NEW YORK UNIVERSITY
JOURNAL OF LAW & BUSINESS

VOLUME 17 SUMMER 2021 NUMBER 3

PROCEEDINGS OF THE 2021 SPRING CONFERENCE: THE IMPACT OF BLOCKCHAIN ON THE PRACTICE OF LAW[1]

PRESENTED BY:
NYU JOURNAL OF LAW & BUSINESS
CLASSICAL LIBERAL INSTITUTE

WELCOMING REMARKS & INTRODUCTION TO BLOCKCHAIN

Isabella Muncan: Good afternoon. My name is Isabella Muncan and I'm the Academic Events editor of the NYU Journal of Law & Business. On behalf of the Journal of Law & Business and the Classical Liberal Institute, I'm pleased to welcome you to The Impact of Blockchain on the Practice of Law.

[1] Editor's Note: The transcript has been edited for clarity. The breakout Q&A sessions with the audience are not reflected in this transcript.

During the first segment of the event, we'll hear from leading academics and practitioners in the fields of financial regulation, estate planning, contract law, and secured transactions. Professor Seth C. Oranburg will begin our discussion with an overview of blockchain technology and then we will hear from our panelists: Aaron Wright, Carly Howard, Angela Walch, Zach Smolinski, and Heather Hughes.

Following the panel discussion, members of the audience will have the opportunity to join breakout rooms of their choice and ask questions with individual panelists. The breakout rooms will be labeled by panelist and subject matter and a member of the Journal of Law & Business will be fielding questions from the audience. Please hold your questions for the breakout discussion. Without further ado, it's my pleasure to introduce the panel moderator, Professor Oranburg, editor of the forthcoming practice manual: Blockchain Law. Thank you.

SETH ORANBURG: Thank you for that introduction, Isabella. And thanks to all of you who are attending and to everyone at the NYU Journal of Law & Business for all of the hard work putting together this special event. Let's get started. My name is Professor Seth C. Oranburg and I teach law at Duquesne University School of Law and I'll be your moderator today. We have an exciting panel. We're here to talk to you about the impact of blockchain on the practice of law. To get us started, I'll talk briefly about the origins of blockchain. Although many of us today are familiar with how blockchain works, I'll give us a refresher on essentially what blockchain is and point out some of its implications for the future, and then I'll turn it over to the real experts for specific doctrinal topics.

So, what is a blockchain? Blockchain is often analogized to a straightforward, old–fashioned accounting ledger, which is a record book in which transactions are recorded. Just like a traditional ledger, a blockchain is a permanent summary of accounts in a system. But unlike a traditional ledger, which is often a singular book or a centrally located file, a blockchain is decentralized. It exists in many places on many computers at once. The magic of the blockchain is that it has built–in incentives for people to verify the records in it, so the system itself ensures its own validity. It's not really possible to explain all the details of how blockchain works in just about a minute, but in brief, a blockchain user transmits a transaction, equivalent to a new ledger entry, to a peer–to–peer network of computers around the world.

So–called miners on the network race to be the first to validate clusters of such transactions called blocks using brute force, cryptography, and code breaking techniques. The first miner to verify the block is rewarded with a coin. The cryptographic value of that block is recorded as a transaction in a new cluster of transactions that forms the next block. And so the system repeats and forms a chain: a blockchain with an essentially immutable timeline of transactions. But in truth, if you really want to understand how blockchain works, I recommend you read the first chapters, in fact, the whole thing, but certainly the first chapters of Professor Aaron Wright's excellent book, Blockchain and the Law: The Rule of Code. He provides a technical overview so straight forward that even lawyers can understand it.

Blockchain as we know it began when an enigmatic person, or people, named Satoshi Nakamoto, published a white paper called Bitcoin: A Peer–to–Peer Electronic Cash System on August 18th, 2008. This seemed to be, at least in part, a response to the great recession and the bank bailouts that happened therein, because when that same Nakamoto produced the Bitcoin software program on January 1st, 2009, which ran the program described in this white paper, the first block in that program referenced those recent bailouts. Indeed, the original purpose of blockchain seemed at least in part to be an effort to avoid central banking and banking intermediaries.

This all sounds great, especially if you're a crypto anarchist; lower transaction costs, no human error, no central control, but what happens if there are bugs in the code itself? What if these systems have vulnerabilities precisely because they are automated? How does the collective decide what is best for this blockchain structure? Panelist and Professor Angela Walch addresses these issues in her work on blockchain governance.

Bitcoin is certainly a big deal today, but the blockchain technology that powers Bitcoin turns out to have much broader applications than just a decentralized currency. Here, we have a system that can verify identity, establish trust, create and enforce contractual agreements, clear and settle transactions, and record ownership. This has the potential to disrupt a wide range of legal functions that involve assets, including trust and estate planning. Unfortunately, lawmakers do not seem to fully understand how blockchain–based transactions fit into our existing legal schemes. But fortunately, we have scholars like professor and panelist, Heather Hughes, who is sorting this out, at least for secured transactions, through her scholarship.

We are already seeing disruptions in financial services. Historically, cross–border payments have been innately complex and inefficient because there's no global payment system. JP Morgan responded to that by taking the blockchain backbone and developing their own JPM Coin to facilitate the instant transfer of digital payments across the globe on what they call the Quorum blockchain platform.

But the possibilities for new financial services based on blockchain technology are far greater than just payment processing. Savings accounts, tax records, and even entire stock exchanges could become powered by blockchain technology. This will create new challenges for estate planning, as we ask questions like "where did grandma put the private key for her blockchain Bitcoins?" Panelist Carly E. Howard has answers for digital asset planning.

More recently, non–fungible tokens, or NFTs, made a big splash when artist named Beeple sold the digital rights to this collage, Everydays: The First 5,000 Days, for an incredible $69 million. Whether or not this is truly the first purely digital work of art, this happening challenges concepts in IP law and economics. Online content was typically considered non–rivalrous, meaning consumption by one person does not prevent simultaneous consumption by another person. In other words, everyone can be playing the same intangible video game code at the same time, unlike that physical Nintendo 64 which your mother told you had to share with your brother. But NFTs create artificial scarcity of digital works, making them rivalrous and exclusive like physical goods. Come to think of it, I'm not even sure I'm allowed to show this slide. Let's call that academic fair use, okay?

Blockchain technology is leading us to ask new questions about the legal status of "stuff." Things on a blockchain can act like investment securities, like digital currency, like intellectual property, like real property, like some mix of all that, or like something else. Take Ripple, please, really, I mean it. Take my Ripple, I can't get rid of this stuff. Trading of XRP or Ripple tokens has been suspended because the SEC took action against ripple for conducting an unregistered securities offering. Ripple's founders claimed that the token is a cryptocurrency, not a security, but the SEC begs to differ, arguing that XRP is different from Bitcoin because it was never decentralized.

Wait, what? Isn't blockchain a decentralized technology. It turns out not all blockchains are created equal. There are public blockchains, like Bitcoin, but there are also private blockchains like JP Morgan's. Although some call that a permission blockchain—let's just say it's complicated. But fortunately, we have experts like our panelist Attorney Zach Smolinski who's appeared on TV to discuss new digital "stuff," like Facebook's Libra cryptocurrency. And so, today, we have a distinguished panel of blockchain experts who are here to help us understand this new technology and its implications for the practice of law.

I'm pleased to present to you Aaron Wright, associate clinical professor of law and founder and director of the Tech Startup Clinic at Cardozo Law who will discuss decentralized finance, affectionately known as DeFi. Carly Howard is an attorney and wealth strategies consultant who will discuss the impact of blockchain on estate planning. Angela Walsh is a professor of law at St. Mary's University School of Law in San Antonio, Texas, and a research associate at the center for blockchain technologies at University College in London who will discuss blockchain and software governance. Zach Smolinski is a registered patent agent and a principal in the IP and transactional law practice at Smolinski Rosario Law in Chicago. He will discuss smart contracts. And Professor Heather Hughes is professor of law at American University and she will discuss the impact of blockchain on secured transaction law.

Before I turn things over to our panelists, I would like to invite anyone in the audience who is interested in advancing our collective understanding of the impact of blockchain on the practice of law to email me or my co–editor, legal technologist Rob Kost. Together, we're editing a new practice manual titled simply Blockchain Law, and we are seeking authors to contribute chapters on practical blockchain and law topics. The manual will be published by Fastcase (Full Court Press), a leading legal publisher that focuses on democratizing access to legal information, a goal that Rob and I share. We have plans to hold more events like this one featuring our chapter authors and others who are interested in speaking about blockchain in the law, so please let us know if you're interested in participating in that adventure.

Presentation 1: Aaron Wright—The Growth & Regulatory Challenges of Decentralized Finance

Seth Oranburg: With that, I'd love to turn this presentation over to Professor Aaron Wright for his perspectives on decentralized finance.

Aaron Wright: Thanks so much, Seth, and thanks for the great introduction. My name's Aaron Wright. I'm a clinical professor at Cardozo Law School and director of Cardozo's Blockchain Project. Just give me a second to share my screen and then we'll get moving. So, Seth started with, I think, a great introduction about blockchain technology. Many folks may have heard about Bitcoin and roughly understand how it works. One way to think about Bitcoin is it's a decentralized payment system, kind of like a decentralized central bank, and that's an analogy that folks have used.

Over the past year, we've really seen a whole new category of blockchain technology emerge and what it's really and squarely focused on is decentralizing other forms of financial services. So I'm going to run through this quickly. I may go pretty fast. The whole presentation is here. But decentralized finance, affectionately known by many in the blockchain ecosystem as "DeFi," is a fast growing sector. It used to be the fastest—probably NFTs, which Seth also mentioned in the introduction, are growing faster at this point. And what they're doing is that they're using smart contracts, or small little bits of code that operate on a blockchain, most often on the Ethereum blockchain, to create financial services and other products that are non–custodial in nature.

So instead of having some centralized intermediary that's facilitating a financial service or product, they're just relying on these automated smart contract–based systems to do that. And ideally, they don't rely on one central party, but in practice, some do. But I think over the longer arc and increasingly, you're going to see core aspects of what we see down in Wall Street, or other parts of the globe when it relates to financial services, managed increasingly by these automated software–based systems. As Angela knows, who is going to speak, the lexicon and the use of phrases in blockchain technology, are often mystifying and often inaccurate, but there's some words that you may increasingly see, especially if you begin to dig in.

DeFi applications are often administered via online portals, often referred to as "dApps," they're supported by individuals that pool together their assets into a liquidity pool, and those that deposit assets into a liquidity pool are referred to as "locking their assets" and often earn fees and/or automatically receive other digital assets also known as "governance tokens." The practice of submitting these assets to DeFi protocol is increasingly referred to as "liquidity mining" and the process of earning fees under governance tokens is referred to as "yield farming." So I just wanted to lay down that foundation because I'm going to use some of those terms throughout the rest of the presentation.

This is a big deal and this number should be updated, it's actually $55 billion. There's about $55 billion of total locked assets in DeFi up from about $1 billion at the beginning of this year. What's really interesting between it is that there's a dynamic emerging between Bitcoin, the grandfather of all digital assets, whereby Bitcoin is being locked into decentralized finance and earning a yield. So for the first time, we have a closed loop system where digital assets can create a return in other digital assets, and I think that's particularly notable. So it's growing super fast and it's also creating this closed loop system which has the potential to grow rapidly.

There are lots of different areas of decentralized finance, just like the financial services industry. I'm going to highlight some, but there are many more that are coming down the pipeline. The kind of the core engine of decentralized finance are DEXes, or decentralized exchanges, which operate a little bit like the New York Stock Exchange or NASDAQ or some other exchange, but without a centralized custodian. There are borrowing and lending protocols that are emerging. Oftentimes, they generate a stable asset known as a "stablecoin." There are more advanced derivatives and synthetic asset protocols, insurance protocols, and other market protocols like prediction markets. On top of all of these different smart contract–based systems, we're starting to see aggregation tools, so

DEX aggregators and yield and asset management protocols. So going back to the way Seth, when he was referring to JP Morgan at the beginning of the program, you can start to see that a lot of these other core functions of the financial services industry are beginning to get filled in.

One way to conceptualize this if you're a little bit more visual is to think about what's emerging in this schema. You have a core blockchain, which is being used as a settlement layer. You're seeing smart contract–based protocols that are emerging on top dealing with these core functions: borrowing, lending, DEXes, etc. Many of these core protocols spit out or rely on other tokens or other assets, including governance tokens, stablecoins, or depend on wrapped assets. And then there's an aggregation layer that's emerging on top. Plugging into this are crypto–to–fiat gateways (those could be centralized exchanges or other services), Oracle services (which are data services—you can think of them as a little bit like Bloomberg, KYC, and identity solutions, which are fast coming, although not here yet), and then token factories (which generate various different things).

Lots of potential benefits that are cited by the developers here: lower cost, greater accessibility, permissionless access, financial inclusion. One notable one, which is really coming into focus, is all of these systems talk to one another. So today, we've got lots of legacy financial infrastructure that the banks or other financial services participants have created. They don't talk well to one another. They were built in an earlier era of computing. Lots of challenges with getting them to be able to work with one another and transmit information to one another. Because this is all being rebuilt with the ground up and 50 plus years of computer science behind it, all these systems have the ability to interact and talk to one another. Great opportunities with that, great risks, as I'm sure some of the other speakers may highlight.

Also, some interesting ideas about having community–run financial infrastructure, which I think goes to Seth's point also at the beginning. Lots of blockchain technology has a veneer of trying to improve the financial services industry and some of the dangers that we saw in 2008. One idea here is to actually have greater and broader stakeholders support them and potentially higher degrees of security. At the same time, lots of problems, right? Really hard to use this stuff—it feels very much like the early Internet if you remember that. There's a lot of leverage that's getting introduced to the system which creates risks. As many regulators know, runs on liquidity, entropy, and complexity that can be created by this composability. And obviously, what's most relevant to us lawyers are regulatory questions.

So I just wanted to kind of run through and unpack a couple of these and then highlight at least how I think some of the regulatory approaches to DeFi may shift a bit. So DEXes are really, really interesting. They rely on a formula and underlying smart contracts to be able to enable folks to trade digital assets without using an order book. I think that that's pretty notable for most markets. I imagine from the time we set up underneath the buttonwood tree to today, there was some order book or order book-like system that was created.

DEXes operate a little bit differently. They pull together assets through a liquidity pool and that lessens the need for an order book. We may see order books kind of appended onto this, but it lessens the need for it. There was no central administrator of that pool. It's maintained by the smart contract. It's open and permissionless, which means that anyone can list a digital asset for exchange to anybody around the globe. And these smart contracts are "alegal." So not illegal, but alegal—they don't necessarily incorporate regulatory compliance.

Pricing on DEXes is accomplished entirely algorithmically. The way it works is that you're making a trade with a pool of assets. So it's not a peer–to–peer trade, it's a pool–to–peer trade. So people pool assets and you're able to get another asset back nearly instantaneously with a pricing that's automatically generated without the need to be matched to a counterparty, which is interesting. At least as of today, the larger an order or a trade relative to the size of the liquidity pool underneath it, the worse rate people receive. Thus, the goal is for many of these AMMs to build very, very large pools of liquidity. And at least looking at more mature markets, they're not even close to that yet.

Pricing is maintained in an interesting way. It assumes kind of where the market is today, that there's going to be algorithmic arbitragers that are going to profit on any price disparities between centralized exchanges and decentralized exchanges, and there's a number of decentralized exchanges. We've seen some large financial services companies emerge that basically engage in this arbitrage. And also, to incentivize people to provide liquidity, the smart contracts award the providers with fees and governance tokens with the right to kind of manage the smart contract set up. Unlike other financial services companies, because all the activity is occurring on an underlying smart contract, people can access and interact with the smart contracts from a whole bunch of different front ends.

Uniswap, which is a notable decentralized exchange, has about 50,000 different, separately, independently run portals that enable you to interact with it. So imagine if JP Morgan, to use an example, had 50,000 different sites to interact with it. Some of these systems are hosted by the original smart contract developers, others are hosted and increasingly will be hosted on decentralized file storage solutions that are not maintained by one central party.

Super low barriers to entry, especially with DEXes. Most of this technology is completely open source, so there's very, very little proprietary rights that are imprinted over the code itself, although there's a little bit of a shift to that recently, and the liquidity providers appear to demonstrate low loyalty to a particular DEX which suggests that over time they may become commoditized.

There are lending protocols. Some notable ones here are Compound, AAVE, and Maker. The way that these work is that people deposit digital assets into a vault, i.e., into a smart contract, and they borrow another token, oftentimes the stablecoin. Some of these protocols create or aim to create a stable digital token through this borrowing and lending function. One example here is that you can deposit some amount, let's say like 1,000 Ether, and get back 200 DAI or stablecoin. And through this kind of overcollateralization, you're able to get a stable loan and a stable asset that comes out of it.

I'm just going to flip forward. One thing to note about this is that often times these rely on outside data feeds—oracles— which determine the value of the collateral deposited by a user and its liquidations are done in an interesting way, pretty much any party is able to liquidate a lending position if it drops below a certain liquidation ratio.

We're also seeing a whole host of more advanced DeFi projects emerge, including decentralized derivative and synthetic asset protocols, and these are probably the most risky parts of DeFi, just like they're the most risky parts of traditional finance. What happens here is that people deposit some amount of an asset of some sort, which they can overcollateralize and pull back a synthetic asset based on that.

So that's just a little bit of an overview of the kind of the base protocols. What's notable here also is that we're starting to see some aggregation layers emerge on top. There are three major types of aggregators: DEX aggregators, yield aggregators, and assets managers. So what DEX aggregators do is they operate a little bit like Google. They search through all the DEXes and all the tokens that are being traded on these DEXes and find you the best price for it, just like Google finds you the link that you want. You can get better pricing if you're a trader, they're entirely non–custodial in nature, but important from a regulator's perspective, they may serve as points of centralization. And just like how we see more regulations heaped on top of Google or other aggregation layers when it comes to information, I wouldn't be surprised that these DEX aggregators are turned to apply an increasing range of financial regulations.

We're also seeing similar aggregation occurring at the yield level. So folks that are looking to maximize the return are using yield aggregators, a notable one here is "Yearn," where they're able to just deposit their assets into Yearn and have the return maximized.

And the last set, which is interesting, is asset managers. We're starting to see new tools that help people either track, manage, or hedge their exposure to different tokens. So you can deposit into a smart contract a basket of tokens and get back another token. It looks like a very basic or rudimentary index fund, also looks like the beginning of securitization.

So just to kind of take a step up, core aspects of the financial services industry are increasingly managed by various different smart contract based systems. This is moving really fast. A lot of this stuff has been built in the last year. So if you fast forward five years, you can start to see really an entirely digital Wall Street that's built.

So let's just touch on, for last couple of minutes, and I know I'm running out of time, Seth, some regulatory considerations. One thing, just to note here, the laws don't go away as I think we all know. The big question is: how decentralized are these systems? Are there any centralized actors? If there's not, who's going to be the party that's responsible if there's an issue? These are questions that the government has begun to look at, most notably starting with the DAO, which was an earlier decentralized autonomous organization and the SEC issued a 21(a) Report related to it.

There are a host of issues here, right? And I'm sure as I was talking, many of the more experienced lawyers in the room were just starting to tear up and cry at the number of regulatory issues, or maybe not crying, maybe they were thinking about different things, but thinking about all the issues that are emerging here. And these fall into well–recognized buckets from AML, KYC, or other laws that are aiming to stamp out fraud or other concerns related to terrorist financing, to commodities exchange act issues (to the extent that some of these assets are considered commodities), to the host of securities–related issues that we saw during the token boom from 2016 to 2018. This is going to raise some big questions related to liability for developers. In general, software development is protected and often protected under the First Amendment. That's not a complete bar. We've had courts in the past impute liability against software developers—wouldn't be surprised if we start to see some activity there.

There's a big question though here about the degree to which and the effectiveness of bringing certain actions against developers as even acknowledged by the CFTC. If you bring an action against a developer of a smart contract, it doesn't do that much. These smart contracts, these systems can't be stopped. They're running on a blockchain and until the blockchain itself either has a fork or in some way is rendered moot, which seems difficult to perceive, these systems will still be available. So it doesn't really have a strong deterrent effect. We may see liability also imputed for maintaining interface relating to the underlying smart contract, some centralized control over some core mechanic, or potentially deploying the smart contract itself.

We've seen approaches like this taken by the SEC in a case called *In the Matter of Zachary Coburn,* which related to an earlier decentralized exchange which was fairly centrally run. These are the factors in part, although not dispositive, that the SEC focused in on. My sense is, over the longer arc though, we'll see expanded theories of secondary liability emerge. There are already hooks for that in the existing regulations where parties that aid and abet or control certain aspects of these systems will be found liable. We've already seen the CFTC kind of edge into this in a case *CFTC v. Edge Financial Technologies* where they relied on the aiding and abetting standard to hold the software developer responsible for some bad activity.

SETH ORANBURG: Aaron, we're just about out of time. So just if you don't mind, just we'll need to close it up.

AARON WRIGHT: Okay. So I think this is where it's going—expanded theories of secondary liability. And just last point to lead here, I do think there are a lot of lessons from the copyright wars that we saw before related to how to impose liability on more decentralized systems. I wouldn't be surprised if we see more conversation around creating kind of a safe harbor to balance the need for innovation with the need to obviously build markets that do not hurt consumers. So thanks and sorry I went a minute over.

SETH ORANBURG: No, it's fine. Thank you, Aaron. That was a really interesting point too about the movement from peer–to–peer lending to pool–to–peer lending. I know LendingClub just stopped their peer–to–peer lending services, and so really a neat preview into what's next for finance. So thank you so much for that introduction, more than introduction, really very, very interesting. And by the way, if you have questions for Aaron, we do have that breakout session afterwards, so please feel free to join his room to talk further.

PRESENTATION 2: CARLY HOWARD—BLOCKCHAIN & ESTATE PLANNING

SETH ORANBURG: Up next, I'd love to introduce Carly Howard who's going to talk to us a bit about estate planning. Carly, feel free to take it away with your slide show at this point.

CARLY HOWARD: Thanks, Seth. Hello, everyone. I have the challenge today of talking about a very vintage area of the law, estate planning, along with very cutting–edge technology, blockchain. So I'll be attempting to merge these two areas of the law in a mere fifteen minutes. Let me share my presentation for you here. Let's see. Play slideshow. Does that look good, Seth?

SETH ORANBURG: Yep. You're all set. Looks great.

CARLY HOWARD: All right. So my career has been a bit different from most of the lawyers that you'll hear from on this call. I've had what they call a portfolio career. I practiced estate planning for high net worth clients and fiduciary litigation in the United States and then moved into wealth management for ultra–high net worth clients, including family offices. That's where I became interested in alternative investments, venture capital, private equity, offshore entities and trust accounts, and eventually digital assets. I have a consulting company. My main client and favorite client right now is Status.im. It's a decentralized messenger app, private browser, and crypto wallet, all in one. Really cool app, right on your phone. They raised $100 million in an ICO in 2017, so I help manage all of the issues related to that and business management as well. I'm also a principal with 01 Ventures, which is a deep tech VC based out of Amsterdam. We invest in startups in the European deep tech scene. Then I have a more traditional estate planning practice with Sibila Law out of Miami, Florida. So my perspective on estate planning is very practical.

There are three main areas of estate planning. One is trust and estates planning or drafting. Another is probate and trust administration. Then there's fiduciary litigation. In a typical law school estate planning class, trust and estates class, they'll talk mostly about the property principles and the foundations of drafting law and maybe probate administration. But I would say it's really important to understand how trust administration works and how fiduciary litigation works, because if mistakes are made in an estate planning document, you may not know it for 30 years or more when your client dies and then it's too late to make changes because they're deceased. So it's really important to know how these documents play out in real life and what happens if you get it wrong.

From a digital assets perspective, we're looking at a global estate planning consideration like we never have before. Estate planning is affected at the state level, federal level, and also globally. And because of the things that Aaron was talking about before—that these decentralized systems, cryptocurrencies have no boundaries, that all of these systems connect and talk well with each other—we really have to take a more global perspective than we ever have before.

The basic estate planning documents that everyone should have are last will and testament, power of attorney (sometimes called a durable power of attorney), healthcare power of attorney, and living will. I like to tell people that they do have an estate plan. Even if you don't have a will, you have the default *state* estate plan, which doesn't usually work for people. Most states have not really addressed cryptocurrencies directly, so I would recommend that anyone holding digital assets goes to an attorney who understands cryptocurrency and digital assets and has an estate plan put together. For additional privacy and some tax planning, we add in some other documents, including a revocable living trust and maybe a life insurance trust.

Then at a more complex level and looking at advanced tax strategy, we start adding in entities such as limited liability companies, grantor retained annuity trusts, private trusts, and the offshore entities that I mentioned before. Charitable planning as well. As much as I would love to dive into these today, because this is the really complicated, fun puzzle piece part of estate planning, we just don't have the time, so I'll move on to the next slide reluctantly.

My point in going over this overview of estate planning is that for digital assets, every step in this process is important. Cryptocurrencies especially are affected at every single part of the process. I'll just say very briefly that there are a lot of tax filings involved in an estate, particularly if an estate is taxable, and in the US, that's a very, very high amount of assets. For a married couple, it's over $20 million. So there aren't many taxable estates, but even for a regular estate, there are tax forms to be prepared, so working with professionals who don't understand cryptocurrencies and don't understand how these things should be reported can lead to some negative consequences.

We've been talking about blockchain today. Digital assets is really what's addressed in estate planning. There isn't much addressing cryptocurrency directly at this point. We'll come around to that in just a moment. But digital assets means domain names, electronically stored photos and videos, emails, social media accounts, blogs, gambling sites, Instagram accounts, Facebook accounts, avatars with rights to real world assets, tokens, cryptocurrencies, and I believe NFTs—again, nothing really addressing that that I'm aware of, but non–fungible tokens really meets the definition that we see under current law. It does not include non–transferable license such as subscriptions. And we're going to talk about some of the model rules that are in effect for all of this in just a moment.

In the beginning, the law around estate planning for digital assets was really set by large corporations in their terms of service and their privacy policies. There's a real discussion going on within the legal community about how these companies are able to draft their own terms of service—essentially creating their own body of law that kind of supersedes the law that is made by our lawmakers and courts. Again, there are some model rules that we'll talk about in a moment, but federal data privacy laws prohibit individuals from accessing another's online content without their permission.

So in the beginning, these large companies, even companies like Facebook, were very adverse to letting even agents under power of attorney or personal representatives of a decedent get access to a Facebook account or some kind of email account, online photos, etc. But it's a little bit different now. Most of those companies now have policies that are easy to work with or they fall in line with the model rules. I make a joke sometimes that dealing with large company terms of service and privacy policies is really like when you need to talk to a customer service agent at a large corporation and you dial the 1–800 number and you're just sitting there and you keep getting transferred and it's very difficult. Dealing with the terms of services for these companies is really a nightmare for a personal representative of a decedent or family member who really doesn't want to be dealing with these kinds of things. So adding the complexities of digital assets on top of that is even more frustrating, especially for personal representatives who are not tech savvy.

We do have the Fiduciary Access to Digital Assets Act which was passed in 2014 and revised in 2015. And I make a little joke here—*at long last*, we have some model rules—because in my opinion, these were about a decade late. 2014 was pretty late to be dealing with digital assets. The revised rules do not specifically mention cryptocurrency because they were passed in 2014 and it really wasn't a hot topic at the time, I suppose. You can fit cryptocurrencies into the definition and rules around digital assets under the revised act, but it's not a great fit and it leaves a lot of gray area.

The real issue is, what kind of permission does a client have to give in order for their personal representative or other agent to have the power to access those digital assets, move and transfer and interact with those digital assets, open and close accounts in the principal's name, etc. So when it comes to cryptocurrencies—where assets are stored in a wallet and there are private keys and it's not a centralized company like a bank account—then we really run into some gray area and the type of permissions that the law is usually looking for are not something that we would do in crypto. In fact, it's the opposite of what we would do in crypto. Most of these laws are looking for your client to give specific permissions and access to what most crypto holders would consider to be a centralized person. So that's a really difficult concept for crypto–savvy clients to kind of wrap their head around. There are also some pitfalls in the revised model rules around how we are going to make changes when there's no centralized party.

Moving on to a more practical perspective, with cryptocurrencies especially, the biggest problem in crypto estate planning is also the biggest problem in crypto: while you're alive, don't lose your private key. This is huge. I have this conversation over and over, whether it's with my clients or just the whole cocktail party situation, as they call it. When I'm around crypto people, this is what we talk about. We know not to give our private key to anyone, but yet, if we become incapacitated or pass away, someone needs to be able to access our cryptocurrencies, access our wallet, and transact with those digital assets. So if we give someone that key phrase now, then they'll have access now. There's really no way to modify that in most circumstances.

We can get around this in various different ways. During lifetime, power of attorney is a document that gives an agent the ability to act for the principal. Those are usually put in place effective immediately, or at least in the past they were. One thing we can do is make those powers of attorney springing so they do not actually become valid until the principal is incapacitated. And that's not usually what estate planners would have recommended previously, but that's one way to get around it. After death, the trick is to try to put those key phrases and private keys somewhere where either only your trusted fiduciaries have access to them, or after your death, after your client's death, access to those key phrases is available. That's more tricky than it sounds. We'll come back around to that in just a moment.

I spend a lot of time just convincing clients to organize their personal affairs. This is for high net worth clients or just "regular Joe" clients. Organization is the number one thing that we struggle with. So that involves not just getting together a list of financial assets, including digital assets, but also tracking IDs, passwords, etc.

SETH ORANBURG: Two minutes, please, Carly.

CARLY HOWARD: Okay. I'll point to this last bullet point before we move on to the next slide. Dual control keys is pretty common. Multi-sig is an industry standard in crypto where one person has part of the private key and another person has the other part of the private key or multiple people are sharing pieces of that private key. That's probably the most commonly used way to protect your wallet.

The next few slides are about fiduciaries. This is what I was talking about before when I said that there's a centralized party in crypto. A fiduciary is a person who is managing in some way, or administering in some way, the assets of another person and there's a higher level of duty there that the trustee or the personal representative or the agent owes to the beneficiary. So this is a centralized party and it kind of flies in the face of everything that the crypto believers are trying to do, so it's kind of hard to even address this with some folks.

This slide, if you want to go back to this, splits out what documents are necessary during lifetime and death to try to explain who the fiduciaries are. Then in the last slide, I'll just wrap up here. The probate administration process can take several years. If it's a smaller estate or less complicated estate, it can move very, very quickly. But it can take a long time depending on complexity. But crypto moves fast, so it's really important to have a plan for all of this.

It's also important to have a fiduciary competent in digital assets management or at least someone that they can talk to, because even if you have a very responsible, trustworthy fiduciary, if they don't know how to access your Bitwarden or your Ledger, which is more complicated than it seems, then that's going to be a problem.

So I'll end by saying, choose your tools wisely, and this is something that our chief security officer at Status is always teaching us about. We have some preferred tools, but pass-word managers are really important. You don't want that to be broken into, but you want someone to be able to access your passwords. Using hardware keys is important. Don't knock the centralized exchanges, like Coinbase and Kraken. Those exchanges have built–in ways to pass on your account to somebody else. So for someone who wants to invest in cryptocurrencies but is not digitally savvy, that's a perfectly valid solution. Ledger is probably the hardware wallet of choice, and then a Liberty Safe and good old pen and paper does wonders. For some of my clients, they write down with a pen and paper what their private keys are, all of their passwords, etc., they put it in an old–school safe that only they have the combination to, knowing that when they die their personal representative will have to go to court, they will have to be named personal representative by the court, and at that time, they will hire a locksmith to come and break that safe open. So that's what some of my crypto elite clients are doing.

SETH ORANBURG: Thank you, Carly.

CARLY HOWARD: That will wrap it up. Thanks, Seth.

SETH ORANBURG: Yes, marrying the high tech and the low tech, that's practical right there, and so absolutely great advice. You definitely need to have a plan because if you forget that private key, that Bitcoin disappears. People have lost millions by losing just a 64–bit number.

CARLY HOWARD: Yeah, and I think we're going to see more of that too as people start passing away and then their representatives can't find their keys.

SETH ORANBURG: Right. I can't even find my car keys, so, I mean, this is going to happen certainly.

PRESENTATION 3: ANGELA WALCH—BLOCKCHAIN EMERGENCIES & OPEN–SOURCE SOFTWARE GOVERNANCE: IS "ROUGH CONSENSUS" A SUICIDE PACT?

SETH ORANBURG: So, next we have Professor Angela Walch. I would love to hear from you about software and governance and how blockchain fits into that as well. So please take it away, Angela.

ANGELA WALCH: Hi. Thank you so much for having me today. I've enjoyed these earlier presentations. Again, my name is Angela Walch, and I'm a professor at St. Mary's University School of Law in San Antonio and a research associate at the UCL Centre for Blockchain Technologies. It's great to be with everyone here today. A lot of this stuff that we have heard discussed ties in with what I am thinking about. My talk is probably a little bit less heavy on the legal intricacies and more on thinking about how lawyers need to be concerned about mechanics that underlie these systems and the "who is doing what" at the base level of these systems.

So my talk here today is called Blockchain Emergencies and Open–Source Software Governance: Is "Rough Consensus" a Suicide Pact? I am fascinated by worst case scenarios, and so that's what you're going to get today. Basically, how we're going to proceed in this talk is to situate ourselves with what I'm referring to here. I am concerned with the governance of these protocols at the base level. I'm concerned with, "How is Bitcoin run? Who gets to make decisions about Bitcoin? How is Ethereum run? Who gets to make decisions about Ethereum?" Why does this matter? Well, it matters because—I think we've already heard a great demonstration of why it matters—these protocols at the base are supporting this whole DeFi structure that Aaron was discussing earlier, right? All the complexities and different complex financial products that are being built there, they sit on top of these infrastructural base level protocols. I think we need to be aware of how these things work and the systemic risks that they can pose if we're not really pressing on assumptions and practices in those areas.

So I will talk about what the normal protocol governance looks like in some of these systems, of course keeping in mind that every one is slightly different. I'll talk about how their governance might differ in emergencies in the systems, and then post some open questions that I think we need to come up with answers to so that the systems we're building atop of the base level are reliable if we're putting big financial systems on top of that.

This was the best picture I could come up with to just kind of show you what I'm thinking about. I wish that it were actually the other way around, that you would have the thin layer at the bottom and go up into this bigger triangle at the top. But basically, I'm concerned with what's happening at the bottom of a structure. When things go wrong at the bottom, at the foundations, that can then make things on top of it fall apart, for instance the decentralized finance infrastructure. So I'm thinking about the very bottom level.

We've heard discussion today about how the systems are decentralized and there's been a lot of writing about how power is shared across the system and there are lots of checks and balances involved so that no one can really force anyone to do anything. So we have software developers who are involved in writing software and maintaining it, looking for bugs, and helping to figure out what upgrades would be helpful to the system and socializing those with the larger community and ultimately proposing those to be adopted. You have people who are running the software in these systems, the nodes in the system, who do not have to run anything that they don't want to run. We've heard also that the code that runs Bitcoin, Ethereum, most of these crypto systems, I would guess all of them—although Aaron noted that there's some new developments in that area—the code is open source. So the idea is that everyone can read the code, they can decide if they want to do a proposed upgrade or not. It's on them, it's their choice, so checks and balances, the developers don't have ultimate power. Same with the mining pools and the miners who are in these networks—the ones that bundle up the transactions and add them to the common ledger that everyone is keeping.

So there's been talk about how, well, look, this is actually a lot like constitutional systems like we have, like in the US. You have different parties who are active in the governance system and power is not absolute in any one of those settings. So here on the screen, you're wondering what I'm talking about of "BIPs" and "EIPs." This is the standard way that changes to the software are made in, for instance, Bitcoin and Ethereum. So we have a BIP, which is a Bitcoin Improvement Proposal, and an EIP, Ethereum Improvement Proposal, that anyone can make if they have a suggestion for how the software of the systems should change. It's important to remember that software is how the systems run—it implements the governance. Software implements the policy choices that people make and that they then reflect in the code that is run on the system.

So there are processes within this open–source software development context that are used in standard situations. Proposals are made, there's a lot of vetting of these proposals by other developers in the system as to whether they are technically sound, they might be a good idea, there's a lot of community discussion about them. Then we go from here to more community discussion. Finally, once there's enough community discussion and the [developers ("devs")] are comfortable with it, they say they've reached kind of "rough consensus" on whether this upgrade is a good idea and the devs will finalize that new software release and push it out to the network for people to choose whether they want to run it or not. So the nodes and the miners don't have to run it—as I said, they get to choose—and the outcome is that either the network will fork or it will stay together. So that's the typical process of software governance. People generally say checks and balances, it's a pretty decentralized system.

So in theory, in non–crisis times, power is decentralized, right? These things that I just said here: checks and balances, no one can force anyone to upgrade, the code is transparent (anyone can look at it and decide for themselves whether they want to run it, and you don't have to upgrade if you decide you don't want to), and if it's a type of software upgrade that would not allow you to stay with the existing blockchain, you can fork, right? You can go on your own and you don't have to be governed by the new proposal. So this is the theory for non–crisis times.

There are also crisis times, and these are the ones I'm really interested in. I like this picture because it was called the apocalypse or something in the database I found the pictures on. So, blockchain emergencies, what are these? They are events that happen such as a bug in the code, a flaw that's discovered perhaps in the cryptographic proofs that help to support the blockchain's operation and they can bring down the system if people exploit them. And we have had a number of blockchain emergencies that have occurred in major blockchains over time.

Just a few examples of these. We saw in Bitcoin, in the fall of 2018, an inflation bug that if exploited could have blown past the famed 21 million limit on Bitcoin. People discovered it in time and worked to fix it. So don't worry. As far as I know, the 21 million cap is still safe. But it was a critical bug in the software. Similarly, we saw in Zcash, another more private crypto system, that there was a flaw in the cryptographic proof that if exploited, again, could have essentially broken the system, made it uncredible and made it lose all its value. This was revealed by the Electronic Coin Company—the people who had discovered this flaw and managed its resolution. They revealed that in 2019.

What's different in these emergencies when these events come up? Well, the normal standard governance processes that I talked about go out the window. Remember, transparency is a big deal in these, socializing with the community, taking time to review, people understanding what they're getting into. All of that goes out the window in emergency situations. In each of these situations—you can go and read the bug reports, and there's lots of very interesting discussion put out by the people who are involved in resolving these issues—only a few people were told about the flaw or the emergency. They determined the severity of the issue and how to handle it. They didn't tell the public the truth about the situation until later on when they were sure that the situation had been fixed by people upgrading their software already. So the fix was kind of hidden in the name of saving the blockchain. Key mining pool operators were told to upgrade first, again, to save the network.

So I know I'm coming probably close to the end of my time. I think we really need to think about these situations given the billions and billions, if not now soon to be trillions of dollars in value riding on these systems, on these base level protocols. What's a blockchain emergency? How do we know when we're entering into this state of exception and go outside our standard governance practices? Who gets to decide? How much has to be at stake? Is it enough for people to lose money? Is it that the core principles of the system, like the cap of 21 million, is at stake here? Who decides what is an emergency? What practices are okay in a state of emergency that are not okay in normal times? Can you forego this critical, crucial tenet of transparency in order to save the system? Who needs to be informed about the problem? Who needs the truth about the problem? And what obligations do those who are running these emergency protocols owe to users and the public? So, if you are familiar with any of the discourse around states of emergency and the discussion around US constitutional law, when do we suspend our normal practices and who's the boss then? Very analogous . . . .

SETH ORANBURG: I think we may have frozen on you, Angela. What a cliffhanger. I think Angela might have frozen just as she was wrapping up, so we'll allow her a minute to respond at the end of our panel. Sorry about that technical issue. But quite an interesting presentation and really reminds me of that miniseries, Chernobyl, where they just didn't want to talk about what was happening at the nuclear power plant and that led to a further disaster and creating the wrong incentives. I love to think about incentives.

PRESENTATION 4: ZACH SMOLINSKI—SMART CONTRACTS

SETH ORANBURG: Let's now hear from Attorney Zach Smolinski. He's going to talk to us about smart contracts and practices in this area. Also a registered patent attorney. Zach, if you would please, we'd love to hear your thoughts on the impact of blockchain.

ZACH SMOLINSKI: Thank you, Seth, and thank you also to Isabella for your work in organizing this event and also to the NYU Journal of Law & Business and to the Classical Liberal Institute for hosting today. I'm going to take a little different approach. I'm not going to refer to slides during my talk here and I'm going to try to keep things relatively simple and a little more freeform.

Let me just go over briefly what my goals will be in my discussion today. I'd like to give the audience an overview of what smart contracts are and why lawyers and law students might care about them. I have a secondary underhanded goal, which is to instill a little bit of skepticism in these topics. There's a lot of boosterism in this space and the boosterism can lead to a lack of clarity around some topics. I'd like to encourage everyone in the audience today to take this discussion as a series of hooks into this topic. Almost everything I say is going to refer to a bunch of other topics. As you've heard from the presenters up to this point, there's really no such thing as an isolated topic in this space. You quickly get into, what are the technical backgrounds behind what we're talking about? What are the legal connections? What are the business and governance issues around these things? For all these topics, it's definitely has gotten to the point where it's an irreducibly complex area. My hope would be that we can just very simply go through some of these topics. Of course, any real questions that remain bring to the breakout sessions afterwards and then also feel free to get in touch with me directly if you'd like.

I start with a discussion of what we're going to talk about, smart contracts, and what are contracts, then, I think is part of that question. As I'll say later, it's not really a valid lead into the topic. Smart contracts are so different from what we think about as being standard legal contracts that it's almost a misnomer. You'll hear later in my talk here that smart contracts have a quite defined area of operation and that at this point is really very limited compared to what we think about in the contractual world more generally. When we think about contracts in law school, we hear about offer, acceptance, consideration; we can talk about the underpinnings of why are contracts enforced and theories of reputation. And I think those are all very interesting topics. You can imagine a situation where everyone knew immediately the reputation of everyone they ever dealt with. Would you need contracts at all? Maybe, maybe not.

Interestingly, Bitcoin and the Bitcoin white paper reaches that very topic with the idea of not needing to trust others as members of this network. And then smart contracts do play into that. So there is this sort of vague overlap with contracts and thinking about contracts. How do we deal with contracts on a day–to–day basis and edging closer to that smart contract topic? Well, contracts as they exist today are hard to create and to enforce. You may need to get an attorney involved, it can be tough to negotiate. They might be hard to read, they might be hard to understand, especially for non–lawyers. A lot of times contracts are signed and forgotten. They can be tough to keep track of. You have corporate contract management systems and breaches of contract are often difficult or impossible to detect. When you're talking about the world of contracts, you're talking about just a multi–varied . . . you could spend your entire career exploring nothing but these topics, and some people do and work within these topics as transactional lawyers and contract lawyers.

We think about how contracts reach into the electronic world. This has been going on for quite some time. E–contracts are nothing new. eBay started in 1995, Amazon, started operations in 1994. But interestingly, if you want to look back a little farther, you can look back to 1869, which was the year of the first court case affirming that an electronic contract was enforceable, and there it was made via telegraph. So the topic is not particularly new. In fact, I think smart contracts arguably in a bit of a stretch, but analogy, go back even further than that.

But moving on, we have these e–contracts as part of our day–to–day life. We click through these agreements and they're a mess, right? If you want to join some new social network, which it seems to be a new one every two weeks or so, you're going to sign on to some list of terms and conditions. The Facebook terms are 4,000 words long. The terms and conditions for the Zoom platform which we're using today, and I'm sure everyone read them before we hopped on today, because why wouldn't you, that's 7,000–word long terms and conditions that underpin this Zoom platform. So, what you see is the technology hasn't solved the complexity of contracts. What the technology has enabled is us to enter into all these unknown and almost unknowable contracts on a regular basis. I couldn't tell you the exact terms under which Zoom is allowing me to speak to all of you today. The idea that technology is somehow easing up the means by which we interact with contracts is a little bit of a stretch in my opinion.

But I guess we're all okay with that. What happens is that blockchain technology comes along and it says in some iterations of blockchain technology, "I'm going to try to make this world easier for you as a user. I'm going to try to make it so that you can enter into agreements more easily, so you can transmit value more easily." One way to think of it is I think, well, almost nobody really understands a whole lot about contract law and almost nobody understands a whole lot about blockchain. So what are we doing? We're glomming together this very complex topic with this other very complex topic and how can any of us hope to ever make sense out of all this?

You heard earlier Professor Wright talk about the complexity of DeFi and the advent of decentralization. So the idea becomes, well, can we decentralize this and through that means give people a little more power and make it better for the average consumer? I think the answer there is sort of maybe. I think the jury is a little bit out on that question.

Stepping back a little bit, why am I even talking about this? I'm talking about this because a lot of the narrative of blockchain, DeFi, smart contracts, is decentralizing access to complex topics, democratizing finance, democratizing contracts, and making things easier for people. When I look at the field, I can honestly say that is not happening. I do not think it is easier for anyone to do almost anything today via a blockchain or via smart contract than it was to do much the same things five or six years ago. Now, others will push back against that, and if you really are into DeFi, you can pool assets and you can yield farm in ways that you couldn't do before. So these options are increasing, but I really question if they're getting any easier. I've talked about this now for almost my entire time and I haven't even really told you what I think a smart contract is.

So, what is a smart contract? Now, sort of giving you the background of where contracts sit in the space of blockchains and crypto globally. What smart contracts are, I think people are often very disappointed to hear that they're at this point relatively simple strings of text that execute as code and they sit as addresses on a blockchain, most notably the Ethereum blockchain. And essentially what they are is that their little scripts. Now, if Vitalik Buterin when he came up with the idea for a Ethereum, if he had called smart contracts scripts or trigger scripts or something like that, fewer attorneys would be really very interested in that.

But we heard the word contract and we say, "oh, okay, well that must be a legal topic—contracts are involved." They are sort of just sitting there and they're waiting for something to happen. This is where my analogy for smart contracts is that they're closer to vending machines than they really are to anything else. So it's this bit of object code that sits out there on this blockchain, and as with the vending machine, if you come up to a vending machine and you drop a coin into it, if it's the right type of coin, it'll give you hopefully what you want if it operates properly. Likewise, if a smart contract is coded properly and operates properly—by the way, those are both big ifs, and if you're going to interact with these things, you really need to check those things out—then the smart contract will sit there, it will wait for a certain type of token to come in and it will dole out what it's supposed to dole out, or it will do an operation behind the scenes that is in line with what it's been told to do. On that point, vending machines, according to some Google searching I've done, date back to the first year CE, like the 1st century CE.

So, the ideas behind the smart contract are almost older than most of the legal ideas that are attached to them. They're extremely simple little scripts that just sit there, and when something happens, they do what they're supposed to do. So when you hear "smart contract" from now on, I would encourage you to think about it in that way, that they're just . . . I hesitate to say it because it's so sort of cliché, but they're dumb. They sit there and they wait for something to happen. And when the thing that they want to have happened, or that they're programmed to do something in relationship to happens, then they do something, and that's all they are.

I see that I'm getting pretty close here to the end of my time, so I want to wrap up with a few high level topics about comparing smart contracts to traditional contracts. Smart contracts are obviously practically speaking a whole lot newer. They're really tough for people to understand if you're not a coder, but you can start to work your way through them. If you are interested in the idea of creating and coding smart contracts, there are some very good tutorials out there that will walk you through this. You could go on YouTube, you can look up something called Solidity. Solidity is the computer language that is probably the most common popular computer language to program smart contracts in.

Maybe I'll stop there, but with an idea sort of what are we going to look at next when we talk about smart contracts and I would just encourage those participants today and those in the audience today to be aware that people are going to be talking about these things as if they're the greatest thing since sliced bread. In a lot of ways, they're much simpler than many people are wanting to admit. I would, again, encourage a bit of skepticism in this space, but also to think about experimenting with them and think about what rules might you want to set up as a lawyer for your clients or for your own business? And can you imagine a situation where you would want a script to do something almost automatically, or definitely automatically, in response to getting a particular type of input? That might be something that a smart contract can be useful for.

With that, I would encourage you to come into the breakout room if you're interested about this topic. There's certainly a lot of different directions we can go on this. Once again, Seth, thank you for your organization and your time here and your work on this event today. Really appreciate it.

SETH ORANBURG: Thanks. That was great, Zach. I think it wouldn't sell as well if we call them dumb contracts. I think this is sort of sales, but absolutely super interesting analogy to the vending machine, because really what you're talking about is something that simply hopefully just operates and doesn't really . . . . This is not intelligence. We'll have another talk about whether artificial intelligence is intelligence. But in any event, definitely join Zach in the breakout room for conversations about how coding interacts with lawyering at the intersection of smart contracts.

PRESENTATION 5: HEATHER HUGHES—BLOCKCHAIN & SECURED TRANSACTIONS

Seth Oranburg: Up next, we have Professor Heather Hughes who is going to talk to us about how blockchain can inform our understanding of secured transactions. So Professor Hughes, if you would, please.

HEATHER HUGHES: Thank you, Seth, and thank you for putting me after Zach, because in the second part of my presentation I will be relying on the concept of smart contracts. They have very interesting implications for secured transactions.

Secured transactions are governed by Uniform Commercial Code Article 9. UCC Article 9 governs *any* extension of credit secured by personalty. If you think about it, this statute governs a *massive* swath of market activity: secured credit facilities, margin trading of securities, asset securitizations, and purchase money transactions for goods, I could name more. But it's a statute that's very wide ranging. Given this expansive scope, blockchain–based transaction platforms have numerous implications for lawyers who deal with secured transactions. In my brief time here, I'm going to identify just two of them.

The first is asset classification. As any UCC Article 9 lawyer knows, the first order of business in a secured transaction is to take whatever assets the client is dealing with and determine what definition they meet under 9–102, which is the list of asset categories. Now, this task is crucial because the rules for assigning an interest and establishing priority in assets change depending on their classification. Blockchain–based assets complicate this basic secured transactions task.

I'm going to illustrate how complicated it can be using the example of cryptocurrencies. If you have a secured transaction involving cryptocurrencies, you have to figure out what the digital currency is in Article 9 terms. So right off the bat, it's not money because money is a medium of exchange currently authorized or adopted by a domestic or foreign government under UCC 1–201. Now, it complicates things that some governments *may* adopt central bank digital currencies. It also complicates things that the UCC definition of money does extend to monetary units of exchange established by agreement between governments. So you could have a deal where you're dealing with central bank digital currency or something recognized by an inter–governmental organization. But apart from those circumstances, deals involving cryptocurrency are not going to involve money in commercial law terms.

So, if we eliminate money as a possibility, cryptocurrency is going to be either a general intangible—that's the residual category under Article 9—or investment property. Now, if cryptocurrency is a general intangible, an investor must file a lien notice in the UCC–1 registry to establish priority. If it's investment property, on the other hand, that's a completely different asset class subject to different rules, including different choice of law rules. Lawyers dealing with these assets have to understand that cryptocurrency will be either general intangibles or investment property depending on how the parties to the transaction are holding and treating them.

Investment property under Article 9 means securities, securities entitlements, commodities, and the like. Now, this is a bit confusing because virtual currencies are not securities under the commercial code. They do not create participations in or contractual claims against the assets of an issuer. But they may qualify as investment property nonetheless if they are held by a securities intermediary.

So, investment property includes financial assets that are what the code calls "securities entitlements." If something is held by a securities intermediary pursuant to a contract in which the client and the intermediary agree to treat cryptocurrency as a financial asset, then all of a sudden, it becomes investment property for secured transactions purposes. In other words, the commercial code enables investment property classification for digital assets that would otherwise be general intangibles. This is important because interest in investment property are subject to rules that enable investors to take control of assets and thereby have assurance of priority in the event of bankruptcy or other threat of subordination.

The governing rules for general intangibles on the other hand do not permit control of assets as a means to establishing priority. So it's very important for lawyers and clients, when companies are seeking to leverage the value of virtual currency, to understand when and how this currency can be investment property under the UCC. Asset classification affects governing law. If in any given deal cryptocurrency is a general intangible, then the law where the debtor is located governs perfection of a security interest. If cryptocurrency qualifies as investment property and an investor is going to establish control over the assets, then the jurisdiction where the securities intermediary is located will govern perfection of the security interest.

The bottom line is that lawyers working on secured transactions involving cryptocurrencies have to be diligent in establishing exactly what kind of asset, in commercial law terms, they are dealing with. You have to assess that correctly before you can prepare deal documents and certainly before you can render a perfection and enforceability opinion letter. When you think about the fact that asset classification affects governing law, you may have to make sure you are licensed in the jurisdiction that is going to govern perfection and the effect of perfection of the security interest before you can render an opinion letter to close a secured transaction involving virtual currencies.

Cryptocurrency is just one blockchain–based asset that presents these types of classification challenges. For example, several states are beginning to recognize decentralized autonomous organization limited liability companies. The classification of membership interests in those entities present analogous issues. I could come up with more digital assets that present these issues as well, cryptocurrency is just one of the most obvious. So asset classification is a major issue for lawyering in the blockchain space.

The second big issue I want to talk about is blockchain–based smart contracts and UCC Article 9. This second topic may be of particular interest to litigators. Agreements that market actors do not currently associate with UCC Article 9, when expressed as smart contracts, behave like secured transactions. For example, consider a blockchain–based smart contract expressing a services agreement that automatically captures assets if one party fails to perform services on time. The parties may not associate their transaction with secured lending, but their agreement partitions assets for the enforcement of an obligation. And as such, a court could conceivably characterize such an agreement as a security interest governed by UCC Article 9. If a court did this, then it could test the asset capture and disposition mechanisms for commercial reasonableness under Section 9–610. If states enact limits on electronic self–help, and some do, then those statutory parameters would apply as well.

Under UCC Section 1–201, a security interest is any interest in personal property or fixtures which secures payment or performance of an obligation. And under Article 9, the statute applies to any transaction regardless of its form that creates a security interest in personal property by contract. Personalty of course is anything that's not realty, so any blockchain–based asset or digital asset. I could talk about digitized deeds to real estate, but I don't want to waste time on that now.

So, smart contracts do not impose duties. As Zach indicated, they're not like contracts really, they do not impose duties, they do not involve an exchange of promises. Rather, they implement a mechanism. They commit to a future outcome by submitting parties to self–executing terms expressed in code. So given that they do not involve duties or obligations to be performed or not at the discretion of the contracting parties, they are different in nature from the traditional contracts to which Section 9–109—the scope provision of Article 9—refers. But despite this difference, parties agree to a smart contract mechanism that dispatches assets in satisfaction of the agreement's terms. Because of this, we can view them as security interests within the scope of the statute. A perhaps very concise way of saying this is that with smart contracts, people say they're neither smart nor contracts, but they have a legal effect in that they segregate assets—they have property consequences—even if they do not have straight forward contract consequences.

As Article 9 lawyers know, to establish a security interest, there are three requirements: to have value given (that's a consideration requirement), the debtor has to have rights in the collateral (that's the property concept that you can only transfer what you have), and there has to be evidence of intent to create a security interest (that's a statute of frauds requirement). You could go through each of those requirements and argue that a blockchain–based smart contract satisfies them.

Now, a litigant opposing security interest treatment for a blockchain–based smart contract could argue against it. Such a litigant could argue the agreement is not a contract within the meaning of the UCC and therefore not a security interest. Or a litigant could argue that blockchain–based asset transfers put the assets beyond the reach of creditors. So there are arguments to be made here.

The bottom line is lawyers should be aware of how the functionality of blockchain–based smart contracts invokes secured transactions law even in context that they might not traditionally associate with secured lending.

SETH ORANBURG: Thank you. That was really informative and it reminded me of how difficult it is to classify these new, well, "things" as I alluded to at the beginning. We had all these issues with . . . is a cryptocurrency as a security? And now also, is it a security interest? So, thank you for all of that.