June 13, 2018

Submitted by James F. Verdonik on behalf of Ward and Smith, P. A.

We represent a wide range of clients who either are investing in, selling, mining, developing, minting, redeeming, converting and exchanging a wide range of digital assets associated with blockchain and other technologies (collectively "**Digital Assets**") or who are in the business of facilitating those who conduct such business activities (collectively, "**Blockchain Businesses**").

Need for Ethics Guidance

As we explain in Part I below, Coins (as defined below) and other types of Digital Assets are playing an ever bigger role in commerce. Many experts have said that blockchain technology that is associated with Coins and other Digital Assets is the biggest technology change since the Internet. As a result, we and other law firms face the challenge of deciding what roles we will play in servicing our clients and how we can adapt to the many changes our clients are making to the way businesses and ordinary people pay for products and services and store and exchange information.

For these reasons, we seek guidance from the NC Bar about the application of ethics rules to how law firms can ethically service clients who are using Coins and other Digital Assets.

We have divided our request into three parts

Part I	Blockchain and Digital Assets Background
Part II	Legal Ethics Questions Presented
Part III	References to Specific Pertinent Ethics Rules
EXHIBIT A	Legal Ethics Opinion re Digital Currencies from State of Nebraska

I. Blockchain and Digital Assets Background

We believe it is impossible to determine how legal ethics rules apply to Coins and other Digital assets without understanding how Coins and other Digital Assets work. Since there are many misperceptions about Coins and other Digital Assets, we offer the following information as background to explain the evolving world of Coins and other Digital Assets, because it is critical that all legal ethics rules about Coins and other Digital Assets be based on a clear understanding of reality these assets actually work rather than on public misperceptions.

Current Coin and Digital Assets Business Environment

Blockchain Businesses and Digital Assets are a growing presence in North Carolina.

Some Digital Assets function as a substitute for government issued currencies ("**Coins**"). Several hundred thousand accounts with more than half a Billion Dollars of Coins are held by North Carolina residents at exchanges that convert Coins to other currencies ("**Coin Exchanges**"). Coins are currently being used to purchase a wide range of products and services around the world (from

high end items like real estate to everyday items like pizza). Bitcoin, the widest issued Coins, is used approximately 200,000 times per day. Total Coin transactions may be twice as large.

There are many dozens of different types of Coins, with each having different properties. Unlike traditional currencies issued by governments, each type of Coin performs different functions and has different technical strengths and weaknesses. Because Coin developers are constantly trying to improve performance and solve new business and technology problems, there will be many more types of Coins.

Coins currently tend to fluctuate in value more than most government issued currencies. Some Coins are highly liquid and can be easily converted into U. S. Dollars and other currencies. Other Coins are less easily convertible.

Other Digital Assets

Coins are not the only Digital Assets. Other Digital Assets are functional and are used to operate blockchain software systems ("**Utility Tokens**"). Other Digital Assets evidence ownership of a security and are a digital substitute for a stock certificate or a promissory note ("**Security Tokens**") Other Digital Assets evidence ownership of other types of assets (such as a deed to real property). Basically, the ownership of any type of asset can be evidenced by a Token.

Nature of Coins and Digital Assets

Coins and other Digital Assets exist only in blockchain(s). Each blockchain is a ledger that records transactions each time a Coin or other Digital Asset is transferred.

There are many blockchains. Some are public and others are private. A blockchain is not located on any single computer server and the network is not controlled by any single entity. Each public blockchain is served by computers all around the world. People who dedicate their computers to servicing a blockchain are called miners. Miners compete for the privilege of verifying bitcoin transactions by solving mathematical problems. In return for doing this processing and verification, blockchain algorithms issue Coins to the miners.

Coins and other Digital Assets are not "stored" in any single location or exist anywhere in any physical form. All that exists are records of transactions stored on the blockchain.

Each Coin or other Digital Asset has a history of transfers that can be traced through the blockchain. Once recorded on the blockchain, the history cannot be erased or changed without it being readily apparent. We will explain why this is true when we discuss hashing below, but for now imagine that you could trace every account a single U. S. Dollar has been deposited into. The blockchain would record:

- When the dollar was first issued
- The accounts the government deposited the dollar into
- Each time that dollar was transferred to another account

Of course, the names of owners of the accounts are not public information, but forensic experts can often identify criminals who conduct many blockchain transactions, because they leave a transaction trail that skilled experts can follow.

http://www.sciencemag.org/news/2016/03/why-criminals-cant-hide-behind-bitcoin

Ownership of Coins and other Digital Assets then is much like the ownership of real estate or an automobile that is recorded in a government office. We determine that someone is the legitimate owner of a piece of real estate or an automobile by tracing title back to the original owner. Likewise, we know that someone is the legitimate owner of a coin or other Digital Asset, because the chain of transfers can be traced through the blockchain from the first owner to the current owner.

A primary difference between Coins and other Digital assets and information about the ownership of other types of assets is that instead of one location, the identical information about Coins and other Digital Assets is recoded in thousands of computers. We also do not know the owner's name. We only know a network address, which we will discuss in the digital wallet section below. Blockchain information is also encrypted. Therefore the details associated with each transfer are not public information. For example, third parties would not know the transfer was made to a law firm to pay a legal fee.

Now, we will discuss blockchain digital wallets, which are the tools a blockchain user uses to "own" and transfer Coins and other Digital Assets, because these digital wallets would be used by law firms and their clients.

Blockchain Digital Wallets for Coins and Tokens

The following explanation of what blockchain digital wallets are and how they function is taken from Blockgeeks.com and Coinbase.com:

https://blockgeeks.com/guides/cryptocurrency-wallet-guide/
https://www.coindesk.com/information/how-to-store-your-bitcoins/

A blockchain digital wallet is hardware or a software program that stores private and public keys and interacts with various blockchain to enable users to send and receive digital currency and monitor their balance. If you want to use any Coin or Token, you need to have a digital wallet.

Blockchain software wallets have three essential components:

A Public Address: This address is recorded in the blockchain. If someone wants to send you a Coin or Other Digital Asset, they use your public address like someone wants to send something to an email or other address. In theory, public addresses are known to the public, but in practice you need to give people your public address if you want them to send you Coins or other Digital Assets. Addresses are very long strings numbers that are translated by software into shorter of letters and numbers. For Bitcoins, the public address change each time a transfer is made. For other Coins, the address may remain unchanged after each transaction. Changing public addresses with each transaction enhances privacy by preventing people from searching the blockchain for your public address to see all the transactions associated with that public address.

A Private Key: The Private Key enables the owner of the wallet to activate the wallet's public address. You cannot send Coins or other Digital Assets from the public address on the blockchain, unless you can activate the wallet's public address. The private key is also a long series of letters and numbers. Maintaining the secrecy of the private key is an import security tool. If someone finds your private key, they can transfer Coins or other Digital Assets from your wallet. Likewise, losing your private key locks you out of your own wallet, which means that you can no longer transfer Coins or Digital Assets from your wallet. In theory you still "own" the Coins or other Digital Assets, but you cannot use them without your private key.

A Public Key: Each private key is assigned a corresponding public key. The public key is a "hashed" version of your private key. We explain below what "hashing" means.

How the Public Address, Private Key and Public Key Work Together.

The way the public address, the public key and the private key operate with the blockchain is that you use your private key to sign or verify that a transaction is valid, but you do not want other people to know your private key. So, to avoid disclosing your private key to people, the blockchain's algorithm assigns your private key a corresponding public key. The algorithm makes it very easy to generate public keys from private keys, but it is very difficult to "reverse" the algorithm to accomplish the opposite.

The public key is then "hashed." Hashing then produces the public address. So, when you send someone your public address, you are also sending them your public key. This is analogous to using code to protect the secrecy of your private key.

The following diagram shows the relationship between the private key, the public key and the public address:

https://blog.wetrust.io/why-do-i-need-a-public-and-private-key-on-the-blockchain-c2ea74a69e76

Hashing

Hashing is an important blockchain tool. Generally, when people say that they store information on a blockchain, they generally mean that the blockchain stores a "hash" of the information. The hash represents the information, but is often much shorter, which creates storage and processing efficiencies.

https://blockgeeks.com/guides/what-is-hashing/

The key to hashing is to represent information that is hashed, however long that information is, into a string of characters called a "hash" that has exactly the same number of characters as every other hash even though there are big differences in the volume of information that was "hashed." All hashes on a blockchain have exactly the same number of characters.

In the context of Coins like Bitcoin, the transactions that transfer Coins from one public address to another public address are taken as an input and run through a hashing algorithm (Bitcoin uses SHA-256) which gives an output of a fixed length.

When you "hash" information, it does not matter whether the information you hashed contains three bits of information or one million bits of information.

The hashed information is always represented in the blockchain by the same number of letters and numbers. The bitcoin "hash" always produces 256 letters and numbers to represent information recorded in the bitcoin blockchain, but each time you produce a hash, the hashing algorithm produces a unique set of 256 letters and numbers.

For example, if you hash a fifty page legal document, the hash that is stored on the blockchain wold be 256 characters.

Further, if you hash the same information over and over again, the hashing algorithm will always produce the exact same combination of 256 letters and numbers. Therefore, if the hash of two documents is exactly the same, you know the two documents are exactly the same.

This enables the blockchain to easily identify information that is the same and information that is different.

Even the slightest difference will produce a very different hash. So, if you hash one million bits of information twice, but you change even one bit before you do the second hash, theblockchain would produce a second hash that is very different from the first hash. Blockchain hashing raises red flags that spotlight even very small differences between two sets of information that might otherwise go unnoticed.

Going back to our example of a 50-page legal document, the way you would very that a copy is an exact duplicate of the 50-page document that was originally hashed is to hash the copy and compare it to the hash that is stored on the blockchain. If the hash of the copy is the same as the hash stored in the blockchain, you know the copy is exactly the same as the original. If, however,

anyone made a very small change in the copy, the hash of the copy would be very different from the hash of the original that is stored on the blockchain.

Hashing amplifies changes. Therefore, humans cannot simply hide changes in a large amount of information. When people say that blockchain information is "immutable," what they mean is that hashing will make possible to verify that information has not been changed by comparing the hashes.

The foregoing only summarize basic principles of blockchains, wallets and hashing. Blockchain software developers deal with many more complicated issues and different developers implement blockchains implement different ways, but the basic principles remain the same.

The important principle for legal ethics purposes is that blockchains produce a more accurate and useful picture of what has occurred than other financial records systems that law firms have been using.

Hacking

Coin Exchanges and other service providers make the transfer of Coins and other Digital Assets simpler than the blockchain digital wallet procedures described above by setting up accounts that users can access using email addresses and other codes just like many other websites. This is simpler for many people than using their actual wallet private keys. Convenience and security often involve a trade-off. The Exchange or other service provider must possess your private key to make the wallet function. If someone hacks the Exchange's website, they can obtain your private key the Exchange to conduct transactions for you. Obtaining your private key would allow the hacker to transfer Coins and other Digital assets from your wallet. Therefore, just like bank and brokerage accounts, weaknesses in the service provider's security system of your own failure to keep your access codes secret can lead to hacking.

You can use a hardware wallet that is not connected to the Internet to prevent hacking.

"Storing" and Transferring Coins and other Digital Assets

Unlike traditional "pocket" wallets, blockchain digital wallets do not store Coins or other Digital Assets. In fact, Coins and other Digital Assets are not "stored" in any single location or exist anywhere in any physical form. All that exist are records of transactions stored on the blockchain. The blockchain is simply a ledger that records transactions.

Blockchain digital wallets are hardware or software programs that store the wallet owner's public and private keys and interface with various blockchain so that the wallet user can monitor the user's balance, send Coins and other Digital Assets and conduct other operations.

When a person sends you Coins or other Digital Assets, they are essentially assigning the chain of ownership of the Coins or other Digital Assets to your wallet's address. This is much like someone assigning the title of a car or a piece of real estate. To verify that the transfer is valid you have to look at the chain of title, because he transferor cannot transfer to you anything that he transferor does not have title to.

To be able to transfer Coins and other Digital Assets, the private key stored in the sender's wallet must match the public address the Coin or other Digital Asset is assigned to. If public and private keys match, the balance in the assignee's digital wallet will increase, and the balance in the sender's digital wallet will decrease accordingly. There is no actual exchange of real coins. The transaction is signified merely by a transaction record on the blockchain and a change in balance in the assignee's and the sender's wallet.

Evolution Not Revolution

Digital transfers of money are not new. Wire transfers, credit cards and ACH transfers are normal parts of commerce. Each transfers system has its own strengths and weaknesses in terms of cost, speed, security, privacy and accuracy. Businesses and individuals choose which transfer systems best fit their needs in different situations.

Likewise, "digital wallets" are not new. PayPal, ApplePay, SamsungPay and Android Pay are all forms of digital wallets. Mobile wallets are a form of digital wallet that most people are familiar with. Mobile wallets are housed in an app on your mobile device, while digital wallets can be accessed via the web on a desktop, laptop or mobile device.

Regulatory Background

There are many misperceptions about Coins and other Digital Assets. One misperception is that Coins and other Digital Assets are not regulated by the government. That misperception was created by some early Coin adapters ignoring government regulations and the need for regulators to determine how existing regulations apply to different types of Coins and other Digital Assets. That regulatory adjustment process is now well underway.

Because Coins and other Digital Assets perform so many functions, they are regulated by many different government agencies.

The Securities and Exchange Commission and state securities administrators regulate Coins and Tokens that are securities under the Securities Act of 1933 and the Securities and Exchange Act of 1934 and their state equivalents.

The U.S. Commodity Futures Trading Commission (CFTC) regulates Coins that are commodities.

FinCEN and the Department of the Treasury regulate Coins that are the equivalent of currency and the businesses that transmit and convert such Coins under the Bank Secrecy Act and other statutes. FinCEN requires money transmitters to be registered and implement know-your-client (KYC) and anti-money laundering (AML) procedures. Some states also regulate Coins under their money transmitter statutes.

II. Questions Presented

A. May an attorney receive Coins and other Digital Assets as payment for legal services?
B. May an attorney receive Coins and other Digital Assets from third parties as payment for the benefit of a client's account?
C. May an attorney hold Coins and other Digital Assets in trust as a prepayment of legal fees
D. May an attorney hold Coins and other Digital Assets in escrow for clients or third parties to facilitate transactions and settlements by clients with third parties?

The terms "Coins" and Digital Assets are defined in Part I above.

Nebraska Legal Ethics Opinion

We have attached for your convenience as **Exhibit A** a legal ethics advisory opinion for State of Nebraska that provides additional background information and legal reasoning.

We note the Nebraska opinion focuses solely on "digital currency." Our request for ethical clarification includes digital currency, but also includes other Digital Assets (as defined in Part I above).

III. References to Specific Pertinent NC Ethics Rules

Following our review of the existing NC ethics rules, we call your attention to the following rules and comments on the rules:

NC RULE	EXCERPT	COMMENTARY
Comment #4 to Rule 1.5	"A lawyer may accept property in payment for services, such as an ownership interest in an enterprise. However, a fee paid in property instead of money may be subject to the requirements of Rule 1.8 (a) (Conflicts of Interest) because such fees often have the essential qualities of a business transaction with a client."	Accepting payment for a fee that has already been earned is the least problematic thing a law firm would do with Coins or other Digital Assets. The Nebraska ethics opinion set forth in **Exhibit A** cites the same comment to the Nebraska rule as the basis for concluding that Nebraska lawyers can accept digital currencies as payment for earned fees. We note that the ABA's model rules contain exactly the same language. Therefore, we expect this will become a national practice for law firms to be permitted to accept payment for earned fees in the form of digital currencies. Each lawyer would need to decide whether accepting this type of payment makes business sense for them and which Coins to accept.

		Coins would involve no ongoing business interaction with a client. Other Digital assets might present conflict of interest issues (E. g. if the Digital Asset evidenced an ownership interest in a client's business). Such other Digital Assets should be judged under the standards set forth in Rule 1.8 (a).
Rule 1.15-2 (b) and (e)	(b) Deposit of Trust Funds. All trust funds received by or placed under the control of a lawyer shall be promptly deposited in either a general trust account or a dedicated trust account of the lawyer. Trust funds placed in a general account are those which, in the lawyer's good faith judgment, are nominal or short-term. General trust accounts are to be administered in accordance with the Rules of Professional Conduct and the provisions of 27 NCAC Chapter 1, Subchapter D, Sections .1300. (e) Location of Accounts. All trust accounts shall be maintained at a bank in North Carolina or a bank with branch offices in North Carolina except that, with the written consent of the client, a dedicated trust account may be maintained at a bank that does not have offices in North Carolina or at a financial institution other than a bank in or outside of North Carolina. A lawyer may maintain a fiduciary account at any bank or other financial institution in or outside of North Carolina selected by the lawyer in the exercise of the lawyer's fiduciary responsibility.	Where a lawyer has not earned a fee, the issues become less clear. One reason is that Coins and other Digital Assets fluctuate in value more widely than traditional currencies. How you would calculate what is to be returned to clients raises issues. These value issues may be resolved by written agreements that specify whether the lawyer or the client benefits or loses based on value fluctuations, but this raises the issue of whether the client should retain independent counsel to advise them about the agreement. Another issue is that many banks and other traditional financial institutions have not established procedures for holding Coins and other Digital Assets. For these reasons newer coin exchanges and transmitters hold most of the Coins and other Digital Assets in circulation. These institutions have not yet implemented procedures that would satisfy the rules for lawyers' trust accounts in most starts, including North Carolina's rules. Faced with these circumstances, the Nebraska ethics opinion included as **Exhibit A** indicated that where digital currencies are sent to a lawyer for the lawyer's trust account, the lawyer should immediately convert the digital currency into traditional currency and deposit the traditional currency into the lawyer's trust account.

Rule 1.15-2 (a) (c) and (d)	(a) Entrusted Property. All entrusted property shall be identified, held, and maintained separate from the property of the lawyer, and shall be deposited, disbursed, and distributed only in accordance with this Rule 1.15. (c) Deposit of Fiduciary Funds. All fiduciary funds received by or placed under the control of a lawyer shall be promptly deposited in a fiduciary account or a general trust account of the lawyer. d) Safekeeping of Other Entrusted Property. A lawyer may also hold entrusted property other than fiduciary funds (such as securities) in a fiduciary account. All entrusted property received by a lawyer that is not deposited in a trust account or fiduciary account (such as a stock certificate) shall be promptly identified, labeled as property of the person or entity for whom it is to be held, and placed in a safe deposit box or other suitable place of safekeeping. The lawyer shall disclose the location of the property to the client or other person for whom it is held. Any safe deposit box or other place of safekeeping shall be located in this state, unless the lawyer has been otherwise authorized in writing by the client or other person for whom it is held.	Lawyers are often called upon by clients and third parties to hold funds and other types of property for reasons that have nothing to do with legal fees. Such circumstances include holding deeds and securities and holding money to be delivered in connection with closing a commercial transaction or settling claims. Here the ethics rules appear to contemplate a more flexible approach to how such assets are to be held. The Nebraska ethics opinion attached as **Exhibit A** allows the same flexibility in dealing with digital currencies as Nebraska's ethics rules allow for other types pf property.

EXHIBIT A

NEBRASKA ETHICS ADVISORY OPINION FOR LAWYERS NO. 17-03

I. Questions Presented

A. May an attorney receive digital currencies such as bitcoin as payment for legal services?
B. May an attorney receive digital currencies from third parties as payment for the benefit of a client's account?
C. May an attorney hold digital currencies in trust or escrow for clients?

II. Summary of Opinion

A. An attorney may receive and accept digital currencies such as bitcoin as payment for legal services. In order to assure that the fee charged remains reasonable under Neb. Ct. R. Prof. Cond. § 3-501.5(a), which prohibits charging unreasonable fees the attorney should mitigate the risk of volatility and possible unconscionable overpayment for services by (1) notifying the client that the attorney will not retain the digital currency units but instead will convert them into U.S. dollars immediately upon receipt; (2) converting the digital currencies into U.S. dollars at objective market rates immediately upon receipt through the use of a payment processor; and (3) crediting the client's account accordingly at the time of payment.

B. An attorney may receive digital currencies as payment from third-party payors so long as the payment prevents possible interference with the attorney's independent relationship with the client pursuant to Neb. Ct. R. of Prof. Cond. §3-501.7(a) or the client's confidential information pursuant to Neb. Ct. R. of Prof. Cond. §3-501.6 by implementing basic know-your-client ("KYC") procedures to identify any third-party payor prior to acceptance of payments made with digital currencies.

C. An attorney may hold bitcoins and other digital currencies in escrow or trust for clients or third parties pursuant to Neb. Ct. R. of Prof. Cond. §3-501.15(a) so long as the attorney holds the units of such currencies separate from the lawyer's property, kept with commercially reasonable safeguards and records are kept by the lawyer of the property so held for five (5) years after termination of the relationship. Because bitcoins are property rather than actual currency, bitcoins cannot be deposited into a client trust account created pursuant to Neb. Ct. R. §§ 3-901 to 3-907 (Trust Fund Requirements for Lawyers).

III. Statement of Facts

Bitcoin and similar computer program protocols are essentially shared ledger books maintained by networked computers. These protocols are often referred to as “digital currencies.” Digital currency that has an equivalent value in real currency, or that acts as a substitute for real currency is referred to as “convertible” virtual currency. Bitcoin is one example of a convertible virtual currency. Bitcoins can be digitally traded between users and can be purchased for, or exchanged

into, U.S. dollars, Euros and other real or virtual currencies. Notice 2014-21, 2014 I.R.B. 938 (4/14/14) entitled I.R.S. Virtual Currency Guidance.

Bitcoin exists on a decentralized peer-to-peer network on the Internet. It is "open source", which means that anyone with the requisite skill can obtain the computer program, review the programming code, evaluate it, use it or create their own version of the software. Bitcoins are stored in a computer file known as a "wallet". A person sending bitcoins to another person uses a "public key", a series of letters and numbers comprising the address to where the funds should be sent. The sender then utilizes a "private key", a code that authorizes the ledger book to make a change that debits the sender's wallet and credits the receiver's wallet.

Bitcoin has an advantage over traditional methods of transmitting value in that there are virtually no fees associated with transfer. Transfers are instant and the shared digital ledger book keeps track of all transactions while also preventing "counterfeiting".

Bitcoin and protocols using similar transactions are not anonymous. They have often been referred to as pseudonymous because it is possible, although difficult, to trace the identity of someone sending bitcoins on the network.

Bitcoin is used by both legitimate businesses and criminals. Legitimate businesses enjoy the ability to quickly receive "digital cash" that guarantees payment without the risk of chargebacks or credit card fees. Criminals, such as the ones that operated the website known as Silk Road, found that their operations were not entirely anonymous. Law enforcement agencies have been able shut down such sites while also arresting the operators and customers of the sites.

Bitcoin and other digital currencies are subject to extensive regulation in the United States. The U.S. Commodity Futures Trading Commission (CFTC), Department of the Treasury and the IRS consider Bitcoin to be property and subject to capital gains taxes. FinCEN and the Department of the Treasury regulate Bitcoin exchangers and money transmitters through authority granted by the Bank Secrecy Act and other statutes. FinCEN requires money transmitters to be registered and implement know-your-client (KYC) and anti-money laundering (AML) procedures. In addition to the Federal framework, each state regulates money transmitters. Some states, including the State of New York, recently adapted their money transmitter statutes to provide for this new technology, allowing for the receipt of digital currencies by merchants but requiring regulatory compliance for businesses selling to consumers. Nebraska's Money Transmitter Act at Neb. Rev. Stat. §8-2701, *et. seq.*, as passed in year 2013 arguably regulates money transmitters who use digital currencies. However, no Nebraska court or administrative body has yet publicly ruled as to whether a money transmission license is required to sell digital currencies and transmit them to buyers.

The price of bitcoins has been volatile. It is traded on dozens of various digital currency exchanges throughout the world. The price 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 bitcoin has recently increased substantially. As of August 30, 2017, the price of a bitcoin was $4,627.77. The price of a bitcoin has been measured objectively using the market prices at various exchanges that sell bitcoins. One such organization, Coindesk, publishes a constant Bitcoin Price Index that considers the weighted average price of a bitcoin at exchanges that meet certain objective requirements such as minimum volume of trade.

In year 2015, the New York Stock Exchange created the NYSE Bitcoin Index with the listing "NYXBT".

Presently there are a large number of Bitcoin payment processors including Coinbase (San Francisco), Bitpay (Atlanta) and Circle (New York). These services claim to eliminate the volatility risk by maintaining consistent exchange rates based on an objective value presented by various exchanges. Of the most established payment processors, Coinbase is licensed by the Nebraska Department of Banking and Finance as a money transmitter under Nebraska's Money Transmitter Act.

A growing number of law firms in other jurisdictions accept bitcoins as payment for services, although it is unknown if they undertook any effort to determine whether such policy is allowed through their respective Bar Associations' Codes of Conduct.

IV. Applicable Rules of Professional Conduct

A. § 3-501.5(a), (b). Fees.

(a) A lawyer shall not make an agreement for, charge, or collect an unreasonable fee or an unreasonable amount for expenses. The factors to be considered in determining the reasonableness of a fee include the following:

(1) the time and labor required, the novelty and difficulty of the questions involved, and the skill requisite to perform the legal service properly;

(2) the likelihood, if apparent to the client, that the acceptance of the particular employment will preclude other employment by the lawyer;

(3) the fee customarily charged in the locality for similar legal services;

(4) the amount involved and the results obtained;

(5) the time limitations imposed by the client or by the circumstances;

(6) the nature and length of the professional relationship with the client;

(7) the experience, reputation, and ability of the lawyer or lawyers performing the services; and

(8) whether the fee is fixed or contingent.

(b) The scope of the representation and the basis or rate of the fee and expenses for which the client will be responsible shall be communicated to the client, preferably in writing, before or within a reasonable time after commencing the representation, except when the lawyer will charge a regularly represented client on the same basis or rate. Any changes in the basis or rate of the fee or expenses shall also be communicated to the client.

B. **§ 3-501.6. Confidentiality of information.**

(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).

(b) A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary:

(1) to prevent the client from committing a crime or to prevent reasonably certain death or substantial bodily harm;

(2) to secure legal advice about the lawyer's compliance with these Rules;

(3) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client, to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved or to respond to allegations in any proceeding concerning the lawyer's representation of the client; or

(4) to comply with other law or a court order.

(c) The relationship between a member of the Nebraska State Bar Association Committee on the Nebraska Lawyers Assistance Program or an employee of the Nebraska Lawyers Assistance Program and a lawyer who seeks or receives assistance through that committee or that program shall be the same as that of lawyer and client for the purposes of the application of Rule 1.6.

C. **§ 3-501.7. Conflict of interest; current clients**.

(a) Except as provided in paragraph (b), a lawyer shall not represent a client if the representation involves a concurrent conflict of interest. A concurrent conflict of interest exists if:

(1) the representation of one client will be directly adverse to another client; or

(2) there is a significant risk that the representation of one or more clients will be materially limited by the lawyer's responsibilities to another client, a former client or a third person or by a personal interest of the lawyer.

(b) Notwithstanding the existence of a concurrent conflict of interest under paragraph (a), a lawyer may represent a client if:

(1) the lawyer reasonably believes that the lawyer will be able to provide competent and diligent representation to each affected client;

(2) the representation is not prohibited by law;

(3) the representation does not involve the assertion of a claim by one client against

another client represented by the lawyer in the same litigation or other proceeding before a tribunal; and

(4) each affected client gives informed consent, confirmed in writing.

D. **§ 3-501.8. Conflict of interest; current clients; specific rules.**

(a) A lawyer shall not enter into a business transaction with a client or knowingly acquire an ownership, possessory, security or other pecuniary interest adverse to a client unless:

(1) the transaction and terms on which the lawyer acquires the interest are fair and reasonable to the client and are fully disclosed and transmitted in writing in a manner that can be reasonably understood by the client;

(2) the client is advised in writing of the desirability of seeking and is given a reasonable opportunity to seek the advice of independent legal counsel on the transaction; and

(3) the client gives informed consent, in a writing signed by the client, to the essential terms of the transaction and the lawyer's role in the transaction, including whether the lawyer is representing the client in the transaction.

(b) A lawyer shall not use information relating to representation of a client to the disadvantage of the client unless the client gives informed consent, except as permitted or required by these Rules.

(c) A lawyer shall not solicit any substantial gift from a client, including a testamentary gift, or prepare on behalf of a client an instrument giving the lawyer or a person related to the lawyer any substantial gift unless the lawyer or other recipient of the gift is related to the client. For purposes of this paragraph, related persons include a spouse, child, grandchild, parent, grandparent or other relative or individual with whom the lawyer or the client maintains a close, familial relationship.

(d) Prior to the conclusion of representation of a client, a lawyer shall not make or negotiate an agreement giving the lawyer literary or media rights to a portrayal or account based in substantial part on information relating to the representation.

(e) A lawyer shall not provide financial assistance to a client in connection with pending or contemplated litigation, except that:

(1) a lawyer may advance court costs and expenses of litigation, the repayment of which may be contingent on the outcome of the matter; and

(2) a lawyer representing an indigent client may pay court costs and expenses of litigation on behalf of the client.

(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.

(g) A lawyer who represents two or more clients shall not participate in making an aggregate settlement of the claims of or against the clients, or in a criminal case an aggregated agreement as to guilty or nolo contendere pleas, unless each client gives informed consent, in a writing signed by the client. The lawyer's disclosure shall include the existence and nature of all the claims or pleas involved and of the participation of each person in the settlement.

(h) A lawyer shall not:

(1) make an agreement prospectively limiting the lawyer's liability to a client for malpractice unless the client is independently represented in making the agreement; or

(2) settle a claim or potential claim for such liability with an unrepresented client or former client unless that person is advised in writing of the desirability of seeking and is given a reasonable opportunity to seek the advice of independent legal counsel in connection therewith.

(i) A lawyer shall not acquire a proprietary interest in the cause of action or subject matter of litigation the lawyer is conducting for a client, except that the lawyer may:

(1) acquire a lien authorized by law to secure the lawyer's fee or expenses; and

(2) contract with a client for a reasonable contingent fee in a civil case.

(j) A lawyer shall not have sexual relations with a client unless a consensual sexual relationship existed between them when the client-lawyer relationship commenced.

(k) While lawyers are associated in a firm, a prohibition in the foregoing paragraphs (a) through (i) that applies to any one of them shall apply to all of them.

E. **§ 3-501.15. Safekeeping property.**

(a) A lawyer shall hold property of clients or third persons that is in a lawyer’s possession in connection with a representation separate from the lawyer’s own property. Funds shall be kept in a separate account maintained in the state where the lawyer’s office is situated. Other property shall be identified as such and appropriately safeguarded. Complete records of such account funds and other property shall be kept by the lawyer and shall be preserved for a period of 5 years after termination of the representation.

(b) A lawyer may deposit the lawyer’s own funds in a client trust account for the sole purpose of paying bank service charges on that account, but only in an amount necessary for that purpose.

(c) A lawyer shall deposit into a client trust account legal fees and expenses that have been paid in advance, to be withdrawn by the lawyer only as fees are earned or expenses incurred.

(d) Upon receiving funds or other property in which a client or third person has an interest, a lawyer shall promptly notify the client or third person. Except as stated in this rule or otherwise permitted by law or by agreement with the client, a lawyer shall promptly deliver to the client or third person any funds or other property that the client or third person is entitled to receive and, upon request by the client or third person, shall promptly render a full accounting regarding such property.

(e) When in the course of representation a lawyer is in possession of property in which two or more persons (one of whom may be the lawyer) claim interests, the property shall be kept separate by the lawyer until the dispute is resolved. The lawyer shall promptly distribute all portions of the property as to which the interests are not in dispute.

V. Discussion

A. Receiving Payments in Digital Currencies as Payment for Services.

Comment 4 of the Neb. Ct. R. Prof. Cond. § 3-501 expressly allows accepting property in payment of services. Therefore, there is no per se rule prohibiting payment of earned legal fees with convertible virtual currency since it is a form of property. However, Nebraska attorneys must be careful to see that this property they accept as payment is not contraband, does not reveal client secrets, and is not used in a money-laundering or tax avoidance scheme; because convertible virtual currencies can be associated with such mischief.

According to Neb. Ct. R. of Prof. Cond. §3-501.5(a), there is a prohibition on unreasonable fees. The values of bitcoins and other digital currencies often fluctuate dramatically. An arrangement for payment in bitcoin 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 the digital currency used as payment quickly fell, the attorney would be underpaid for services.

To mitigate or eliminate the risk of volatility, it is possible to value or convert bitcoins and other digital currencies into U.S. dollars immediately upon receipt. The conversion rate would be market based such as from an exchange or based upon the New York Stock Exchange Price Index, for example. In this way, the bitcoins would serve to credit the client's account and there would be no risk to the client of value fluctuation. As part of this process, a law office would need to disclose to the client that the firm would not be retaining the bitcoins but converting them to cash upon receipt. Through this method, the client is informed that an increase in the value of their bitcoins will not additionally fund their outstanding account. In addition, clients need not be concerned if the value of the bitcoins they sent for payment suddenly dropped.

Such a process should include (1) notifying the client that the attorney will not retain the digital currency units but instead will convert them into U.S. dollars immediately upon receipt; (2) converting the digital currencies into U.S. dollars at objective market rates immediately upon receipt through the use of a payment processor; and (3) crediting the client's account accordingly at

the time of payment. Providing the client the notifications described in this opinion can best be accomplished by including the appropriate notifications in the fee agreement between lawyers and client. Under this framework, the client is properly informed, the use of bitcoins as payment would not result in unconscionable fees to the attorney and the receipt of bitcoins as payment to the attorney would conform to the Nebraska Code of Professional Conduct.

B. **Receiving Payments in Digital Currencies from Third-Party Payers.**

Any time a client arranges for a third party to pay the client's attorney fees the attorney must keep in mind his or her obligations under the Nebraska Code of Professional Conduct. The Code allows an attorney to accept payment from a third party only if the arrangement would not interfere with the attorney's independence or relationship with the client (Neb. Ct. R. of Prof. Cond. §§3-501.7(a), 3-501.8(f)) nor interfere with the client's confidential information (Neb. Ct. R. of Prof. Cond. §3-501.6).

The dilemma faced by an attorney in identifying a third-party payer is that the use of bitcoins is pseudonymous and often close to anonymous. An attorney should comply with the requirements by use of standard Know Your Client ("KYC") procedures when receiving payments from third parties. Most Bitcoin payment processing services require the disclosure of the user's identity. Bitcoin payment processors including Coinbase (San Francisco), Bitpay (Atlanta) and Circle (New York) require the payer to complete a KYC form in order to use their service for payment. In 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 Trust or in Escrow.**

It is permissible to hold bitcoins and other digital currencies in escrow or trust for clients or third parties pursuant to Neb. Ct. R. of Prof. Cond. §3-501.15(a). This Rule allows attorneys to store property as well as currency on behalf of a client. The property must be held separate from the lawyer's property, be properly safeguarded and records must be kept by the lawyer of account funds or other property for five (5) years after termination of representation. Bitcoins are treated as property for federal tax purposes.

Due to the volatility in the value of bitcoins and other digital currencies, the client and parties should be advised that the property held in trust or escrow will be held and not converted into U.S. dollars or other currency. Records of that notice and the records of the separate wallet used to store the bitcoins would be maintained by the lawyer. The shared nature of the blockchain allows anyone, including the client or regulators, to verify the amount of bitcoins and any transactions regarding the separate wallet maintained by the attorney.

Due to security concerns, an attorney opting to receive client payments in Bitcoin or storing them on behalf of clients, whether in trust or in escrow, must take reasonable security precautions. There is no bank or FDIC insurance to reimburse a Bitcoin holder if a hacker steals them. Once lost, bitcoins could be gone forever. Reasonable methods could include encryption of the private key required to send the bitcoins. Another method may include utilization of more than one private key (known as a "multi- signature account" or "multi-sig") for access to the bitcoins. Other reasonable measures may include maintenance of the wallet in a computer or other storage device that is

disconnected from the Internet (also known as "cold storage"), a method that would also allow for off-line storage of one or more private keys.

However, unless converted to U.S. dollars, bitcoins cannot be deposited in a client trust account created pursuant to Neb. Ct. R. §§ 3-901 to 3-907 (Trust Fund Requirements for Lawyers). Thus, if a lawyer receives bitcoins intended to reflect a retainer to be drawn upon when fees are earned in the future, the lawyer must immediately convert the bitcoins into U.S. dollars in accord with section V(A) of this opinion.