INTERNATIONAL REVIEW OF LAW, COMPUTERS & TECHNOLOGY
2019, VOL. 33, NO. 1, 34–52
https://doi.org/10.1080/13600869.2019.1565105

Routledge
Taylor & Francis Group

Anonymous Bitcoin v enforcement law

Fulya Teomete Yalabık and İsmet Yalabık

Independent Researcher

ABSTRACT

Bitcoin is the most prominent cryptocurrency that is frequently debated nowadays, basically defined as decentralised 'currency', 'payment system' and 'investment tool' which is an opportunity offered by today's digital age. In this article, we aim to fulfil the analysis of the legal basis of the matter from both technical and legal point of view. Despite there are many legal issues related to Bitcoin, we will particularly draw attention to some of the fundamental legal problems caused by the anonymity feature of the Bitcoin. Among these problems that may arise, only the disputes that may fall within the scope of the cases relating to debt and asset which have an impact on enforcement law will be examined. We will discuss the anonymity feature, considering the possibility of accessing an anonymous Bitcoin wallet. The article examines the situation where a debtor or one of the parties in a lawsuit may conceal their assets unfairly via Bitcoin (with the anonymity feature) in civil disputes relating to debt and assets. Has Bitcoin turned into a tool that malevolent debtors can hide their wealth while at the same time, a secret place where they can invest their money? In this study, we will offer solutions on overcoming the anonymity feature in practice and how to reveal and reach the wealth that are stored via Bitcoin wallet. Likewise, it will be underlined what malevolent debtors or parties in a lawsuit who want to obscure their wealth via Bitcoin wallet can do to strengthen their anonymity. Finally, we provide a specific and practical guideline for judges and especially creditor's lawyers in order to reduce the potential adverse situation that Bitcoin's anonymity feature can cause.

ARTICLE HISTORY
Received 26 August 2018
Accepted 28 December 2018

KEYWORDS
Bitcoin; anonymity; enforcement law

I. Introduction

The theme of this article is mainly anonymity of the Bitcoin and its implications on enforcement law. The main reason for this preference is obviously a desire to find a solution for the possible needs of particularly the creditors' and spouses' lawyers (in a divorce case) who may be in a position struggling with opposite party's attempt to hide his/her assets via Bitcoin. The reason why we notably chose to examine cases related to debt and assets involving divorce cases is that parties in such cases have really tendency to try to hide their wealth against their disclosure obligations. Bitcoin may be a good alternative to become a weapon for creditors and divorcing spouses during court battles. It can be said that one of the most effective and innovative methods for hiding money can be

CONTACT Fulya Teomete Yalabık fteomete@gmail.com

the Bitcoin in the modern era. This can be seen as a technological form of burying a sack of cash in the woods (Camp).

Various articles have been written about Bitcoin, and many different problems have been raised. However, when it comes to finding, attaching and seizure of the Bitcoin, one may directly conclude that these procedures are not possible for Bitcoin because it is anonymous and decentralised. In this direction, the question of the possibility of attaching and seizure or simply finding Bitcoin has stirred our minds. For example, if a debtor or one of the spouse in a divorce case hid his/her assets in a secret bank account, and the creditor or the other spouse is in doubt about the existence of such hidden assets and also has some evidence about its existence, will he/she not be able to reach these secret accounts and will wait desperately? Analogously, a safe is found during a search in the debtor's property. If the debtor does not give the key of the safe or does not tell the password, in such a situation, does it mean that it is impossible to reach the safe to attach it? These examples are in fact showing us that it is not impossible to find and attach the Bitcoin assets if we consider a Bitcoin wallet like a hidden bank account or a secret safe with a hidden key.

Nowadays, technology enables individuals to exchange currency quicker and more effectively with virtual currencies. Bitcoin, the most prominent virtual currency has become increasingly popular as a 'decentralised currency', a method of 'payment system' and 'investment tool'. This paper is not a detailed examination of this financial instrument, which has many complex features in its essence.

The inception of Bitcoin has inflamed many legal questions and unprecedented issues. Bitcoin has recently become quite noticeable in cryptocurrencies and has led to the need for examination and interpretation in detail the legal and technical aspects of Bitcoin. On the basis of the studies on Bitcoin, the necessity to subject this decentralised virtual currency to a certain regulation. The courts have been largely silent for the Bitcoin, which is making a tremendous impact all over the world and is often discussed about its current and potential legal problems. Until now, legal cases about Bitcoin has been criminal prosecutions or disputes between Bitcoin companies (Raskin 2015, 969). However, there are extensive possible civil actions involving Bitcoin (Raskin 2015, 972). Since the process of characterising Bitcoin is problematic and contentious, many people do not technically understand the notion of Bitcoin. Even though there are many academic and newspaper articles written on this subject with a wide range of debates, the complexity of the subject, and therefore the fact that governments still want to act reluctantly regarding Bitcoin, has led to the lack of an official regulation. A corroborative legal classification would give debtors, creditors, and judges guidance on how to treat Bitcoin.

Actually, the focus of this paper is after simplifying the main subject and interpretation of the major issues, to suggest straightforward solutions that everyone can understand.

Almost all of the articles about Bitcoin have been written either by engineers from a technical point of view without examining legal aspects sufficiently or by law academics explaining legal aspects with a simple reference to the technical articles without considering and explaining enough the technical elements. Regrettably, due to Bitcoin's complexity, we have not encountered an article that examines Bitcoin's essence embracing both the technical and legal aspects and draws attention to the related basic problems. In this article, we aim to fulfil the analysis of the legal basis of the matter from both technical and legal point of view. Therefore, the subject matter has been expressed plainly and

clearly for both lawyers, technical people, and laymen who are interested in the issues regarding Bitcoin.

In this paper, despite there are many legal issues related to Bitcoin, we will particularly draw attention to some of the fundamental legal problems caused by the anonymity feature of the Bitcoin. Among these problems that may arise, only the disputes that may fall within the scope of the cases relating to debt and asset which have an impact on enforcement law will be examined. In other words, the purpose of this article is to bring light to the implications of the anonymity feature of the Bitcoin on enforcement law. We will discuss the anonymity feature, considering the possibility of accessing an anonymous Bitcoin wallet.

If we ask in the simplest and basic way, in an action of debt will a debtor who hides his/her assets via Bitcoin wallet, abuse the civil process by virtue of the anonymity feature of Bitcoin? In other words, may this debtor negatively affect the enforcement process or even preclude it? In another situation such as a divorce case, may one of the spouses be able to hide his/her assets from the other spouse via an anonym Bitcoin wallet and cause the case to end up in the direction of his/her own interest in a malignant way by unfairly affecting the process of the case? For example, in a very contentious divorce process, parties sometimes act unjustly and attempt to conceal their assets from their spouse that would otherwise be subject to equitable distribution (Centeno 2017). As another illustration and another question, if the existence of the Bitcoin wallets of a debtor or a spouse who hide his/her assets for his/her benefit through this method, has been discovered then what will happen in this case? How can be this anonymous Bitcoin wallet found or is there any possibility to even make it accessible? In short, does the anonymity feature particularly transform Bitcoin usage to a concealment place or safe that enables to hide the assets by abusing its impact?

We want especially to emphasise that it will be a very wrong thought if someone thinks that even Bitcoin's implications are alarming, that does not able to cause any damage because it is not being widely used; or since it is very volatile, it is not difficult to be collapsed. It would be a big mistake not to create a legal consciousness in this matter or regulate it legally. Because, Bitcoin is not anymore the sole crypto-currency, as many others have been evolving, such as Ripple, Litecoin, Peercoin, Darkcoin and Dogecoin (Mandjee 2016, 162).[1] Bitcoin is the cornerstone of decentralised currency, and many other virtual currencies exemplified above are modelled on the same or similar principles (Cook 2014, 568). If Bitcoin's financial value were to downfall, its users would shift to another currency, such that there is still a need to focus on the apprehensions caused by crypto-currencies that are steadily acquiring significance (Mandjee 2016, 160).[2]

The basis of the discussions analysed in this study is particularly the perverse picture caused by Bitcoin wallet's anonymity feature. This article examines the situation where a debtor or one of the parties in a lawsuit may conceal his/her assets unfairly via Bitcoin (with the help of the anonymity feature) in civil disputes relating to debt and assets in England and Wales. Since the ownership of this financial instrument can be anonymous when a defendant is subject to a civil action to ascertain the full extent of his/her assets may be difficult or even impossible. In addition, even if this is known, how can a creditor collect his/her debt? Has Bitcoin turned into a tool that malevolent debtors can hide their wealth while at the same time, a secret place where they can invest their money?

II. What is Bitcoin from an integral of legal and technical perspective?

A. How does Bitcoin basically work?

Bitcoin is an Internet-wide payment system that does not depend on a central power to ensure and administer its money supply. Especially both its anonymity feature and being decentralised makes it such an astonishing payment system and virtual currency. In the process, there is no bank, no credit unions nor lenders.

Bitcoin is not the sole digital currency, nor the only prosperous one. What makes Bitcoin special is that, unlike other online (and offline) currencies, it is neither designed nor managed by a single power such as a central bank.[3] Anyone who wants to follow the network can download the software and build an account from which 'electronic money' can be transferred to different accounts. This authorises anyone in the world to pay anyone else in the world any amount of value of Bitcoin by simply transferring ownership of the corresponding slot in the ledger (Andreessen 2014). Since it is decentralised even everyone knows that the transfer has realised, nobody can question the legality of the transfer.

At this point, it is worth mentioning briefly the music and movie industry, which does not have a central authority. In light of the case of A&M Records v. Napster, Inc.[4] we want to emphasise the different effects of centralised-decentralised networking. Napster, Inc. was the pioneer in peer to peer networking with a central server to route music transmission (Cook 2014, 562). However, more complex file sharing programmes have become decentralised (Cook 2014, 562). The essence of how it performs is very comparable to Bitcoin. Each user had to download software and login to a network similar to Bitcoin's virtual wallet and address (Cook 2014, 562).[5] After this procedure has been done once, users were free to exchange music mutually and upload/download any music that they select. It may be acceptable for the people who can upload and download music gratuitous, however, for the people who are the owners of the copyrights of the data that was traded, it should be very disappointing and damaging (Cook 2014, 562). Since Napster, Inc. had a central authority, it was not troublesome for A&M Records to investigate and claim it for copyright infringement. The Court held that Napster, Inc. had infringed on many copyrights and ordered an injunction that effectively shut the site down.[6] Since then, other groups have imitated the 'Napster approach' (Cook 2014, 563). Applying a decentralised network, they simulate the configuration that Bitcoin functions and underlines some of the problems in regulation (Cook 2014, 563). Although there is no central authority, the music and movie business struggles to restrict illegal file sharing by investigating and suing the largest infringers though (Cook 2014, 563).

The public ledger is very important; it is the technology that stores all transactions taking place in the process. It is separated into blocks of transactions, connected to the previous block, forming what is called the 'blockchain'. The blockchain is crucial to track every Bitcoin transaction made and guarantee that no one is double spending the Bitcoins they possess. Every exchange of Bitcoins records the time and the public wallet addresses of the parties involved. As a result, each Bitcoin holds the link to all its previous transactions, the time the transaction took place, and the public addresses of the parties involved (Dion 2013, 167; Cook 2014, 539). This procedure replaces the function of a central administrator who would have to carry out policies against double spending (Mandjee 2016, 162).

The method behind a transaction can be compared to the obtaining a seat on a stock exchange (Mandjee 2016, 162). Basically, one buys into the ledger a fixed number of slots for cash or by selling a product and service for Bitcoin. That person can then sell out of his/her spot in the ledger by trading his/her Bitcoin to someone who wants to buy in the ledger, without the necessity of any authorisation, and at almost no fees. Instead of money, the slots in the ledger are exchanged.

B. The importance of the private key in the process

One of the fundamental elements of the process of Bitcoin is the utilisation of public addresses and private keys (Raskin 2015, 975). In authorising a transaction, a person uses his/her private key to sign the transaction. A private key is a number that symbolises a person's account, whose signature will be confirmed with the matching public key (Nakamoto 2009; Krohn-Grimberghe and Sorge 2013). The main aspect that outlines ownership of Bitcoin is the ownership of the private key (Nakamoto 2009, 2). If a person administers the private key, he/she controls the Bitcoin and is able to transfer those Bitcoins and declare authority over them (Nakamoto 2009, 2). A person dominates a private key whenever he/she is able to join that private key to the Bitcoin network and uses the key to spend or transfer the Bitcoins (Raskin 2015, 1002). Therefore, Bitcoins are situated wherever a court can have power over a private key by transmitting the Bitcoins into the court's wallet (Raskin 2015, 1003).

A court's control over Bitcoins makes it different from the control over intangibles. For example, if there is a private key situated in a safety deposit box in a court's jurisdiction, the court can assign a sheriff to the bank with an order to seize the private key (Raskin 2015, 1004).[7] The sheriff would then transmit those Bitcoins into a wallet owned by the court. Since Bitcoins are eligible to be transferred into a court's possession and that possession would be exclusive, Bitcoins are much like houses (Raskin 2015, 1004). Nevertheless, a Bitcoin is not like a house for the reason that a house cannot exist in multiple locations. On one end of the spectrum is the private key printed out on a sheet of paper and stored in a bank vault where that private key is the only one in existence as 'cold storage' (Acheson 2018). This makes the Bitcoin virtually equal to a house (Raskin 2015, 1005). On the other hand, a Bitcoin private key that is both administered by multiple parties and exists on servers or computers in multiple transnational jurisdictions provokes problems (Raskin 2015, 1005). For example, a third party wallet service like Coinbase, which has servers in various states and countries and empowers multisignature technology complicates to reach the Bitcoin wallet. Accordingly, the type of the private key used for has great importance.

Since Bitcoin stands under the control of the party keeping the private key, it may be complicated to enforce the legal process. To whom should the order of attachment or freezing order be delivered? Furthermore, in the event that the debtor transfers the funds out of such an account, it may be difficult or even impossible for a creditor to recover anything, even with a court order. Because Bitcoin can be easily transferable worldwide and this will shield the true identity of transferees (Martinson and Masterson 2014, 18).

It can be said that the secret Bitcoin wallet can be reached by accessing mainly via the private key. In other words, if the private key is accessible, then the assets hidden via Bitcoin wallet can become reachable.

C. Different storage types of the Bitcoin

All digital information is stored as files in our computers today. Bitcoin is also stored in the form of digital files. Storage solutions differ in terms of security, accessibility and privacy.

1. Electronic wallet

Electronic wallets are special software that can either be downloaded or hosted by a cloud backend service. These wallets are only storing Bitcoins as binary files (transaction address and private key) on users' computer or mobile device (Acheson 2018).

Owners should be aware of backing up software regularly to prevent possible loss due to the theft of the computer or fatal system failure that damages the local hard drive and corrupts files. Even if the user removes the application from his/her mobile device or computer, generally user data related to the application would still remain on permanent disk store of user's computer. For that reason, any Bitcoin asset hidden by a debtor can be conveniently recovered by inspecting the debtor's device by the experts. That is to say, even a debtor or a spouse who tries to hide his/her assets via Bitcoin with an electronic wallet, it is possible to uncover the usage of an electronic wallet. Although the party who hides assets can transfer the Bitcoin assets before the court attaches them, to discover an electronic wallet will be evidence of hiding assets and so contempt of court.

The cloud-based version of software generally stores Bitcoins and private keys in a cloud-based storage. Bitcoin owners should trust third-party cloud storage to secure their digital assets and private keys.

In case of collecting debts from a debtor who owns an electronic wallet is straightforward, because the electronic wallet holds all transaction identifiers and private keys. Once transaction addresses and private keys are acquired, the attachment process of those assets should be straightforward.

2. Software wallet

Although software wallets resemble electronic wallets in so many ways, they are more complicated than electronic wallets as they provide more security and capability in terms of ease of usage and simple configurability. These are software applications that can be downloaded from Application Stores like GooglePlay, App Store and installed on a computer or mobile device. These wallets offer easy interfaces to transfer Bitcoins like generating QR codes to scan. Well-known issues with Software wallets are the possibility of losing digital assets when storage hardware issues arise or an intruder or a thief either steal owner's computer or gains control over the digital asset and private key. Therefore, keeping regular backups is the best practice to overcome such situations.

Due to the huge size[8] of the ledger, most Bitcoin software wallets today are called as 'light wallets' or Simplified Payment Verification. These wallets do not acquire entire ledger, but they are capable of synchronising transactions with the real ledger. They also provide extra security and capability to store Bitcoins offline. This method is called 'cold wallet'.

As electronic wallets, creditors can easily find and attach debtors' Bitcoin assets via gaining access to the debtor's computer or mobile device. Since Bitcoin can be transferred to another person in a very short period of time, gaining access to debtors' devices is a time critical operation to attach someone's digital assets.

3. Online wallet

Online wallets are actually centralised institutions or corporations that provides a convenient and secure way to access owner's Bitcoin wallet. These wallets use centralised online data to keep owner's Bitcoins and private keys safely and securely. Some of the online wallets offer mixing. These support easy tools to convert Bitcoins to certain currency or another cryptocurrency (Böhme et al. 2015, 213–238). Online wallets come with mobile and desktop applications that help Bitcoin owners to send and receive Bitcoins in a most convenient way. In terms of security, these corporations are under heavy threat of cyber intruders as the other banking corporations are.

In most countries, online wallets have started to be regulated by financial criteria. For that reason, it would be possible to reach out debtors' digital assets via contacting online wallet providers.

4. Hardware wallet

Hardware wallets are physical devices that introduce advanced encryption and security to store the Bitcoins. They are rarely offline and almost impossible to hack. They could be in the form of an external hard drive or USB memory stick. Large investors generally use hardware wallets and keep these wallets somewhere secure like bank vaults.

Hardware wallets are the most secure way to store Bitcoins. If the device could not be discovered, it could be extremely difficult to prove if a debtor takes possession of Bitcoin assets.

5. Paper wallet

Paper wallets are the least complex of all these wallets. Private, public keys and Bitcoin address are printed on paper. Since they are physically written on a piece of paper, they give the impression of a currency that is in circulation today. They are secure because of the absence of a network connection; on the other hand, once they are stolen or badly damaged, the owner can lose his/her Bitcoin assets.

6. Physical coins

Physical coins are metal coins that hold a certain amount of Bitcoins. Each physical coin has its own private key as an embedded paper covered by tamper-resistant hologram. These coins are designed for person to person transactions like any physical currency. On the other hand, once its value redeemed, coins have no further value.

Since they are physical, once someone found them, there is no need to do further research unlike the other wallet storage types. Search order would be a convenient procedure in order to trace the physical coins.

All these storage mechanisms provide different levels of security, availability and mobility. Most secure ones are hardware wallets because of increased digital security. A debtor can easily hide his/her digital assets by withholding hardware wallet to somewhere else. Paper, Physical, Electronic and Software wallets can be easily identified by investigating the debtor's computers or mobile devices. In term of online wallets, debt collectors or law enforcement officers should contact corporations that give online wallet services. Most of these corporations are regulated by government or non-government organisations. They should reply to any request coming from a court to reveal

identities of a wallet owner and the amount of cryptocurrencies kept in those online wallets.

D. The implications of different storage types of Bitcoin on enforcement law

First of all, we would like to emphasise that under this heading we are not aiming to elaborate on the positive and negative aspects of the type of storing private keys. Our main goal is to draw attention to the implications of these different private keys on enforcement law.

Private keys can be printed on pieces of paper, they can be learnt by heart and exist solely in an individual's head, they can be saved on servers and hard drives, and they can even be subdivided into constitutive keys (Buterin 2014).

Private keys can exist in many forms, and it is these plenty of modes that cause the jurisdictional problems. For example, it is possible for an individual to produce a private key originated from a password that he/she can keep solely in his/her head which is called 'brain wallet' (Vasek et al. 2017). He/she can transfer his/her Bitcoins by merely expressing to the transferee the password, which would then give the transferee admission to the Bitcoin wallet (Raskin 2015, 998). In order for a court to control Bitcoins to transfer them, it would be essential to have some kind of power over the owner and the knowledge he/she has in his/her head (Raskin 2015, 998). In such a case, a court could order the Bitcoin owner to unencrypt access to the Bitcoins and by this means it allows the court to have charge of them.[9] If the Bitcoin owner rejects to disclose the key, then he/she could be held in contempt of court.[10] Because a hard drive is a storage device, just like a closet, cupboard or a safe and should be subject to the same rules. According to enforcement rules, to be able to reach the available assets of a debtor with a search order one can enter the debtor's house against the owner's wishes, and may search the place, open every door, pull up the floorboards and dig up the yard if needed, to search available assets. Similarly, if a debtor can be forced to open a locked safe, then to force a debtor for revealing Bitcoin key password should also be possible. It is possible in criminal cases in US law and for the Bitcoin it should be applicable also in civil cases.

One of the other storage types of private key multisignature technology allows an individual to split a private key into constitutive parts and requires a certain number of those sub-keys to validate a transaction.[11] You can specify, for example, two of six people must sign the transaction. Multisignature wallets make the job of a plaintiff more difficult in finding a way to gather the private keys (Raskin 2015, 1001). Instead of detecting one private key, the plaintiff or the court may now have to uncover more than one private sub-keys. This has an equivalent in bankruptcy law where the assets of an estate are anywhere in the world, making the job of creditors a worldwide effort (Raskin 2015, 1002).

If an individual has the private key, then he/she can spend the Bitcoins in the associated address. This public key cryptography system is much like a safety deposit box made of glass for anyone in the world to see, but only those with the private key can open the glass box to spend those Bitcoins (Raskin 2015, 975).

Each individual Bitcoin can easily be traced back through all transactions in which it was used, and to the start of its circulation (Böhme et al. 2015, 215). All Bitcoin transactions are lucid, and records that are stored in a widely replicated data structure are readable by everyone. This point will shed light on the essence of our article. Since all Bitcoin

transactions are recorded and can be traced back is actually the evidence of the fact that the assets hidden via Bitcoin wallets can also be tracked in some way.

It is necessary to consider that the irreversibility of Bitcoin payments creates intensive transaction risk (Böhme et al. 2015, 227). If Bitcoins are transferred due to error or fraud, the Bitcoin system does not provide a procedure to nullify the mistake. Obviously, a buyer and seller can voluntarily settle to alter errors, but the Bitcoin protocol has no procedure to recover the funds compulsorily (Böhme et al. 2015, 227). Irreversibility feature of Bitcoin is also important in terms of enforcement law. Even if Bitcoin wallet was discovered, since Bitcoins in the Bitcoin wallet can be transferred in a very short period of time like 10 minutes, it will be no longer possible to reverse the transaction that is realised by the malicious debtors who have realised that their assets were uncovered. For example, even if a creditor identifies a debtor's Bitcoin wallet, there is no guarantee that the money will be there when the creditor attempts to obtain.

III. Anonymity feature of the Bitcoin and its implications on enforcement law

A. An overview of the anonymity feature of the Bitcoin

Transactions administered in Bitcoin are anonymous. It means that the anonymity of Bitcoin prevents determination of its users. Every Bitcoin transaction is recorded in a publicly available ledger known as the Blockchain. The Blockchain only records the addresses of each party involved in a transaction, not the identity of the parties holding each address (Martinson and Masterson 2014, 14). However, someone who wants to de-anonymize its users will try to build the one-to-many mapping between users and public-keys and associate information external to the system with the users (Reid and Harrigan 2012, 1).

Each Bitcoin owner can use different private and public keys in each transaction. Because there is no central source of truth that links keys to actual user and feasibility to generate different key values for each transaction, it is hard to reveal the real-life identity of the user. This is also known as anonymity feature of Bitcoin. However, computer scientists rather call it pseudonym rather than anonymity. The main reason behind this distinction is that anonymity can only be achieved by being impossible to link pseudonym identities hold by a single individual. Unless direct or indirect links between these new identities or key exist, complete anonymity cannot be achieved.

Even though, it is not easy, it is not impossible that a party's identity can be uncovered through careful research surrounding a Bitcoin purchase. Next topics will examine this issue and suggest some paths in order to uncover anonymous Bitcoin wallets and reach the hidden assets.

B. How to increase the effect of the anonymity feature?

Bitcoin transaction records display each transaction made from each payer to each payee with the public keys serving as pseudonyms of each. This means Bitcoin causes various privacy hazards, most notably the risk that transactions can be correlated to the people who made them. Bitcoin transactions are not absolutely anonymous. Instead they are pseudonymous, that each transaction designates account information (Böhme et al.

2015, 221). As a result, anyone who notices the identity of any user from any transaction-perhaps from the mailing address used for delivery of purchased goods, or the bank account used to purchase Bitcoins, or real names as funds are exchanged to or from currencies in traditional banks, or when purchases from retailers uncover a customer name-can trace that user's other transactions made with the same pseudonym, both before and since (Böhme et al. 2015, 221, 9).

Several writers (Reid and Harrigan 2012, 1–28) identify the public Bitcoin transaction record, finding a set of heuristics that can benefit to associate Bitcoin accounts with real world identities as long as some further data is available for a linked transaction. Some of these writers (Androulaki et al. 2013, 34–51) determined that nearly half of the users can be recognised by their transaction patterns.

In this direction, two methods that help to increase the anonymity of the Bitcoin are overviewed below.

1. Mixing

Mixing is a technique that a pool of Bitcoin owners lends their assets to a provider (this could be a third party trusted company or online wallet), provider either combines these individual sums of Bitcoins or keeps them as it is. When lenders withdraw their Bitcoins, providers either separate joint sum of Bitcoins or shuffles loaned Bitcoins to provide different Bitcoins than the owner had loaned. For example, Jane, Adam and Charlie have J, A, C Bitcoins respectively. One of the mixing technique sums up all these three coins into one Bitcoin asset valued (J+A+C). Whenever one of these users wants to withdraw their Bitcoin asset, mixing system returns random portion of withdrawal Bitcoin value from the combined wallet.

Another technique for mixing is to distribute Bitcoins randomly without summing up. For example, Charlie wants to withdraw 6 Bitcoins from mixing service. Service takes 2 Bitcoins from Jane, 2 Bitcoins from Adam, and 2 Bitcoins from Charlie. This method mixes initial deposits from users in a random fashion.

There are two main problems with the first implementations of mixing: (Ziegeldolf et al. 2015, 75–86) 1-Users should trust without hesitation to mixing services about theft of their assets; 2-Mixing services should show their algorithmic notion if they are enforced by regulators or governments.

In order to overcome these two issues, decentralised mixing services have been proposed. One of the popular mixing technique is called CoinParty (Ziegeldolf et al. 2015, 75–86) that proposes a more secure decentralised and scalable peer to peer protocol. CoinParty increases the degree of the anonymity to a large extent.

2. Using anonymous encrypted peer to peer networks

Nowadays, every person who has access to the Internet is using many different internet protocols. Even if these protocols provide a basic level of security, most of the data transmission is carried through without any disguise method like encryption. The lack of encryption during data transmission makes user data to be mirrored, and tracked by broadband providers. In addition to this, every individual location (either home or work) has an IP address. Broadband providers keep track of user activities, and IP assignments. This makes it simple to locate any illegal activity with the help of the broadband providers.

In order to establish a complete anonymous network connection, users can use software like TOR. TOR (the name is coming from its original project name 'The Onion Router') is a free software that connects directly to the other computers that are using the same software and transmits data through these computers via establishing encryption over the data. Because broadband providers cannot decrypt the contents of the data which is transmitted by TOR network, it is almost impossible to reveal user's location and data usage. Combination of TOR and Bitcoin together can prevent debtor to reveal his/her identity up to a certain point.

C. Some techniques to de-anonymise the Bitcoin

In this section, techniques and research on de-anonymizing Bitcoin will be discussed. Techniques that we will introduce can be applied when there is no access to any of the wallets types mentioned in the previous section.

1. Clustering Bitcoin addresses with selection of appropriate network representation

Each single Bitcoin transaction contains a link between previous owner and current owner. These links are publicly available through blocks in Blockchain. Even if these owner addresses are some sort of keys that can be generated separately for each transaction, one can draw a graph between these identities. For example, Alice is buying a coffee from a store, when she completes the transaction there is a link between Alice's public key to the store's public key. Later, John buys a tea from the same store and creates another link between John's public key to the store's public key. Collecting all these links between entities, we can build a network of transactions. Connection points between links would show real-life entities like Alice, John and the store. Reid et al. (Reid and Harrigan 2012, 1–28) proposed a method by selecting a proper topological network representation to identify and group same entities in this network. Authors inspected the ways of acquisition and expenditure of Bitcoins to identify similar entities. They used this technique to track Bitcoin flow of a well-known Bitcoin theft.

In addition to this research, Androulaki et al. (2012, 596) took similar approach with different clustering methods (K-Means and Hierarchical Agglomerate) to simulate behavioural patterns in a university setting. They claimed that measures of Bitcoin that is in place right now are not sufficient to secure Bitcoin Owners.

There are multiple uses of these approaches. By grouping transactions, expert witnesses appointed by the court can identify most commonly used transaction. If you consider the setup above, once the real-life identity of the store is revealed, any Bitcoin address that linked to this store can be tracked by financial and customer transaction histories. By using these methods, experts can match public keys with the Bitcoin addresses of Alice and John.

2. Clustering Bitcoin addresses with transaction Internet Protocol addresses

Koshy, Koshy, and McDaniel (2014, 469–485) proposed another network clustering method by leveraging the Internet Protocol (IP) addresses acquired from connected peers in network and transaction addresses provided. All transactions should be verified by Bitcoin miners that are receiving data from individuals to validate their transactions with Blockchain. This method proposes planting multiple mining software that listens to

network traffic. If two different validators receive data from same IP address, they assume that this IP address is now owned by the same user. Due to reachability of IP addresses to real-life identities or locations via broadband suppliers, this method provides a clear way to reach the Bitcoin asset owner.

3. Clustering Bitcoin addresses with shared spending and idioms of use

Meiklejohn et al. (2013, 127–140) suggest another clustering mechanism to group public keys to map with real-life identities. Their proposed work is based on two heuristics. If a person who owns N and M Bitcoins would like to buy an item valued N+M Bitcoins, he/she needs to first combine their Bitcoins in a single Bitcoin N+M, then transact with the seller to transfer N+M Bitcoins to finalise the purchase. The first heuristic is that if two Bitcoins are combined from two separate public keys, they should have same owners.

In order to increase the effect of the anonymity, it is suggested to use different addresses for each transaction. Users often apply 'one-time address change' to acquire a different address in every new transaction. Another heuristic is based on this assumption that one-time address change is accomplished by the same user most of the time.

In order to approve their methodology, authors completed 344 Bitcoin transactions from mining pools, wallets, bank exchanges, non-bank exchanges, vendors and gambling services. They were able to assign real-life entities to the clusters by matching public keys of these transactions. Authors claim that this method can be easily extendable to individuals.

4. Website analytic cookies to reveal identities

Every time a user browses a website or places an order on online shopping websites, third-party trackers receives sufficient information to identify individual purchases. By using this information, creditors can easily locate Bitcoin transaction for a debtor by cross-matching information and data on Blockchain (Goldfeder et al. 2017) If there exists a link between two transactions of the same debtor with associated Blockchain entries that exposed by web tracker, it is possible to identify user's addresses and transactions cross-matching on Blockchain. In such a case, the debtor will be still traceable even if he/she tries to increase his/her anonymity with popular techniques such as CoinJoin.

IV. Is it impossible to discover an anonymous Bitcoin wallet?

A. Finding and attaching assets

The primary goal of this article is to find an answer to the question if it is possible to discover and access hidden Bitcoin wallets, and how hidden assets via Bitcoin wallets can be reachable or uncoverable. In such a case is it possible to use procedures like pre-trial asset tracing techniques, freezing orders, or the other enforcement methods that are able to be used in searching traditional assets. The dispute relating to a debt or assets involving Bitcoin may be based on enforcement of a judgment, or the dispute may occur in the process of valuing the spouses' assets in a divorce case, and one of the parties may attempt to conceal his/her assets via Bitcoin wallet.

For instance, in civil disputes relating to assets like divorce cases, due to Bitcoin's novelty, it can remain undiscovered by the courts more easily than physical money

in a bank account. Unless a spouse explicitly alleges that Bitcoin has been owned, it is quite easy to conceal from the Court (Croft 2014; Hou 2015, 75–76). Moreover, it is very simple for spouses to quickly transfer their money through Bitcoin anonymously. For example, in matrimonial matters, each party has the right and power to carry out discovery into the economic situation of the other party, issue subpoenas and interrogatories, and conduct depositions. If large amounts of money are being transferred to a Bitcoin exchange where someone can purchase Bitcoin with fiat currency, that will exactly catch the attention (Centeno 2017). Also, if there are considerable cash withdrawals or transfers that were used to purchase Bitcoin from Bitcoin exchange companies or another peer to peer point of sale, this may potentially appear to be an attempt to hide asset via Bitcoin (Centeno 2017). On such an occasion, if it is not achievable to reveal the relationship with these cash withdrawals and the suspected spouse cannot produce evidence as what he/she is doing with that cash, then it is with a high degree of probability that unauthorised withdrawals are expending marital assets and therefore, the division of equitable distribution should be diminished accordingly (Centeno 2017).

Before advancing on cases involving Bitcoin, the problem of how to find and attach hidden assets in England and Wales will be overviewed. Besides, some useful correlations will be constituted between disputes concerning Bitcoin and traditional asset tracing cases. Consequently, we will analyse the subject in consideration of only the practice in England and Wales instead of a comprehensive examination of the pre-trial asset tracing methods and rules regulating freezing orders and enforcement methods.

During the course of lawsuits or arbitrations, defendants or respondents sometimes attempt to remove substantial assets from their domain to cover them against enforcement proceedings. Asset shielding manoeuvres can appear in many different manners. It can be straightforward transferring assets to a family member or a corporate entity, to schemes involving offshore trusts (Centeno 2017). Now we may include Bitcoin to these asset shielding manoeuvres.

It is important to note that there are a number of pre-trial procedures as well as some procedures during and after the proceeding in order to find and attach the hidden assets. We will briefly discuss all three phases below.

B. How to find and attach assets in England and Wales and some correlations with Bitcoin

A party trying to enforce in England and Wales should, if he/she does not already have the necessary information about the financial situation of the counterparty, seek to determine whether there exist any or adequate assets in this jurisdiction to compensate the judgment or award debt (Byrne and Farris 2016, 110). The enforcing party can apply to the court to get information from the defendant or third parties (Byrne and Farris 2016, 110).

A creditor who cannot convince (generally by debt collection agencies) the debtor to pay may take court action to receive judgment for the debt. Only a limited number of civil claims for debt are defended, and in most of the cases, the creditor obtains judgment by default (Tolmie 2003). Over half of all default judgments do not outcome in payment to

the creditor (Tolmie 2003). If the debtor still does not pay, then creditors who have obtained a judgment against a debtor will need to pursue to enforce the judgment.

The debtor may be summoned to court for an oral examination in order to provide the creditor to inquire into the debtor's economic situation and determine the most adequate and efficient procedure for enforcing the judgment.[12] In oral examination process, a standard list of questions will be inquired[13], but also the creditor can ask further questions. A debtor who deliberately decline to co-operate with the process risks imprisonment for contempt (Tolmie 2003).

Once the judgment has been rendered, an order can be obtained[14] requiring a judgment debtor to appear before court to produce information about his/her wealth or any other information necessary for the objective of enabling a judgment creditor to enforce a judgment (Byrne and Farris 2016, 113). This order also contains a penal notice, warning that failure to comply with the order may be contempt of court, causing to imprisonment, a fine or seizure of assets.[15]

In our opinion, the procedure mentioned above can also be applied to the cases involving Bitcoin. The enforcing party may appeal to the court to request information from the defendant or third parties about the defendant's means, particularly information about defendant's probable Bitcoin wallet. We suggest particularly to creditors and their counsel to add diligence questions specifically regarding Bitcoin assets. For example, a creditor or the court can directly ask whether a debtor maintains a Bitcoin wallet, holds any Bitcoin assets, or conducts business using Bitcoin. By this way, it will be guaranteed that such assets are not overlooked (Martinson and Masterson 2014, 17). If the defendant does not give the court right and honest information, then it should be accepted as contempt of court. The third parties that the court may apply to are the Bitcoin exchange companies. The court should be able to request information from the exchange companies in the jurisdiction by giving defendant's concrete details on the case without an attempt to procure any fishing expedition.

In England and Wales, a popular tactic when determining the assets of a judgment debtor is the use of 'enquiry agents' to investigate and prepare a report on the assets of the company or individual in dispute (Byrne and Farris 2016, 111–112). Such reports should be produced in a form that can depend on by the enforcing party in Court as an affidavit (Byrne and Farris 2016, 111–112).

The enforcing party who suspects that the judgment debtor has been hiding his/her assets via Bitcoin wallet should able to apply to an enquiry agent to ask a research on judgment debtor's means. A report prepared by the enquiry agent can be presented to the court as an affidavit however, it poses a great risk that the judgment debtor's Bitcoin can be transferred immediately so that the report may remain useless. Nevertheless, if a Bitcoin wallet which was provided to hide the debtor's assets was discovered at the time investigation conducted, the judgment debtor should be punished within the scope of contempt of court.

The Court has the competence to order for disclosure against a person not a party to the proceeding at the pre-action stage. By this way, court orders a potential party to disclose documents for subsequent proceedings. These documents must be documents as to which there would probably be a disclosure order once proceedings have been begun. As long as they either support or adversely affect the other parties to the proceedings, and disclosure is decisive in order to present the claim equitably or to save costs.[16]

If the court orders a disclosure to a prospective party in the pre-trial phase, this prospective party who owns Bitcoin assets should have to present the information about these assets that effect the case. The legal status or classification of the Bitcoin should not be a matter in a proceeding. Bitcoin has an economic value at its core, and if this is not presented to the court under disclosure rules, then this act should be considered equal to hiding assets from the court. If it is discovered later that the party did not present relevant Bitcoin assets, it should be accepted as contempt of court.

It is also possible that the Court can order a non-party for disclosure.[17] At the pre-action phase, a party may collect documents and information from a third party under the procedure known as 'Norwich Pharmacal'[18] jurisdiction. This procedure is generally applied to facilitate in determining an actual wrongdoer, a cause of action or the location of assets (Brun et al. 2014, 72). This procedure can be used at any stage of the proceedings. However, it is unclear whether the Court would make such an order in support of enforcement proceedings and whether this would be an effective tool in enforcement proceedings (Byrne and Farris 2016, 111).

In asset tracing cases concerning the Bitcoin, it should be possible to obtain information that helps to find the location of the hidden assets from the third parties in the pre-trial phase and during the litigation under disclosure rules. This third party may be the Bitcoin exchange company, as well as any person who knows the location of the Bitcoin (or more precisely the location of the key) such as the spouse of the Bitcoin owner or business partner.

Another type of order that can be applied in order to find assets is 'Bankers Trust order'.[19] With this order, a bank should provide details ordinarily protected by the bank's confidentiality (Brun et al. 2014, 72; Byrne and Farris 2016, 111). Thanks to this order the claimant has the right to trace assets which, without such disclosure, would have been impossible (Byrne and Farris 2016, 111).

Bankers trust order can play an important role in finding the Bitcoin wallet. For example, a debtor may hide the existence of his/her Bitcoin wallet. If this debtor stores his/her asset in the Bitcoin exchange company (usually these specialised Bitcoin companies are preferred to do secure transaction and investment) then bankers trust would be reasonable to order. Because in order to open a Bitcoin wallet in an exchange company, it is required to transfer money from a traditional bank account to the exchange company. It is possible to buy Bitcoins in the UK using a credit card, debit card or bank transfer. So, with the bankers trust order, hidden assets via Bitcoin wallet can be accessible if the debtor stores his/her assets in an exchange company. In order to do that, one should apply to the debtor's bank and request debtor's credit card history, bank account or eft information and then by establishing a connection with these transactions, one can find the exchange company. However, if the debtor does not store his/her Bitcoins in an exchange company, then this Bankers trust order seems to be unnecessary. Nevertheless, even the probability that the debtor stores his/her asset in an exchange company it worths applying for this order. We believe that in order to apply to this order, a reasonable suspicion about the existence of a bitcoin wallet should exist.

The English Court has also significant powers to assist an enforcing party to determine and protect the assets of a judgment debtor at the interim stage by interim measures (Byrne and Farris 2016, 113). These powers can be appealed to at any stage of proceedings, including post-judgment.

The interim measures can be utilised also in arbitration proceedings according to section 44 of the Arbitration Act 1996. By this way, court powers are exercisable in support of arbitral proceedings. Unless otherwise agreed by the parties, the court has the same power of making orders about the matters as it has for the purposes of and in relation to legal proceedings.[20] The court may also grant an interim injunction such as freezing injunction in support of arbitral proceedings, and the injunction may be particularly useful if suspicions arise that one party is seeking to transfer its assets out of the sphere of the party, whether before, during or after arbitration (Byrne and Farris 2016, 114).

Accordingly, in arbitration proceedings, the court may order interim injunction as it does in litigation. It would therefore be appropriate for a court to order interim injunction in an arbitration case involving Bitcoin in the same way.

One of the most notable interim measures is a freezing order which is formerly known as Mareva Injunction.[21] The function of a freezing order is to prevent a defendant from expending or trading with its assets up to the value specified because assets up to a certain value should be preserved until a judgment or award can be enforced (Byrne and Farris 2016, 114). A freezing order obligates any third party who has notice of it. In particular, this means that traditional banks which store assets of a defendant must assure that the terms of a freezing order are adhered to (Byrne and Farris 2016, 115). This is an important feature of a freezing order because it means that a defendant is unable to dissipate its assets even it was attempted to (Byrne and Farris 2016, 115). An additional feature of a freezing order is a requiring the defendant to disclose its assets within a certain period (Byrne and Farris 2016, 115). So it is crucial to realise the disclosure process in a short time. A defendant must give the value, location and details' of all its assets above a certain specified value to the applicant's solicitors by a certain date (Byrne and Farris 2016, 115). The necessity to provide this information is often as valuable as the freezing of assets and the freezing order policed effectively (Byrne and Farris 2016, 115).

In asset tracing cases involving Bitcoin, the freezing order can be directed against the virtual exchange company since it is not possible to store Bitcoin in a traditional bank. However, firstly it is necessary to investigate that the debtor's hidden Bitcoin wallet is in which exchange company. If as a first step, the payments made from the debtor's traditional bank account to the virtual exchange company is displayed, then it will be possible to identify the exchange company. Afterwards, a freezing order can be issued to the relevant exchange company. Freezing order, which is an order that must be realised very quickly, may remain dysfunctional despite the quick transferrable feature of Bitcoin.

Another type of interim relief which may be utilised to determine assets is a 'search order' which is formerly known as 'Anton Piller order'.[22] This order lets a claimant's representative to enter a defendant's premises without notice and research, copy and seize documents or material mentioned in the search order. This type of interim relief can be authorised against a disobedient defendant who declines to disclose the place and amount of its assets compatible with earlier orders.

Through the search order, the claimant's representative can try to search for any sign or evidence of the existence of any Bitcoin wallet such as a paper private key. In fact, this can be thought of as trying to find the key of the debtor's safe to be able to open it. As a result

of this search, private keys stored on a piece of paper, in a computer disk or server can be found. Or these potential tools can be copied or seized and can be investigated by computer scientists as experts appointed by the court. Thus, it may be possible to access the Bitcoin wallet. However, to provide a quick process is very crucial in asset tracing cases particularly involving Bitcoin. If there are other copies of private keys, then these persons may dissipate or transfer the Bitcoin wallet before the court access it.

V. Conclusion

Both the anonymity and decentralisation features that are being widely admired in Bitcoin practice are the most significant issues at the same time. As a result of Bitcoin's this structure, discovering and obtaining the Bitcoin assets in an enforcement scenario is at best difficult. On the basis of this paper, we underlined that Bitcoin is not as much anonymous as it is claimed. We cannot come to a conclusion that it is quite obvious to access the owners of the Bitcoin with a pseudonym and attach the Bitcoin assets they attempted to conceal. Unlike what people might think it is not impossible either. If a creditor in a debt action, or a spouse in an asset related case, in which one of the party is suspicious about the other party's possession of a Bitcoin wallet, this suspicious party should absolutely try to find and identify this Bitcoin wallet.

In the light of our suggestions for weakening the anonymity of the Bitcoin, technical people such as computer scientists should be assigned as experts by the court in this matter. Although appointment of experts would require qualified personnel and may be costly, assuming Bitcoin wallets inaccessible in anyway and letting the abuse of process implicitly, may lead to very unfair consequences for one of the party and for a fair litigation.

Because of the fact that Bitcoin is not legally recognised and not regulated, also is decentralised, significant concerns on various law fields particularly on enforcement law cause the alarm bells start to ring. Even though, we do not recommend using Bitcoin because of risks it carries, we believe that it should be regulated as soon as possible to reduce these risks. If we accept the technology that Bitcoin and the other cryptocurrencies create, even we want it willingly or not, we need to update our legislation faster compatible with the changes this technology brings. In conclusion, we consider that without waiting for the legal regulations in reference to Bitcoin, the interim injunctions that is ordered in traditional asset tracing disputes should also be used in disputes concerning Bitcoin.

Notes

1. They are all based on the Bitcoin with some distinctions, Tara Mandjee, Bitcoin, Its Legal Classification and Its Regulatory Framework, 15 J. Bus.& SEC. L. 157 (2016), p. 162.
2. Mandjee, *supra* note 4, p. 160; Mining Digital Gold, *Economist* (April 13, 2013), https://www.economist.com/news/finance-and-economics/21576149-even-if-it-crashes-bitcoin-may-make-dent-financial-world-mining-digital.
3. Mining Digital Gold, *Economist* (April 13, 2013), https://www.economist.com/news/finance-and-economics/21576149-even-if-it-crashes-bitcoin-may-make-dent-financial-world-mining-digital.
4. A&M Records v. Napster, Inc., 239 F 3d. 1004, 1010-12 (9th Cir. 2001).

5. Id.; For a comprehensive examination of the effects of Napster, Inc's working procedure, see GartnerG2 and The Berkman Center for Internet & Society at Harvard Law School, Copyright and Digital Media in a Post-Napster World, https://cyber.harvard.edu/wg_home/uploads/254/2003-05.pdf.
6. A&M Records v. Napster, Inc., 239 F. 3d 1004, 1010, 1011, 1027 (9th Cir. 2001).
7. Id., p. 1004, just as the FBI did by seizing the Silk Road Bitcoins, United States v. Ulbricht, 31 F. Supp. 3d 540 (S.D.N.Y. 2014).
8. Blockchain Size, https://blockchain.info/charts/blocks-size.
9. In re Boucher (No. 2:06-mJ-91, 2009 WL 424718), is a federal criminal case in Vermont, which was the first to directly address the question of whether investigators can 'compel a suspect to reveal their encryption passphrase or password', despite the U.S. Constitution's Fifth Amendment protection against self-incrimination. A magistrate judge held that producing the passphrase would constitute self-incrimination. Boucher's motion to quash the subpoena was denied. He was ordered to provide an unencrypted version of the hard drive in question. Some more examples that the court compels individuals to unencrypt hard-drive: United States v. Fricosu, 841 F. Supp. 2d 1232, 1236 (D. Colo. 2012) or divulging the password: United States v. Kirschner, 823 F. Supp. 2d 665, 669 (E.D. Mich 2010).
10. FED. R. CIV. P: 45(g).
11. For more information about multisignature technology see Gregory Maxwell/ Andrew Poelstra/ Yannick Seurin/ Pieter Wuille, Simple Schnorr Multi-Signatures with Applications to Bitcoin, (January 15, 2018), https://eprint.iacr.org/2018/068.pdf.
12. CPR Part 71.
13. For individuals: Form EX140, https://formfinder.hmctsformfinder.justice.gov.uk/ex140-eng.pdf and for officer of company or corporation https://formfinder.hmctsformfinder.justice.gov.uk/ex141-eng.pdf.
14. CPR Rule 71.
15. CPR Rule 71.2(7).
16. CPR 31.16 and 31.17 (3) a-b.
17. CPR 31.17.
18. Norwich Pharmacal Co. Customs and Excise Commissioners, [1974] A.C. 130 (H.L).
19. Bankers Trust Co v. Shapira [1980] 1 WLR 1274 CA.
20. Arbitration Act 1966, Section 44(1).
21. See Mareva Compenia Naviera SA v. International Bulk Carriers SA [1975] 2 Lloyds Rep 509.
22. Anton Piller KG v Manufacturing Processes [1976] Ch 55, CA.

Disclosure statement

No potential conflict of interest was reported by the authors.

References

Acheson, Noelle. 2018. "How to Store Your Bitcoin." https://www.coindesk.com/information/how-to-store-your-bitcoins/.

Andreessen, Mark. 2014. "Why Bitcoin Matters." *New York Times*. https://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/.

Androulaki, E., G. Karame, M. Roeschlin, T. Scherer, and S. Capkun. 2012. "Evaluating User Privacy in Bitcoin." In 596. IACR Cryptology ePrint Archive.

Androulaki, Elli, Ghassan O. Karame, Marc Roeschlin, Tobias Scherer, and Srdjan Capkun. 2013. "Evaluating User Privacy in Bitcoin." In *Financial Cryptography and Data Security*, 34–51. Berlin: Springer.

Böhme, R., N. Cristin, B. Edelman, and T. Moore. 2015. "Bitcoin: Economics, Technology, and Governance." Review of *Journal of Economic Perspectives* 29 (3):213–238.

Brun, Jean-Pierre, Pascale Helene Dubois, Emile van der Does de Willebois, Jeanne Hauch, Sarah Jais, Yannis Mekki, Anastasia Sotiropoulou, and Katherine Rose Sylvester. 2014. *Public Wrongs, Private Actions: Civil Lawsuits to Recover Stolen Assets*. Washington, DC: The World Bank.

Buterin, Vitalik. 2014. "Bitcoin Multisig Wallet: The Future of Bitcoin." *Bitcoin Magazine*. https://bitcoinmagazine.com/articles/multisig-future-bitcoin-1394686504/.

Byrne, Ruth M. D., and Henry Farris. 2016. "Chapter 9: England and Wales." In *Finding, Freezing and Attaching Assets: A Multi-Jurisdictional Handbook*, edited by Jacob C. Jörgensen, 110–115. Alphen aan den Rijn: Kluwer Law International B.V.

Camp, Mat. "Bitcoins: The Latest Innovation for Hiding Assets in Divorce." https://mensdivorce.com/bitcoins-hiding-assets-divorce/.

Centeno, David. 2017. "Hiding Assets with Bitcoin in Divorce." *Huffpost*. https://www.huffingtonpost.com/entry/hiding-assets-with-bitcoin-in-divorce_us_58ae640ce4b0ea6ee3d035ca.

Cook, R. Joseph. 2014. "Bitcoins: Technological Innovation or Emerging Threat?" Review of *The John Marshall Journal of Information Technology & Privacy Law* 30 (3): 535–570.

Croft, Jane. 2014. "Bitcoin Could Be Used to Hide Assets in Divorces." *Financial Times*.

Dion, Derek A. 2013. "I'll Gladly Trade You Two Bits on Tuesday for a Byte Today: Bitcoin, Regulating Fraud in the E-Conomy of Hacker-Cash." Review of *University of Illinois Journal of Law, Technology & Policy* 2013: 167.

Goldfeder, S., H. Kalodner, D. Reisman, and A. Narayanan. 2017. "When the Cookie Meets the Blockchain: Privacy Risks of Web Payments via Cryptocurrencies." https://arxiv.org/abs/1708.04748.

Hou, Caline. 2015. "A Bit-ter Divorce: Using Bitcoin to Hide Marital Assets." Review of *North Carolina Journal of Law & Technology* 16: 75–76.

Koshy, P., D. Koshy, and P. McDaniel. 2014. "International Conference on Financial Cryptography and Data Security." In *Financial Cryptography and Data Security*, 469–485. Berlin: Springer.

Krohn-Grimberghe, Artus, and Christoph Sorge. 2013. "Practical Aspects of the Bitcoin System." https://arxiv.org/pdf/1308.6760.pdf.

Mandjee, Tara. 2016. "Bitcoin, Its Legal Classification and Its Regulatory Framework." Review of *Journal of Business & Securities Law* 15 (2): 157–218.

Martinson, Pamela J., and Christopher P. Masterson. 2014. "Bitcoin and the Secured Lender." *Banking & Financial Services Policy Report*, 14, 17, 18.

Meiklejohn, S., M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage. 2013. "A Fistful of Bitcoins: Characterizing Payments among Men with No Names." In *Internet Measurement Conference*, 127–140. Barcelona: ACM.

Nakamoto, Satoshi. 2009. "Bitcoin: A Peer-to-Peer Electronic Cash System." Bitcoin Project. Accessed January. https://bitcoin.org/bitcoin.pdf.

Raskin, Max I. 2015. "Realm of the Coin: Bitcoin and Civil Procedure." Review of *Fordham Journal of Corporate & Financial Law* 20: 969–1011.

Reid, Fergal, and Martin Harrigan. 2012. "An Analysis of Anonymity in the Bitcoin System." https://arxiv.org/pdf/1107.4524.pdf.

Tolmie, Fiona. 2003. *Corporate and Personal Insolvency Law*. London: Cavendish Publishing.

Vasek, Marie, Joseph Bonneau, Ryan Castellucci, Cameron Keith, and Tyler Moore. 2017. "The Bitcoin Brain Drain: Examining the Use and Abuse of Bitcoin Brain Wallets." In *International Conference on Financial Cryptography and Data Security*. Berlin: Springer.

Ziegeldolf, J. H., F. Grossmann, M. Henze, N. Inden, and K. Wehrle. 2015. "CoinParty: Secure Multi-Party Mixing of Bitcoins." Paper presented at the Proceedings of the 5th ACM Conference on Data and Application Security and Privacy. New York: ACM