AMERICAN ACADEMY AAML OF MATRIMONIAL LAWYERS

JOURNAL OF THE AMERICAN ACADEMY OF MATRIMONIAL LAWYERS

This issue is devoted to:
THE FUTURE OF FAMILY LAW

A Divorce Practitioner's Bitcoin Primer

by
Richard West and Jonathan Fields

Volume 33 2020 Number 1

A Divorce Practitioner's Bitcoin Primer

by
Richard West* and Jonathan Fields**

> If you don't believe it or don't get it, I don't have the time to try to convince you, sorry.
>
> Satoshi Nakamoto

While the initial media mania about bitcoins and the thousands of other digital currencies or cryptocurrencies has subsided, "there is no question that the technology in this sector has the potential to fundamentally change traditional payment systems, the way we do business, and people's everyday lives."[1] Since the market capitalization of all cryptocurrencies exceeds two hundred fifty billion dollars, and young people and other countries with unstable governments are increasingly committed to it, a primer on cryptocurrencies for divorce practitioners is timely, if not overdue.

"Satoshi Nakamoto"[2] created Bitcoin in response to the financial crisis of 2008 when he published his white paper "Bitcoin-A Peer to Peer Electronic Cash System."[3] In general, since bitcoin is used in daily speech as a synonym for cryptocurrencies (like Kleenex for tissue), the authors use "bitcoin" as a generic term for all cryptocurrencies even though it is not technically correct.[4]

---

* Richard West, Esq. is the founder and Managing Partner of West Family Law group in Orlando, Florida.

** Jonathan Fields, Esq., is a founding partner of Fields and Dennis, LLP, a matrimonial practice in Wellesley, Massachusetts.

1 Kenneth A. Blanco, Director Financial Crimes Enforcement Network (FinCEN) NYU Law Program on Corporate Compliance and Enforcement, https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-blanco-nyu-law-program-corporate-compliance-and (last visited on June 9, 2020).

2 It is unknown if this pseudonym is one person or a group.

3 *See* Satoshi Nakamoto, *Bitcoin – A Peer to Peer Electronic Cash System* (Oct. 31, 2008), https://bitcoin.org/bitcoin.pdf.

4 Since "Bitcoin" is both a currency and a protocol, capitalization can be confusing. Accepted practice is to use "Bitcoin" (singular with an upper-case

Because bitcoins are incorporeal, have no intrinsic value (such as gold or silver), and are not backed by any government or financial institution, a host of problems must be addressed. Among these are classification as a currency or investment asset, valuation, taxation, and, in a divorce, finding and dividing them. This article will briefly touch on these issues.

A basic glossary is included in Appendix "A" to assist the reader in understanding the terminology used in this article.

I. The Basics

Unlike fiat currency, Bitcoin was introduced in 2009 to operate without a centralized institution such as a bank or the Federal Reserve.[5] Nakomoto had a deep distrust of central banks, writing they "must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve."[6] Nakomoto's creation, then, was designed to be impervious to the monetary policies of central bankers and politicians.

Bitcoins are unlike traditional currencies because there is no central bank, nation state, or regulatory authority backing it. Bitcoins do not rely on gold or silver as a basis of value. Nakomoto's concept was to create a means of exchange, without any central authority, that could be transferred electronically in a secure, verifiable, and immutable manner. This is known as decentralization, which means no single institution controls the Bitcoin network. Instead of a central authority validating transactions, they are recorded on a public ledger, called the blockchain.

While not the first digital currency, Bitcoin was the first to solve the "double spend" problem. Cash does not have the problem digital currency does. Because bitcoins don't have a physical existence, like a dollar bill, how can one ensure the bitcoins won't be spent more than once? The blockchain permanently monitors the exchange of cryptocurrency so nobody can spend the same bitcoins twice, solving the "double-spend problem." A

---

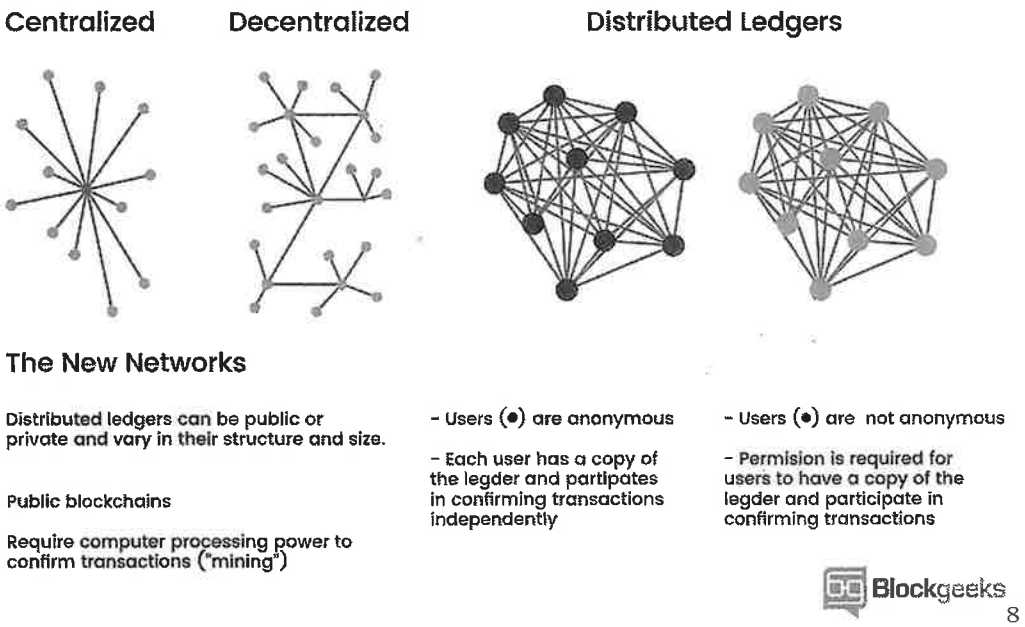
letter B) to label the protocol, software, and community, and "bitcoin" (with a lower-case b) to label units of the currency.

5 Traditional government-backed money is known as "fiat currency."

6 *See* Satoshi Nakomoto, *Bitcoin Open Source Implementation of P2P Currency* (Feb. 11, 2009), https://satoshi.nakamotoinstitute.org.

transaction does not become part of the blockchain until verified by "miners," whose computers perform mathematical calculations for the Bitcoin network to confirm transactions.

The blockchain is "a peer-to-peer immutable distributed ledger which generates computational proof of the chronological order of the transactions, an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value."[7] Imagine a spreadsheet copied thousands of times across a network of computers. Then imagine the network updates the spreadsheet every ten minutes and you have a basic understanding of the blockchain. The blockchain database is not stored in a specific location, or under the control of a single authority, meaning the records it keeps are public and verifiable. No centralized version of this information exists for a hacker to corrupt. Hosted by millions of computers simultaneously, its data is accessible to anyone. Every transaction back to the very first, known as the "genesis block," can be viewed. This is good news for divorce lawyers who have the public and private addresses in question.



Bitcoin and its blockchain are basically a collection of computers, or nodes, around the world that all have Bitcoin's code

---

7 Don Tapscott & Alex Tapscott, Blockchain Revolution (2016).

8 Blockgeeks, https://blockgeeks.com/ (last visited Aug. 28, 2020).

downloaded on them. Each of these computers have all of Bitcoin's blockchain stored on them. This means that each computer has the entire history of bitcoin transactions, which ensures that no one can cheat the system, since every computer would deny the transaction. In this way, Bitcoin is entirely transparent, and no one can make a transaction without everyone seeing it happen. Even those who do not participate in the network as a node or miner can view the transactions taking place live by looking at block explorers,[9] which are browsers for the blockchain, similar to how browsers like Mozilla or Google Chrome work for internet web pages.

II. Price and Value

Where does the value in bitcoins come from? Warren Buffett famously called Bitcoin "a mirage" in 2014, saying "it's a method of transmitting money . . . The idea that it has some huge intrinsic value is just a joke in my view."[10] Is there a distinction between price[11] and value? It is not backed by a valuable commodity like gold or silver. It is not issued by a central bank or backed by a government. It is not like buying shares in a company where one can examine corporate balance sheets or earnings history. So, do bitcoins have value?

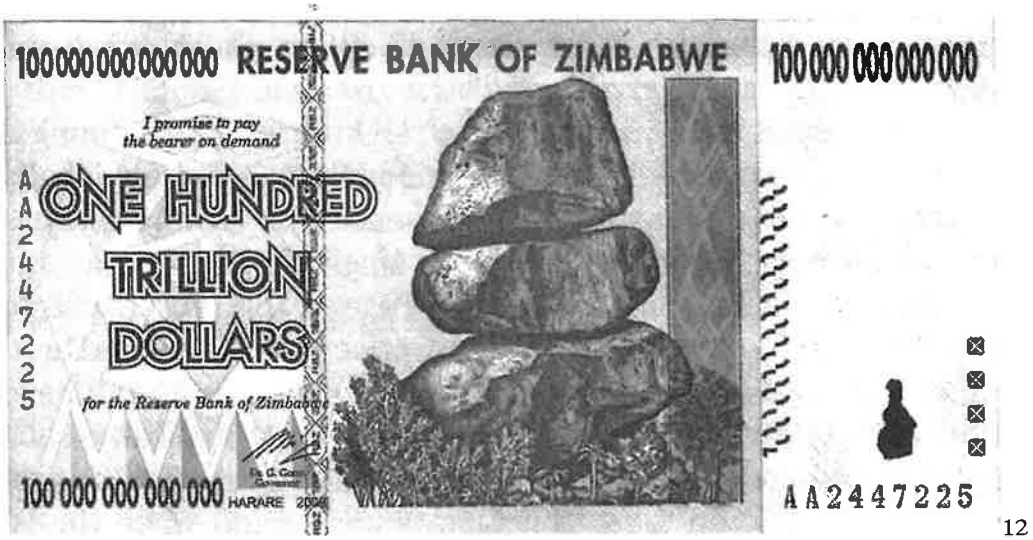
This same question can be asked about fiat currencies. As citizens of a country with both a stable government and economy, Americans have faith in the "greenback." Historically, people probably had faith in the Confederate dollar, the German Deutschmark, and the Zimbabwe dollar. Of course, these currencies were nearly worthless after the Civil War, after World War II, and after 2008 in Zimbabwe (when the government increased the money supply in response to rising national debt, significant declines in economic output and exports, poor government expectations, political corruption, and a weak economy).

---

9 INVESTOPEDIA, https://www.investopedia.com (last visited on June 7, 2020).

10 *Why Does Bitcoin Have Value and How Is the Price Determined?*, LUNO (Mar. 17, 2017), https://www.luno.com/blog/en/post/how-bitcoin-price-determined

11 *See* COINDESK, https://www.coindesk.com/price/bitcoin for price history (last visited on June 7, 2020).



12

The value in bitcoins comes from simple economics: scarcity, utility, supply, and demand. If something is rare and desirable, those characteristics create value. Gold has value because it is rare and desirable. The price of gold is determined by supply and demand.

Bitcoins are scarce by design. No more than 21 million bitcoins can ever exist. The common characteristics of all traditional currencies are scarcity, portability, durability, and divisibility. Bitcoins are more portable than fiat currencies and not easily subject to governmental controls. Bitcoins can easily cross borders. Bitcoins are more durable than physical currency because they have no physical existence to wear out. Each bitcoin is divisible to the 8th decimal place, so each can be split into 100,000,000 units. Each unit of bitcoin, or 0.00000001 bitcoin, is called a satoshi.

Price is determined by the market in which bitcoins trade: by means of supply and demand. This is the same way the price of your secondhand car, a dozen eggs in the supermarket, an ounce of gold, and just about every other commodity is set.

When determining price, one must also consider the amount buyers are currently willing to pay for the *future* value of a specific item. In other words, if the market believes the price of something – like property, a certain stock, or bitcoins – will in-

12 http://1.bp.blogspot.com/-Y9XJ0cv3Pz8/TZM1VebkUyI/AAAAAAAACEw/u1foQRwIHIM/s1600/zimbabwe1.JPG.

crease in the future, they are more likely to pay more for it now.[13]

Valuation of bitcoins is not as straightforward as valuing a publicly traded security. First, the prices fluctuate dramatically from hour to hour – making it much more volatile than, say, a share of Disney. Second, there is no single fixed price at any given moment in time as with stocks. Parties, therefore, tend to agree they will look to any number of price indices – CoinDesk, Winkdex, and Coinbase are popular. Third, bitcoins do not have a closing day price, as do publicly traded stocks. Typically, such stocks are valued as of the closing price on a given day. Practitioners ought to keep these considerations in mind when the issue of dividing these assets arises. The easiest solution, if appropriate for the case, avoiding valuation complexities, is to divide the assets (on a percentage basis) at an agreed time. In other words, simply transfer the assets, in real time, from wallet to wallet. Both parties would individually bear the losses or profits associated with future price fluctuations.

III. Classifying Bitcoin

Trying to classify bitcoins as a currency, a security, a commodity, or property is like trying to classify H_2O as a liquid, gas, or solid. It just depends. Trying to classify a new asset that is only a little more than a decade old is confounding financial experts as well as U.S. government agencies.

Bitcoin, of course, was conceived as a currency and is used as one by millions of people. Companies such as Whole Foods and Starbucks accept it as currency, for example.

On the other hand, some argue that its price volatility can make it unreliable as a currency. One investor, Kevin O'Leary, of *Shark Tank* fame, explained that he tried to consummate a deal with a European company using about $200,000 in Bitcoin. Since it was an international transaction, the notion was that Bitcoin would avoid the problems inherent in currency exchanges. The European company, however, was too nervous about Bitcoin volatility and wanted O'Leary to guarantee its value against the

---

13 *Why Does Bitcoin Have Value and How Is the Price Determined?*, LUNO (Mar. 17, 2017), https://www.luno.com/blog/en/post/how-bitcoin-price-determined.

price of the dollar. O'Leary balked, not wanting to take the risk either. That neither party was willing to take the risk suggested to O'Leary that Bitcoin was "a long way from being a currency."[14]

The Internal Revenue Service, for taxation purposes, also considers Bitcoin and cryptocurrency as assets.[15]

IV. Acquiring Bitcoins

Bitcoins can be obtained in a few different ways. They can be "mined." Bitcoin mining is performed by high-powered computers that solve complex computational math problems which tax even the most powerful computers.[16]

More commonly, people buy bitcoins on exchanges. This is as easy as opening an account at, say, Coinbase or Kraken, and buying bitcoins with a credit card. Exchanges provide the most convenient use of bitcoins because, in addition to buying and selling bitcoins, they provide storage for the bitcoins, and the ability to pay for goods and services. This is done through apps downloaded on computers or mobile devices.

Critical for the divorce practitioner to know: many of these exchanges have "know your customer" requirements requiring identity verification. Further, U.S.-based exchanges (such as Coinbase or Kraken) report certain transactions to the Internal Revenue Service. The company completes a 1099-K for customers receiving at least $20,000 in cash for sales of virtual currencies that are related to at least two hundred separate transactions in a

---

14 Ali Montag, *Kevin O'Leary Explains One Big Thing People Don't Understand About Bitcoin (but Need To)*, CNBC (Dec. 7, 2017), https://www.cnbc.com/2017/12/07/kevin-oleary-bitcoin-is-an-asset-not-a-currency.html.

15 See Section VI, *infra.* Readers interested in an in-depth discussion, including arguments for and against whether Bitcoin should be treated as a currency, security, commodity, or property, are directed to *Is Bitcoin a Currency, Security, Property, Commodity, or "Mirage,"?*, BITIRA (Aug. 22, 2018), https://www.bitira.com/is-bitcoin-a-currency-security-property-commodity-or-mirage/. *See also* United States v. Faiella, 39 F. Supp. 3d 544, 545 (S.D.N.Y. 2014) (finding that Bitcoin clearly qualifies as "money" or "funds" for purposes of the federal money transmitter statute because "Bitcoin can be easily purchased in exchange for ordinary currency, acts as a denominator of value, and is used to conduct financial transactions" (citing SEC v. Shavers, No. 4:13-CV-416, 2013 U.S. Dist. LEXIS 110018, 2013 WL 4028182, at *2 (E.D. Tex. Aug. 6, 2013))).

16 Luke Fortney, *Bitcoin Mining, Explained*, INVESTOPEDIA (May 14, 2020), https://www.investopedia.com/terms/b/bitcoin-mining.asp.

calendar year. Some states have their own requirements. Massachusetts, for example, requires that institutions complete the 1099-K for Massachusetts customers with transactions of $600 or more in a calendar year. A few other states have different thresholds: Arkansas ($2,500), Mississippi ($600), Missouri ($1,200), District of Columbia ($600), New Jersey ($1,000), Vermont ($600).[17]

There are more furtive ways to acquire cryptocurrency as well. A person can buy anonymously through a source (often an individual) listed on a decentralized peer-to-peer network such as LocalBitcoins.com. In contrast to the exchanges like Coinbase, this modality permits transactions without identity verification. Cryptocurrencies can be purchased via credit card and bank wire but also for cash; in many cases, the buyer will meet the seller at an agreed upon physical location and the exchange will take place there. In the context of a divorce, this can be very difficult to discover. Moreover, it should be noted that issuing subpoenas would be ineffective in most cases since the website would have no information on the transacting spouse. This is because these sites operate effectively as classified advertising; a prospective buyer typically responds directly to the seller's offer by email, text, or cell and not within the website.

Spouses can buy cryptocurrency, as noted above. But it can be a part of the fabric of the divorce in other ways as well. For example, a business-owner spouse might offer discounts for payments in cryptocurrency (just as they would with cash) and build up a stockpile that could remain hidden.

V. Bitcoins Storage

Once it is determined that bitcoins have been acquired, the next inquiry is identifying how and where the bitcoins are stored. Bitcoins, essentially long alphanumeric keys (public and private addresses) and not physical objects, are stored in different ways. Storage can be either "hot" (connected to internet) or "cold" (not connected).

---

17 *See Form 1099-K Tax Information for Coinbase Pro and Prime*, COINBASE, https://help.coinbase.com/en/pro/taxes-reports-and-financial-services/taxes/1099-k-tax-forms-faq-for-coinbase-pro-prime-merchant (last visited on June 9, 2020).

Simply put, a private address (or private key) is a secret, alphanumeric password used to spend or send bitcoins to another address. The private key enables the transaction of bitcoins and opens the door to all information regarding them. It is a 256-bit long number picked randomly when a wallet is created. The degree of randomness and uniqueness is defined by cryptographic functions for security purposes. Because the private key allows for the sale of the bitcoins, it must be carefully guarded. *If the private address is lost, the bitcoins are gone forever.*

A private address always starts with 5 and looks like this:

5Kb8kLf9zgWQnogidDA76MzPL6TsZZY36hWXMssSzNydYXYB9KF

A public address (or public key) is an alphanumeric address/number which is derived from a private address only by using cryptographic math functions. It is impossible to reverse engineer and reach the private address from which it was generated. A public address is used to publicly receive bitcoins.

A public address always starts with 1 and looks like this:

1EHNa6Q4Jz2uvNExL497mE43ikXhwF6kZm

Writing the public and private addresses on paper, a "paper wallet," is the simplest method of cold storage. This is not practical for everyday use because bitcoin transactions require a computer. Another cold storage option is storing the addresses on a memory stick. Either of these methods make the addresses almost impossible to find.

Another storage option is in a mobile "software wallet" app on a cellphone or tablet such as Edge, Mycelium, Bither, or Breadwallet. With a software wallet, unlike with an exchange app, the user must install and manage a Bitcoin wallet program, backup the data as with a computer, and prevent the loss of the wallet's password or data files.

Exchanges such as Coinbase and Kraken have their own built-in hot wallets. Exchange customers, therefore, would not necessarily need a separate software wallet app.

Another hot wallet is a hardware digital wallet which is a physical device connected to the internet without the need for a computer, smart phone, or tablet. These devices, made by companies such as Trezor and Ledger, allow users to store, send, and receive bitcoins.

VI. Taxation[18]

In 2014, the Internal Revenue Service issued guidance to taxpayers, IRS Notice 2014-21, 2014-16 I.R.B. 938, characterizing cryptocurrencies as capital assets, if they are convertible to cash. If cryptocurrencies are bought and sold as investments, gains and losses are calculated the same as when buying and selling stock. The same rules apply when it comes to basis, holding period, and a triggering event.

Capital gains and losses are determined by calculating how much the value has increased or decreased from the time of acquisition until there is a taxable event. A taxable event is a sale or exchange of an asset. A taxable event occurs when cryptocurrencies are traded for cash or other cryptocurrencies or used to buy goods or services. Each purchase of goods or services is treated as a sale. If one cryptocurrency is traded for another, a taxable event occurs.

Practitioners who become aware of a party's history of Bitcoin transactions not reported in their tax returns should, unless the practitioner is qualified to handle it, refer the client to a CPA or tax attorney to consider filing amended returns. Furthermore, careful consideration to drafting appropriate indemnification language for the divorce agreement is essential. This is because underpayments attributable to virtual currency transactions may subject the parties to accuracy-related penalties under I.R.C. § 6662.[19] Additionally, failure to timely or correctly report virtual currency transactions may be subject a client to information reporting penalties under §§ 6721 and 6722.[20]

Presently, the IRS does not require exchanges to report on Bitcoin, so there is no form 1099-B issued by the exchange. Some companies like Coinbase will provide Form 1099-K to some users who have received at least $20,000.00 cash for sales of cryptocurrencies related to at least two hundred transactions in a calendar

---

18 Most questions dealing with the taxation of Bitcoin are dealt with on the IRS webpage, "Frequently Asked Questions on Virtual Currency Transactions" found at https://www.irs.gov/individuals/international-taxpayers/frequently-asked-questions-on-virtual-currency-transactions (last visited June 7, 2020).

19 26 U.S.C. § 6662 (2018).

20 26 U.S.C. §§ 6721, 6722 (2018).

year. Coinbase can create a report that gives a summary of transactions and cost basis which is useful to trace transactions.

For 2020, long term capital gains rates (those held more than a year) range up to 20%. The marginal tax rate of the taxpayer will apply to short-term gains taxed as ordinary income. Realized gains and losses are reported on Schedule D and transferred to the reconciliation page of form 1040. No Schedule D is filed if there are no realized gains or losses.

Generally, parties who have a financial interest over $10,000 in foreign financial accounts must file a Foreign Bank Account Report ("FBAR"). The Financial Crimes Enforcement Network ("FinCEN") recently advised FBAR reporting is not required in order to comply with FBAR rules. Nonetheless, practitioners should keep in mind this situation may change in the near future. Prudence suggests checking with an experienced advisor conversant with this area of taxation.

Finally, practitioners should note that, since 2019, the IRS, on its Schedule 1, "Additional Income and Adjustments to Income," has inquired directly whether the taxpayer received, sold sent exchanged or otherwise acquired "any financial interest in any virtual currency."[21]

VII. Dissipation

Dissipation may come into play in divorce cases involving Bitcoin. Because the Bitcoin market is especially volatile, some courts may regard losses as dissipation of the marital estate. Practitioners, however, ought to be wary of this characterization. Consider, for example, *Kittredge v. Kittredge*.[22] In that case, the husband had $400,000 in gambling losses and the Massachusetts Supreme Judicial Court affirmed the trial court's refusal to treat most of the losses as marital waste because, for the most part, the losses never affected the lifestyle of the parties. Note that while gambling may be considered marital waste in many states, these authors could find no reported decisions that determined bitcoin

---

21 Darla Mercado, *The IRS Has a New Tax Form Out and Wants to Know About Your Cryptocurrency*, CNBC.COM (Dec. 6, 2019), https://www.cnbc.com/2019/12/06/the-irs-has-a-new-tax-form-and-wants-to-know-about-your-cryptocurrency.html.

22 803 N.E.2d 306 (Mass. 2014).

was akin to gambling, and, therefore, marital waste. Further, it is worth noting "negligent mismanagement of marital property does not constitute dissipation of marital assets" in most states.[23]

VIII. Discovery

Practitioners should question clients at the outset of a matter to determine whether Bitcoin may play a role in the divorce. Inquiries might include whether the client or their spouse: (a) is tech savvy; (b) has ever bought and sold bitcoins; and (c) has ever received bitcoins in exchange for goods and services.

If there is a history of Bitcoin ownership, further inquiries should include: (a) How did the client or spouse store or transact in bitcoins? (b) Where are important records kept and does the client have access to them? (c) What electronic devices does the client or spouse own? (d) Does the client have physical access to such electronic devices?

If the practitioner determines Bitcoin discovery is warranted, the first step in a sound discovery plan is to send a "preservation letter" to the spouse's attorney reminding that spouse to preserve evidence on phones and computers. If evidence is not preserved, the letter helps to establish a claim for spoliation, an element of which is bad faith and a conscious disregard of the duty to preserve relevant evidence. If a court finds spoliation, it may preclude evidence or make an adverse inference should the matter go to trial. Because every time a person continues to use a computer or phone, there is the potential that relevant data is overwritten, the letter should remind the opponent to "image" (copy/ghost) their drives immediately so there is a record of them at or about the point in time the preservation letter was received.

While seemingly perplexing, Bitcoin discovery is no different from tracing more traditional assets and may even provide more information. Blockchain transactions are not strictly anonymous, but rather pseudonymous, since they can be linked to a public address. Because of the immutable nature of the blockchain, information on every transaction remains available

---

23 Erica Driskell, Comment, *Dissipation of Marital Assets and Preliminary Injunctions: A Preventive Approach to Safeguarding Marital Assets*, 20 J. AM. ACAD. MATRIM. LAW. 135, 137 (2006). *See also* Segall v. Segall, 708 So.2d 983, 986 (Fla. Dist. Ct. App. 1998).

forever, unlike conventional financial institutions which may only keep records for seven years. Interrogatories, document requests, and depositions simply need to be tailored to use the new terminology of Bitcoin.

Examination of bank or credit card statements might reveal payments to Bitcoin exchanges (e.g., Coinbase). If they do, records can be obtained from the exchanges showing the history of all transactions. In *United States v. Coinbase, Inc.*,[24] the IRS successfully enforced a summons (subpoena) to obtain the records of Coinbase customers. These records included transaction logs, records of payments processed, correspondence between the exchange and the other spouse, amongst others.[25]

The most direct method of obtaining the complete history of Bitcoin transactions is to obtain the private address. If a court has personal jurisdiction over the other spouse, the court can order that spouse to provide the private address, just as a court could order them to provide account logins and passwords.

A forensic examination (with or without the private address) of the other spouse's computer, smartphone, or tablet may yield evidence of past or present use of wallet apps (e.g., Mycelium) or exchange apps (e.g., Coinbase). If the attorney is fortunate and obtains the private keys associated with the bitcoins, a forensic expert will be able to examine the blockchain and trace the movement and amount of every transaction the other spouse has made.

Once a court orders the examination of the contents of a hard drive, several considerations come into play since a party is not going to simply hand over a hard drive to the other side. Therefore, it is critical to work with a computer forensic expert to draft pleadings or stipulate to a protocol. The protocol must have search parameters such as keywords (e.g., "Bitcoin," "Mycelium") and a date range, as well as a procedure to deal with privileged communications and irrelevant data. The protocol must require the device owner to provide his or her password. Although the world of Bitcoin is cutting-edge, as noted above, the

---

24 *See* United States v. Coinbase, Inc., No. 17-cv-01431-JSC, 2017-2 U.S. Tax Cas. (CCH) P50,423, 120 A.F.T.R.2d (RIA) 2017-6671, 2017 WL 5890052 (N.D. Cal. Nov. 28, 2017).

25 *See* Appendix B for samples of areas of inquiry.

fundamental discovery rules about breadth and scope and the use of protective orders still apply.[26]

The shrewdest of spouses may well evade even the ablest forensic investigator by a process known as "bitcoin mixing."[27] By using a mixing service or tumbler, such as UltraMixer or CoinMixer, the user can break the link between addresses by either creating temporary addresses or by swapping coins with other addresses of the same value. Another way people are maintaining the secrecy of cryptocurrencies is "private coins" such as Monero and Zcash. Mixers and private coins make the trail hard to follow on the blockchain.

Regarding the examination of computer devices, many clients are tempted to resort to self-help. They might search their spouse's cell phone or computer, or install key-stroking software and, in so doing, depending on the circumstances, violate state or federal privacy laws.[28] Practitioners, therefore, must consider these statutes, and other applicable laws, before counselling clients regarding self-help.

Conclusion

As indicated by the title, this is a primer intended to provide the practitioner a 50,000-foot view of Bitcoin, the fundamental concepts of this emerging currency, and the technology on which it relies. If this article achieved the intended purpose, the reader should be able to identify cases in which Bitcoin may play a role.

This basic knowledge should allow the family lawyer to determine if a forensic expert, experienced in tracing Bitcoin assets, is needed and to communicate effectively with the expert to formulate a discovery plan. This knowledge should be helpful in convincing clients, opposing counsel, and courts of the necessity of the proposed discovery plan in an articulate manner. This primer provides the practitioner with the ability to recognize potential issues, including valuation, dissipation, distribution, and taxation of Bitcoin assets.

---

26 *See, e.g.*, Rule 26 in states that have substantially adopted the Federal Rules of Civil Procedure.

27 *See* Appendix A, Glossary.

28 *See, e.g.,* Stored Communications Act, 18 U.S.C. § 2703 (2018); Wiretap Act, 18 U.S.C. § 2511 (2018); Computer Fraud and Abuse Act, 18 U.S.C § 1030 (2018).

As the use of Bitcoin increases, both as an investment and as currency, the savvy divorce practitioner would do well to continue to keep current on technical and legal developments.

Appendix "A"
Glossary

Address

A Bitcoin address, or key (see private key below) refers to either public or private addresses. Public addresses are used to send and receive bitcoins. A crucial difference, however, is that each address should only be used for a single transaction.[29]

Bit

A bit is one one-millionth of 1 bitcoin, or 1,000,000 bits equals 1 bitcoin. A bitcoin can also be divided to 8 decimal places or 0.00000001 bitcoin, is called a satoshi. This is important because, for a currency to be useful it must be easily divisible.

Bitcoin

When capitalized "Bitcoin" refers to open source software used to create the bitcoin virtual currency and the peer-to-peer network formed as a result. The individual units of the bitcoin virtual currency (when lowercase). e.g., "I sent ten bitcoins today"; it is also often abbreviated BTC or XBT.[30]

Bitcoin mixing

"Bitcoin mixers are solutions (software or services) that let users mix their coins with other users, in order to preserve their privacy."[31]

Block

These are where all the details of transactions are stored. All transactions recorded in the block are considered immutable – they cannot be altered – and transparent. This way, users can

---

29 Bitcoin.org, https://bitcoin.org/en/vocabulary (last visited Aug. 29, 2020).

30 *Id.*

31 *What Are Bitcoin Mixers*, Bitcoin Mag. https://bitcoinmagazine.com/guides/*what*-are-bitcoin-mixers (last visited July 29, 2020).

see[32] where they were recorded, and which transactions took place. Once a block is full, all new transactions are automatically moved to a new block and so on.

Blockchain

The block chain is a "public record of Bitcoin transactions in chronological order. The block chain is shared between all Bitcoin users. It is used to verify the permanence of Bitcoin transactions and to prevent double spending."[33]

BTC

"BTC is a common unit used to designate one bitcoin." ₿

Confirmation

"Confirmation means that a transaction has been processed by the network and is highly unlikely to be reversed. Transactions receive a confirmation when they are included in a block and for each subsequent block. Even a single confirmation can be considered secure for low value transactions, although for larger amounts like $1,000, it makes sense to wait for 6 confirmations or more. Each confirmation *exponentially* decreases the risk of a reversed transaction."[34]

Convertible Virtual Currency

Virtual currency that has an equivalent value in real currency or that acts as a substitute for real currency.[35]

---

32 Bitcoinexchnageguide.com, *Blockchain Glossary & Cryptocurrency Vocabulary Terms,* https://bitcoinexchangeguide.com/blockchain-glossary-cryptocurrency-vocabulary-terms/#g (last visited Aug. 29, 2020); Montclair University, *Course Hero, ACCT510 Class_Bitcoin and Blockchain Exercise (1).docx* https://www.coursehero.com/file/52177964/ACCT510 (last visited Aug. 29, 2020).

33 *Id.*

34 https://coinira.com/cryptocurrency-glossary/ (last visited Aug. 29, 2020).

35 *Virtual Currencies*, IRS, https://www.irs.gov/businesses/small-businesses-self-employed/virtual-currencies (last visited July 30, 2020).

Cryptography

"Cryptography is the branch of mathematics that lets us create mathematical proofs that provide high levels of security. Online commerce and banking already use cryptography. In the case of Bitcoin, cryptography is used to make it impossible for anybody to spend funds from another user's wallet or to corrupt the block chain. It can also be used to encrypt a wallet, so that it cannot be used without a password."[36]

Double Spend

"If a malicious user tries to spend their bitcoins to two different recipients at the same time, this is double spending. Bitcoin mining and the block chain are there to create a consensus on the network about which of the two transactions will confirm and be considered valid."[37]

Fiat Currency

Fiat currency is "legal tender whose value is backed by the government that issued it. The U.S. dollar is fiat money, as are the euro and many other major world currencies. This approach differs from money whose value is underpinned by some physical good such as gold or silver, called commodity money."[38]

Mining

Bitcoin mining is the process of making computer hardware do mathematical calculations for the Bitcoin network to confirm transactions and increase security. As a reward for their services, Bitcoin miners can collect transaction fees for the transactions they confirm, along with newly created bitcoins. Mining is a specialized and competitive market where the rewards are divided up according to how much calculation is done. Not all Bitcoin

---

36 https://dash-docs.github.io/en/vocabulary (last visited Aug. 29, 2020).

37 WAYNE WALKER, THE DEFINITIVE GUIDE TO MASTERING BITCOIN & CRYPTOCURRENCIES (2018).

38 Jason Hall, *Fiat Currency: What It Is and Why It's Better Than a Gold Standard*, MOTLEY FOOL (Dec. 6, 2015), https://www.fool.com/investing/general/2015/12/06/fiat-currency-what-it-is-and-why-its-better-than-a.aspx.

users do Bitcoin mining, and it is not an effortless way to make money.

P2P

"Peer-to-peer refers to systems that work like an organized collective by allowing everyone to interact directly with the others. In the case of Bitcoin, the network is built in such a way that each user is broadcasting the transactions of other users. And, crucially, no bank is required as a third party."[39]

Private Key

A private key is "a secret piece of data that proves your right to spend bitcoins from a specific wallet through a cryptographic signature. Your private key(s) are stored in your computer if you use a software wallet; they are stored on some remote servers if you use a web wallet. Private keys must never be revealed as they allow you to spend bitcoins for their respective Bitcoin wallet."[40]

Signature

A cryptographic signature "is a mathematical mechanism that allows someone to prove ownership. In the case of bitcoin, a Bitcoin wallet and its private key(s) are linked by some mathematical magic. When your Bitcoin software signs a transaction with the appropriate private key, the whole network can see that the signature matches the bitcoins being spent. However, there is no way for the world to guess your private key to steal your hard-earned bitcoins."[41]

Wallet

A Bitcoin wallet is "loosely the equivalent of a physical wallet on the Bitcoin network. The wallet actually contains your private key(s) which allow you to spend the bitcoins allocated to it in

---

39 *Bitcoins Terms/Vocabulary*, BitBuy https://bitbuy.at/about-bitcoin/terms/ (last visited Aug. 29, 2020).

40 U.S. Sentencing Commission, *Bitcoin Glossary: 2018 National Seminar*, https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018-materials/emerging-tech_glossary-crypto.pdf.

41 *Id.*

the blockchain. Each Bitcoin wallet can show you the total balance of all bitcoins it controls and lets you pay a specific amount to a specific person, just like a real wallet. This is different to credit cards where the merchant charges you."[42]

---

42 Id

Appendix "B"

According to attorneys Janice Boback and Stephanie L. Tang,[43] discovery to the opposing party either by interrogatories or deposition should include:

1. Do you own any form of cryptocurrency?
2. Have you ever owned any form of cryptocurrency?
3. Does anyone now, or in the past, hold any cryptocurrency for you?
4. Are any held by overseas exchanges?
   If yes;
5. Do you have any form of E-wallet? (generic term)
6. Have you ever had an E-wallet?
7. If you have a crypto account what exchange or exchanges do you use?
8. Which have you used in the past?
9. What is your private key?
10. What is your public key?
11. Have you reported/intend to report capital gains?
12. If not, will you be filing an amended return?

Looking at the Order in the Coinbase case, at a minimum, document requests to Coinbase or other exchanges should include:

1. Complete user profiles;
2. Know-your-customer due diligence;
3. Documents regarding third-party access;
4. Transaction logs;
5. Records of payments processed;
6. Correspondence between the exchange and the other spouse;
7. Account or invoice statements;
8. Records of payments.

The address for Coinbase is: **Coinbase, Inc.**
548 Market Street #23008
San Francisco, CA 94104

---

43 Janice L. Boback & Stephanie L. Tang, *Cryptocurrency in Divorce Proceedings,* https://illinoislawforyou.com/property-division/cryptocurrency-divorce-proceedings/, (last visited Aug. 29, 2020).

Documents To Be Produced

1. All account statements solely or jointly in the name of _____.
2. All documents regarding detailed account activity for Coinbase accounts solely or jointly in the name of _____.
3. All documents regarding deposits of currency or money in Coinbase accounts solely or jointly in the name of _____.
4. All documents regarding deposits of bitcoins or cryptocurrencies in Coinbase accounts solely or jointly in the name of _____.
5. All documents regarding withdrawals of currency or money from Coinbase accounts solely or jointly in the name of _____.
6. All documents regarding withdrawals of bitcoins or cryptocurrencies from Coinbase accounts solely or jointly in the name of _____.
7. All documents regarding storing, buying, selling, trading, exchanging, sending, receiving, or using bitcoins or cryptocurrencies in Coinbase accounts solely or jointly in the name of _____.
8. All documents regarding converting or exchanging bitcoins or cryptocurrencies into currency, products, services or otherwise in Coinbase accounts solely or jointly in the name of _____.
9. All documents regarding converting currency, products, services or otherwise into bitcoins or cryptocurrencies in Coin base accounts solely or jointly in the name of _____.
10. All account opening documents for all Coinbase accounts solely or jointly in the name of _____.
11. All documents regarding the codes or identification of bitcoins or cryptocurrencies in Coinbase accounts solely or jointly in the name of _____.
12. All documents regarding wallets, blockchains, transaction I.D.' s, inputs of transactions and input keys in Coinbase accounts solely or jointly in the name of _____.

All documents in Coinbase's file on _____.