests and suggestions and proposals for the filling of gaps. I think it has come back around again because of the recent ransomware attacks and the focus on that. So obviously there is a lot of attention on this right now, but these kinds of discussions have been happening for a long time.

What do you think needs to be done to control the recent wave of cybercrimes and hacking, which often end in ransom payments paid in crypto?

FinCEN, along with its law enforcement partners, is going to continue to use the many legal authorities and investigative tools we have to address this activity. That includes holding covered entities such as cryptocurrency exchanges and other financial service providers to their obligations under the Bank Secrecy Act. Our primary mission is to administer the BSA to ensure that the entities providing financial services are not allowing their platforms to be used for illicit purposes.

What is it about crypto that's attracted criminal elements and money laundering?

The global reach and speed at which the transactions occur without ever having to touch a financial intermediary is what is likely attracting criminals. Also, you can send very large dollar amounts of crypto cross-border with just the push of a button on your phone, making it an attractive money laundering tool compared to cash, which can be physically burdensome to transfer in bulk and, of course, comes with the risk that you're going to be caught holding the bag.

So in terms of cash versus crypto, what's easier to trace?

I think they both have their pros and cons for anti-money laundering efforts. One of the benefits of crypto for those who are tasked with following the money, so to speak, is that for the cryptocurrency to operate on transparent blockchain there is the visible and immutable record in those blockchains. That allows us to effectively trace the transactions. Generally, the same is not true for cash transactions, unless the cash touches an intermediary that has reporting requirements or the transaction is subject to physical surveillance. So there's actually a lot of visibility with crypto that you don't have with cash.

Looking back, what was your most memorable or important case while at the DOJ?

The ItalianMafiaBrussels drug trafficking organization case was particularly interesting and important because it involved multiagency U.S. law enforcement as well as working collaboratively with our international law enforcement partners. This was a drug trafficking organization operating in various darknet markets, and a lot of the evidence and details of the case involved the use of cryptocurrency. They were shipping boatloads of illegal substances to customers primarily in the U.S. and some in Canada, while operating out of different countries and jurisdictions in the EU.

As the lead prosecutor assigned to the investigative team, you run the case from the minute it's opened through the entire investigation, including the collection of the evidence and all the legal tools you use all the way to sentencing. We successfully shut down the organization. It resulted in the extradition, conviction and sentencing of its leaders, who were operating in a number of countries but primarily out of Romania. There were seizures of assets and a substantial money judgment that was part of the sentence with the lead defendant. [The organization was dismantled in 2016, and its leader received an 11-year prison sentence in 2018].

--Editing by Alanna Weissman.

All Content © 2003-2021, Portfolio Media, Inc.

LAW360®

Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Anti-Money Laundering Risks Amid Rising NFT Popularity

By **Katherine Kirkpatrick, Luke Roniger and Read Mills** (May 21, 2021, 4:47 PM EDT)



Katherine Kirkpatrick



Luke Roniger



Read Mills

While nonfungible tokens, or NFTs, have existed for several years, the market for NFTs grew considerably during 2020 and into 2021, as a number of high-profile NFT sales grabbed headlines and well-known brands and organizations began exploring the use of NFTs.

One report shows that NFT sales in the first quarter of 2021 grew to more than $2 billion, over 20 times the volume of the previous quarter.[1]

As the NFT market and the digital art world continue to grow and as prices soar, NFT marketplaces specializing in digital art may become subject to suspicious activity reporting standards under the Bank Secrecy Act. On Jan. 1, Congress passed the Anti-Money Laundering Act, which provides the most comprehensive update to anti-money laundering laws under the BSA since the USA Patriot Act.[2]

Both the AMLA and BSA enable the U.S. Department of the Treasury's Financial Crimes Enforcement Network to regulate the activity of financial institutions, including through various record-keeping and reporting obligations. Although the AMLA does not directly mention NFTs, several provisions ought to be considered by individuals and financial institutions contemplating NFT transactions.

Is an NFT a value that substitutes for currency or funds?

Although the AMLA formally extended BSA reporting obligations to cryptocurrency exchanges, direct regulation of NFTs and related marketplaces will require additional action by Congress.

Section 6102(d) of the AMLA expanded the definition of "financial institutions" to include businesses involved in the exchange of "value that substitutes for currency or funds," thus codifying FinCEN's long-standing position that cryptocurrency exchanges — which convert fiat currency such as the U.S. dollar into cryptocurrency and vice versa — are money services businesses subject to BSA reporting requirements.[3]

This requires cryptocurrency exchanges to engage in customer due diligence to verify the identity of their customers, identify any beneficial owners of accounts, develop customer risk profiles and monitor transactions to submit suspicious activity reports, among other things.[4]

Cryptocurrencies are clearly a value that substitutes for currency, but it is less likely NFTs would be deemed the same. Currencies and their substitutes derive their utility, in part, from their inherently fungible nature.[5] Generally speaking, NFTs would not be considered a currency nor a substitute because, by definition, they lack fungibility.

NFTs are more akin to legal instruments, such as a deed, containing a unique signature demonstrating ownership of an asset. That lack of fungibility arguably pushes NFTs outside the reach of the AMLA, and further action from Congress would be necessary to apply anti-money laundering regulations to NFTs and their marketplaces directly.

FinCEN has yet to issue anything specifically on NFTs, and has similarly not indicated whether NFT players are or may become subject to the AML regime. That said, regulators have certainly begun formalizing procedures for applying current laws to digital assets.

Just one example is the U.S. Department of Justice's recently published Asset Forfeiture Policy Manual that provided guidance regarding seizure of cryptocurrencies and digital tokens.[6] And given the high degree of scrutiny and ongoing expansion of AML obligations to the cryptocurrency space, NFTs may not escape additional rulemaking or legislation.

Are NFT marketplaces art dealers?

As explained more fully below, Congress is in the process of expanding the BSA's reach and could reasonably conclude that NFT exchanges constitute art dealers and should therefore be subject to the law's reporting requirements.

The AMLA sought to address, among other things, the multibillion-dollar black market trade in art and antiquities, which is estimated to be the "third largest type of black market after illegal drugs and the arms trade."[7]

Forthcoming regulations from FinCEN are expected to expand BSA reporting obligations to antiquities dealers, and in January 2022 Congress is scheduled to receive the results of an ongoing study by FinCEN that will "inform debates over whether to extend BSA requirements to art dealers."[8]

Extending reporting obligations to art dealers could have the effect of sweeping NFT exchanges into the scope of such obligations. If reporting obligations are extended, art dealers will be required to grapple with a number of anti-money laundering protocols more familiar to financial services entities. The rule would also make it far more difficult for buyers and sellers to obscure their identities through shell companies or offshore entities.

NFT marketplaces such as OpenSea, Rarible and SuperRare function much like an auction house or an art dealer by connecting buyers and sellers who transact directly. In fact, SuperRare describes itself as "Instagram meets Christies,"[9] and Mark Cuban is building an online art gallery to display his NFTs.[10]

Given their similarities, NFT marketplaces share many of the characteristics that make the art trade susceptible to money laundering — namely, "buyer secrecy, informal and self-regulated markets, non-transparent pricing, [and] high value transactions," according to a Standard Chartered PLC report.[11]

In early March, for example, an NFT consisting of a digital copy of a limited-edition Banksy print sold for nearly $400,000 in Ethereum on OpenSea to a bidder with the screen name GALAXY, whose profile lacks any identifying information.[12]

The buyer behind the $69.3 million sale of "Everydays: The First 5000 Days" by Beeple was also initially pseudonymous, although the purchaser later revealed his identity.[13]

Given that many of these transactions are completed using cryptocurrencies — which can be hard to trace to actual individuals — the NFT trade faces similar money laundering risks as the art trade more generally.[14] As Congress considers subjecting art dealers to the BSA, it could also decide to define "art dealers" broadly to bring NFT marketplaces specializing in digital art within the BSA's ambit.

In addition, several prominent auction houses have started to participate in NFT sales,[15] and those firms should be mindful that the compliance considerations applicable to traditional art sales

should be applied to NFT sales as well.

Tumblers present NFT and anti-money laundering risks.

So-called tumbling poses an added layer of anti-money laundering concerns with respect to NFTs. One distinct feature of cryptocurrencies is that the ownership history of a particular coin can be traced, as each transaction is publicly recorded on the blockchain.[16]

Cryptocurrencies are held in wallets, which function as the digital address, or identity, of the wallet holder.[17] When a cryptocurrency coin is passed to another wallet, the data is recorded in a transaction block that lists the digital wallet addresses of the sender and recipient.[18] Each transaction block is then automatically recorded and stored publicly on the blockchain, which functions as a public digital ledger of all transactions.[19]

Working backward, it is generally possible to trace the ownership history of a coin by analyzing the coin's transaction blocks to see all the digital wallets through which it has passed.[20] Although the digital addresses of each wallet do not directly identify the actual owner, wallets can be linked to real people by mapping IP addresses and other forms of data analytics.[21]

Cryptocurrency tumblers can increase the difficulty of tracing a coin's ownership history, however, by circulating that coin through multiple transactions[22] and thus washing its potential connection to suspicious wallets or transactions.[23] Significant time, patience, data and processing power is required to "untumble" coins — the more a coin is tumbled, the harder it is to trace.[24]

FinCEN guidance considers cryptocurrency tumbling to be a money transmitting business, thus requiring registration with FinCEN, compliance with both BSA reporting requirements and know-your-customer due diligence obligations, and implementation of an anti-money laundering compliance program.[25]

This guidance has been tested and upheld in U.S. v. Harmon, an ongoing criminal money laundering case in the U.S. District Court for the District of Columbia against Larry Dean Harmon for operating Helix — a tumbling service that was allegedly used on the dark web to conceal cryptocurrencies used for black-market activities.[26]

Harmon was indicted for money laundering and operating an unlicensed monetary business in violation of the BSA. In upholding the indictment, the court noted that tumblers "work by literally mixing up a user's payment with lots of other payments from other users" to obfuscate their ownership history, thus qualifying as a money transmitting business by "receiving bitcoin and transmitting that bitcoin to another location or person."[27]

The Harmon prosecution is still ongoing with jury selection set for later this year,[28] and it is possible that the district court's rationale in upholding the indictment could be reevaluated on appeal.

Theoretically, NFT marketplaces could be leveraged to achieve the same result as tumbling.[29] Given the extraordinarily high value of some NFTs, individuals could execute multiple NFT transactions whereby a significant number of coins are spread to different accounts.

By repeating this process, individuals could distance themselves from coins linked to dark web activities or cryptocurrency exchanges that do not comply with anti-money laundering and customer due diligence requirements. In short, NFT transactions could be used as another way to add multiple "blocks" to a coin's ledger, thereby obfuscating the transaction history and associated accounts.[30]

Although NFT marketplaces may in some cases help obfuscate ownership of cryptocurrency linked to illicit activities, NFT marketplaces are unlikely to qualify as a money transmitting business because they merely (1) allow NFT purchasers and sellers to connect and transact without an intermediary, i.e., a peer-to-peer platform, and (2) do not directly handle or otherwise process the cryptocurrencies used to purchase NFTs. Indeed, one DappRadar blog post described an NFT

marketplace as "eBay on the blockchain."[31]

Given that NFT marketplaces pose similar money laundering risks as auction houses and art dealers involved in high-value transactions, Congress could decide to independently subject NFT marketplaces to BSA reporting requirements, know-your-customer due diligence, and other requirements.

Regardless of future regulatory changes, crypto exchanges and traditional financial institutions handling NFT transactions should beware of obligations for reporting suspicious activity.

Both cryptocurrency exchanges and traditional financial institutions are subject to the BSA and therefore may be required to file suspicious activity reports, or SARs, for transactions involving NFTs for digital art and other tethered assets.

In fact, recent guidance from FinCEN was issued to "provide specific instructions for filing SARs related to trade in antiquities and art."[32] Under the guidance, to comply with BSA obligations, financial institutions — a definition that now includes cryptocurrency exchanges — are required to submit SARs for suspicious activity related to art and antiquities.

The guidance explains that SAR filings should:

- Include a detailed description of how the questionable activity is tied to art and antiquities;
- Provide identifying information, including IP addresses, for the purchasers, sellers, and any other intermediaries or agents; and
- State the volume and dollar amount of the suspicious transactions.

Additionally, SARs ought to identify any "other transactions or proposed transactions that may involve antiquities or art" and identify where the reported individuals or entities are currently operating.

Given the similar money laundering risks shared between high-value art transactions and NFTs, financial institutions and cryptocurrency exchanges may be obligated to file SARs when executing NFT transactions on behalf of their clients. They should therefore have in place controls for identifying suspicious activity relating to NFTs, as well as determining when and how to report it.

Conclusion

Traditional financial institutions are no strangers to the stringent BSA and other anti-money laundering compliance requirements. Those institutions' involvement with NFT-related transactions may generate new compliance obligations.

Unless and until NFT-specific guidance is provided, companies should look to guidance on analogous services and products. Given the money laundering risks shared between NFTs and the art and antiquities markets, financial institutions should pay special attention to the opaque and often anonymous NFT market and should consider filing SARs if they detect any suspicious activity related to an NFT transaction.

In this rapidly evolving area, both financial institutions and cryptocurrency exchanges should also consider reexamining their existing anti-money laundering compliance programs to meet the needs of their clients and federal regulators.

Katherine Kirkpatrick is a partner, and Luke Roniger and Read William Mills are associates, at King & Spalding LLP.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] See Robert Frank, NFT sales top $2 billion in first quarter, with twice as many buyers as sellers, CNBC (Apr. 13, 2021), available at https://www.cnbc.com/2021/04/13/nft-sales-top-2-billion-in-first-quarter-with-interest-from-newcomers.html.

[2] Anti-Money Laundering Act of 2020, Pub. L. No. 116-283, H.R. 6395, 116th Cong. § 6101 et seq. (enacted Jan. 1, 2021) (to be codified at 31 U.S.C. § 5323), available at https://www.govtrack.us/congress/bills/116/hr6395/text.

[3] Fin. Crimes Enf't Network, U.S. Dep't of the Treasury, FIN-2019-G001, Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies 3 (2019), available at https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

[4] See 31 C.F.R. § 1010 et seq.

[5] C.f. United States v. Faiella , 39 F. Supp. 3d 544, 545 (S.D.N.Y. 2014) (finding that Bitcoin qualifies as money precisely because "Bitcoin can be easily purchased in exchange for ordinary currency, acts as a denominator of value, and is used to conduct financial transactions"); United States v. Ulbricht, 31 F. Supp. 3d 540, 570 (S.D.N.Y. 2014) (defining "money" as "an object used to buy things" and concluding that "the only value for Bitcoin lies in its ability to pay for things" because "Bitcoins can be either used directly to pay for certain things or can act as a medium of exchange and be converted into a currency which can pay for things"). See also Sebastian Omlor, The CISG and Libra: A Monetary Revolution for International Commercial Transactions?, 3 Stan. J. Blockchain L. & Pol'y 83, 90 ("The two basic functions of money are to be a unit of account and a universal means of exchange.").

[6] See U.S. Dep't of Justice, Asset Forfeiture Policy Manual 26 (2021), available at https://www.justice.gov/criminal-afmls/file/839521/download.

[7] Combating Illegal Antiquities Trade, Standard Charted Bank (Dec. 2018), available at https://av.sc.com/corp-en/others/Combating-Illegal-Antiquities-Trade_FINAL.pdf.

[8] Transnational Crime Issues: Arts and Antiquities Trafficking, Congressional Research Service (Mar. 1, 2021), https://crsreports.congress.gov/product/pdf/IF/IF11776.

[9] Frequently Asked Questions, SuperRare (last visited May 3, 2021), available at https://superrare.co/about.

[10] Shalini Nagarajan, Billionaire Mark Cuban is setting up a digital art gallery that allows users to display NFTs in any form, report says, Business Insider (Mar. 24, 2021), available at https://markets.businessinsider.com/news/stocks/billionaire-mark-cuban-setting-up-digital-art-gallery-for-nfts-2021-3-1030240151.

[11] Combating Illegal Antiquities Trade, supra at note 12, available at https://av.sc.com/corp-en/others/Combating-Illegal-Antiquities-Trade_FINAL.pdf.

[12] See Jamie Redman, Burned Banksy NFT Sale Captures Close to $400K, Critics Claim Buyers Are 'Morons', Bitcoin.com (Mar. 8, 2021), available at https://news.bitcoin.com/burned-banksy-nft-sale-captures-close-to-400k-critics-claim-buyers-are-morons/; User Profile: "Galaxy", OpenSea, available at https://opensea.io/accounts/GALAXY.

[13] Robert Frank, Crypto investor who bought Beeple's NFT for $69 million says he would have paid even more, CNBC (Mar. 30, 2021), available at https://www.cnbc.com/2021/03/30/vignesh-sundaresan-known-as-metakovan-on-paying-69-million-for-beeple-nft.html.

[14] See United States v. Harmon, No. 19-CR-395-BAH, 2021 WL 1518344 (D.D.C. Apr. 16, 2021) (explaining the role of cryptocurrency "tumblers" in relation to multi-count money laundering indictment against the operator of a tumbler service). For a general overview of the difficulty of tracing the ownership history of cryptocurrencies, see P. Vigna and C. Ostroff, Why Hackers Use Bitcoin and Why It Is So Difficult to Trace, Wall Street J. (July 16, 2020) available at https://www.wsj.com/articles/why-hackers-use-bitcoin-and-why-it-is-so-difficult-to-trace-11594931595.

[15] See, e.g., Lucas Matney, CryptoPunks NFT bundle goes for $17 million in Christie's auction, TechCrunch (May 11, 2021), available at https://techcrunch.com/2021/05/11/cryptopunks-nft-bundle-goes-for-17-million-in-christies-auction/.

[16] See John Bohannon, Why criminals can't hide behind Bitcoin, Science Magazine (Mar. 9, 2016), available at https://www.sciencemag.org/news/2016/03/why-criminals-cant-hide-behind-bitcoin.

[17] Id. at 17.

[18] Id.

[19] Id.

[20] See id. at 46.

[21] See John Bohannon, Why criminals can't hide behind Bitcoin, Science Magazine (Mar. 9, 2016), available at https://www.sciencemag.org/news/2016/03/why-criminals-cant-hide-behind-bitcoin.

[22] See Mark Rash, Bitcoin Tumbling Leads to Multicount Indictment, Security Boulevard (Feb. 27, 2020), available at https://securityboulevard.com/2020/02/bitcoin-tumbling-leads-to-multicount-indictment/.

[23] Toshendra Kumar Sharma, How is Blockchain Verifiable by Public and Yet Anonymous?, Blockchain Council (last visited May 2, 2021), available at https://www.blockchain-council.org/blockchain/how-is-blockchain-verifiable-by-public-and-yet-anonymous/.

[24] See id.

[25] See Fin. Crimes Enf't Network, U.S. Dep't of the Treasury, FIN-2019-G001, Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies 21 (2019), available at https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf; see also 31 U.S.C. § 5330; 31 C.F.R. § 1022.380.

[26] See United States v. Harmon, 474 F. Supp. 3d 76 (D.D.C. 2020) [Harmon I]; Harmon II, No. 19-CR-395 (BAH), 2020 WL 7668903 (D.D.C. Dec. 24, 2020); Harmon III, No. 19-CR-395 (BAH), 2021 WL 1518344 (Apr. 16, 2021).

[27] Harmon I, 474 F. Supp. 3d at 82, 109 (quoting Usha R. Rodrigues, Law and the Blockchain, 104 Iowa L. Rev. 679, 712 n.224 (2019)).

[28] See Joint Mot. to Continue Trial and Pretrial Dates, ECF No. 89, United States v. Harmon, No. 19-CR-395 (BAH) (D.D.C.).

[29] According to Tim Swanson, Head of Market Intelligence for the London-based blockchain firm Clearmatics: "NFTs are just another way of achieving the same goal, of breaking down the provenance and walking away with 'clean' or screened coins." See Simon Chandler, Money Laundering Might Taint NFTs Too, Prepare for Tighter Controls, CryptoNews (Mar. 27, 2021), available at https://cryptonews.com/exclusives/money-laundering-might-taint-nfts-too-prepare-for-tighter-co-9689.htm.

[30] Id.

[31] See Top NFT Marketplaces: Beginners Guide, DappRadar (Apr. 4, 2021), available at https://dappradar.com/blog/top-7-nft-marketplaces-beginners-guide ("OpenSea is the first and biggest peer-to-peer NFT marketplace for crypto goods. You can think of it as eBay on the blockchain.").

[32] Fin. Crimes Enf't Network, U.S. Dep't of the Treasury, FIN-2021-NTC2, FinCEN Informs Financial Institutions of Efforts Related to Trade in Antiquities and Art 1 (2021), available at https://www.fincen.gov/sites/default/files/2021-03/FinCEN%20Notice%20on%20Antiquities%20and%20Art_508C.pdf.

All Content © 2003-2021, Portfolio Media, Inc.

INVESTING CRYPTOCURRENCY

Advertiser Disclosure

U.S. Officials Send Mixed Messages on Crypto Regulation. Here's What It All Means for Investors

Ryan Haar
November 2, 2021 | 7 MIN READ


Getty Images

Senate Majority Leader Chuck Schumer (D-NY) spoke on Capitol Hill on Tuesday, Aug. 3, as the Senate looks to pass a $1 trillion infrastructure bill that includes provisions on cryptocurrency regulation.

Next Weekly
Learn all about finances in next to no time with our weekly newsletter.
In your inbox every Tuesday
Email address
Sign up
I would like to subscribe to the NextAdvisor newsletter. See privacy policy

Editorial Independence

We want to help you make more informed decisions. Some links on this page — clearly marked — may take you to a partner website and may result in us earning a referral commission. For more information, see **How We Make Money.**

One of the founding principles of cryptocurrency is that it's decentralized and unregulated. But the U.S. government isn't too worried about crypto's founding principles.

In fact, cryptocurrency regulation has been a frequent point of interest lately for U.S. lawmakers and government agencies. A recent report from the Biden administration outlines proposed legislation that would bring more regulation to the cryptocurrency market. And in recent months, U.S. Federal Reserve Chairman Jerome Powell, and Security and Exchange

Commission (SEC) Chairman Gary Gensler have both expressed concern over lack of cryptocurrency regulation.

But in spite of all the back-and-forth, a few key themes have emerged on the subject of new U.S. cryptocurrency regulation: stopping cryptocurrency crime and tax evasion, stablecoin regulation, and the potential for investment vehicles like crypto ETFs and other funds.

For many crypto enthusiasts, the decentralized nature of digital currencies — which, unlike traditional currencies, aren't backed by any institution or government authority — is a big draw. But regulatory guidance can help protect investors. "As much as I like the decentralization and the lack of government [involvement], I am glad that they are paying attention because unfortunately with cryptocurrency, there are a lot of scams," says Kiana Danial, author of "Cryptocurrency Investing for Dummies."

Here's a rundown of the proposals we've seen so far, and how they may affect cryptocurrency investors in the future:

RELATED: Top Crypto News This Week

Cryptocurrency Crime and Tax Evasion

Cryptocurrency regulation has been included in bipartisan infrastructure bill talks by U.S. legislators in recent months.

One possible provision would expand the definition of a brokerage to include companies that facilitate digital asset trades — like cryptocurrency exchanges. This kind of change would mean increased tax reporting responsibility to help the IRS track crypto tax evasion.

Additionally, Gensler has spoken about a need to increase regulation and help prevent more ransomware attacks, like the one that shut down the Colonial Pipeline in May 2021. The pipeline attack was one of a number of high-profile instances of hackers seeking Bitcoin ransoms.

While Gensler hasn't said exactly how the SEC planned to help stop these crimes, he did say that the agency would continue to exercise the full extent of its power.

"[The SEC] will continue to take our authorities as far as they go," Gensler said during an appearance at the Aspen Security Forum in Colorado.

A recent U.S. Treasury report voiced the same concerns as Gensler, saying cryptocurrency "poses a significant detection problem by facilitating illegal activity broadly including tax evasion."

[READ MORE]: Cryptocurrency Crime Is Booming. Here's How to Invest Safely

What Investors Should Know

Under a potential new law that has been considered by lawmakers, companies that facilitate crypto trades would be required to report tax information about those trades to the IRS (just as brokers of traditional investments like stocks do) starting in the 2024 tax season.

"The bill is generally investor-friendly because it makes crypto tax compliance easier for investors," says Shehan Chandrasekera, CPA, head of tax strategy at CoinTracker.io, a crypto tax software company. "This is because if the bill passes, exchanges will have to issue 1099-B tax forms with cost basis information to investors."

That means the exchange would provide a record of taxable events on the platform, like how much your Bitcoin was worth when you bought it and when you sell it back into U.S. dollars. Today, only some exchanges report this info.

"This will significantly reduce the crypto tax filing burden," Chandrasekera says.

It's already important to keep your own records of any capital gains or losses on your crypto trades, which you should report on your federal tax returns. But this regulation would make it even more essential, since the IRS would more easily be able to find any cases of tax evasion related to crypto.

Stablecoin Regulation

The Biden administration released a report on Nov. 1 that includes specific proposed legislation that would bring new regulation to stablecoins. The proposed legislation would effectively classify stablecoin issuers as banks, subjecting them to similar oversight aimed at protecting consumers.

Stablecoins are a type of cryptocurrency pegged to an existing currency, like USDT (Tether). USDT is tied to the price of the U.S. dollar, so its value is constantly $1. And the SEC isn't the only agency that's taken interest.

Gensler has hinted in the past that increased stablecoin regulation could help with the cryptocurrency crime problem, as "the majority of what happens [on cryptocurrency exchanges and platforms] is cryptocurrency to cryptocurrency."

Gensler says that by bypassing the involvement of U.S. dollars in direct crypto-to-crypto trades, bad actors may be more able to evade public policy measures and other sanctions aimed at preventing money laundering or ensuring tax compliance.

PRO TIP

Apart from federal regulation, there have been many state-specific cryptocurrency legislations passed. Know what regulations apply in your state.

While legislators would need to enact new legislation to put the Biden administration's report into action, it does show U.S. officials are paying close attention to the cryptocurrency market. "The absence of appropriate oversight presents risks to users and the broader [cryptocurrency] system," Treasury Secretary Janet Yellen said in the report.

What Investors Should Know

Stablecoins are most commonly used by more advanced traders to reduce fees on crypto-to-crypto trades, but the Biden administration report hints at stablecoins' potential as a more mainstream digital payment system in the future. Crypto is still in its relative early days as an asset class, so any new regulation has potential to impact investors' portfolio.

Investors probably don't need to make any immediate changes to their portfolio based on the proposed new legislation, as stablecoins are not as great a store of value as more volatile cryptos like Bitcoin. If you're investing in crypto looking for long-term growth, experts

recommend sticking with more established coins like Bitcoin or Ethereum.

In anticipation of any coming guidance, you should also make sure to choose a cryptocurrency exchange that maintains compliance with evolving federal and state regulators in the United States. This includes many established, high-volume U.S.-based exchanges, like Coinbase and Gemini.

"I only purchase my cryptocurrency assets from regulated brokers at this point, because we have the luxury of doing so. Of course in other countries they don't have it, but we do," says Danial.

Cryptocurrency ETFs

While the government considers how to make it harder to use cryptocurrency for illicit activities and tax evasion, there is still no way for Americans to buy into crypto using more traditional investment accounts like those at a Fidelity or a Vanguard.

While a Bitcoin-linked ETF did recently debut on the stock market, the SEC has yet to approve a cryptocurrency ETF (exchange-traded fund) — despite several proposed funds from different institutions and exchanges — but Gensler revealed on Tuesday that it may be coming.

"We do it in the equity market, we do it in the bond markets, people might want it here," Gensler said. While acknowledging there have already been SEC filings for ETFs, "I anticipate we'll have some new ones under what's called the Investment Companies Act — and when combined with other federal laws, the law provides significant investor protections," he says.

The Investing Companies Act requires companies, including mutual funds, to disclose information about their finances and investments on a "regular basis," according to the SEC.

Until an ETF gets approved, "there's not really a way to buy a security that closely tracks the price of a specific cryptocurrency," says Jeremy Schneider, the personal finance expert behind Personal Finance Club. That means the only way for investors to really do that is to buy coins directly from an exchange.

While there has been some confusion about whether cryptocurrencies are securities (and under SEC regulation), Gensler made clear that every initial coin offering (ICO) he has seen is a security: "Generally, folks buying these tokens are anticipating profits, and there's a small group of entrepreneurs and technologists standing up and nurturing the projects ... I believe we have a crypto market now where many tokens may be unregistered securities, without required disclosures or market oversight."

But Gensler reiterated that the SEC has jurisdiction, and "our federal securities laws apply."

What Investors Should Know

Cryptocurrency ETFs are not yet available in the U.S., but may offer a way for investors to get into cryptocurrency without having to buy directly from an exchange in the future.

If you're interested in crypto, these funds could help you diversify your holdings across different coins, like a conventional ETF or index fund. But they're still just as speculative as any crypto investment; if you're waiting for a Bitcoin ETF because you're unwilling to take on the risk, you may want to reconsider whether crypto belongs in your portfolio at all.

In the meantime, Gensler's stance that every ICO is a security could mean investors should look to the SEC for protections as regulation becomes more concrete.

Up Next

HOME EQUITY

How a HELOC Can Help (or Hurt) Your Credit Score

6 MIN READ

INVESTING

Index Funds vs. ETFs: How Each Can Help You Build Wealth

4 MIN READ

CREDIT CARDS

Crypto Rewards Are the Latest Credit Card Trend. But Are They A Good Idea?

13 MIN READ

MORTGAGE NEWS

Mortgage Rates Stayed Just Over 3% Last Week — More Good News for Homeowners Looking to Refinance

3 MIN READ

At NextAdvisor we're firm believers in transparency and editorial independence. Editorial opinions are ours alone and have not been previously reviewed, approved, or endorsed by our partners. We do not cover every offer on the market. Editorial content from NextAdvisor is separate from TIME editorial content and is created by a different team of writers and editors.

SUBSCRIBE TO OUR NEWSLETTER

Email address Sign up

I would like to subscribe to the NextAdvisor newsletter. See privacy policy

INSURANCE
Car Insurance
Home Insurance
Life Insurance
Insurance Company Reviews

INVESTING
Cryptocurrency
Retirement

CALCULATORS
CD Calculator
Mortgage Calculator
Amortizatio Calculator
Savings Calculator

Citi
Discover
Wells Fargo
Credit Card Comparisons

FOLLOW US

BANKING
CDs
Checking
MMA
Savings

LEGAL & PRIVACY
Privacy Policy
Cookie Settings
Do not sell my info
Terms of Use

© 2021 NextAdvisor, LLC A Red Ventures Company All Rights Reserved. Use of this site constitutes acceptance of our Terms of Use, Privacy Policy (Your California Privacy Rights) and California Do Not Sell My Personal Information. NextAdvisor may receive compensation for some links to products and services on this website. Offers may be subject to change without notice.



What are smart contracts on blockchain?

Smart contracts are digital contracts stored on a blockchain that are automatically executed when predetermined terms and conditions are met

Smart contracts defined

Smart contracts are simply programs stored on a blockchain that run when predetermined conditions are met. They typically are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary's involvement or time loss. They can also automate a workflow, triggering the next action when conditions are met.

→ Learn more about blockchain technology

→ Learn more about IBM Blockchain

How smart contracts work

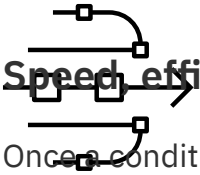
Smart contracts work by following simple “if/when…then…” statements that are written into code on a blockchain. A network of computers executes the actions when predetermined conditions have been met and verified. These actions could include releasing funds to the appropriate parties, registering a vehicle, sending notifications, or issuing a ticket. The blockchain is then updated when the transaction is completed. That means the transaction cannot be changed, and only parties who have been granted permission can see the results.

Within a smart contract, there can be as many stipulations as needed to satisfy the participants that the task will be completed satisfactorily. To establish the terms, participants must determine how transactions and their data are represented on the blockchain, agree on the “if/when…then…” rules that govern those transactions, explore all possible exceptions, and define a framework for resolving disputes.

Then the smart contract can be programmed by a developer – although increasingly, organizations that use blockchain for business provide templates, web interfaces, and other online tools to simplify structuring smart contracts.

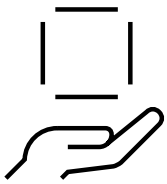
→ What is blockchain for business?

Benefits of smart contracts



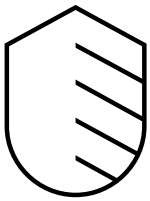
Speed, efficiency and accuracy

Once a condition is met, the contract is executed immediately. Because smart contracts are digital and automated, there's no paperwork to process and no time spent reconciling errors that often result from manually filling in documents.



Trust and transparency

Because there's no third party involved, and because encrypted records of transactions are shared across participants, there's no need to question whether information has been altered for personal benefit.



Security

Blockchain transaction records are encrypted, which makes them very hard to hack. Moreover, because each record is connected to the previous and subsequent records on a distributed ledger, hackers would have to alter the entire chain to change a single record.



Savings

Smart contracts remove the need for intermediaries to handle transactions and, by extension, their associated time delays and fees.

Applications of smart contracts

Smart contracts can be used across industries to streamline and automate doing business down the street or around the world.

Reimagine dispute resolution

Discrepancies in financial settlements are costly, taking weeks or months to research and resolve. Smart contracts that codify agreed-upon business rules automate processes such as identifying discrepancies, reconciling documents, settling transactions, and resolving disputes.

Read the blog on invoice reconciliation and dispute resolution

Build a resilient supply chain

IBM Blockchain supply chain solutions use smart contracts to streamline the flow of goods by automatically triggering next steps when conditions are met, such as shipping, delivery,

and acceptable IoT data about conditions during handling. Participants can act earlier to prevent disruptions should an unexpected event occur.

→ Learn about IBM Blockchain for Supply Chain

Bring trust to trade finance

Smart contracts are an essential component of we.trade, the trade finance network convened by IBM Blockchain that is creating an ecosystem of trust for global trade. Standardized rules and simplified trading options encoded in smart contracts decrease risk and help participants find new opportunities.

Watch we.trade transforming trade finance (03:38)

Reinvent bank letters of guarantee

Using blockchain and smart contracts, a consortium of banks digitized and transformed the bank guarantee process for both financial and performance guarantees. The new platform, Lygon, enables applicants, issuers and beneficiaries to obtain legally binding guarantees in one day.

See how Lygon took the paper out of bank guarantees (03:20)

Resources

RESOURCES

Notices

Antiquities and Art (https://www.fincen.gov/sites/default/files/2021-03/FinCEN%20Notice%20on%20Antiquities%20and%20Art_508C.pdf)

Speeches

FIBA (3/22/21) (https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-virtually-florida)

News

Beneficial Ownership ANPRM (https://www.fincen.gov/news/news-releases/fincen-launches-regulatory-process-new-beneficial-ownership-reporting)

Get FinCEN News Updates

Stay informed of updates to the FinCEN website!

Get News Updates (https://service.govdelivery.com/accounts/USFINCEN/subscriber/new)

The Anti-Money Laundering Act of 2020



On January 1, 2021, Congress enacted the FY2021 National Defense Authorization Act (NDAA), which included significant reforms to the U.S. anti-money laundering (AML) regime. The NDAA includes the Anti-Money Laundering Act of 2020 (AML Act) and, within the AML Act, the Corporate Transparency Act (CTA).

The AML Act seeks to strengthen, modernize, and streamline the existing AML regime by promoting innovation, regulatory reform, and industry engagement through forums, such as the Bank Secrecy Act Advisory Group (BSAAG) and FinCEN Exchange. The Act also calls for FinCEN to work closely with our regulatory, national security, and law enforcement partners to identify risks and priorities and provide valuable feedback to our industry partners.

The CTA establishes uniform beneficial ownership reporting requirements for corporations, limited liability companies, and other similar entities formed or registered to do business in the United States. The CTA authorizes FinCEN to collect that information and share it with authorized government authorities and financial institutions, subject to effective safeguards and controls.

Many provisions of the AML Act and the CTA require rulemaking or periodic reporting to Congress on implementation efforts, assessments, and findings. Some key requirements include:

1. Establishing standards for the reporting of information on beneficial ownership, building an IT system to collect and secure the data, and creating access protocols;
2. Establishing national anti-money laundering and countering the financing of terrorism priorities;
3. Enhancing the whistleblower provisions to provide for a robust whistleblower program and new anti-retaliation protections;
4. Reviewing, and revising as appropriate, Currency Transaction Report (CTR) and Suspicious Activity Report (SAR) reporting requirements, and other existing Bank Secrecy Act (BSA) regulations and guidance;
5. Expanding BSA requirements and obligations to persons engaged in the trade of antiquities, and mandating a study on the potential expansion of BSA requirements to persons engaged in the art trade;
6. Codifying the FinCEN Exchange program;
7. Hosting a Financial Crimes Tech Symposium, and establishing new BSAAG subcommittees and a supervisory committee to address public-private partnerships;
8. Establishing a BSA Analytical Hub;
9. Law enforcement reporting to FinCEN on the use of BSA data, procedures for additional feedback between FinCEN and financial institutions on the usefulness of SARs, and semi-annual publication of review of SAR activity and other BSA reports, including threat patterns, trends, and typologies; and
10. Codifying a pilot program to allow financial institutions to share SARs with their foreign branches, subsidiaries, and affiliates.

Timely and effective AML Act implementation will be challenging and is FinCEN's top priority, and we are working diligently with our domestic and international industry partners and law enforcement and regulatory stakeholders to further the national security of the United States and protect the American people.


FINANCIAL CRIMES
ENFORCEMENT NETWORK

Harvard Law School Forum on Corporate Governance

An Introduction to Smart Contracts and Their Potential and Inherent Limitations

Posted by Stuart D. Levi and Alex B. Lipton, Skadden, Arps, Slate, Meagher & Flom LLP, on Saturday, May 26, 2018

Tags: **Blockchain**, **Contracts**, **Cybersecurity**, **Financial technology**, **Legal systems**, **Risk**, **Risk management**
More from: **Alex Lipton**, **Stuart Levi**, **Skadden**

Editor's Note: **Stuart D. Levi** is a partner and **Alex B. Lipton** is an associate at Skadden, Arps, Slate, Meagher & Flom LLP. This post is based on their Skadden publication.

"Smart contracts" are a critical component of many platforms and applications being built using blockchain or distributed ledger technology. Below, we outline the background and functions of smart contracts, discuss whether they can be deemed enforceable legal agreements under contract law in the United States, and highlight certain legal and practical considerations that will need to be resolved before they can be broadly used in commercial contexts.

An Introduction to Smart Contracts

How Smart Contracts Function

"Smart contracts" is a term used to describe computer code that automatically executes all or parts of an agreement and is stored on a blockchain-based platform. As discussed further below, the code can either be the sole manifestation of the agreement between the parties or might complement a traditional text-based contract and execute certain provisions, such as transferring funds from Party A to Party B. The code itself is replicated across multiple nodes of a blockchain and, therefore, benefits from the security, permanence and immutability that a blockchain offers. That replication also means that as each new block is added to the blockchain, the code is, in effect, executed. If the parties have indicated, by initiating a transaction, that certain parameters have been met, the code will execute the step triggered by those parameters. If no such transaction has been initiated, the code will not take any steps. Most smart contracts are written in one of the programming languages directly suited for such computer programs, such as Solidity.

At present, the input parameters and the execution steps for a smart contract need to be specific and objective. In other words, if "x" occurs, then execute step "y." Therefore, the actual tasks that smart contracts are performing are fairly rudimentary, such as automatically moving an amount of cryptocurrency from one party's wallet to another when certain criteria are satisfied. As the adoption of blockchain spreads, and as more assets are tokenized or go "on chain," smart contracts will become increasingly complex and capable of handling sophisticated transactions. Indeed, developers already are stringing together multiple transaction steps to form more complex smart contracts. Nonetheless, we are, at the very least, many years away from code being able to determine more subjective legal criteria, such as whether a party satisfied a commercially reasonable efforts standard or whether an indemnifications clause should be triggered and the indemnity paid.

Before a compiled smart contract actually can be executed on certain blockchains, an additional step is required, namely, the payment of a transaction fee for the contract to be added to the chain and executed upon. In the case of the Ethereum blockchain, smart contracts are executed on the Ethereum Virtual Machine (EVM), and this payment, made through the ether cryptocurrency, is known as "gas." **[1]** The more complex the smart contract (based on the transaction steps to be performed), the more gas that must be paid to execute the smart contract. Thus, gas currently acts as an important gate to prevent overly complex or numerous smart contracts from overwhelming the EVM. **[2]**

Smart contracts are presently best suited to execute automatically two types of “transactions” found in many contracts: (1) ensuring the payment of funds upon certain triggering events and (2) imposing financial penalties if certain objective conditions are not satisfied. In each case, human intervention, including through a trusted escrow holder or even the judicial system, is not required once the smart contract has been deployed and is operational, thereby reducing the execution and enforcement costs of the contracting process.

As just one example, smart contracts could eliminate the so-called procure-to-pay gaps. When a product arrives and is scanned at a warehouse, a smart contract could immediately trigger requests for the required approvals and, once obtained, immediately transfer funds from the buyer to the seller. Sellers would get paid faster and no longer need to engage in dunning, and buyers would reduce their account payable costs. This could impact working capital requirements and simplify finance operations for both parties. On the enforcement side, a smart contract could be programmed to shut off access to an internet-connected asset if a payment is not received. For example, access to certain content might automatically be denied if payment was not received.

Historical Background

The term “smart contract” was first introduced by computer scientist and cryptographer Nick Szabo some 20 years ago as a graduate student at University of Washington. According to Szabo:

> New institutions, and new ways to formalize the relationships that make up these institutions, are now made possible by the digital revolution. I call these new contracts “smart,” because they are far more functional than their inanimate paper-based ancestors. No use of artificial intelligence is implied. A smart contract is a set of promises, specified in digital form, including protocols within which the parties perform on these promises. **[3]**

Szabo’s use of quotes around the word “smart” when comparing smart contracts to paper-based contracts, and his eschewing of artificial intelligence are important. Smart contracts may be “smarter” than paper contracts because they automatically can execute certain pre-programmed steps, but they should not be seen as intelligent tools that can parse a contract’s more subjective requirements. Indeed, the classic example of a smart contract offered by Szabo is a vending machine. Once a purchaser has satisfied the conditions of the “contract” (*i.e.*, inserting money into the machine) the machine automatically honors the terms of the unwritten agreement and delivers the snack.

Smart contracts today also find their origin in Ricardian Contracts, a concept published in 1996 by Ian Grigg and Gary Howland as part of their work on the Ricardo payment system to transfer assets. Grigg saw Ricardian Contracts as a bridge between text contracts and code that had the following parameters: a single document that “is a) a contract offered by an issuer to holders, b) for a valuable right held by holders, and managed by the issuer, c) easily readable by people (like a contract on paper), d) readable by programs (parsable like a database), e) digitally signed, f) carries the keys and server information, and g) allied with a unique and secure identifier.” **[4]**

The Interplay With Traditional Text Agreements

One of the difficulties with discussing smart contracts is that the term is used to capture two very different paradigms. The first involves smart contracts that are created and deployed without any enforceable text-based contract behind them. For example, two parties reach an oral understanding as to the business relationship they want to capture and then directly reduce that understanding into executable code. We refer to these below as “code-only smart contracts.” The second paradigm involves the use of smart contracts as vehicles to effectuate certain provisions of a traditional text-based contract, in which the text itself references the use of the smart contract to effectuate certain provisions. We refer to these as “ancillary smart contracts.”

Are Smart Contracts Enforceable?

There is no federal contract law in the United States; rather, the enforceability and interpretation of contracts is determined at the state level. Thus, while certain core principles apply consistently across state lines, and there has been a drive to harmonize state laws by the National Conference of Commissioners on Uniform State Laws, any conclusions regarding smart contracts must be tempered by the reality that states may adopt different views.

A discussion regarding the enforceability of smart contracts must start with the fundamental distinction between an agreement and a "contract." States generally recognize that although two parties can enter into a variety of "agreements," a contract means that the agreement is legally binding and enforceable in a court of law. **[5]** In order to determine enforceability, state courts traditionally look to whether the common law requirements of offer, acceptance and consideration are satisfied. These basic requirements surely can be achieved through ancillary smart contracts. For example, an insurer might develop a flight insurance product that automatically provides the insured with a payout if a flight is delayed by more than two hours. **[6]** The key terms, such as delineating how the delay is calculated, can be set forth in a text-based contract, with the actual formation of the contract (payment of the premium) and the execution (automatic payout upon a verifiable delay) handled through an ancillary smart contract. Here, the insurer has made a definite offer for a flight insurance product that is accepted by the insured upon payment of the premium as consideration.

Although, today, certain contracts must be in writing, and additional formalities may be required such as those under the Uniform Commercial Code (UCC) and state statutes of frauds, **[7]** agreements do not always need to be in writing to be held enforceable. **[8]** Thus, many code-only smart contracts also will be enforceable under state laws governing contracts. Szabo's example of a vending machine is instructive in this regard. There, while the buyer has many implied rights, a contract was formed without any meaningful written terms other than a price display for each item. Thus, the fact that an agreement is rendered only in code, such as the case with code-only smart contracts, presents no particular barrier to contract formation outside the barriers imposed by the UCC and statutes of frauds. Indeed, a variety of laws and legal constructs have long considered the role of information technology in contract formation.

For example, the Uniform Electronic Transactions Act (UETA) which dates back to 1999 and forms the basis for state law in 47 states, provides that, with limited exceptions, electronic records, which include records created by computer programs, and electronic signatures (*i.e.*, digital signature using public key encryption technology) be given the same legal effect as their written counterparts. **[9]** UETA even goes so far as recognizing the validity of "electronic agents," which it defines 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." **[10]** 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," **[11]** arguably a prescient acknowledgment of smart contracts.

Similarly, the federal Electronic Signatures Recording Act (E-Sign Act) not only recognizes the validity of electronic signatures and electronic records in interstate commerce, but also provides that a contract or other record relating to a transaction "may not be denied legal effect, validity, or enforceability solely because its formation, creation, or delivery involved the action of one or more electronic agents so long as the action of any such electronic agent is legally attributable to the person to be bound." **[12]** The term "electronic agent" means 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 at the time of the action or response." **[13]**

Though an understanding of the current legal framework is important to evaluating the enforceability of smart contracts today, those using smart contracts in the future may not need to rely on laws that pre-date the development of blockchain technology. Arizona and Nevada already have amended their respective state versions of UETA to explicitly incorporate blockchains and smart contracts. **[14]** The fact that these states have adopted decidedly different definitions of those critical terms suggests that as more states follow their lead, there may be increasing pressure to adopt unified definitions to reflect blockchain and smart contract developments.

Challenges With the Widespread Adoption of Smart Contracts

Given the existing legal frameworks for recognizing electronic contracts, it is quite likely that a court today would recognize the validity of code that executes provisions of a smart contract—what we have classified as ancillary smart contracts. There is also precedent to suggest that a code-only smart contract might enjoy similar legal protection. The challenge to widespread smart contract adoption may therefore have less to do with the limits of the law than with potential clashes between how smart contract code operates and how parties transact business. We set forth below certain of these challenges:

How Can Non-technical Parties Negotiate, Draft and Adjudicate Smart Contracts?

A key challenge in the widespread adoption of smart contracts is that parties will need to rely on a trusted, technical expert to either capture the parties' agreement in code or confirm that code written by a third party is accurate. While some analogize this to hiring a lawyer to explain "the legalese" of a traditional text-based contract, the analogy is misplaced. Non-lawyers typically can understand simple short-form agreements as well as many provisions of longer agreements, especially those setting forth business terms. But a non-programmer would be at a total loss to understand even the most basic smart contract and is therefore significantly more beholden to an expert to explain what the contract "says."

To some extent, the inability of contracting parties to understand the smart contract code will not be a hindrance to entering into ancillary code agreements. This is because for many basic functions, text templates can be created and used to indicate what parameters need to be entered and how those parameters will be executed. For example, assume a simple smart contract function that extracts a late fee from a counterparty'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 the amount of the late fee. However, a party may want to confirm that the underlying code actually will 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 the accuracy of the underlying code. This review will require a trusted third party with programming expertise.

In cases where such templates do not exist, and new code must be developed, the parties will need to communicate the intent of their agreement to a programmer. Simply handing that programmer a copy of the legal agreement would be inefficient since it would require the programmer to try and decipher a legal document. Parties relying on ancillary smart contracts therefore may need to draft a separate "term sheet" of functionality that the smart contract should perform and that can be provided to the programmer.

The parties also may want written representations from the programmer that the code performs as contemplated. The net result is that for customized arrangements that do not rely on an existing template, the parties may need to enter into a written agreement with the smart contract programmer, not unlike the contract that parties may enter into with a provider of services for Electronic Data Interchange (EDI) transactions today.

Insurance companies could also create policies to protect contracting parties from the risk that smart contract 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 protection given that the parties might miss errors when reviewing the code. The parties would also take some additional comfort from the fact that the insurance company likely conducted its own code audit before agreeing to insure the code.

Code-only smart contracts used for business-to-consumer transactions could pose an additional set of issues that will need to be addressed. Courts are wary of enforcing agreements where the consumer did not receive adequate notice of the terms of the agreement, **[15]** and may be hesitant to enforce a smart contract where the consumer was not also provided with an underlying text agreement that included the complete terms.

Finally, as the validity or performance of smart contracts increasingly become adjudicated, courts may need a system of court-appointed experts to help them decipher the meaning and intent of the code. Today, parties routinely use their own experts when technical issues are at the center of a dispute. While both federal courts and many state courts have the authority to appoint their own experts, they rarely exercise that authority. **[16]** That approach may need to change if the number of standard contract disputes that center on interpreting smart contract code increases.

Smart Contracts and the Reliance on "Off-chain" Resources

Many smart contract-proposed use-cases assume that the smart contract will receive information or parameters from resources that are not on the blockchain itself—so-called off-chain resources. For example, assume a crop insurance smart contract is programmed to transfer value to an insured party if the temperature falls below 32 degrees at any point. The smart contract will need to receive that temperature data from an agreed source. This presents two issues. First, smart contracts do not have the ability to pull data from off-chain resources; rather, that information needs to be "pushed" to the smart contract. Second, if the data at issue is in constant flux, and since the code is replicated across multiple

nodes across the network, different nodes may be receiving different information, even just a few seconds apart. In our example, Node-1 may receive information that the temperature is 31.9 degrees, while Node-2 may receive information that the temperature is actually 32 degrees. Given that consensus is required across the nodes for a transaction to be validated, such fluctuations can cause the condition to be deemed "not satisfied."

Contracting parties will be able to solve this conundrum by using a so-called "oracle." Oracles are trusted third parties that retrieve off-chain information and then push that information to the blockchain at predetermined times. In the foregoing 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 an elegant solution to accessing off-chain resources, this process adds another party with whom the parties would need to contract to effectuate a smart contract, thus somewhat diluting the decentralized benefits of smart contracts. It also introduces a potential "point of failure." For example, an oracle might experience a system flaw and be unable to push out the necessary information, provide erroneous data or simply go out of business. Smart contracts will need to account for these eventualities before their adoption can become more widespread.

What is the "Final" Agreement Between the Parties?

When analyzing traditional text-based contracts, courts will examine the final, written document to which the parties have agreed in order to determine whether the parties are in compliance or breach. Courts have long emphasized that it is this final agreement that represents the mutual intent of the parties—the "meeting of the minds."

In the case of code-only smart contracts, the code that is executed—and the outcome it produces—represents the only objective evidence of the terms agreed to by the parties. In these cases, email exchanges between the parties as to what functions the smart contract "should" execute, or oral discussions to that effect, likely would yield to the definitive code lines as the determinative manifestation of the parties' intent.

With respect to ancillary smart contracts, a court likely would look at the text and code as a unified single agreement. The issue becomes complicated when the traditional text agreement and the code do not align. In the crop insurance example described above, assume the text of an agreement specifies that an insurance payout will be made if the temperature falls below 32 degrees, while the smart contract code triggers the payment if the temperature is equal to or below 32 degrees. Assuming that the text agreement does not state whether the text or code controls in the event of an inconsistency, courts will need to determine—perhaps on a case-by-case basis—whether the code should be treated as a mutually agreed amendment to the written agreement or whether the text of the agreement should prevail. In some respects, the analysis should be no different than a case where the provisions of a main agreement differ from what is reflected in an attached schedule or exhibit. The fact that here the conflict would be between text and computer code and not two text documents should not be determinative, but courts may take a different view.

One solution will be for parties to use a text based contract where the parameters that trigger the smart contract execution are not only visible in the text but actually populate the smart contract. In our example, "less than 32 degrees" would not only be seen in the text, but also would create the parameter in the smart contract itself, thereby minimizing the chances of any inconsistency.

The Automated Nature of Smart Contracts

One of the key attributes of smart contracts is their ability to automatically and relentlessly execute transactions without the need for human intervention. However, this automation, and the fact that smart contracts cannot easily be amended or terminated unless the parties incorporate such capabilities during the creation of the smart contract, present some of the greatest challenges facing widespread adoption of smart contracts.

For example, with traditional text contracts, a party can easily excuse a breach simply by not enforcing the available penalties. If a valued customer is late with its payment one month, the vendor can make a real-time decision that preserving the long-term commercial relationship is more important than any available termination right or late fee. However, if this relationship had been 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 a late fee from the customer's account or the suspension of a customer's access to a software program or an internet-connected device if that is what the smart

contract was programmed to do. The automated execution provided by smart contracts might therefore not align with the manner in which many businesses operate in the real world.

Similarly, in a text-based contractual relationship, a party may be willing to accept, on an *ad hoc* basis, partial performance to be deemed full performance. This might be because of an interest in preserving a long-term relationship or because a party determines that partial performance is preferable to no performance at all. Here, again, the objectivity required for smart contract code might not reflect the realities of how contracting parties interact.

Amending and Terminating Smart Contracts

At present, there is no simple path to amend a smart contract, creating certain challenges for contracting parties. For example, in a traditional text-based contract, if the parties have mutually agreed to change the parameters of their business deal, or if there is a change in law, the parties quickly can draft an amendment to address that change, or simply alter their course of conduct. Smart contracts currently do not offer such flexibility. Indeed, given that blockchains are immutable, modifying a smart contract is far more complicated than modifying standard software code that does not reside on a blockchain. The result is that amending a smart contract may yield higher transaction costs than amending a text-based contract, and increases the margin of error that the parties will not accurately reflect the modifications they want to make.

Similar challenges exist with respect to terminating a smart contract. Assume a party discovers an error in an agreement that gives the counterparty more rights than intended, or concludes that fulfilling its stated obligations will be far more costly than it had expected. In a text-based contract, a party can engage in, or threaten, so-called "efficient breach," *i.e.*, knowingly breaching a contract and paying the resulting damages if it determines that the cost to perform is greater than the damages it would owe. Moreover, by ceasing performance, or threatening to take that step, a party may bring the counterparty back to the table to negotiate an amicable resolution. Smart contracts do not yet offer analogous self-help remedies.

Projects are currently underway to create smart contracts that are terminable at any time and more easily amended. While in some ways this is antithetical to the immutable and automated nature of smart contracts, it reflects the fact that smart contracts only will gain commercial acceptance if they reflect the business reality of how contracting parties act.

Objectivity and the Limits of Incorporating Desired Ambiguity Into Smart Contracts

The objectivity and automation required of smart contracts can run contrary to how business parties actually negotiate agreements. During the course of negotiations, parties implicitly engage in a cost-benefit analysis, knowing that at some point there are diminishing returns in trying to think of, and address, every conceivable eventuality. These parties no longer may want to expend management time or legal fees on the negotiations, or may conclude that commencing revenue generating activity under an executed contract outweighs addressing unresolved issues. Instead, they may determine that if an unanticipated event actually occurs, they will figure out a resolution at that time. Similarly, parties may purposefully opt to leave a provision somewhat ambiguous in an agreement in order to give themselves the flexibility to argue that the provision should be interpreted in their favor. This approach to contracting is rendered more difficult with smart contracts where computer code demands an exactitude not found in the negotiation of text-based contracts. A smart contract cannot include ambiguous terms nor can certain potential scenarios be left unaddressed. As a result, parties to smart contracts may find that the transaction costs of negotiating complex smart contracts exceed that of a traditional text-based contracts.

It will take some time for those adopting smart contracts in a particular industry to determine which provisions are sufficiently objective to lend themselves to smart contract execution. As noted, to date, most smart contracts perform relatively simple tasks where the parameters of the "if/then" statements are clear. As smart contracts increase in complexity, parties may disagree on whether a particular contractual provision can be captured through the objectivity that a smart contract demands.

Do Smart Contracts Really Guarantee Payment?

One benefit often touted of smart contracts is that they can automate payment without the need for dunning notices or other collection expenses and without the need to go to court to obtain a judgment mandating payment. While this is

indeed true for simpler use cases, it may be less accurate in complex commercial relationships. The reality is that parties are constantly moving funds throughout their organization and do not "park" total amounts that are due on a long-term contract in anticipation of future payment requirements. Similarly, a person obtaining a loan is unlikely to keep the full loan amount in a specified wallet linked to the smart contract. Rather, the borrower will put those funds to use, funding the necessary repayments on an *ad hoc* basis.

If the party owing amounts under the smart contract fails to fund the wallet on a timely basis, a smart contract looking to transfer money from that wallet upon a trigger event may find that the requisite funds are not available. Implementing another layer into the process, such as having the smart contract seek to pull funds from other wallets or having that wallet "fund itself" from other sources, would not solve the problem if those wallets or sources of funds also lack the requisite payment amounts. The parties might seek to address this issue through a text-based requirement that a wallet linked to the smart contract always have a minimum amount, but that solution simply would give the party a stronger legal argument if the dispute was adjudicated. It would not render the payment operation of the smart contract wholly automatic. Thus, although smart contracts will render payments far more efficient, they may not eliminate the need to adjudicate payment disputes.

Risk Allocation for Attacks and Failures

Smart contracts introduce an additional risk that does not exist in most text-based contractual relationships—the possibility that the contract will be hacked or that the code or protocol simply contains an unintended programming error. Given the relative security of blockchains, these concepts are closely aligned; namely, most "hacks" associated with blockchain technology are really exploitations of an unintended coding error. As with many bugs in computer code, these errors are not glaring, but rather become obvious only once they have been exploited. For example, in 2017 an attacker was able to drain several multi-signature wallets offered by Parity of $31 million in ether. **[17]** Multi-signature wallets add a layer of security because they require more than one private key to access the wallet. However, in the Parity attack, the attacker was able to exploit a flaw in the Parity code by reinitializing the smart contract and making himself or herself the sole owner of the multi-signature wallets. Parties to a smart contract will need to consider how risk and liability for unintended coding errors and resulting exploitations are allocated between the parties, and possibly with any third party developers or insurers of the smart contract.

Governing Law and Venue

One of the key promises of blockchain technology, and by extension smart contracts, is the development of robust, decentralized and global platforms. However, global adoption means that parties may be using a smart contract across far more jurisdictions than might exist in the case of text-based contracts. The party offering terms under a smart contract would therefore be best-served by specifying the governing law and venue for that smart contract. A governing law provision specifies what substantive law will apply to the interpretation of the smart contract, whereas a venue clause specifies which jurisdiction's courts will adjudicate the dispute. In cases where governing law or venue is not specified, a plaintiff may be relatively unconstrained in choosing where to file a claim or in arguing which substantive law should apply given the wide range of jurisdictions in which a smart contract might be used. Given that many early disputes concerning smart contracts will be ones of first-impression, contracting parties will want some certainty surrounding where such disputes will be adjudicated.

Best Practices

Given that we are at the nascent stages of smart contract adoption, best practices for implementing such code is still evolving. However, the checklist below should help developers design effective smart contracts and guide companies who plan to use them.

- For now, parties entering into any type of contractual arrangement would be best served using a hybrid approach that combines text and code. As noted, there are strong arguments that code-only smart contracts should be enforceable, at least under state contract law in the U.S. However, until there is greater clarity on their validity and enforceability, code-only smart contracts should be used only for simpler transactions. Parties will continue to want text-versions of agreements so they can read the agreed-upon terms, memorialize terms that smart contracts are not equipped to address and have a document they know a court will enforce.

- In a hybrid contract using text and code, the text should clearly specify the smart contract code with which it is associated, and the parties should have full visibility into the variables that are being passed to the smart contract, how they are defined and the transaction events that will trigger execution of the code.
- When relying on oracles for off-chain data, the parties should address what would happen if the oracle is unable to push out the necessary data, provides erroneous data or simply goes out of business.
- The parties should consider risk allocation in the event of a coding error.
- The text agreement accompanying the code should specify the governing law and venue, as well as the order of precedence between text and code in the event of a conflict.
- The text agreement should include a representation by each party that they have reviewed the smart contract code, and that it reflects the terms found in the text agreement. Although such a representation cannot force a party to examine the code, it will help the counterparty defend against a claim that the code was never reviewed. Parties may also choose to insure against the risk that the code contains errors. As noted, parties may need to involve third-party experts to review the code.

Future of Smart Contracts

Today, smart contracts are a prototypical example of "Amara's Law," the concept articulated by Stanford University computer scientist Roy Amara that we tend to overestimate new technology in the short run and underestimate it in the long run. Although smart contracts will need to evolve before they are widely adopted for production use in complex commercial relationships, they have the impact to revolutionize the reward and incentive structure that shapes how parties contract in the future. To that end, and when thinking about smart contracts, it is important not to simply think how existing concepts and structures can be ported over to this new technology. Rather, the true revolution of smart contracts will come from entirely new paradigms that we have not yet envisioned.

Endnotes

[1] *See* "What is the 'Gas' in Ethereum?" *Cryptocompare*, November 18, 2016, **available here**.
(go back)

[2] *Id.*
(go back)

[3] Nick Szabo, "Smart Contracts: Building Blocks for Digital Market," 1996, **available here**.
(go back)

[4] Ian Grigg, "The Ricardian Contract," **available here**.
(go back)

[5] *See, e.g.*, "Restatement (Second) of Contracts," Section 1, American Law Institute, 1981. In the U.S., contract law is ordinarily a function of state law. Although this article outlines general contract law principles that are common across states, we note that state law differences may impact the enforceability of smart contracts in certain states.
(go back)

[6] At least one company, AXA, currently offers such a product. ***See here***.
(go back)

[7] *See, e.g.*, UCC § 2-201.
(go back)

[8] *See, e.g., Lumhoo v. Home Depot USA, Inc.*, 229 F. Supp. 2d 121, 160 (E.D.N.Y. 2002) (holding that the plaintiffs adduced sufficient evidence to support an inference that the parties formed an oral contract for payment by their employer

at an overtime rate for any hours worked in excess of eight hours per day).
(go back)

[9] Uniform Electronic Transactions Act (Unif. Law Comm'n 1999)—New York, Illinois and Washington have state-specific laws relating to the validity of electronic transactions.
(go back)

[10] *Id*. § 2(6).
(go back)

[11] *Id.* § 2 cmt. 5.
(go back)

[12] 15 U.S.C. § 7001(h).
(go back)

[13] 15 U.S.C. § 7006(3).
(go back)

[14] *See* 2017 Ariz. HB 2417 44-7061 and Nev. Rev. Stat. Ann. § 719.090.
(go back)

[15] *See, e.g., Nicosia v. Amazon.com, Inc.*, 834 F.3d 220 (2d Cir. 2016) (reversing the district court's dismissal for failure to state a claim and holding that reasonable minds could disagree as to whether Amazon provided the consumer with reasonable notice of the mandatory arbitration provision at issue).
(go back)

[16] *See* Charles Alan Wright & Arthur R. Miller, *Federal Practice and Procedure*, Section 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."), and 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).
(go back)

[17] *See* Haseeb Qureshi, "A Hacker Stole $31M of Ether—How it Happened, and What it Means for Ethereum," *FreeCodeCamp*, (July 20, 2017), **available here**.
(go back)

Both comments and trackbacks are currently closed.