MASLON

Blockchain, Smart Contracts, and Cryptocurrency: Addressing Litigation Risks

Maslon LLP
Judah Druck & David Suchar
April 28, 2022

Crypto is everywhere. What were once niche terms and concepts—"DeFi," "Web3," "initial coin offering"—have now become ubiquitous, with billions of dollars being poured into the world of crypto by banks, hedge funds, governments, and individual investors. Decentralized finance is no longer reserved for individual futurists: Coinbase went public in April with a nearly $100 billion valuation. TurboTax will now allow users to deposit tax refunds into crypto accounts. El Salvador accepts Bitcoin as legal tender. Jamie Dimon once called Bitcoin a "fraud"; now, JPMorgan has a bank in the "Metaverse." The debate over whether crypto is here to stay, appears to have subsided.

But, as with all trends, the growth in crypto raises novel legal issues and risks. Coinbase has been sued for allegedly doing too little to prevent the hacking of and theft from user accounts. Celebrities like Kim Kardashian and Floyd Mayweather have been drawn into litigation for participating in alleged crypto "pump and dumps." The SEC is currently engaged in a first-of-its-kind litigation with Ripple Labs over its offering of a digital coin in violation of federal securities laws. Corporations have filed a new wave of lawsuits seeking to protect their intellectual property from NFT "owners."

None of the questions implicated by these lawsuits lend themselves to obvious answers. Indeed, they raise fundamental questions regarding the ways in which preexisting laws can (and should) be applied in this new world. This article assesses the litigation risks within four primary areas in the world of crypto (blockchain, cryptocurrencies, NFTs, and the Metaverse), and how statutory and common law has been applied to ameliorate—but often exacerbates—these risks.

I. BLOCKCHAIN

Any discussion of decentralized finance must start with the blockchain, which serves as its keystone. The blockchain is a public, universally distributed ledger that records transactions, including, but not limited to, those involving the exchange of cryptocurrencies or other crypto-assets. Before a transaction can occur, it must be verified to ensure that the transfer is valid, which includes confirmation that the funds (say, Bitcoins) being transferred are not duplicates or counterfeit. Once the transaction is verified, its details (including source, destination, and date/time) form a "block," which is added to the ever-expanding blockchain. This process repeats itself each time a transaction takes place.

The transparent nature of the ledger assures its trustworthiness. Any attempt to change transaction records or edit the underlying code would be futile, as millions of users, each with their own copy of the blockchain, would quickly spot inconsistencies and discard them. Blockchain users continue to develop additional ways to maintain the ledger's security, with companies like JP Morgan and Toshiba recently introducing quantum physics as a way to protect the blockchain from computer attacks.

Despite the inherent benefits in the blockchain—trust, decentralization, improved security and privacy—courts have expressed skepticism about its reliability. In *Hunichen v. Atonomi LLC*,[1] for

[1] No. C19-0615-RAJ-MAT, 2020 WL 6875558 (W.D. Wash. Oct. 6, 2020)

example, a Washington federal court refused to take judicial notice of blockchain evidence, explaining that it was not convinced such evidence "is necessarily complete, its contents not subject to reasonable dispute or varying interpretation, and its use not improper as a defense to otherwise cognizable claims." The court's skepticism went even further, noting that defendants had "fail[ed] to identify a single case in which a Court has found such evidence properly considered in support of a Rule 12(b)(6) motion to dismiss." Thus, while the blockchain is increasingly gaining acceptance in the financial industry, attorneys should be aware that courts may be less enthusiastic (or less familiar) with the emerging technology.

Nor is the blockchain's purported freedom from third-party oversight without limits. In *United States v. Gratkowski*,[2] the Fifth Circuit considered whether an individual had a privacy interest in the information held on the blockchain (which consists of the amount transferred, the address of the sending party, and the address of the receiving party). Federal agents had used an outside service to analyze blockchain and identify the Bitcoin addresses controlled by an illicit website, which they then used to subpoena Coinbase for the identity of any accounts that had sent Bitcoin to the website's addresses. Defendant was one such customer, whose motion to suppress such evidence presented the "novel question" of whether an individual has a Fourth Amendment privacy interest in the records of their Bitcoin transactions. The Fifth Circuit answered in the negative. Citing caselaw concerning bank records and cell-site location information ("CSLI"), the court explained that "Bitcoin users are unlikely to expect that the information published on the Bitcoin blockchain will be kept private," and that even though users "enjoy a greater degree of privacy than those who use other money-transfer means," it was "well known that each Bitcoin transaction is recorded in a publicly available blockchain," which made it "possible to determine the identities of Bitcoin address owners by analyzing the blockchain." Thus, Defendant lacked a privacy interest in his information on the blockchain. Users of blockchain technology should therefore be wary that the "decentralized" and "anonymous" nature of blockchain does not currently carry any constitutional privacy protections or any true "confidentiality" at all.

II. CRYPTOCURRENCIES

Cryptocurrencies are digital assets that resemble regular currencies—they can be purchased, traded, and exchanged. Rather than relying on bank or government control, however, cryptocurrencies are wholly decentralized, allowing anyone to easily transfer funds with few restrictions. Transactions are recorded on the blockchain, and while Bitcoin was the world's first cryptocurrency, it is now joined by thousands of alternatives (known as "altcoins"), including Ethereum, Dogecoin, and Tether (a "stablecoin" pegged to the US dollar).

As with the blockchain, courts and regulators struggle to fit cryptocurrencies into preexisting legal concepts. In fact, how to even *define* cryptocurrencies remains an open question. While courts have agreed that cryptocurrencies are "commodities in interstate commerce" and, therefore, subject to regulation by the Commodities Futures Trading Commission,[3] they are not currently

[2] 964 F.3d 307 (5th Cir. 2020).

[3] *Dekrypt Cap., LLC v. Uphold Ltd.*, No. 82606-9-I, 2022 WL 97233 (Wash. Ct. App. Jan. 10, 2022).

treated as "legal tender" or even "money" under federal law.[4] Nor is it clear at this time whether cryptocurrencies are "commodities" or "securities." While the Securities and Exchange Commission successfully sued a company for offering a cryptocurrency, alleging that the defendant failed as part of a public sale of securities to file a registration statement.[5] The treatment of cryptocurrencies is still being debated, and indeed is central to the SEC's current dispute with Ripple Labs.[6] Companies looking to participate in a coin offering should make sure to keep up to date on the latest regulatory guidance.

Separate from determining which regulatory scheme should properly encompass cryptocurrencies, end-users have been at the forefront of recent litigation concerning cryptocurrencies. In *Archer v. Coinbase, Inc*.,[7] the court considered the responsibilities of cryptocurrency exchange platforms to its users when a theft occurs. In *Archer*, plaintiff sued Coinbase after his third-party cryptocurrency coin ("Bitcoin Gold") was stolen through a hack. Coinbase refused to support the new currency, but plaintiff alleged that Coinbase was negligent and breached the parties' contract.

The court granted summary judgment in Coinbase's favor, explaining that the parties' User Agreement did not require that Coinbase "provide services related to any particular digital currency created by a third party," and that "Coinbase had no legal duty to provide any services beyond those it agreed to provide in the user agreement." Parties, therefore, face litigation risks if they are unfamiliar with the contractual terms they enter into with an exchange or other third-party cryptocurrency facilitators, including by failing to appreciate the scope of the contractual relationship and/or the responsibilities of the parties.

Finally, litigation risks may arise using "smart contracts," which are self-executing agreements placed on the blockchain. For example, an apartment rental "smart contract" may require that a certain amount of Bitcoin be automatically transferred to the owner every month; a failure to transfer will automatically lock the apartment. The use of such agreements has increased in recent years, given their removal of intermediaries, the need to monitor and enforce the contract, and any concerns of theft, misappropriation, or tampering. But the use of "contract" is a misnomer of sorts, as it is currently unclear whether a smart contract is subject to the same contract laws applicable to a typical written instrument. Is a smart contract a "written" agreement such that the Uniform Commercial Code is applicable? Where is the smart contract located for purposes of determining a proper forum and state's law to apply in the event of litigation? Are disputes concerning smart contracts arbitrable? How might a court interpret ambiguous terms in a smart contract, notwithstanding the automatic execution of the smart contract's terms? Such questions remain unresolved, leaving those entering the smart contract space with few guaranteed legal protections.

---

[4] *Atwal v. NortonLifeLock, Inc*., No. 20-CV-449S, 2022 WL 327471 (W.D.N.Y. Feb. 3, 2022).

[5] *U.S. Sec. & Exch. Comm'n v. Kik Interactive Inc*., 492 F. Supp. 3d 169 (S.D.N.Y. 2020).

[6] "Ripple's Legal Brawl With SEC Could Help Settle When Cryptocurrencies Are Securities," Wall Street Journal (February 2, 2022), *available at* https://www.wsj.com/articles/crypto-industry-hopes-looming-legal-brawl-will-thwart-secs-regulation-push-11643724002.

[7] 53 Cal. App. 5th 266 (2020).

III. NFT

A non-fungible token ("NFT") is a blockchain-based token tied to a specific digital asset, like a drawing of an ape wearing clothing (known as a "Bored Ape" for example, each one part of the "Bored Ape Yacht Club," a 10,000 NFT grouping with a current floor price of approximately $235,000 per NFT). Ownership of the NFT reflects ownership of that asset: thus, while users can save a picture of an ape on their own computers, true ownership lies with the individual listed as having purchased the token on the blockchain (much in the same way a tourist with a picture of the Mona Lisa does not actually "own" the Mona Lisa). The discussion of the merits of and investment in NFTs is largely moot; the market has spoken. Indeed, the NFT market grew to approximately $41 billion in 2021, including the sale of an NFT by internet artist Beeple for $69 million.

NFTs have been the subject of numerous lawsuits focused on the "ownership" component of the NFT, as well as intellectual property disputes concerning the subject of the underlying digital asset itself. For example, in *Playboy Enterprises Int'l, Inc. v. www.playboyrabbitars.app*,[8] a district court issued an injunction against a website selling Playboy Rabbit NFTs, which improperly used the Playboy trademark. Companies like Nike have filed similar lawsuits to protect their intellectual property from the growing NFT market.[9] Individuals seeking to buy or sell NFTs should, therefore, investigate all IP implications, including whether the NFT at issue is truly an original work and/or whether the IP owner has provided permission for its sale/distribution.

Additionally, and as seen with cryptocurrency exchanges, NFT purchasers have taken action against marketplace websites for the theft of their assets. OpenSea—one of the largest NFT marketplaces—was sued in February by a user whose Bored Ape NFT was stolen due to an alleged exploit within the website.[10] As in *Archer*, the determination of OpenSea's liability will likely turn on the user agreement entered into between OpenSea and its NFT vendors, including any contractual obligations or responsibilities arising therefrom (if any).

IV. METAVERSE

Finally, the "Metaverse" introduced an entirely new set of litigation risks. The Metaverse, as described by a district court in the recent high-profile antitrust litigation between Epic Games and Apple, is "a digital virtual world where individuals can create character avatars and play them through interactive programed and created experiences," which "both mimics the real world by providing virtual social possibilities, while simultaneously incorporating some gaming or simulation type of experiences for players to enjoy."[11] As the court recognized, the Metaverse represents "an ongoing trend of converging entertainment mediums where the lines between each medium are beginning to mesh and overlap." Such overlap makes the introduction of legal

[8] No. 21 CIV. 08932 (VM), 2021 WL 5299231 (S.D.N.Y. Nov. 13, 2021).

[9] *Nike, Inc. v. Stockx LLC*, No. 1:22-CV-00983 (S.D.N.Y. Feb. 3, 2022).

[10] *McKimmy v. OpenSea*, No. 4:22-CV-00545 (S.D. Tex. Feb. 18, 2022).

[11] *Epic Games, Inc. v. Apple Inc*., No. 4:20-CV-05640-YGR, 2021 WL 4128925, at *13 (N.D. Cal. Sept. 10, 2021).

concepts even more difficult. In the *Epic* litigation, for example, the court recognized the difficulty in determining whether the Metaverse constituted a "video game" or merely "entertainment," a question it believed was best left "to the academics and commentators."

These questions remain unanswered, even with Facebook's recent entry into the Metaverse (along with its corresponding name change to "Meta"). But we can glean some of the larger legal implications of the Metaverse from earlier cases involving similar digital worlds. In *Evans v. Linden Research, Inc.*,[12] a California federal court certified a class action filed by users of Second Life, an "internet role-playing virtual world" that allows users to buy and sell "virtual items," including property. The dispute in question concerned the meaning of "ownership" within Second Life. Plaintiffs argued that they were entitled to "an actual ownership interest in the virtual land and items in Second Life's virtual world," while defendants argued that users only possessed copyrights. The case settled before any rulings on the merits occurred but the case represents an example of similar disputes that will likely arise over "ownership" in the virtual world, particularly with certain "lots" of Metaverse property exceeding millions of dollars.

As with NFTs, IP rights will likely be a significant source of litigation in the Metaverse. Users in Second Life have sued one another for alleged copyright infringement, including over the alleged copying of "virtual animal" breeds.[13] Users have also obtained Certificates of Registration from the U.S. Copyright Office for digital artwork in Second Life and have sued to enforce those rights.[14] Procedural law has also been implicated, including when a court ruled that representations made by Second Life's CEO to a global audience were sufficient to establish minimum contacts for specific personal jurisdiction, while also declaring Second Life's arbitration clause within its terms of service unconscionable.[15] Similar disputes will undoubtedly arise in the Metaverse, making it critical that participants think through these issues before setting up a virtual shop.

[12] *Evans v. Linden Rsch., Inc.*, No. C 11-01078 DMR, 2012 WL 5877579 (N.D. Cal. Nov. 20, 2012).

[13] *Amaretto Ranch Breedables v. Ozimals Inc*., No. C 10-05696 CRB, 2012 WL 359729 (N.D. Cal. Feb. 2, 2012).

[14] *FireSabre Consulting LLC v. Sheehy*, No. 11-CV-4719 CS, 2013 WL 5420977 (S.D.N.Y. Sept. 26, 2013).

[15] *Bragg v. Linden Rsch., Inc*., 487 F. Supp. 2d 593, 598 (E.D. Pa. 2007).