Lawyers' Acceptance of Digital Currencies:
Nebraska Ethics Advisory Opinion No. 17-03 (2017)
and Remaining Risk Management Concerns

By Gilda T. Russell[1]

I. Introduction.

Recently, the Nebraska Lawyers' Advisory Committee ("Committee") issued Ethics Advisory Opinion 17-03 (2017) ("Opinion"), approving lawyers' acceptance of digital currencies as payment for legal services and from third-parties for the benefit of clients. The Committee also approved lawyers' holding digital currencies in trust or escrow for clients and third parties. The Opinion, the first formal ethics opinion dealing with this subject, cited several ethics rules applicable to lawyers' acceptance and holding of digital currencies and required that certain safeguards be followed for lawyers to be compliant with the rules.

While the Opinion applies to Nebraska lawyers, the relevant Nebraska ethics rules are largely identical to the corresponding American Bar Association Model Rules of Professional Conduct ("ABA Rules"). Given that almost all states' ethics rules are based to large extent on the ABA Rules,[2] the Opinion will likely have some impact on other jurisdictions' assessments in this area.

However, notwithstanding the Committee's ethics assessments, there remain several risk management concerns with regard to law firms' acceptance of digital currencies. The Opinion and these remaining risk management concerns and their recommended resolution are discussed below.

II. Operation of Bitcoin and Other Digital Currencies.

At the outset of its Opinion, the Committee gave a brief history of digital currencies, focusing primarily on Bitcoin. The Committee stated "Bitcoin and similar computer program protocols are essentially shared ledger books maintained by networked computers" and are called "digital currencies."[3] [4]"Digital currency that

---

[1] Gilda T. Russell is a Paragon Consultant and Preferred Service Provider. She has practiced, taught, and written in the professional responsibility and risk management fields for many years.

[2] California is the only state that has not yet adopted a version of the ABA Rules. However, the approach under the relevant California ethics rules is very similar to that under the Nebraska ethics rules cited in the Opinion as well as the corresponding ABA Rules.

[3] Throughout the Opinion, the Committee's assessment of Bitcoin applies, as well, to other digital currencies. There are a very large number of digital currencies, with Bitcoin, Ethereum, Bitcoin Cash, Litecoin, being among the largest. *See* Duggan, "On the Breadth of Cryptocurrency: How Many Kinds of Digital Currencies Are There?," Benzinga.com, August 8, 2017. https://www.benzinga.com/general/education/17/08/9893336/on-the-breadth-of-cryptocurrency-how-many-different-kinds-of-digital

has an equivalent in real currency, or that acts as a substitute for real currency, is referred to as 'convertible' virtual currency," with Bitcoin being an example. Bitcoin is digitally traded and "can be purchased for, or exchanged into, U.S. dollars, Euros and other real or virtual currencies."[5]

The Committee further explained that "Bitcoin exists on a peer-to-peer network on the Internet," and is "open sourced," which means that anyone can obtain the Bitcoin computer program and programming code, evaluate and use the same, "or create their own version of the software." Bitcoins are stored in a computer file called a "wallet," and can be sent to others via a "public key," comprised of numbers and letters constituting the digital address to where the funds are to be sent. Also, the sender "uses a 'private key,' a code that authorizes the ledger book to …debit the sender's wallet and credits the receiver's wallet."

The Committee noted Bitcoin's advantages in that there are "virtually no fees associated with transfers, "[t]ransfers are instant"[6] and the shared digital ledger book [blockchain] keeps track of all transactions while also preventing 'counterfitting.'"[7] The Committee also noted that digital currency transactions "are

---

[4] The "shared ledger book" technology for Bitcoin is known as "blockchain." The blockchain keeps a record of all transactions that take place. For more discussion of blockchain, *see*, *infra*, footnotes 7 and 9.

[5] *See* Notice 2014-21, 2014 I.R.B. 938, entitled I.R.S. Virtual Currency Guidance. (4/14/14) https://www.irs.gov/irb/2014-16_IRB#NOT-2014-21

[6] Notwithstanding the Committee's statement that Bitcoin has virtually no fees and that transfers are instant, Bitcoin fees appear to be increasing and transaction times slowing. *See* "Bitcoin's New Problem: High Fees," PYMNTS.com, July 4, 2017. https://www.pymnts.com/news/payment-methods/2017/bitcoins-new-problem-high-fees/

[7] Recent commentary on "blockchain" provides a succinct explanation of the technology: "Think about a blockchain as a distributed database that maintains a shared list of records. These records are called blocks, and each encrypted block of code contains the history of every block that came before it with timestamped transaction data down to the second. In effect . . . chaining those blocks together. Hence blockchain." Rob Marvin, "Blockchain: The Invisible Technology That's Changing The World," PCMag.com, August 29, 2017. https://www.pcmag.com/article/351486/blockchain-the-invisible-technology-thats-changing-the-wor

Another commentator has written: "The blockchain is [a] … potent technology. In essence it is a shared, trusted, public ledger that everyone can inspect, but which no single user controls. The participants in a blockchain system collectively keep the ledger up to date: it can be amended only according to strict rules and by general agreement. [The] … blockchain ledger … keeps track of transactions continuously." "The Trust Machine, The promise of the blockchain, The technology behind bitcoin could transform how the economy works," The Economist, October 31, 2015. https://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine

See footnote 9, *infra*, for further discussion of blockchain technology.

not anonymous," but rather "pseudonymous" "because it is possible, although difficult, to trace the identity" of those sending digital currencies.[8]

The Committee acknowledged that digital currencies, such as Bitcoin, are used by both legitimate business enterprises as well as criminals. The Committee stated that the appeal to legitimate businesses is "the ability to quickly receive 'digital cash'" with the payment not being subject to "chargebacks or credit card fees." While the Committee did not specify the appeal to those engaged in criminal activity, it appears obvious. The pseudonymity of digital currency transactions appeals to those who wish to hide illegal financial dealings.[9]

---

[8] For a discussion of the pseudonymity of Bitcoin transactions, *see* "Bitcoin Transactions Aren't As Anonymous As Everyone Hoped," MIT Technology Review, August 23, 2017. https://www.technologyreview.com/s/608716/bitcoin-transactions-arent-as-anonymous-as-everyone-hoped/

[9] The Committee pointed out that the infamous "Silk Road" website, which operated as a means of selling illegal drugs and engaging in other serious criminal activities, was shut down by the FBI. The Silk Road operation was terminated by the FBI in 2013 and resulted in criminal charges, convictions and substantial sentences for the website operator (life imprisonment) as well as others who used the site for illegal transactions.

Recently, the CEO of JPMorgan Chase Jamie Dimon, caused a stir and a temporary dip in Bitcoin value when he stated that Bitcoin and other digital currencies are a fraud and "not a real thing." Given that digital currencies are used for illicit purposes, Dimon predicted that eventually they will be closed down by governments and will be "the emperor without clothes." Dimon was quick to explain, however, that he was not speaking about "blockchain" technology, but rather about digital currency. *See* CNBC.com, September 12, 2017. https://www.cnbc.com/2017/09/12/jpmorgan-ceo-jamie-dimon-raises-flag-on-trading-revenue-sees-20-percent-fall-for-the-third-quarter.html

Blockchain technology exists apart from digital currency. It has been "widely touted to solve a number of seemingly intractable and longstanding problems, such as reducing transaction costs, speeding up processing time, expanding financial services, and empowering consumers." Reggie O'Shields, "Smart Contracts: Legal Agreements for the Blockchain," 21 N.C. Banking Inst. 177 (2017) (footnote omitted) (O'Shields, "Smart Contracts: Legal Agreements for the Blockchain ("Smart Contracts and Blockchain"). http://scholarship.law.unc.edu/ncbi/vol21/iss1/11/

One of the areas in which use of blockchain technology has been touted is that of "smart contracts." An excellent description of blockchain use with regard to smart contracts is found in the "Smart Contracts and Blockchain" article. The author explains:

> "Smart contracts self-execute the stipulations of an agreement when predetermined conditions are triggered. The parties 'sign' the smart contract using cryptographic security and deploy it to a distributed ledger, or blockchain. When the conditions in the code are met, the program triggers the required action. For example, once a good or service has been delivered, the smart contract could enforce payment through the distributed ledger. In the event of nonpayment, it could initiate recovery of the good or suspension of the service. This technology has a large and expanding number of potential uses, such as trading in financial instruments, syndicated lending transactions, and securities settlement."

The Committee noted that digital currencies are heavily regulated in the United States. For tax purposes, digital currencies are considered "property" and subject to capital gains tax.[10] The Committee also stated that U.S. Futures and Trading Commission considers digital currencies to be commodities governed by the Commodity Exchange Act,[11] and has brought enforcement actions thereunder.[12] The Financial Crimes Enforcement Network ("FinCEN") of the U.S. Department of Treasury regulates digital currency exchangers and money transmitters under the Bank Secrecy Act.[13] The Committee stated that such regulation "requires money transmitters to be registered and implement know-your client (KYC) and anti-money laundering (AML) procedures."[14] The Committee also noted state regulation of money transmitters.

The Committee emphasized the volatility of digital currencies stating that the price of Bitcoin "fluctuated from approximately $7.00 per bitcoin in January of 2013 to over $1,200.00 by December of 2013. Bitcoin sometimes fluctuates in value as much as ten percent (10%) per day. The price of a [B]itcoin has recently increased substantially. As of August 30, 2017, the price of a [B]itcoin was $4,627.77." Indeed, since the date of the Committee's opinion on September 11, 2017, the price of Bitcoin has continued to fluctuate. As of the opening of business on November 10,

---

"Smart Contracts and Blockchain," *supra*, at 179 (footnotes omitted). However, the author also notes legal ethics concerns that may arise with regard to blockchain and smart contracts, including aiding the unauthorized practice of law, sharing fees with non-lawyers, and forming partnerships with non-lawyers. "Smart Contracts and Blockchain," *supra*, at 192-93 (footnotes omitted).

[10] Under IRS Notice 2014-21, *supra*, footnote 5, digital currency is considered "intangible" property, subject to capital gain and loss treatment and is also considered "income" if received for goods or services.

[11] *See* 7 USC &1a (9).

[12] *See* "The Commodities Futures Trading Commission: Effective Enforcement and The Future of Derivatives Regulation Before the S. Comm. On Agric., Nutrition, and Forestry," 111th Congress 55 (2014) (Statement of Timothy Massad, Chairman of the Commodity Futures Trading Commission.) https://www.scribd.com/document/321962898/SENATE-HEARING-113TH-CONGRESS-THE-COMMODITY-FUTURES-TRADING-COMMISSION-EFFECTIVE-ENFORCEMENT-AND-THE-FUTURE-OF-DERIVATIVES-REGULATION
See also Matthew Kluchenek,"Bitcoin and Virtual Currencies: Welcome to Your Regulator," Harvard Business Law Review (2016). http://www.bakermckenzie.com/en/-/media/files/people/kluchenek-matthew/ar_na_mkluchenek_bitcoinvirtualcurrency_2016.pdf

[13] FinCEN Advisories, FIN-2013-G001.

[14] *See* Department of Treasury, FinCEN, "Customer Due Diligence Requirements for Financial Institutions, Final Rule," 31 CFR Parts 1010, 1020, 1023, *et al*. (2016), and Amendments (2017).

2017, the price of Bitcoin was $7214.71 on the New York Stock Exchange Bitcoin Index.[15]

Yet, the Committee noted that digital currency payment processors claim "to eliminate the volatility risk by maintaining consistent exchange rates based on an objective value presented by various exchanges." Indeed, one such processor has stated that Bitcoin can be "instantly" sold to it "to avoid exposure to … volatility."[16]

Finally, before analyzing the ethics rules applicable to Nebraska lawyers' acceptance of digital currency and safeguards required to be compliant with the rules, the Committee noted that "a growing number of law firms in other jurisdictions accept [digital currency] as payment for services." However, the Committee appeared to criticize such firms' acceptance of digital currency stating: "[I]t is unknown if [the firms] undertook any effort to determine whether such policy is allowed" under the applicable state rules of professional conduct.

III. Lawyers' Acceptance of Digital Currencies--Applicable Ethics Rules and Required Safeguards.

The Committee analyzed three situations in which lawyers might properly accept digital currencies under the Nebraska ethics rules: (A) as payment for legal services, (B) from third parties for the benefit of clients, and (C) holding in trust or escrow for clients and third parties. The Committee's analysis of each situation, applicable ethics rules, and required safeguards are discussed below. While the Committee based its Opinion on Nebraska ethics rules, the corresponding ABA Rules are similar and, in most instances identical, and are largely the same or similar to other states' provisions. Both the relevant Nebraska rules and corresponding ABA Rules are referenced below.

A. Accepting Digital Currencies as Payment for Services.

The Committee found that lawyers could properly accept digital currencies as payment for services under Neb. Ct. R. Prof. Cond. &3-501, Comment 4. ABA Rule 1.5, Comment 4, is identical to the Nebraska rule. Both rules provide: "A lawyer may accept property in payment for services…." Inasmuch as digital currency is considered a form of "property," the Committee reasoned that there was "no per se rule prohibiting payment of earned legal fees with convertible virtual currency."

However, the Committee commented that certain other cautions arise because of the "mischief" associated with digital currency. The Committee stated does not reveal client secrets, and is not used in a money laundering or tax avoidance scheme."

---

[15] https://www.nyse.com/quote/index/NYXBT .

[16] *See* cover page of Coinbase.com, https://www.coinbase.com/merchants?locale=en-US

In addition, the Committee stated that ethics prohibitions against unreasonable fees, Neb. Ct. R. of Prof. Cond. §3-501.5(a), are invoked with regard to accepting digital currency. The Nebraska rule and the corresponding ABA provision, ABA Rule 1.5 (a), are identical and provide in pertinent part: "A lawyer shall not make an agreement for, charge, or collect an unreasonable fee…" The Committee noted that accepting payment in digital currency could result in unreasonable fees due to the dramatic volatility of the currency. The Committee gave the following example of this concern:

> "An arrangement for payment in [digital currency] for attorney services could mean that the client pays $200.00 an hour in one month and $500.00 an hour the next month, which the client could very easily allege as unconscionable. Conversely, if the market value of digital currency used as payment quickly fell, the attorney would be underpaid for services."[17]

In order to mitigate or eliminate these volatility risks, and to comply with the ethics rules prohibiting unreasonable fees, the Committee reasoned that digital currency should be valued and converted into U.S. dollars immediately on receipt. The conversion rate should be "market based such as from an exchange or based upon the New York Stock Exchange Price Index…" The Committee determined that operating in this way would eliminate the "risk to the client of value fluctuation," either with regard to potential increases or decreases in the value of digital currency.

The Committee required the following safeguards to be followed in order to accept digital currencies and comply with the ethics rules:

> (1) The client must be notified that the attorney will not retain the digital currency, but will convert it into U.S. dollars immediately on receipt. Such notification should take place in the engagement letter or fee agreement,
>
> (2) The digital currency should be converted into U.S. dollars at objective market rates through the use of a payment processor, and
>
> (3) The client's account should be credited at the time of payment.

The Committee concluded that, under this "framework," the client would be properly informed, the use of digital currency would not result in an "unconscionable" fee, and the payment would conform to applicable ethics rules.

---

[17] The potential for Bitcoin payments constituting unreasonable fees was previously raised in 2014 commentary, published by the Orange County (California) Bar Association. *See* Jennifer R. Bagosi, "Controversial Currency: Accepting Bitcoin as Payment for Legal Fees," Orange County Bar Association, June, 2014. http://www.ocbar.org/AllNews/NewsView/tabid/66/ArticleId/1324/June-2014-Controversial-Currency-Accepting-Bitcoin-as-Payment-for-Legal-Fees.aspx

B. Accepting Payments in Digital Currencies from Third-Party Payers.

The Committee next addressed the issue of whether it was ethically proper to accept payments in digital currencies for the benefit of clients from third-party payers. The Committee reasoned that such payments would not violate the Nebraska ethics rules if they did not interfere with the independent professional judgment of the lawyer, the lawyer's relationship with the client (Neb. Ct. R. of Prof. Cond. &&3-501.7 (a), 3-501.8 (f)), or a client's confidential information (Neb. Ct. R. Prof. Cond &3-501.6).

The ABA Rules are to similar effect. ABA Rule 1.7 (a), regarding conflicts of interest, is identical to Neb. Ct. R. of Prof. Cond. &3-501.7 (a), and prohibits concurrent conflicts of interest where there is a significant risk that a lawyer's representation of clients "will be materially limited by the lawyer's responsibilities to …a third person…." ABA Rule 1.8 (f), specifically addresses third-party payments for a client's representation, and is identical to Neb. Ct. R. of Prof. Cond. &3-501.8 (f). ABA Rule 1.8 (f) provides:

> "(f) A lawyer shall not accept compensation for representing a client from one other than the client unless:
>
> (1) the client gives informed consent;
>
> (2) there is no interference with the lawyer's independence of professional judgment or with the client-lawyer relationship; and
>
> (3) information relating to representation of a client is protected as required by Rule 1.6."[18]

In its analysis, the Committee did not emphasize the method for resolution of the conflict of interest associated with a third-party payer of a client's fee, whether the payment is made in digital currency, U.S. dollars, or foreign currency. Resolution of such conflict requires that a lawyer, contemplating accepting a digital fee payment from a third-party payer on behalf of a client, should, *before* accepting the payment: (1) notify the prospective third-party payer in writing of the lawyer's above-stated obligations to the client, (2) discuss with the client the conflict of interest created by the prospective third-party payment and the lawyer's obligations to the client, and (3) secure from the client in writing the client's consent and waiver of the conflict of interest associated with the third-party payment.

In addition to the concerns raised by the third-party payment conflict of interest rules, the Committee pointed out the issue of the "pseudonymity" of digital currency use. The Committee stated that an attorney should employ "Know Your

[18] ABA Rule 1.6, concerning protecting client confidential information, is similar to Neb. Ct. R. of Prof. Cond. &3-501.6, referenced by the Committee.

Client" ("KYC") standards with regard to third-party payers.[19] The Committee noted that digital currency payment processing services require disclosure of the user's identity.[20] And, the Committee advised further that, "[i]n any other situation, the attorney should request sufficient KYC information from the third-party payer prior to acceptance of the digital currency payment."

C. Receiving and Holding Digital Currencies in Escrow or Trust.

Finally, the Committee found it permissible under the Nebraska's "safekeeping property" ethics rule, Neb. Ct. R. of Prof. Cond. &3-501.15 (a), for lawyers to receive and hold digital currencies in trust or escrow for clients and third-parties. Both the Nebraska rule and corresponding ABA Rule 1.15 (a) require a lawyer to hold such property separately from the lawyer's own property and to properly safeguard the property. Also, under both rules, a lawyer must keep complete records of the account funds or other property for five (5) years after the representation has ended.

The Committee again referenced the volatility of digital currency, and, on account of such, stated that lawyers should advise clients and third-parties that the digital currency accepted and held in trust or escrow would not be converted into U.S. dollars or other currency. And, lawyers are to keep records of the notice to clients or third-parties as well as of the "wallet" used to store the digital currencies.

The Committee addressed the difficult issue of "securing" digital currencies received or held in trust or escrow. For example, if hackers "steal" the digital currency, the Committee pointed out that there is not a bank or the FDIC to turn to

---

[19] Lawyers should establish Know Your Client (KYC) checklists for all prospective clients, including those wishing to pay fees with digital currency. *See* recent commentary on the importance of lawyers and firms having KYC policies and procedures in Anthony Davis, "Client Intake: Know Your Client – Or Else," New York Law Journal (July 3, 2017).

With regard to protecting against unwittingly participating in illegal activity including money laundering, lawyers should refer to *ABA Formal Opinion* 463 (2014) on client due diligence, money laundering, and terrorist financing.
https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/formal_opinion_463.authcheckdam.pdf,
as well as "A Lawyer's Guide to Detecting and Preventing Money Laundering," (2014), published by the International Bar Association, the American Bar Association, and the Counsel of Bars and Law Societies of Europe.
https://www.americanbar.org/.../2014oct_abaguide_preventingmoneylaundering.auth.
Indeed, it is also recommended that lawyers have Anti Money Laundering (AML) compliance policies. *See* Kristine Safos, "Why U.S. Firms Need Anti-Money Laundering Policies," Law 360, Lexis-Nexis (May 9, 2017). https://www.law360.com/.../why-us-law-firms-need-anti-money-laundering-policies

[20] The Committee stated that digital currency payment processors, such as Coinbase, Bitpay, and Circle, require payers to submit KYC information to use the processors' services.

for reimbursement.[21] As such, the Committee suggested reasonable security methods such as encryption of the "private key" required to send the digital currencies, more than one private key known as "multi-signature accounts ("multi-sig") for access to the digital currencies, and/or maintenance of the "wallet" or private keys in a computer or other device "disconnected from the Internet," otherwise known as "cold storage."[22]

---

[21] For a not so tongue-in-cheek assessment of how Bitcoin can be stolen, *see* Adrianne Jeffries, "How to Steal Bitcoin in Three Easy Steps," The Verge Tech Report, December 19, 2013. https://www.theverge.com/2013/12/19/5183356/how-to-steal-bitcoin-in-three-easy-steps *See also* Alex Hern, "A History of Bitcoin Hacks," The Guardian, March 18,, 2014. https://www.theguardian.com/technology/2014/mar/18/history-of-bitcoin-hacks-alternative-currency

In addition to these concerns, law firms should also be very careful with regard to the holding of any client or third-party funds in escrow, whether in regular or digital currency. For a recent discussion of the ethics dangers associated with holding funds in escrow, *see* Laura Ernde, "Escrow, money laundering cases draw attention to the perils of handling client money, California Bar Journal, February, 2017. http://www.calbarjournal.com/February2017/TopHeadlines/TH1.aspx

[22] An succinct summary of security protections for digital currencies can be found in "Paper Wallet Guide: How to Protect Your Cryptocurrency," Blockgeeks.com, https://blockgeeks.com/guides/paper-wallet-guide/
For recommended law firm cyber security controls in general, *see* American Bar Association, Section of Labor & Employment Law, "Abstract, Ethics and Cybersecurity: Obligations to Protect Client Data," pp. 11-13 (March, 2015) ("ABA, Ethics and Cybersecurity"), https://www.americanbar.org/content/dam/aba/events/labor_law/2015/march/tech/wu_cybersecurity.authcheckdam.pdf. The Abstract discusses administrative, physical, and technical safeguards, including procedures for response to cyber attack. *See also* American Bar Association, "Revised Resolution 109, Cybersecurity Legal Task Force, Section of Science & Technology Law, Resolution and Report to the House of Delegates," (August, 2014). https://www.americanbar.org/content/dam/aba/events/law_national_security/2014annualmeeting/ABA%20-%20Cyber%20Resolution%20109%20Final.authcheckdam.pdf

A recent interesting paper by the American Bar Association Cybersecurity Legal Task Force provides a checklist for the use of third-party vendors in cyber security and addresses several issues "from due diligence and vendor selection through contracting and vendor management." American Bar Association, Cybersecurity Legal Task Force, "Vendor Contracting Project: Cybersecurity Checklist," (April 13, 2017). https://www.americanbar.org/content/dam/aba/images/law_national_security/Cybersecurity%20Task%20Force%20Vendor%20Contracting%20Checklist%20v1.1%2004-13-2017.pdf

Cyber attacks involving law firms are not new. However, recent notorious cyber security hacks of law firms in the data breach cases of the Paradise Papers and Panama Papers, and the 2017 shutting down of DLA Piper's computer systems, illustrate the very serious consequences of such attacks. (It has been reported that some firms have even gone to extraordinary lengths to prepare for such attacks by "preemptively opening Bitcoin wallets to pay ransom in case their data is hacked." Camilla Hodgson, "Law firms are preemptively opening Bitcoin wallets to pay ransoms," Business Insider, October 25, 2007. http://www.businessinsider.com/law-firms-bitcoin-pay-ransoms-2017-10)

Ethics requirements also are applicable in the area of cyber security, particularly concerning lawyers' obligations under ABA Rule 1.6 (c) and Comment 18 to competently safeguard client confidential

The Committee ended its analysis by discussing payments to lawyers in digital currencies which are to serve as *retainers* to be drawn on as fees are earned. The Committee pointed out that digital currencies cannot be deposited into client trust accounts under applicable trust fund requirements.[23] Yet, retainers paid to lawyers to be drawn on as fees are earned *are required*, under both Nebraska rules[24] and ABA Rule 1.15 (c), to be deposited into client trust accounts. Given such requirements, the Committee stated that, if a lawyer receives digital currencies to be used as a retainer to be drawn on as fees are earned, the lawyer must immediately convert such digital currencies into U.S. dollars to be deposited into a client trust account.

IV. Remaining Risk Management Concerns.

As seen from the above discussion, Nebraska Ethics Advisory Opinion No. 17-03 (2017) analyzed several applicable ethics rules and mandated safeguards regarding Nebraska lawyers' acceptance and holding of digital currencies. And, as discussed above, the relevant ABA Rules are, in large part, identical to the Nebraska rules cited in the Opinion, which may lead other jurisdictions with similar provisions to similar conclusions. Yet, notwithstanding the guidance of the Opinion, there are several remaining risk management concerns for law firms considering accepting, or continuing to accept, digital currencies. These concerns and their recommended resolution are discussed below.

---

information from disclosure. For analysis of this and other applicable ethics requirements, *see*, ABA, "Ethics and Cybersecurity," *supra*, at pp. 6-11.

In addition to undertaking cyber security measures, law firms also should assess whether they have sufficient liability coverage to protect against potential loss, including separate cyber security insurance. Cyber security insurance may protect against digital currency theft, as well as other types of "internet" loss. However, a firm's standard professional liability insurance may not be broad enough to cover the cyber loss in question, and, in fact, certain types of losses may be excluded. In addition, cyber security riders to standard professional liability insurance policies may not provide as extensive coverage as stand-alone cyber policies. For discussion in this area, *see* Casey C. Sullivan, "6 Things Lawyers Need to Know About Cyber Insurance," Technologist, FindLaw Legal Technology Blog, March 24, 2017. http://blogs.findlaw.com/technologist/2017/03/6-things-lawyers-need-to-know-about-cyber-insurance.html

Indeed, firms should *ensure* that their cyber insurance policies cover not only the potential theft of digital currency, but also other cyber loss events such as cyber extortion/ransom-ware, business interruption, loss of reputation associated with cyber breach, forensic expenses, regulatory fines, penalties, investigation expenses, expert vendor costs, and cyber losses occurring in a firm's foreign offices, among others.

[23] The Committee cited Neb. Ct. R. &&3-901 to 3-907 in this regard. This is the case under most if not all states' "Interest on Lawyer Trust Accounts" (IOLTA) rules.

[24] *See* Neb &3-501.15 (c).

A. Is the acceptance of digital currencies ethically permitted in the jurisdictions in which a firm practices and what safeguards are required to ensure compliance with the ethics rules?

A firm's decision whether to accept digital currencies should include an assessment of whether, under the ethics rules of the jurisdiction/s in which the firm practices, acceptance is ethically permitted, and, if so, what safeguards are required to ensure compliance with the ethics rules. Why? The Nebraska Opinion provided guidance to Nebraska lawyers, although the relevant Nebraska rules are in most cases identical to the ABA Rules. And, states' versions of the ABA Rules may lead other jurisdictions to reach similar assessments. However, it is also possible that interpretation of the ethics rules in a particular jurisdiction might lead to a different conclusion regarding the ethical propriety of lawyers' acceptance and holding of digital currencies and appropriate safeguards. As such, a firm should undertake research in this area and perhaps seek bar hotline and/or ethics opinion advice.

B. Assuming that it is ethically appropriate in the firm's jurisdiction/s to accept digital currencies, who in the firm makes the decision to accept the currencies, under what circumstances are they to be accepted, and how are digital currencies to be held and managed?

Assuming that it is ethically appropriate to accept digital currencies in a firm's jurisdiction/s, firm Management, in consultation with the firm's General Counsel's office, Legal Department, or Risk Management personnel, Practice Leaders, Records Management, and IT Department, should decide, as firm policy, whether digital currencies will be accepted and under what circumstances. A firm should also establish protocols for such acceptance, conversion to U.S. dollars (or foreign currency if applicable), client notification, storage, security, and overall management.

These protocols should include best practices with regard to:

1. Client and third-party due diligence including identification, Know Your Client assessments, and anti terrorist, avoiding receipt of contraband, and anti money laundering precautions.

2. Advance notification and explanation to clients in engagement letters/ fee agreements (or in writings to third-parties with regard to third-party payments), of firm policy concerning receipt of digital currencies, conversion to U.S. dollars (or foreign currency if applicable), holding of digital currencies in trust or escrow, storage, security, management, and approach as to retainers to be drawn on as fees are earned.

3. Establishing firm cyber security measures for digital currencies. In order to establish such procedures, a firm should draw on the guidance of its insurer, bar association and other published writings on the subject, and perhaps consult with established and vetted third party vendors.

4. Establishing procedures for firm response to potential cyber loss of digital currencies. As with regard to security measures, in order to establish procedures for response to cyber loss, a firm should draw on the guidance of its insurer, bar association and other published writings on the subject, and perhaps consult with established and vetted third party vendors.

5. Firm management of digital currencies including implementation and adherence to the above-noted protocols.

C. Does a firm have sufficient insurance to provide coverage for the potential loss of digital currencies?

A firm's decision to accept and hold digital currencies should be accompanied by an assessment whether the firm's current liability policy provides sufficient coverage to protect against potential loss of digital currencies, and/or whether a separate cyber insurance policy should be acquired. While a firm's professional liability insurance policy may cover some cyber losses, others may be excluded from coverage. Also, cyber security insurance riders may not provide as extensive coverage as would exist under a separate cyber policy. In making such assessments, a firm should, of course, consult with its insurer.

D. What conflict of interest assessments and resolutions are required with regard to acceptance from a third-party of digital currencies for a client's benefit?

Just as with a proposed third-party payment to a law firm of U.S. dollars or foreign currency for the benefit of a client, applicable conflict of interest rules must be followed concerning a third-party payment of digital currencies for a client's benefit.

1. Thus, *prior to accepting* a digital currency payment for the benefit of a client, a firm should *notify the third-party in writing* that the payment:

a. Will not create an attorney-client relationship between the firm and the third-party,

b. The payment will not interfere with the law firm's professional judgment to be exercised solely on behalf of the client, and

c. Client confidential information will not be shared with the third-party.

2. In addition, *prior to accepting* a third-party digital currency payment for the benefit of a client, a firm should:

a. Discuss with the *client* the *conflict of interest* created by the prospective payment and the above-stated obligations the firm has to the client, and

b. Secure from the *client in writing the client's consent and waiver* of *the conflict of interest* associated with the third-party payment.

E. What is firm policy with regard to accepting digital currencies from clients or third-parties to hold in trust or escrow?

As is the case with a firm's accepting of U.S. dollars or foreign currency in trust or escrow for clients or third-parties, firm policy should be formulated as to whether a firm will hold digital currencies for clients or third parties in trust or escrow. If so, criteria for holding the digital currencies in trust or escrow must be established and policy formulated as to notification, storage, security, and management.

Similarly, firm policy should be formulated concerning digital currencies paid to a firm as retainers to be held and drawn on as fees are earned, the conversion of such digital currencies to U.S. dollars or foreign currency, and the depositing of such converted funds as required into client trust accounts.