
Blockchain Law

Liability rumblings along the blockchain

Robert A. Schwinger, *New York Law Journal* – July 16, 2019

In his Blockchain Law column, Robert A. Schwinger writes: When parties interact in transactions conducted via blockchain technology, they may find themselves in relationships to one another that the law has not yet had the opportunity to clearly define. Courts, commentators, governmental officials, litigants and legislatures are now exploring which participants in various kinds of blockchain-based activities might be subject to liabilities for injuries or wrongs allegedly arising from those activities.

When parties interact in transactions conducted via blockchain technology, they may find themselves in relationships to one another that the law has not yet had the opportunity to clearly define. Courts, commentators, governmental officials, litigants and legislatures are now exploring which participants in various kinds of blockchain-based activities might be subject to liabilities for injuries or wrongs allegedly arising from those activities.

Liability for smart contract coders?

Because courts have held that certain blockchain applications, such as virtual currencies, may be subject to the regulatory authority of the Commodity Futures Trading Commission (CFTC), *CFTC v. McDonnell*, 287 F. Supp. 3d 213 (E.D.N.Y. 2018); *CFTC v. My Big Coin Pay*, 334 F. Supp. 3d 492 (D. Mass. 2018), participants in those blockchains potentially can be subject to CFTC enforcement activity or other liabilities under

the Commodity Exchange Act (CEA), 7 U.S.C. §1 et seq. In the fall of 2018, CFTC Commissioner Brian Quintenz addressed the subject of how, “[i]n the context of decentralized blockchains, ... on top of which multiple applications can run autonomously via smart contracts,” the CFTC should “identify[] who is responsible for ensuring that activity on the blockchain complies with the law.” [Remarks of Commissioner Brian Quintenz at the 38th Annual GITEX Technology Week Conference](#) (Oct. 16, 2018).

Commissioner Quintenz focused his discussion on “blockchain networks [that] allow smart contracts to be integrated into the chain,” explaining smart contracts to refer to “computer code containing all terms of the contract [that] is self-enforcing—meaning the software can execute the terms of the contract without additional input from the parties.” He asked “what steps should the CFTC take if it learns of a smart contract protocol that may implicate its regulations?” In other

Robert A. Schwinger is a partner in the commercial litigation group at Norton Rose Fulbright US LLP.

More than 50 locations, including London, Houston, New York, Toronto, Mexico City, Hong Kong, Sydney and Johannesburg.

Attorney advertising

Reprinted with permission from the July 16, 2019 edition of the *New York Law Journal* © 2019 ALM Media Properties, LLC. All rights reserved. Further duplication without permission is prohibited. www.almreprints.com · 877-257-3382 · reprints@alm.com

words, if “the hypothetical product at issue is within our jurisdiction, but is not being executed in a manner compliant with CFTC rules,” then “[w]ho should be held responsible for this activity?”

There are some parties involved with the blockchain in this smart contract scenario that Commission Quintenz felt could not appropriately be held responsible. He rejected placing liability on “the core developers of the underlying blockchain code” if they themselves “had no involvement in the development of the smart contract code” that programmed the violation of CFTC rules into the system. He commented that “it seems unreasonable to hold them accountable for every subsequent application that uses their underlying technology, without further evidence of knowledge or intent.” “Similarly,” he said, “miners and general users of the blockchain are not in a position to know and assess the legality of each particular application on the blockchain.”

However, Commissioner Quintenz said he was inclined to allow liability to be placed on “the developers of the smart contract code that underlies these event contracts.” The “appropriate question,” he said, was “whether these code developers could reasonably foresee, at the time they created the code, that it would likely be used by U.S. persons in a manner violative of CFTC regulations.” If the smart contract code developers reasonably could have foreseen the use of their creation for such an illicit purpose, then “I think a strong case could be made that the code developers aided and abetted violations of CFTC regulations” so as to face liability to the CFTC under CEA §13(a), 7 U.S.C. §13c(a). His logic would also permit such persons additionally to face liability in private civil damages actions under the aiding and abetting provisions of CEA §22(a)(1), 7 U.S.C. §25(a)(1).

Not everyone shares Commissioner Quintenz’s views, however. Some have characterized his vision as a “novel use of a longstanding form of liability” on which “it may prove difficult for the CFTC to prevail ... when the smart contract at issue is executed on a public permissionless blockchain.” See Jonathan Marcus et al., “Smart Contract Coders May Face Aiding and Abetting Risk,” Law360 (Feb. 27, 2019). These commentators note that because of “the anonymized nature of blockchain transactions” and the seeming lack of any “direct or special relationship” between the participants, it may be difficult for the CFTC to “identify a primary violator” or “establish[] that the smart contract coder had knowledge of the primary violation, and intentionally assisted the primary violator,” because “[s]mart contract coders may create code and make it available for use by others without necessarily

knowing who is using the smart contract or why they are using it.” Id. So far, however, there has not been actual litigation that puts either side’s view to the test.

Liability for cryptocurrency trading platforms?

Actual litigation is already in motion, however, over what non-contractual duties might be owed in a different blockchain setting, that of a cryptocurrency trading platform. *Berk v. Coinbase* is a federal court litigation pending in the Northern District of California (Case No. 3:18-cv-01364-VC) arising from the launch of the cryptocurrency Bitcoin Cash in late 2017 in the wake of “hard fork” of the cryptocurrency Bitcoin.

Berk arose out of the fact that in mid-2017 a group of developers who wanted to change some of the technical parameters for the blockchain for the cryptocurrency Bitcoin proposed a code change. Others, however, wanted to leave Bitcoin operating as it was. This led to a so-called “hard fork,” whereby some of the computer nodes that were part of the Bitcoin blockchain verification process upgraded to the new software while others did not. The result was two separate blockchains and two separate digital currencies. The new cryptocurrency that arose out of the 2017 Bitcoin fork was known as Bitcoin Cash, or BCH.

The plaintiffs in *Berk*, a putative class action, alleged that Coinbase (an exchange for trading, buying and selling cryptocurrencies) mishandled the launch of Bitcoin Cash on its platform by suddenly starting the launch with little advance notice and then shutting it down precipitously, thus interfering with its customers’ purchases and sales and causing them various losses, and then allegedly altering data and rewriting the trading rules. The plaintiffs sought relief under consumer protection laws as well as common-law claims for fraud and negligence.

As to negligence, the *Berk* plaintiffs asserted that Coinbase owed them “a duty of reasonable care, which it breached by engag[ing] in misfeasance, when it suddenly opened BCH for full trading before it was fully prepared to do so.” They charged that Coinbase “fail[ed] to make accurate pre-announcements about the Launch, and to take deposits sufficiently in advance to allow liquidity to develop, and to be able to open an orderly market,” thus causing the plaintiffs foreseeable harm. They added that “there is moral blame attached to this conduct as Coinbase’s conduct in allowing this manipulation infects the entire cryptocurrency community; and ... there should be a policy of preventing such future harm.”

Coinbase moved to dismiss. As to the negligence claim, Coinbase argued that it had no special relationship with the plaintiffs that might create any tort duties beyond the limited contractual obligations it assumed under its user agreements with the plaintiffs, with which Coinbase argued it had complied. At oral argument of the motion to dismiss in late April, however, it was reported that Judge Vincent Chhabria “interrupted to argue the company’s responsibility goes above and beyond those contracts. Since Coinbase created a platform where a market for a commodity is established and presides over its exchange, it has an obligation to be careful with users’ money regardless of its user agreement, he said.” A. Lancaster, [“Judge Says Coinbase’s Trading Launch Was Bungled, But It Likely Wasn’t Fraudulent,”](#) The Recorder (April 25, 2019).

Judge Chhabria was further reported to have said, “I think the special relationship Nasdaq or Coinbase has with people trading on platforms—there’s a duty to ensure the trading isn’t going to be a disaster,” noting that Coinbase “targeted a class of investors” and “established a relationship of trust.” With respect to Coinbase’s argument that the price “slippage” plaintiffs complained they experienced in their cryptocurrency trading was specifically addressed in their user agreements, Judge Chhabria reportedly stated that “[t]he slippage concept is assuming a fair and orderly market, and you might not get the price you agreed to because of slippage,” whereas “[t]his is setting up a market that is dysfunctional and will not allow for orderly trading.”

As of this time, however, Judge Chhabria has not yet issued a formal written ruling on the motion to dismiss. It thus remains to be seen whether the eventual ruling on the negligence claim will align with the judge’s reported comments from oral argument, and whether the judge will hold there to be any implicit tort duties that exist as a matter of law among persons involved with exchange platforms for cryptocurrency or other digital tokens.

Define-it-yourself liabilities in Vermont?

Rather than leave it for courts, litigants and regulators to work out who owes what duties to whom in blockchain contexts, the State of Vermont has taken a different approach—allowing parties to write their own liability rules for those involved in their blockchain ventures. Section 7 of Vermont Bill 205 of 2018, “An act relating to blockchain business development”, which took effect July 1, 2018, created a new type of business entity, a “blockchain-based limited liability company” (BLLC), which has such powers. 11 Vt. Stat. Ann. §4172.

A BLLC in its operating agreement must address various issues, one of which is to “specify the rights and obligations of each group of participants within the BLLC, including which participants shall be entitled to the rights and obligations of members and managers.” Id. §4173(2)(F). “Participants” with respect to a BLLC’s blockchain is expansively defined to consist of:

- (A) each person that has a partial or complete copy of the decentralized consensus ledger or database utilized by the blockchain technology, or otherwise participates in the validation processes of such ledger or database;
- (B) each person in control of any digital asset native to the blockchain technology; and
- (C) each person that makes a material contribution to the protocols.

Id. §4171(2). The statute defines the blockchain’s “protocols” as referring to “the designated regulatory model of the software that governs the rules, operations, and communication between nodes on the network utilized by the participants.” Id. §4171(3).

Vermont’s BLLC statute responds to concerns that blockchain ventures could pose untested wide-ranging liability risks because of their structure. As one commentator explained, because some blockchain ventures “exist largely as a loose network of independent operators,” the consequence is that “[t]his organizational looseness could pose a number of significant challenges for participants in such a [venture],” including “the potential for collective liability for the participants.” Oliver Goodenough, [“Why Blockchain Governance Matters”](#) (Nov. 19, 2018). For example, “[i]f the miners and nodes of a cryptocurrency were deemed to be partners in its business—and there are good, although not necessarily conclusive, arguments to suggest they could be—they could face the potential of daunting liability” in the event that another party were injured by a problem with the operation of the blockchain underlying the cryptocurrency, or due to issues with the use or trading of the cryptocurrency. See id. Thus, the Vermont law “allows blockchain companies to protect owners, managers and blockchain participants from unwarranted liability by forming BLLCs.” Id.

Still, liability questions may continue to arise even for such Vermont BLLCs. Is every “participant” in the blockchain, such as every individual digital asset holder, deemed to be on notice of any liability restrictions set forth in the BLLC’s operating

agreement, and thus bound by them by some kind of implicit consent? What if the terms of the operating agreement were neither known by nor reasonably available to a particular participant? Is that participant then exempt from the operating agreement's provisions—or is the participant nevertheless subject to them on a kind of “assumption of the risk” rationale?

Another question is that while the statute allows the operating agreement to “specify the rights and obligations of each group of participants within the BLLC,” is that specification always intended to be exclusive, so as to give the BLLC very broad powers to supersede literally any right or obligation pertaining to the blockchain that might exist in tort, contract or otherwise under common law? Or is the BLLC merely empowered to supplement any perceived gap between the protections blockchain participants want and what the common law would otherwise provide them, but not necessarily to wipe out all existing protections?

Conclusion

The legal system is just now starting to grapple with deciding what rights and liabilities are appropriate when disputes arise involving parties who interact in transactions conducted via blockchain technology. Blockchain ventures and their participants are likely to face an uncertain period of theorizing, experimentation, legislation, regulation and litigation before the legal system comes to consensus on what legal rights they enjoy and what liabilities such participants may face in their dealings with one another.

Norton Rose Fulbright

Norton Rose Fulbright is a global law firm. We provide the world's preeminent corporations and financial institutions with a full business law service. We have more than 4000 lawyers and other legal staff based in more than 50 cities across Europe, the United States, Canada, Latin America, Asia, Australia, Africa, the Middle East and Central Asia.

Recognized for our industry focus, we are strong across all the key industry sectors: financial institutions; energy; infrastructure, mining and commodities; transport; technology and innovation; and life sciences and healthcare. Through our global risk advisory group, we leverage our industry experience with our knowledge of legal, regulatory, compliance and governance issues to provide our clients with practical solutions to the legal and regulatory risks facing their businesses.

Wherever we are, we operate in accordance with our global business principles of quality, unity and integrity. We aim to provide the highest possible standard of legal service in each of our offices and to maintain that level of quality at every point of contact.

Norton Rose Fulbright Verein, a Swiss verein, helps coordinate the activities of Norton Rose Fulbright members but does not itself provide legal services to clients. Norton Rose Fulbright has offices in more than 50 cities worldwide, including London, Houston, New York, Toronto, Mexico City, Hong Kong, Sydney and Johannesburg. For more information, see nortonrosefulbright.com/legal-notices.

The purpose of this communication is to provide information as to developments in the law. It does not contain a full analysis of the law nor does it constitute an opinion of any Norton Rose Fulbright entity on the points of law discussed. You must take specific legal advice on any particular matter which concerns you. If you require any advice or further information, please speak to your usual contact at Norton Rose Fulbright.