Bloomberg BNA

BNA's
Banking Report™

VIRTUAL CURRENCY

Blockchain Technology and Legal Implications of 'Crypto 2.0'

BY JUDITH ALISON LEE, ARTHUR LONG, JEFFREY STEINER, STEPHENIE GOSNELL HANDLER AND ZACHARY WOOD

Virtual currencies—digital representations of value that can be transferred, stored and traded electronically—have steadily become more widespread, with the most well-known, Bitcoin, increasing to a market capitalization of nearly $4 billion since its creation in 2009.[1] While much of the focus on virtual currencies has been directed at their potential to act as a substitute for or complement to fiat currencies, there is a growing view that the true innovation is the infrastructure underlying virtual currencies: the decentralized ledger of transactions called the ''blockchain.'' Proponents of blockchain technology believe that this underlying system could have far-reaching effects in a wide variety of industries and applications.

Judith A. Lee is Co-Chair of Gibson, Dunn & Crutcher LLP's International Trade Practice Group and a partner in the Washington, D.C., office. Arthur S. Long is Co-Chair of the firm's Financial Institutions Practice Group and a partner in the New York office. Jeffrey L. Steiner is a derivatives regulations counsel in the Washington, D.C., office. Stephenie Gosnell Handler is a corporate associate in the Washington, D.C., office and Zachary Wood is a litigation associate in the Palo Alto, Calif., office.

Virtual Currencies and the 'Blockchain.' Bitcoin's system of transactions is decentralized: no central authority tracks, approves or secures transactions made on the Bitcoin network. To achieve a secure and usable system, Bitcoin's database (the ''blockchain'') relies on cryptography. The blockchain is essentially a publicly viewable ledger that records all transactions on the network, with each user on the Bitcoin network retaining a copy of the ledger. When a new transaction is initiated by a Bitcoin user,[2] it is grouped with other transactions and these groupings—or ''blocks''—are periodically added to the ledger. The blocks are distributed to each user of the network, and the veracity of the block is confirmed by the distributed computing power of the users connected. Once a transaction is approved and sent, it is irreversible because only the authorization of the sending party is needed to initiate the decentralized process (although additions to the technology could implement functionally reversible transactions).

While Bitcoin is the most prominent virtual currency, there are over 500 other virtual currencies in existence

[1] *Crypto-Currency Market Capitalizations*, CoinMarketCap.com (Mar. 18, 2015), http://coinmarketcap.com/.

[2] Transactions on the blockchain are initiated by inputting a private key, which acts as an authorization for the transaction.

today, many of which offer their own technological variations.[3] Ripple, which has the next largest market capitalization, at over $340 million,[4] seeks to allow inexpensive and fluid transfer between currencies, both virtual and fiat. The Ripple protocol is both a decentralized payment system with its own native currency, the XRP, as well as a distributed currency exchange that supports any currency (i.e., other virtual currencies, fiat currencies and other stores of value such as airline miles).

The technology underlying the blockchain used by virtual currencies is not inherently limited to transfers of digitally stored value. A blockchain can be utilized in any application in which transaction verification or a trusted repository of information is needed. A growing number of organizations are starting to use blockchain technology to build infrastructure to support decentralized applications. One example is the Ethereum Foundation, which is developing a blockchain infrastructure on top of which decentralized, peer-to-peer applications and ''smart'' contracts can be built. Other organizations are attempting to create decentralized versions of existing internet applications. For instance, both OpenBazaar and Bitmarkets are recent open-source efforts to develop a fully decentralized marketplace whereby users would access the marketplace by directly connecting to their peers in the network. The use of a blockchain, such as the Bitcoin blockchain, could allow such a system to track reputation ratings for users and allow buyers and sellers to engage in escrow transactions with other peers acting as agreed-upon arbitrators in case of dispute.

These decentralized, peer-to-peer applications raise a number of legal questions, which we discuss below. In addition to these legal implications, there are also law enforcement concerns—many of which are the same as for the illicit use of virtual currencies or fiat currencies. However, one distinguishing characteristic is that if individuals or organizations use these applications to violate the law, such as by selling contraband on decentralized marketplaces, there is effectively no way to shut down the system, as would be possible if the market were located on a web server.

Potential Applications of Blockchain Technology and Legal Implications. To date, most regulators and enforcement agencies have focused on the use of virtual currencies in financial transactions.[5] With Crypto 2.0[6] and the expanded use of blockchain technology, the legal landscape could become even more complicated. The following is a brief list of emerging areas that may have legal implications, which we discuss in more detail below:

- financial transfers;
- multi-signature transactions;
- ''colored coins;''
- property registers;
- intellectual property;
- smart contracts;
- other data stored on blockchain;
- decentralized organizations; and
- securities.

Financial Transfers. The direct financial applications of virtual currencies and their underlying technology are the most obvious. Virtual currencies are already being used as speculative investments and as a medium of exchange in both online and real-world purchases. The decentralized ledger of the blockchain can also be used to rapidly and cheaply transfer currencies around the world. The exchange and transfer applications of a decentralized ledger may find application to such industries as global remittances, cross-border currency exchanges, inter-bank transfers and personal transfers between accounts.

While there has been increased attention to the legal issues raised by financial transactions using virtual currencies, the legal landscape gets significantly more complex when discussing the implications of blockchain technology. The addition of intermediaries and more distributed control may further confuse the distinction between what constitutes a currency, property and a commodity. Existing laws and regulations—and even proposed regulations specifically aimed at virtual currency business activities—may not be well-suited to regulate the use of blockchain technology beyond direct financial transfers. Cross-border, and even interstate transfers in the U.S., further complicate the legal landscape.

Multi-Signature Transactions. Financial transfers can also be more tailored. Escrow can be accomplished via the blockchain by using ''multi-signature transactions.'' A multi-signature transaction might consist of three parties: the two parties at either end of the transaction and a third-party ''escrow.'' Such an escrowed transaction would involve depositing the funds to a virtual currency address to initiate the transaction. Completing or refunding the transaction would then require two of the three parties to sign the transaction (enter their private keys): the satisfied buyer and seller, or one dissatisfied party and the escrow party. This arrangement allows for digital escrow in situations where the transacting parties have no basis for trust (and only requires intervention of an escrow party in the case of an actual dispute). Multiple signature transactions can also be used in situations where multiple authorizations are desir-

[3] *See Crypto-Currency Market Capitalizations*, CoinMarketCap.com (Mar. 18, 2015), http://coinmarketcap.com/ (listing the market capitalizations of over 500 virtual, cryptographic currencies).

[4] *Id.*

[5] *See* Judith Lee, et. al., ''Bitcoin Basics: a Primer on Virtual Currencies,'' *Business Law International* (Jan. 2015).

[6] Crypto 2.0 is the name given to all virtual currencies created after Bitcoin.

able, such as for approving expenditures in an organization.

While there has been increased attention to the legal issues raised by financial transactions using virtual currencies, the legal landscape gets significantly more complex when discussing the implications of blockchain technology.

While multi-signature transactions can allow for ''escrow'' services, the arbitrator in such a transaction does not actually take possession of the virtual asset. Rather, the asset is locked in what can be thought of as a virtual ''vault'' that requires, in the most basic scenario, two of three keys to unlock. So, while certain fiduciary concepts may be transferable to multi-signature escrows, legal frameworks designed to regulate escrow agents who assume full control over the asset or currency are not designed to accommodate this type of blockchain transaction. Existing state laws may also be poor fits for these arrangements. For example, California, which requires licenses for escrow agents including ''Internet escrow agents,'' defines escrow using language such as ''delivers'' and ''to be held.''[7] Existing laws may prove to be incongruous with transactions in which nothing is actually delivered to or held by the escrow party (indeed, the escrow party may take no action whatsoever in a successful transaction).

Merchant-Issued Virtual Currencies and 'Colored Coins.' Advances such as ''colored coins'' or merchant-issued cryptographic currencies would also blur the lines between spheres of regulation. For example, the current revision of New York's Department of Financial Services' ''BitLicense'' exempts ''gift cards,'' defined in part as payment devices that are usable at merchants or service providers, ''issued for a specified amount,'' and ''purchased . . . on a prepaid basis for the future purchase or delivery of goods or services.''[8] A fixed-value virtual currency created and accepted by a merchant would operate similarly to existing gift card systems. The concept of ''colored coins'' further blurs the boundaries of regulations. ''Colored coins'' are tags representing assets that are overlaid on an existing virtual currency. The resulting digital products can then be distributed as replacements for gift cards, discount coupons or other voucher-based systems like loyalty rewards. For example, a merchant could tag Bitcoin such that one Bitcoin represents a voucher redeemable for $1,000 of merchandise. However, the underlying Bitcoin still retains its own value, so the resulting product is a combination of virtual currency and asset voucher.

Property Registers and Intellectual Property. Blockchains could also be used to supplement or replace systems of recordation of ownership or other registries. Titles to property could be stored and verified via a blockchain ledger, and transfers of title could be effected—and verified—without the use of a centralized third party. Ownership of intellectual property (''IP'') could be similarly recorded on a decentralized ledger. Tokens that represent individual sticks from the bundle of property or IP rights could be individually transferred. For example, the right to perform a copyrighted work could be sold as a token on a blockchain without the need to affect other exclusive rights or renegotiate upstream licensing agreements. Government agencies may be reluctant to move official registries onto a decentralized blockchain ledger, but private systems and government departments willing to more rapidly adopt new technology may one day utilize potential blockchain advantages such as higher security, reduced opportunities for fraud and decreased cost to effectuate transfers and associated recordings of transfers.

The use of blockchain technology in the context of IP would require a further doctrinal and legislative shift. Current IP licensing law focuses on contractual relationships between parties, not a transferrable *in rem* property right that could be sold downstream. However, blockchain systems could more immediately change intellectual property law as applied to digital products, such as the doctrine of first sale in copyright. Under the first sale doctrine,[9] a purchaser of a copy of a work has the right to resell that copy. This doctrine has been problematic with regard to digital files, because there is no way to know if the original purchaser has resold the original file or simply made a second copy and kept the original. A blockchain ledger system would allow copies of digital works to be individually identified such that a seller could verifiably and fully transfer the copy, allowing application of the first sale doctrine.

Storage and Transfer of Other Data. Other information could also be transferred or stored via a blockchain. For instance, the public, decentralized verification aspect of the technology could be used to provide for secure digital signatures. Identity information could be stored and verified via a blockchain ledger, and the resulting verified identities (which could remain pseudonymous) could be used to reduce fraud on peer-rating sites, such as Yelp, or provide trust ratings for peer-to-peer marketplaces or lending services. Protocol data, such as that which serves as the basis for the internet domain name system, could also be stored on a blockchain.

[7] C.A. Fin. Code, § 17003(b).

[8] N.Y. State Dep't of Fin. Servs., Proposed New York Code, Rules and Regulations (Feb. 4, 2015), § 200.2(f).

[9] 17 U.S.C. § 109.

Although cryptographic ledgers are widely seen as secure, if personally identifiable data from other sources were exposed and correlated to blockchain data, or if blockchain data were aggregated and analyzed, transactions could be tracked and compared even though the ledger is pseudonymous.

Legal implications could include privacy concerns relating to blockchain-based identity verifications and whether a right to privacy would exist in such applications. Further, there could potentially be data breach concerns with the creation of a massive repository of information. Although cryptographic ledgers are widely seen as secure, if personally identifiable data from other sources were exposed and correlated to blockchain data, or if blockchain data were aggregated and analyzed, transactions could be tracked and compared even though the ledger is pseudonymous. In addition, as seen with the many hacks of exchanges and Bitcoin companies, while the protocol itself has not been hacked, the interface infrastructure can be ''broken'' and information intercepted at various points.

Smart Contracts. More advanced uses of blockchain technology center around ''smart contracts,'' which are self-executing computer programs that automatically fulfill the terms of the programmed arrangement. Basic versions of smart contracts would exist entirely online: a user could make a donation to a blog author, with the donation automatically transferring to the blogger after a defined number of new articles are written and posted. Smart contracts could also facilitate the sale of digital goods, with activation codes being sent via a blockchain only after payment is received and recorded in the decentralized ledger. Smart contracts could also reach into the corporeal world in the slightly more distant future. With the move toward the ''Internet of things'' and the proliferation of connected devices, transactions involving physical objects could be digitally verified and secured. Under a smart contract arrangement, failure to make a payment on a car loan could result in the car being automatically deactivated until payment becomes current, or a customer could automatically unlock a rental unit (such as at a hotel or through a service like AirBnB) by sending payment and signing a digital contract.

Smart contracts raise a number of legal issues. First, their automatically enforcing nature would make difficult the application of some classic contract doctrines. These ''contracts'' might not, for example, be voidable or cancelable even if coerced, unconscionable or rendered undesirable due to changed circumstances. Smart contracts might also be programmed to be impossible to breach, efficiently or otherwise. Second, these interactions would carry the same privacy concerns as any blockchain application. Contracts between parties would be publicly viewable in the ledger, and in the more advanced applications third parties could potentially track where a person rents a room or hotel and who is behind on car payments. Finally, smart contracts could lead to changes in the legal industry. Lawyers may be called upon to craft these auto-executing arrangements. And, although smart contracts would not require enforcement via legal action, adjudication would still be required to address liability arising from these contracts and to resolve disputes over the (irreversible and automatically completed) terms.

In more sophisticated systems, company actions could be taken automatically by the smart contracts; for instance, after a vote by the members of the organization authorizing a dividend, a dividend payment in virtual currency could automatically be distributed based on record ownership.

Decentralized Organizations. Even more complex applications of smart contracts would allow for decentralized organizations. Blockchain technology could be used to distribute rights that mirror those of traditional organizations. For example, voting rights and dividend or equity rights could be allocated through a blockchain ledger. In more sophisticated systems, company actions could be taken automatically by the smart contracts; for instance, after a vote by the members of the organization authorizing a dividend, a dividend payment in virtual currency could automatically be distributed based on record ownership.

Decentralized organizations raise issues of liability, because ultimate responsibility may be difficult to define. Because the ''management'' of the organization is conducted automatically, legal systems would have to decide who to hold responsible if laws are broken: the users/customers of the system, the creator of the initial code or the computer system itself. Similarly, the legal status of such organizations will be in question. It remains an open discussion as to whether existing legal frameworks pertaining to corporations and other business entities could be applied to decentralized organizations, or whether new regulations would need to be developed to address their unique structure and function.

Securities and Financial Products. The development of block chain technology is likely to increasingly implicate securities laws. Early attempts to offer securities in exchange for Bitcoin online have drawn Securities and Exchange Commission (''SEC'') enforcement actions.[10] More sophisticated companies have raised funding through the sale of their own native tokens while assert-

[10] SEC, *SEC Charges Bitcoin Entrepreneur with Offering Unregistered Securities*, Press Release, SEC.GOV, *available at* http://www.sec.gov/News/PressRelease/Detail/PressRelease/1370541972520#.VQE3ZPnF-Sp.

ing that these crowd sales are not securities but rather a pre-sale of access to the technology.[11] Whether a token sale is a security will be a highly fact-dependent inquiry, and the answer may vary even between multiple uses of the same underlying technology.[12] Finally, financial products can be created and executed using smart contracts, such as an ownership token for a company that automatically distributes a portion of profits to holders or a derivative contract that automatically accesses online market data. Regulators and exchanges could write rules into these smart contracts such that the rules must be met before the contracts can be executed by market participants.

Conclusion Blockchain technology and the innovation it is driving will likely continue to generate new possibilities for the way we interact and exchange information and value. In turn, these new possibilities will generate new, challenging and complex legal issues. Virtual currencies have pushed the boundaries of existing laws and necessitated a changing approach to regulation. Blockchain applications will similarly continue to require thoughtful application of existing legal frameworks combined with new legal solutions. Proponents of decentralized, distributed technology envision a future where information and interaction is unconstrained by any centralized authority, while others warn that allowing for too much automation of laws, contracts, and information flows could lead to ''tyranny of code.''[13] In any future, it is likely that blockchain technology will have some place in our business and personal lives, and legal frameworks will need to be adapted or devised to accommodate the resulting innovations.

[11] *See, e.g.*, Kashmir Hill, *The First 'Bitcoin 2.0' Crowd Sale Was a Wildly Successful $7 Million Disaster*, Forbes.com, http://www.forbes.com/sites/kashmirhill/2014/06/03/mastercoin-maidsafe-crowdsale/.

[12] *See, e.g.*, Pete Rizzo, *When is a Token a Security? Research Analyzes Blockchain Under US Law*, CoinDesk.com, http://www.coindesk.com/token-security-research-analyzes-blockchain-us-law/ (reporting on a working paper produced by SWARM, a decentralized crowdfunding startup, in consultation with attorneys, policy groups and scholars from Harvard and MIT). At the time of this writing, the SWARM working paper is available via link in the CoinDesk article.

[13] *See, e.g.*, Primavera De Filippi, *Tomorrow's Apps Will Come from Brilliant (And Risky) Bitcoin Code*, Wired.com, http://www.wired.com/2014/03/decentralized-applications-built-bitcoin-great-except-whos-responsible-outcomes/.