laws

MDPI

Article

When Criminals Abuse the Blockchain: Establishing Personal Jurisdiction in a Decentralised Environment

Casey Watters

Faculty of Law, Bond University, Gold Coast 4226, Australia; cwatters@bond.edu.au

Abstract: In August of 2022, the United States Department of Treasury sanctioned the virtual currency mixer Tornado Cash, an open-source and fully decentralised piece of software running on the Ethereum blockchain, subsequently leading to the arrest of one of its developers in the Netherlands. Not only was this the first time the Office of Foreign Assets Control (OFAC) extended its authority to sanction a foreign 'person' to software, but the decentralised nature of the software and global usage highlight the challenge of establishing jurisdiction over decentralised software and its global user base. The government claims jurisdiction over citizens, residents, and any assets that pass through the country's territory. As a global financial center with most large tech companies, this often facilitates the establishment of jurisdiction over global conduct that passes through US servers. However, decentralised programs on blockchains with nodes located around the world challenge this traditional approach as either nearly all countries can claim jurisdiction over users, subjecting users to criminal laws in countries with which they have no true interaction, or they limit jurisdiction, thereby risking abuse by bad actors. This article takes a comparative approach to examine the challenges to establishing criminal jurisdiction on cryptocurrency-related crimes.

Keywords: cryptocurrency; extra-territorial jurisdiction; universal jurisdiction; Bitcoin; crime; fraud; ICO; individual rights; human rights; criminal law

check for updates

Citation: Watters, Casey. 2023. When Criminals Abuse the Blockchain: Establishing Personal Jurisdiction in a Decentralised Environment. *Laws* 12: 33. https://doi.org/10.3390/laws12020033

Academic Editors: Mohamed Arafa and Patricia Easteal

Received: 28 February 2023
Revised: 9 April 2023
Accepted: 10 April 2023
Published: 15 April 2023

1. Introduction

Cryptocurrency has exploded in popularity in recent years, with Bitcoin adopted as a national currency in two countries. The blockchain technology on which cryptocurrency is built is an important tool used not only to facilitate a medium of exchange but also in many industries, including healthcare and education. As with all technologies, blockchain is a tool and can be abused by malicious actors. However, the decentralised nature of the technology creates an obstacle to establishing jurisdiction in transnational crimes.

For Bitcoin and most cryptocurrencies, the association with cybercrime and fraud is not due to a lack of transparency but rather the ease of use in international transactions, something that increases the complexity of establishing jurisdiction. While Bitcoin and many cryptocurrencies are on public ledgers, transferring money between banks and across borders creates barriers to identifying the criminals, as it takes time for law enforcement to obtain information from each bank, which may require time-consuming processes in each country, and banks may even be owned by criminal actors (Levi 2002). If banks in any jurisdiction stop cooperating, the trail is lost (Hedayati 2012). In order to truly remain anonymous, cybercriminals could use stolen identities to transfer funds and eventually withdraw the cash, making them nearly untraceable. However, selecting a specific currency is inefficient for those engaging in cybercrime. Human time is valuable while running code is low cost. As such, cybercriminals play a numbers game allowing code to attack any computer with identified vulnerabilities or assume the identities of anyone whose information has become available, often through phishing attacks (Ghazi-Tehrani and Pontell 2021). Insisting on bank transfers in dollars would make sense in the US; however, if the victim's computer is located in Poland or China, a request to transfer dollars to a US bank account may pose a greater challenge and prevent the criminals from receiving some of the funds. As cryptocurrency is jurisdiction-non-specific, cybercriminals can establish a single demand message for a virus that can harm systems globally. Due to the global nature of cryptocurrency, which uses a distributed ledger system, the appropriate jurisdiction for those involved in crypto-related crime is not always clear.

This article explores the difficulties in ensuring that states can protect their citizens by prosecuting bad actors while simultaneously protecting individual rights and upholding the rule of law by following clear legal standards to establish jurisdiction. In doing so, it expands on the literature addressing jurisdiction over internet crimes by extending the discussion to those crimes involving decentralised blockchains. After addressing the methodology in Section 2, this article first provides a background section (Section 3) that explains how blockchain technology, and Bitcoin in particular, operates. The section addresses the role of nodes, types of consensus mechanisms, and how individuals interact with the blockchain. With this foundation, Section 4 introduces the types of crimes involving crypto assets with short case studies, including ICO scams, the FTX fraud, the Mt Gox hack, and allegations of money laundering with Tornado Cash. Through the lens of these types of crimes, Section 5 then addresses the approaches to establishing extra-territorial jurisdiction and argues that to protect the rights of individuals and rule of law, non-territorial jurisdiction should only be extended in cases where the criminal act necessarily causes direct harm. This article then concludes in Section 6.

2. Methodology and Limitations

This research is primarily doctrinal (Pradeep 2019) in nature, using comparative (Farrar 2001) and normative analysis (Indriati and Nugroho 2022; Schauer 2021) to evaluate the current state of criminal personal jurisdiction regarding crimes involving the use of cryptocurrencies and addressing challenges posed by the existing legal landscape. To this end, this article seeks to answer the question of when jurisdictions can exercise personal jurisdiction over criminal defendants for alleged crimes involving decentralised digital assets (cryptocurrencies). This paper also addresses when countries should not exercise jurisdiction. Several small case studies are used to critically examine the impact and weaknesses of existing legal frameworks. As an emerging technology, there is limited literature addressing criminal jurisdiction and cryptocurrency (Lukings and Habibi Lashkari 2022). However, there is a large body of literature addressing civil jurisdiction (Yang 2022; Co 2021; Pecharsky and Yahya 2022) and the scope of regulatory authority (Caudevilla 2022), including whether digital assets are securities (Gonzalez 2022; Colesanti 2022). These were reviewed in addition to the literature on internet and cybercrime jurisdiction as they have important implications for cryptocurrencies. The relevant literature is addressed in its respective sections.

This article is limited to criminal jurisdiction and focuses on the use of cryptocurrency as a medium of exchange. It does not address civil jurisdiction or crimes that are specific of web3 (Wu et al. 2023), the use of governance tokens, or the possibility of criminal liability for decentralised autonomous organisations (DAOs) as legal persons (Kotlán et al. 2023), an important area for future study now that some jurisdictions are permitting the incorporation of DAOs (Moore 2021; Mondoh et al. 2022; Gurkov 2022). This article also does not address the use of governance structures or on-chain dispute resolution to resolve issues (Guillaume and Riva 2022).

3. Background: Cryptocurrency and Blockchain Technology

Bitcoin and other cryptocurrencies are a form of distributed ledger that uses blockchain to record transactions (Soltani et al. 2022; Pinto et al. 2022; Gorbunova et al. 2022). As a record of assets, ledgers are ordinarily kept by one centralised person or entity, requiring trust in that entity. For example, when someone opens a bank account, the bank does not store physical money for the customer but rather maintains a ledger tracking how much money to which the customer is entitled. As a highly regulated sector, people trust that banks will maintain accurate ledgers instead of changing the amount in customer accounts (Cardona 2022). With cryptocurrencies, the ledger is stored across multiple nodes around the world and the blockchain functions to prevent improper changes to the record. The greater number of nodes and the greater the decentralisation, the more secure a cryptocurrency is. Startup projects may be susceptible to attack. However, Bitcoin has never been successfully hacked and, with around 15,000 full nodes, (Bailey and Warmke 2023) is a permissionless and trustless network. It is said to be permissionless in that anyone who holds Bitcoin can transfer it and create new wallets (like accounts) without the need for a bank or any other intermediary, and trustless in that the code is open source and the ledger is distributed so no one can make unauthorised changes to the ledger (Arote and Kuri 2022).

A new Bitcoin block is created approximately every 10 min, and the chain goes back to 2009, when Bitcoin was first created in response to irresponsible banking behavior causing the 2008 financial crisis (Aboura 2022). At the time of writing this article, there are 777,949 blocks on the Bitcoin blockchain (Blockchain.com 2023). Although Bitcoin is good for international transfers, it is not ideal for most retail purchases due to the 10 min delay. As such, a second layer has been added, known as the lightning network (Divakaruni and Zimmerman 2023; Liu and Au 2022; van Dam and Kadir 2022). The lightning network facilitates nearly instant Bitcoin transactions at a fraction of a cent (Dylan LeClair 2022). In El Salvador, where Bitcoin was adopted as an official currency (Taylor 2022), the lightning network was used by the government to transfer Bitcoin to its citizens.

Bitcoin uses a distributed consensus mechanism commonly referred to as "mining" to confirm transactions and update the blockchain. Encrypted numbers with 64 digits act as digital fingerprints, called hashes, which are used to secure the system (Allenotor and Oyemade 2021). Miners use the hash from the previous block and try to calculate the next hash. This connection of the hashes is what creates the chain between blocks, preventing someone from altering the ledger (Wezza et al. 2022). Proof of work, where miners use large amounts of computing power to secure the blockchain, is a useful tool for securing the blockchain and has been proposed for other things, including preventing denial of service attacks on email servers (Soria Ruiz-Ogarrio 2022). However, it has been criticised for its high degree of energy consumption (Wendl et al. 2023), largely within the context of ESG (Rudd 2023). As such, many other projects have opted for a consensus mechanism called proof of stake. In proof of stake, holders of a cryptocurrency can "stake" their currency to give a validator the authority to confirm transactions (Ibañez and Rua 2023). The theory is that those who own the currency have a stake in ensuring the security and accuracy of the system. In some cryptocurrencies, the stakers will lose their staked currency if the validator where they stake misbehaves.

In order to transact on the blockchain, users have two items, a public key and a private key (Liu et al. 2017). The public key is like an email address on the blockchain, and others can use it to send cryptocurrency to that address. The private key is like a password and allows the user to send from any address to which they have the private key. Therefore, only the person with a private key can move funds on the blockchain. This both ensures the security of the blockchain and means that if a user loses their private key, they lose access to their cryptocurrency. To simplify the process, digital wallets are used to store the private key and streamline transactions (Suratkar et al. 2020). These wallets are said to "hold" the cryptocurrency, but they only display the user's account balance (which is public on the blockchain) and hold the private key. All cryptocurrency is on the decentralized blockchain, not on the wallet or any one device.

Aside from assets like Bitcoin that are meant as a permissionless and decentralised medium of exchange, digital assets can be divided into multiple asset classes, including:

1. Stable coins, which are pegged to the value of a specific asset, often the US dollar (Ante et al. 2023);

2. Governance tokens, which allow the holder to vote on decisions for a decentralised project (Fan et al. 2022; Makridis et al. 2023); and

3. Smart contract-capable digital assets, an important part of web3, can be used for a variety of purposes including securing patient records in healthcare (Aloini et al. 2023; Ghosh et al. 2023; Kaur et al. 2023; Wenhua et al. 2023) and increasing efficiency in the energy sector (Mololoth et al. 2023; Zanghi et al. 2023; Khezami et al. 2022).

While these are important, this article focuses on the use of these digital assets as a currency.

Despite the many benefits of the technology, cryptocurrency has been criticised for energy usage[1] (Truby 2018; Rudd 2023) and the perceived risk of money laundering (Mahalaxmi and Srinivas 2022; Sun et al. 2022; Anthony 2022b; Hossain 2023), fraud (Scharfman 2023b; Sanz-Bas et al. 2021), tax evasion (Mezquita et al. 2023; Noked 2018), and use in the drug trade (Mezquita et al. 2023).[2] Some jurisdictions banned or heavily regulated cryptocurrencies while others have sought to embrace digital assets as a source of innovation (Novak 2020). At the time of writing this article, El Salvador (Alvarez et al. 2022; Analytica 2021; Kshetri 2022b; Sparkes 2022) and the Central African Republic (Katterbauer et al. 2022; Kshetri 2022a; Neti 2022) have even adopted Bitcoin as legal tender within the countries.

Decentralised digital assets lack a clear regulatory framework in most countries. To address this and in response to Executive Order 14067, the US Department of Justice (DOJ) issued a report on crimes related to digital assets (DOJ 2022). In this report, the DOJ expresses concerns over the use of cryptocurrency in crimes including sanctions evasions. The report calls for greater cooperation, both internationally and between government departments, and discusses the current state of the law, which lacks a comprehensive regulatory framework specific to decentralised digital assets, but where enforcement actions have nevertheless been taken. In spite of the fact that the US does not recognise cryptocurrency as legal tender, 18 U.S.C. § 1960, which prohibits "unlicensed money transmitting businesses" has been held to apply to cryptocurrency transmitting businesses.

On the regulatory front, the Financial Action Task Force (FATF), a 39-member body that establishes standards aimed at preventing money laundering, identifying funds related to the illicit drug trade, and terrorist financing, issued its recommendations on regulating digital assets (FATF 2021; de Koker et al. 2022). The FATF adopts the terms "virtual assets" (VAs) and "virtual asset service providers" (VASPs) in their recommendations. As a developing technology, whether something is considered a VASP under the recommendations may not always be clear. The focus of the recommendations is information collection and monitoring, with mandatory disclosure requirements, such as the 'travel rule' and information sharing central to these recommendations. Although the recommendations are not law, FATF recommendations set global standards that usually lead to broad adoption.

4. Crimes Involving Digital Assets

Many of the laws surrounding cryptocurrency are vague and require clarification (Náñez Alonso 2019). Cryptocurrency, like any other tool, can be used for positive or nefarious purposes. Most crimes where cryptocurrency is used involve fraud or theft, in the form of crypto wallets being hacked. In the early days of Bitcoin, it was associated with criminal activity, largely due to its use in the Silk Road, a dark web marketplace that facilitated trade in drugs and other illicit material. At the time, Bitcoin lacked wide-spread adoption and it was believed that it provided anonymity to users (Christin 2013; Phelps and Watt 2014). While cryptocurrency, as with any currency, can be used in transactions for illicit goods or money laundering, most of the crimes involving cryptocurrency today are fraud or hacks, often where a victim's lack of knowledge of the industry is exploited by criminals to steal cryptocurrency (Nickerson 2019). This section will provide four examples

[1] Attacks based on energy usage are common in business and law literature, while the use of blockchain to improve energy usage has been an important theme in the engineering field. See (Khezami et al. 2022; Hallinan et al. 2023; Liang et al. 2022).

[2] It should be noted that the blockchain is also a powerful tool in the fight against counterfeit drugs in the medical industry (Kordestani et al. 2023).

of crimes or alleged criminal activity involving cryptocurrency, including the jurisdictional challenges.

4.1. ICO Frauds

When companies need to raise funds, they can issue stock. Crypto projects selling tokens to raise money is known as initial coin offerings (ICO) (Tao et al. 2023). Not all projects have an ICO, but they are common for projects that will require a substantial amount of development over time. This makes the projects centralised in their reliance on the development team and in that a small group initially holds all the coins. Centralised projects are more likely to be considered securities and thus fall under the jurisdiction of securities regulators like the US Securities and Exchange Commission. Not all cryptocurrencies have used an ICO. For example, Bitcoin did not have an ICO and therefore began in a substantially decentralised manner.

Investors in coins being offered through ICOs pay a premium based on the belief that those offering the coins will continue to develop the project. Many fraudulent actors have taken advantage of this trust through what the industry terms a "rug pull" (Kerr et al. 2023; Wronka 2023). In this type of fraud, a group creates a basic crypto token and publishes a document known as a white paper that details the long-term development plans for the project based on that token. Once the money is received, the scammers cease development and move on with the money (Scharfman 2023a; Alshater et al. 2023; Cong et al. 2023). These scams were extremely common in 2017 when the cryptocurrency market capitalisation surged to what, at the time, were all-time highs. Fraudulent ICOs both harm investors and undercut legitimate projects' ability to raise capital.

In the case of OneCoin, the founders advertised and sold packages to assist investors in mining OneCoin tokens—a fake cryptocurrency that was never actually created (Scharfman 2023c). This resulted in victims being defrauded of over USD 4 billion, the conviction of an affiliated attorney for conspiracy to commit money laundering and bank fraud (DOJ 2019), and the indictment of OneCoin's Bulgarian founder, Ruja Ignatova, in the United States for conspiracy and securities fraud charges (United States v Ruja Ignatova 2018). This indictment, from the Southern District of New York, connects Ms. Ignatova to the jurisdictions by stating that she and her employees "caused to be made false statements and misrepresentations soliciting individuals throughout the world, including the Southern District of New York, to invest in 'OneCoin'". Whether prosecutors can assert jurisdiction over global activities or only those that specifically and intentionally targeted people in the United States remains to be seen as Ms. Ignatova disappeared with much of the stolen money in 2017, earning her a spot on the FBI's most wanted list. However, advertisements and something likened to rallies where potential investors were motivated to invest took place around the world, and the founders of OneCoin were physically present and proactively advertised in many jurisdictions, suggesting that the founders submitted to the personal jurisdiction in those locations.

4.2. FTX Fraud

The FTX fraud is not an example of a problem with cryptocurrency but with criminal activity at a centralised exchange (Chohan 2023; Kerr et al. 2023). The collapse of FTX caused users to lose billions of dollars, but anyone who had removed their assets to a private wallet was largely unaffected. Rather than hold the assets of customers on their behalf like a storage company, customers of banks are creditors, and banks are not required to keep enough money to pay all accounts on demand. Most crypto exchanges work the same way, but unlike banks, exchanges are not government-insured. If a customer transfers money onto an exchange and purchases a Bitcoin, the account may state that the customer holds a Bitcoin. However, the exchange may not have purchased sufficient Bitcoin to provide all their customers. It is only once the customer transfers the Bitcoin off the exchange into their own non-custodial wallet that the Bitcoin is truly theirs. In the case of FTX, the exchange loaned substantial amounts of customer funds to an affiliated investment firm named Alameda Research. When the value of one of the assets FTX held dropped substantially, the exchange became insolvent and did not have sufficient funds to purchase the crypto owed to customers. The FTX fraud, namely taking customer funds and transferring them to a related company to make risky investments, is a crime involving cryptocurrency but is the failure of a centralised exchange.

Aside from the leadership of FTX and Alameda Research being US citizens, being regulated in a jurisdiction, as was the case with FTX US, may signify an intent to come within the jurisdiction's laws. FTX actively advertised to US customers, including naming a stadium and advertising during the Super Bowl. Although FTX was managed from the Bahamas, its management carried out business in the US and personal jurisdiction would be established by both objective and subjective personal jurisdiction. However, what about all the other countries where account holders are located? The extent of non-territorial personal jurisdiction will be discussed in the next section.

4.3. Hacking/Theft—Mt Gox

Perhaps the most significant hack to date is that of the Mt Gox cryptocurrency exchange in 2014. Mt Gox was based in Tokyo and began in 2007 as an online trading platform for the card game Magic the Gathering (Linton et al. 2017). The name itself means Magic the Gathering Online Exchange (Ma 2017). Over time, the exchange began trading Bitcoin until it was responsible for around seventy percent of Bitcoin's global trading volume. The exchange stopped trading in 2014, reporting that hackers stole approximately 850,000 Bitcoin from the exchange. At the time of writing, Bitcoin is trading at USD 23,200, meaning this Bitcoin would be worth USD 19.7 billion. The exchange filed for bankruptcy in the Tokyo district Court in 2014 and was ordered to liquidate that same year. The process, however, is still not complete, and creditors are waiting to receive some of the Bitcoin they are owed from the bankrupt exchange.

Hacking and the theft of cryptocurrency are closely related because hackers may target those with cryptocurrency in hopes of obtaining their private key. If a holder of cryptocurrency "stores"[3] their currency in a digital wallet that is on a device connected to the Internet (hot wallet) then a hacker could steal the owner's cryptocurrency if that device is compromised by the hacker. Therefore, users are advised not to carry large amounts of cryptocurrency in a hot wallet, just as someone should not carry large amounts of cash. Similarly, users that save a copy of their private key in digital form risk it being found and used to steal funds. Hackers can create software that searches for private keys in compromised devices. Thus, users saving a private key to a digital device or in a cloud server place themselves at significant risk of losing their cryptocurrency.

While gaining unauthorised access to a computer system, commonly referred to as hacking, is covered by specific statutes, such as the Computer Fraud and Abuse Act, it is unclear whether using otherwise legally obtained private keys to steal cryptocurrency would constitute hacking (Thomas 2023). If not, it may limit the jurisdiction of courts. This is because the system is designed to be permissionless and facilitate anyone with the private key to make transactions. The user would be accessing the network as intended and not otherwise gaining access to another computer. However, in jurisdictions where cryptocurrency is recognised as property, this would constitute larceny. In establishing jurisdiction, the larceny would take place in the physical location of the bad actor. However, it is difficult to also apply the jurisdiction of the victim as the nodes are located globally and the individual committing larceny may not know the location of the victim.

4.4. Tornado Cash and Allegations of Money Laundering

The belief that most major cryptocurrencies, including Bitcoin, are anonymous is a common misconception. All transactions are permanently recorded on the blockchain and

[3] Technically, the currency is represented through the ledger and stored across all nodes on the network. The wallet is only used to store the private key and more easily interact with the blockchain. However, to a user that is not familiar with how blockchain operates, the wallet will appear to hold the cryptocurrency.

can be downloaded or viewed online using a blockchain explorer. The fact that anyone can create a crypto wallet, one of the benefits of cryptocurrency as it provides a secure means to store funds for many in developing countries that do not have access to bank accounts, has caused currencies like Bitcoin to be described as pseudo-anonymous (Kerr et al. 2023). This is because all transactions are recorded but the general public may not know who controls each wallet (Shovkhalov and Idrisov 2021). Nevertheless, there remains significant privacy concerns because once an individual is tied to a wallet, all past and future transactions are connected to the person. Most exchanges also require customers to provide identification in compliance with know your customer (KYC) laws (Brasse and Hyun 2023). This acts as a double-edged sword in that it allows governments to know who controls cryptocurrency wallets and thereby identify and arrest those engaged in illegal activity, but it also poses a risk of data leaks that would expose transaction histories of individuals using exchanges. For many transactions, such as buying food at the local store, this may not appear a concern, but there are many circumstances where privacy is important, including issues related to safety, medical conditions, and political affiliations. For example, a stigma remains for people with some medical conditions, such as HIV, and those with such conditions should be able to pay for treatment without the payments being viewed by others. Similarly, removing anonymity could put victims of abuse at risk as abusers could identify their location. In order to provide this privacy, programmers developed privacy tools, including one commonly referred to as a mixer (Nadler and Schär 2023).

Mixers allow individuals to "deposit" pre-defined units of cryptocurrency and then withdraw them later into a new wallet. Because deposits and withdrawals are restricted to specific denominations and many people interact with the mixer, it theoretically becomes impossible to determine which user is withdrawing funds. One of the most popular mixers, known as Tornado Cash, was placed on the sanctioned entities list by the US Department of Treasury (Anthony 2022a) as it is alleged that North Korean hackers used the mixer to launder hacked funds. There is still an important legal question on whether software can be sanctioned, as Tornado Cash is not an entity but rather open-source software. Shortly after this, one of the Etherium founders, Vitalik Buterin, admitted to using Tornado Cash to donate anonymously to Ukraine in 2022. The mixture of bad actors and privacy-focused individuals has made mixers a controversial topic. In the wake of this, one of the developers of Tornado Cash, Alexey Pertsev, was arrested in the Netherlands where he is a resident (Schickler 2022a, 2022b). Although at the time of writing, the investigation by prosecutors is ongoing, it is reported that he is being held on allegations of facilitating money laundering and concealing criminal financial flows stemming from his role as a developer of Tornado Cash. Whether developers should be held accountable for the actions of others using their open-source software is beyond the scope of this article. However, if a crime were to be committed, the Netherlands would be an appropriate jurisdiction as it is the alleged place of the criminal act and the residence of the accused. Establishing extra-territorial jurisdiction in such cases would pose a problem as it could subject developers of decentralised applications to the laws in every country around the world. This is because nodes exist around the world and the software can be used by anyone. This creates a risk of developers needing to comply with inconsistent laws and would require knowledge of the laws in every jurisdiction.

As can be seen from these examples, crimes involving cryptocurrency commonly involve fraud and hacking. Although a much smaller portion of the criminal activity, they can also involve the use of cryptocurrency in illicit transactions and money laundering. The next section discusses the traditional approaches to extra-territorial jurisdiction and their application to cryptocurrency-related crimes. As there is limited jurisprudence or literature addressing personal jurisdiction for cross-border crimes involving cryptocurrency, this section looks to cybercrimes generally for guidance on how courts are likely to rule on jurisdictional issues.

5. The Extent of Extra-Territorial Jurisdiction

The two primary traditional bases for jurisdiction are territoriality and nationality, (Zajac 2019) each of which can be divided into categories, with these also joined by universal jurisdiction.

The fundamental principle of criminal law that no crime can exist without law (*nullum crimen sine lege*) requires the *ex ante* establishment of standards of behavior. This stands in contrast to international law, which often exists as an *ex post* standard flowing from political realities that is used to justify state actors while also having an *ex ante* role of establishing customs for future interactions between states. Traditional concepts of jurisdiction were established as customs for relations between sovereigns without regard to individual rights and in an era where human rights were not recognised (Zajac 2019). Nevertheless, jurisdiction requires "a genuine link that comes either in the form of a geographic territory or citizenship" (Saghir and Kafteranis 2022). While this restriction stems from the need for countries to avoid interreference in each other's sovereignty, it also can offer some protection to individuals by restricting the ability of countries to extend jurisdiction over individuals with whom the country has no connection.

5.1. Territorial Jurisdiction

The most obvious form of jurisdiction is territorial (Osmanollaj 2023). This stems both from the concept that states can regulate the behavior within their own territory and the reality that states cannot set a standard of behavior outside their territory without infringing on the sovereignty of other states. Territorial jurisdiction can be further divided into objective and subjective jurisdiction (Foysal 2023). Objective territorial jurisdiction is the exercising of jurisdiction over the defendant because they were present in the state at the time of the alleged crime. As their presence in the state is an objective fact, this is the simplest form of territorial jurisdiction to establish.

Subjective territorial jurisdiction is based on the subjective intent of the actor to direct their activity towards the foreign state, thereby subjecting themselves to the state's jurisdiction. The traditional law school example is the person standing on the border between two countries that then shoots someone on the other side of the border. The state where he is standing has objective territorial jurisdiction, but because he intended to harm someone that he knew was in the other state, his subjective intent to impact that state subjects him to its jurisdiction. For cryptocurrency-related crimes, cross-border fraud will often fit in this category as the perpetrator will know the location of the victims. However, theft of crypto assets can be more complicated because the assets sit on nodes around the world. As such, the subjective intent of a defendant to submit to the laws of a foreign jurisdiction is less clear than the shooting example. Certainly, the argument for extra-territorial jurisdictions is strengthened if the bad actor knew the location of the victim. However, this may be difficult to establish. When expanding jurisdiction to states that might be affected, it is important to place strict limitations as, without clear restraints, the approach may be the "beginning of the end to meaningful territorial limits on legislative jurisdiction" (Parrish 2008).

5.2. Nationality

Nationality-based jurisdiction asserts that states have jurisdiction over the actions of their nationals, even if that action takes place outside the state's territory (Gerber 1984). States have gradually increased this power to cover not only citizens but residents. Nationality as a basis of jurisdiction has its basis in European history, where the sovereign was deemed to have divine authority over their subjects, irrespective of where these subjects may travel. The term "subject of the king" was used in England in reference to nationality and, at the time of US independence in 1776, the US was the only country to use the term citizen to reference something similar to a national (McGovney 1911). The top-down notion that the state, through divine authority, has global authority over its subjects is antithetical to the bottom-up Western democratic view that government authority flows from the people and that democracy allows laws to reflect local standards. Regardless, states continue to use nationality as a basis to extend jurisdiction beyond their borders. There is, however, a presumption that laws are limited to a state's territory unless explicitly stated otherwise by the legislature.[4]

In addition to asserting extra-territorial jurisdiction over nationals, known as active jurisdiction, countries sometimes assert jurisdiction over crimes conducted abroad against their nationals. Known as passive-nationality jurisdiction, this form of jurisdiction is particularly controversial and often contested (Chehtman 2010). The primary purpose of criminal law is to protect members of society, both through creating clear standards of conduct and through removing particularly dangerous actors from society. In the case of passive nationality, these goals are not met, as the bad actor is a member of a different society. As such, for ordinary crimes, use of the passive nationality principle is largely limited to cases where the state is merely seeking retribution. However, in the case of cybercrimes, incentives change. Whereas a state is motived to prevent violent crime and protect its citizens, a state may not be motivated to arrest those engaged in online fraud or hacking if the targets are in another jurisdiction. Indeed, the state may benefit from the proceeds of these crimes, increasing the wealth of the local population. As such, to the extent that a state can obtain custody of a criminal actor, passive nationality jurisdiction may have an important role in fighting cryptocurrency theft, fraud, and other related cybercrimes in jurisdictions where governments are unable or unwilling to stop bad actors.

The territorial and nationality approaches to establishing jurisdiction also protect the rights of defendants against improper extra-territorial expansion of power by requiring that defendants have sufficient "minimum contacts" with the state. Individuals are seen as either benefiting from the protection of the state or, if traveling into another state, having voluntarily submitted to that state's jurisdiction, thereby justifying the application of the foreign state's laws. Similarly, if a person intentionally directs an act at another jurisdiction, then they can be viewed as having voluntarily submitted to the laws of the place toward which the harm was aimed. In the case of cryptocurrency, this is complicated because the currency is simply a record on a digital ledger that is stored on computers around the world. Therefore, the assertion of jurisdiction based on the server being within a state's borders is no longer a reasonable approach, as it would grant every state jurisdiction over an individual's actions with decentralised digital assets. Not only would it be impossible for individuals to research laws in every jurisdiction, but laws in different countries could create inconsistent obligations. For example, one country may require disclosure of a counter party's information as part of anti-money laundering laws while another country may require that information to be kept confidential as part of privacy laws. Therefore, an individual attempting to comply with the laws in one jurisdiction may find themselves criminally charged in another. This complexity could also destroy the crypto industry and continued technological development as developers may be afraid to innovate, not knowing if they risk breaking a law in some foreign jurisdiction.

5.3. Universal Jurisdiction

Universal jurisdiction is the right to assert global jurisdiction in the absence of any ordinary links between the defendant and the state. This is done under the theory that "some crimes are so troublesome as to constitute a threat to international peace and security" (Ireland-Piper 2012). In principle, universal jurisdiction should be limited to crimes that are a global threat, such as piracy, genocide, and other war crimes. Universal jurisdiction comes largely out of necessity. Even egregious crimes, such as murder, can be dealt with within the jurisdiction of the act and, therefore, would not warrant universal jurisdiction. However, crimes such as genocide are conducted by people using either the power of the state or in a location where the state is too weak to prevent the crimes. These crimes constitute a threat to international peace and, therefore, out of necessity, other states are empowered

[4] See Morrison v National Australia Bank Ltd., 561 U.S. 247 (2010).

to assert jurisdiction. Crimes that fit in this category are ordinarily viewed as crimes against humanity generally as opposed to any one individual and are, therefore, larger in scope. One of the dangers of universal jurisdiction is the tendency for courts to increase the scope of their authority over time. When faced with the choice between releasing a defendant the court believes committed a reprehensible act and extending the court's authority beyond its legal limits, courts are often tempted to extend their jurisdiction. In an individual circumstance, many people would view this as a moral approach. However, over time, jurisdiction can be improperly increased to the extent that it undermines the law by violating the rights of defendants and the principle that there is no crime without law—a principle that protects individuals by ensuring they are held to a specific legal standard and not to the laws of any court in the world that decides to assert jurisdiction.

The difficulty in establishing the location of a criminal carrying out a cybercrime is often cited as a hindrance to determining applicable law and jurisdiction (Saghir and Kafteranis 2022). The use of virtual privacy networks and other technologies may make a criminal's location difficult to determine. However, this issue applies primarily to the investigation stage and not the jurisdiction to prosecute. If authorities can determine who has committed a crime, then absent the rare case of the cybercriminal that was travelling across borders around the time of the criminal acts, the physical location of the defendant when committing the crime should be easy to identify. As identify theft is a common element in cybercrimes, the inability to identify the physical location of the criminal activity and connect it with the defendant will, in most cases, imply that authorities have insufficient proof to convict the defendant. As such, granting jurisdiction to any state where the defendant is not physically located, and potentially any state outside the defendant's domicile, creates a high risk of extradition and detainment of innocent parties. Jurisdiction may be difficult to determine at the beginning of an investigation. However, once law enforcement has sufficient evidence to charge a defendant, the location of the defendant's actions and, therefore, a territorial jurisdiction[5], should ordinarily be clear.

5.4. Establishing Inherent Harm as a Requirement for Extra-Territorial Jurisdiction

Crimes have historically been divided into two categories: inherently wrong actions and actions that are prohibited but not otherwise immoral (Velasco 2015). Inherently wrong actions include crimes such as murder, theft, and assault. Fraud, including those committed using cryptocurrency, would also fall into this category. Other actions, such as jaywalking or possessing marijuana may have been banned by society but are not inherently wrong. Money laundering would also fall into this category (Young 2009; Dimock 2016), as the laundering itself does not create harm. One problem with this distinction is that moral standards vary across jurisdictions, and states have thus incorporated a degree of subjectivity into the analysis. For example, possession of cocaine or methamphetamine, because it does not pose a direct harm to others, may be viewed as merely prohibited in some jurisdictions but inherently wrong in others. Similarly, prostitution is viewed as a prohibited activity in some jurisdictions but viewed as immoral and, therefore, inherently wrong in others. Yet still, it is legal in some jurisdictions. In the international context, for the distinction to have significance, the test should be whether a particular crime necessarily creates a direct harm to an identifiable person or persons. The claim that something harms society generally is insufficient to meet this requirement as the standard is too subjective to account for differences in cultures and standards around the world. For example, it is impossible for a person to commit murder or fraud without harming someone. However, while the possession or sale of drugs may lead to harm, the harm is not certain.

To protect the rights of individuals while ensuring states can protect their citizens, this distinction could also be applied so that, aside from territorial-based jurisdiction, countries only extend extra-territorial jurisdiction where it is impossible to commit the crime without

[5] If another jurisdiction was intentionally targeted, there may be more than one country with territorial jurisdiction.

directly harming someone. To ensure respect for other countries and remove the risk of countries imposing their beliefs on other cultures, this test should have a further restriction that if an activity is legal in any country, then it is deemed as being only prohibited and not inherently immoral (harmful). Under this approach, individuals would still be subject to the laws where they are located but would not need to worry about running afoul of foreign laws, so long as their actions were not harmful.

The use of cryptocurrency in extortion or fraud is inherently wrong, and the defendant's state of nationality, the jurisdiction where the defendant was located at the time they committed the crime, and, if the harm was aimed at a specific state, the target state may all have jurisdiction over the crime. However, if the crime is failure to meet some reporting requirement, the defendant should only be liable within the territory they are located.

One of the greatest risks in international criminal law is the erosion of individual rights against the goal of comity between states. When it comes to establishing jurisdiction, "[c]onsiderations of international human rights law are usually lost in the shuffle" (Drake 1992). In upholding the presumption of innocence, disruption to the defendant's life should be minimised prior to conviction. Arrest and extradition will have a detrimental physical, phycological, and economic impact on a defendant. In establishing jurisdictional rules, courts and legislatures must recognise that law enforcement will not accurately identify the criminal actor in every circumstance and therefore create systems that are minimally harmful and disruptive to the accused. Fortunately, the domicile of the defendant will often also be the location where most evidence is located, another important factor in determining where a trial should take place (Maillart 2019).

The more morally egregious a crime, the higher the risk of false conviction as society demands "justice" in the form of a conviction and punishment. For example, a combination of moral outrage and prejudice have historically resulted in some African Americans being falsely convicted of serious crimes. Further, statutes of limitations are often increased or removed for particularly egregious crimes, increasing the risk of false convictions as the falsely accused are unable to explain evidence that suggests their guilt or refute testimony as exculpatory evidence is lost and alibies are difficult to find years after an alleged crime takes place, especially for the falsely accused.

Another fundamental principle of the law states that if the law is ambiguous, it should be decided in favour of the accused (Lin and Watters 2018). *In dubio pro reo*, or 'in doubt for the accused', has been weakened over the years by court decisions and statutes stating that courts should apply the law as the legislature intended. Courts then apply statutes to prevent the perceived bad acts as opposed to applying the text and granting the defendant the benefit of the doubt. This trend undermines the rule of law and human rights and is paralleled by the extra-territorial extension of jurisdiction where defendants have not submitted to the jurisdiction and cannot reasonably be expected to comply with foreign law. The risk is compounded with increased international travel as countries around the world may have different cultures and customs and interpret law differently (Campanini and Arafa 2020; Bertotti et al. 2021; Arafa and Burns 2015). Additionally, decentralised technology like cryptocurrency does not fit well within the traditional framework for establishing extra-territorial jurisdiction. States claiming jurisdiction any time a node is within their territory will undermine the need for certainty and the rule of law. Absent an international convention that would provide certainty and establish clear jurisdictional standards, requiring a criminal act to necessarily create direct harm will protect the rights of individuals by reducing the risk of defendants being charged without knowingly engaging in harmful behaviour or that they know to be illegal, and will still facilitate prosecution of those involved in cross-border fraud or the theft of cryptocurrency.

6. Conclusions

Cryptocurrency and other blockchain-based digital assets are an important technology that is becoming increasingly popular, with Bitcoin adopted as an official currency in El Salvador and the Central African Republic. However, the decentralised nature of the technology makes it impossible to connect a coin to a specific location as the ledger is hosted on nodes around the world. This makes territorial jurisdiction difficult to establish in many crypto-related transnational crimes, including hacking and fraud. However, if those engaging in fraud or hacking only target people in foreign jurisdictions, the local government may not be motivated to expend the cost of investigating, prosecuting, and incarcerating those responsible. In fact, the local government may benefit from the additional resources brought into the local economy by the criminals. As such, a balance must be struck when a country applies nationality-based jurisdiction to protect its citizens to ensure the individual rights of defendants are protected. Not only is the protection of individual human rights and establishing clear legal standards essential to maintain the rule of law, but at least some of those suspected of engaging in illegal activity will be innocent. As one restriction to help strike this balance, this article suggests that non-territorial-based jurisdiction, including nationality-based jurisdiction, only be extended if a crime would necessarily create direct harm to a person or persons. This objective standard will facilitate establishing extra-territorial jurisdiction where bad actors engage in fraud or steal crypto assets, acts that the perpetrator will know are wrong. Simultaneously, it will protect anyone who unintentionally violates a foreign regulation, thereby reducing compliance costs and supporting the development of the industry.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The author does not own any cryptocurrency and declares no conflict of interest.

References

Aboura, Sofiane. 2022. A note on the Bitcoin and Fed Funds rate. *Empirical Economics* 63: 2577–603. [CrossRef] [PubMed]

Allenotor, David, and D. A. Oyemade. 2021. An Optimized Parallel Hybrid Architecture for Cryptocurrency Mining. Available online: https://www.isteams.net/_files/ugd/185b0a_6f88b82981424f87850d11fea3f52e1b.pdf (accessed on 27 February 2023).

Aloini, Davide, Elisabetta Benevento, Alessandro Stefanini, and Pierluigi Zerbino. 2023. Transforming healthcare ecosystems through blockchain: Opportunities and capabilities for business process innovation. *Technovation* 119: 102557. [CrossRef]

Alshater, Muneer M., Mayank Joshipura, Rim El Khoury, and Nohade Nasrallah. 2023. Initial Coin Offerings: A Hybrid Empirical Review. *Small Business Economics*, 1–18. [CrossRef]

Alvarez, Fernando E., David Argente, and Diana Van Patten. 2022. *Are Cryptocurrencies Currencies? Bitcoin as Legal Tender in El Salvador*. Cambridge: National Bureau of Economic Research.

Analytica, Oxford. 2021. El Salvador bitcoin experiment comes with risks. *Expert Briefings*, July 12.

Ante, Lennart, Ingo Fiedler, Jan Marius Willruth, and Fred Steinmetz. 2023. A Systematic Literature Review of Empirical Research on Stablecoins. *FinTech* 2: 34–47. Available online: https://www.mdpi.com/2674-1032/2/1/3 (accessed on 27 February 2023). [CrossRef]

Anthony, Nicholas. 2022a. Treasury's Tornado Warning. Available online: https://policycommons.net/artifacts/2643457/treasurys-tornado-warning/3666218/ (accessed on 27 February 2023).

Anthony, Nicholas. 2022b. Warren Targets Financial Privacy in Wake of FTX Fall. Available online: https://www.cato.org/blog/warren-targets-financial-privacy-wake-ftx-fall (accessed on 27 February 2023).

Arafa, Mohamed A., and Jonathan G. Burns. 2015. Judicial Corporal Punishment in the United States?: Lessons from Islamic Criminal Law for Curing the Ills of Mass Incarceration. *Indiana International & Comparative Law Review* 25: 385–420.

Arote, Prerna, and Joy Kuri. 2022. ZCC: Mitigating Double-spending Attacks in Micropayment Bitcoin Transactions. Paper presented at 2022 Fourth International Conference on Blockchain Computing and Applications (BCCA), San Antonio, TX, USA, September 5–7.

Bailey, Andrew M., and Craig Warmke. 2023. Bitcoin is King. In *Cryptocurrency: Concepts, Technology, and Issues*. Edited by J. Liebowitz. London and New York: Taylor & Francis, pp. 175–97.

Bertotti, Bárbara Mendonça, Cynthia Gruendling Juruena, and Mohamed Arafa. 2021. Polygamy Against Moral or Against Law? A Comparative Study Between Brazilian Law and Islamic Law. *Revista Do Direito* 63: 26–48. [CrossRef]

Blockchain.com. 2023. Latest BTC Blocks. Available online: https://www.blockchain.com/explorer/blocks/btc?page=1 (accessed on 27 February 2023).

Brasse, Antonio, and Samuel Hyun. 2023. Cryptocurrency Exchanges and the Future of Cryptoassets. In *The Emerald Handbook on Cryptoassets: Investment Opportunities and Challenges*. Bentley: Emerald Publishing Limited, pp. 341–53.

Campanini, Massimo, and Mohamed Arafa. 2020. Islam and Democracy: Appreciating the Nuance and Complexity of Legal Systems with a Basis in Religion. *Barry Law Review* 26: 1.

Cardona, Mercedes. 2022. Lessons Learned: Andrew Gray. *Journal of Financial Crises* 4: 613–16.

Caudevilla, Oriol. 2022. Global Blockchain-Based Trade Finance Solutions: Analysis of Governance Models and Impact on Local Laws in Six Jurisdictions. *Global Journal of Comparative Law* 11: 167–96.

Chehtman, Alejandro. 2010. *The Philosophical Foundations of Extraterritorial Punishment*. Oxford: Oxford University Press.

Chohan, Usman W. 2023. FTX, Sam Bankman-Fried, and the Cryptoexchange Problem. *Frontiers in Environmental Science* 10: 897496. [CrossRef]

Christin, Nicolas. 2013. Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. Paper presented at 22nd international conference on World Wide Web, Rio de Janeiro, Brazil, May 13–17.

Co, Niji Oni. 2021. Jurisdictional Issues on Cryptocurrency Transactions. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3830568 (accessed on 27 February 2023).

Colesanti, J. Scott. 2022. Sorry, They Were on Mute: The SEC's "Token Proposal 2.0" as Blueprint for Regulatory Response to Cryptocurrency. *Corporate and Business Law Journal* 3: 1.

Cong, Lin William, Kimberly Grauer, Daniel Rabetti, and Henry Updegrave. 2023. The Dark Side of Crypto and Web3: Crypto-Related Scams. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4358572 (accessed on 27 February 2023).

de Koker, Louis, Talha Ocal, and Pompeu Casanovas. 2022. Where's Wally? FATF, virtual asset service providers, and the regulatory jurisdictional challenge. In *Financial Technology and the Law: Combating Financial Crime*. Edited by Doron Goldbarsht and Louis De Koker. Cham: Springer Nature, pp. 151–83.

Dimock, Susan. 2016. The Malum prohibitum—Malum in se Distinction and the Wrongfulness Constraint on Criminalization. *Dialogue: Canadian Philosophical Review/Revue Canadienne de Philosophie* 55: 9–32. [CrossRef]

Divakaruni, Anantha, and Peter Zimmerman. 2023. The Lightning Network: Turning Bitcoin into Money. *Finance Research Letters* 52: 103480. [CrossRef]

DOJ. 2019. *Former Partner of Locke Lord LLP Convicted in Manhattan Federal Court of Conspiracy to Commit Money Laundering and Bank Fraud in Connection with Scheme to Launder $400 Million of OneCoin Fraud Proceeds*; Edited by US Department of Justice. Available online: https://www.justice.gov/usao-sdny/pr/former-partner-locke-lord-llp-convicted-manhattan-federal-court-conspiracy-commit-money (accessed on 27 February 2023).

DOJ. 2022. *The Report of the Attorney General Pursuant to Section 8(b)(iv) of Executive Order 14067*; Washington, DC: U.S. Department of Justice.

Drake, Mason H. 1992. United States v. Yunis: The DC Circuit's Dubious Approval of US Long-Arm Jurisdiction over Extraterritorial Crimes. *Northwestern University Law Review* 87: 697.

Dylan LeClair, Sam Rule. 2022. The State Of Lightning Network Adoption. *Bitcoin Magazine*, June 10.

Fan, Sizheng, Tian Min, Xiao Wu, and Cai Wei. 2022. Towards understanding governance tokens in liquidity mining: A case study of decentralized exchanges. *World Wide Web*, 1–20. [CrossRef]

Farrar, John H. 2001. In pursuit of an appropriate theoretical perspective and methodology for comparative corporate governance. *Australian Journal of Corporate Law* 13: 1–18.

FATF, ed. 2021. *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*. Paris: FATF.

Foysal, Quazi Omar. 2023. A tale of two international law principles: Ensuring justice and accountability for the Rohingya. In *The Rohingya Crisis*. London: Routledge, pp. 73–95.

Gerber, David J. 1984. Beyond balancing: International law restraints on the reach of national laws. *Yale Journal of International Law* 10: 185.

Ghazi-Tehrani, Adam Kavon, and Henry N. Pontell. 2021. Phishing evolves: Analyzing the enduring cybercrime. *Victims & Offenders* 16: 316–42.

Ghosh, Pranto Kumar, Arindom Chakraborty, Mehedi Hasan, Khalid Rashid, and Abdul Hasib Siddique. 2023. Blockchain Application in Healthcare Systems: A Review. *Systems* 11: 38. [CrossRef]

Gonzalez, Nicholas E. 2022. Does Cryptocurrency Staking Fall under SEC Jurisdiction? *Fordham Journal of Corporate & Financial Law* 27: 521.

Gorbunova, Maria, Pavel Masek, Mikhail Komarov, and Aleksandr Ometov. 2022. Distributed ledger technology: State-of-the-art and current challenges. *Computer Science and Information Systems* 19: 65–85. [CrossRef]

Guillaume, Florence, and Sven Riva. 2022. Blockchain Dispute Resolution for Decentralized Autonomous Organizations: The Rise of Decentralized Autonomous Justice. In *Blockchain and Private International Law*. Leiden: Brill Nijhoff.

Gurkov, Alexander. 2022. Alignment of a traditional cooperative identity to the design of decentralised autonomous organisations. *Nottingham Insolvency and Business Law e-Journal* 2022: 1–25.

Hallinan, Kevin P., Lu Hao, Rydge Mulford, Lauren Bower, Kaitlin Russell, Austin Mitchell, and Alan Schroeder. 2023. Review and Demonstration of the Potential of Bitcoin Mining as a Productive Use of Energy (PUE) to Aid Equitable Investment in Solar Micro- and Mini-Grids Worldwide. *Energies* 16: 1200. Available online: https://www.mdpi.com/1996-1073/16/3/1200 (accessed on 27 February 2023). [CrossRef]

Hedayati, Ali. 2012. An analysis of identity theft: Motives, related frauds, techniques and prevention. *Journal of Law and Conflict Resolution* 4: 1–12.

Hossain, Mohammad Belayet. 2023. Acquiring an awareness of the latest regulatory developments concerning digital assets and anti-money laundering. *Journal of Money Laundering Control*. [CrossRef]

Ibañez, Juan Ignacio, and Francisco Rua. 2023. The Energy Consumption of Proof-of-Stake Systems: A Replication and Expansion. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4324137 (accessed on 27 February 2023).

Indriati, Ervina Dwi, and Nunung Nugroho. 2022. Philosophy of Law and the Development of Law as a Normative Legal Science. *International Journal of Educational Research and Social Sciences (IJERSC)* 3: 314–21. [CrossRef]

Ireland-Piper, Danielle. 2012. Extraterritorial criminal jurisdiction: Does the long arm of the law undermine the rule of law? *Melbourne Journal of International Law* 13: 122–57.

Katterbauer, Klemens, Hassan Syed, and Laurent Cleenewerck. 2022. The impact of the legalization of Bitcoin in the Central African Republic—A legal analysis. *Cuadernos de Economía* 713: 746.

Kaur, Arpneek, Sandhya Bansal, and Vishal Dattana. 2023. Blockchain in Healthcare: A Systematic Review and Future Perspectives. In *Deep Learning for Healthcare Decision Making*. London: Routledge.

Kerr, David S., Karen A. Loveland, Katherine Taken Smith, and Lawrence Murphy Smith. 2023. Cryptocurrency Risks, Fraud Cases, and Financial Performance. *Risks* 11: 51. [CrossRef]

Khezami, Nadhira, Nourcherif Gharbi, Bilel Neji, and Naceur Benhadj Braiek. 2022. Blockchain Technology Implementation in the Energy Sector: Comprehensive Literature Review and Mapping. *Sustainability* 14: 15826. Available online: https://www.mdpi.com/2071-1050/14/23/15826 (accessed on 27 February 2023). [CrossRef]

Kordestani, Arash, Pejvak Oghazi, and Rana Mostaghel. 2023. Smart contract diffusion in the pharmaceutical blockchain: The battle of counterfeit drugs. *Journal of Business Research* 158: 113646. [CrossRef]

Kotlán, Pavel, Miroslav Ondrúš, Alena Kozlová, Igor Kotlán, Pavel Petr, and Radim Kalabis. 2023. Criminal Compliance Program as a Tool for Criminal Liability Exculpation of Legal Persons in the Czech Republic. *Laws* 12: 20. Available online: https://www.mdpi.com/2075-471X/12/2/20 (accessed on 27 February 2023).

Kshetri, Nir. 2022a. Bitcoin's Adoption as Legal Tender: A Tale of Two Developing Countries. *IT Professional* 24: 12–15. [CrossRef]

Kshetri, Nir. 2022b. El Salvador's bitcoin gamble. *Computer* 55: 85–89. [CrossRef]

Levi, Michael. 2002. Money laundering and its regulation. *The Annals of the American Academy of Political and Social Science* 582: 181–94. [CrossRef]

Liang, Yuan, Casey Watters, and Michał K. Lemański. 2022. Responsible Management in the Hotel Industry: An Integrative Review and Future Research Directions. *Sustainability* 14: 17050. [CrossRef]

Lin, Xifen, and Casey Watters. 2018. Understanding the presumption of innocence in China: Institution and practice. In *Chinese Legal Reform and the Global Legal Order: Adoption and Adaptation*. Cambridge: Cambridge University Press, pp. 44–62.

Linton, Marco, Ernie Gin Swee Teo, Elisabeth Bommes, C. Y. Chen, and Wolfgang Karl Härdle. 2017. *Dynamic Topic Modelling for Cryptocurrency Community Forums*. Berlin/Heidelberg: Springer.

Liu, Mengling, and Man Ho Au. 2022. Practical Anonymous Multi-hop Locks for Lightning Network Compatible Payment Channel Networks. Paper presented at Network and System Security: 16th International Conference (NSS 2022), Denarau Island, Fiji, December 9–12.

Liu, Yi, Ruilin Li, Xingtong Liu, Jian Wang, Lei Zhang, Chaojing Tang, and Hongyan Kang. 2017. An efficient method to enhance Bitcoin wallet security. Paper presented at 2017 11th IEEE International Conference on Anti-counterfeiting, Security, and Identification (ASID), Xiamen, China, October 27–29.

Lukings, Melissa, and Arash Habibi Lashkari. 2022. Conflicts of Law. In *Understanding Cybersecurity Law in Data Sovereignty and Digital Governance: An Overview from a Legal Perspective*. Berlin/Heidelberg: Springer, pp. 85–115.

Ma, Di. 2017. Taking a byte out of Bitcoin regulation. *Albany Law Journal of Science and Technology* 27: 1.

Mahalaxmi, G., and T. Aditya Sai Srinivas. 2022. Data Analysis with Blockchain Technology: A Review. *IUP Journal of Information Technology* 18: 7–23.

Maillart, Jean-Baptiste. 2019. The Limits of Subjective Territorial Jurisdiction in the Context of Cybercrime. *Era Forum* 19: 375–90. [CrossRef]

Makridis, Christos A., Michael Fröwis, Kiran Sridhar, and Rainer Böhme. 2023. The rise of decentralized cryptocurrency exchanges: Evaluating the role of airdrops and governance tokens. *Journal of Corporate Finance* 79: 102358. [CrossRef]

McGovney, Dudley O. 1911. American Citizenship. *Columbia Law Review* 11: 231. [CrossRef]

Mezquita, Yeray, Dévika Pérez, Alfonso González-Briones, and Javier Prieto. 2023. Cryptocurrencies, Survey on Legal Frameworks and Regulation Around the World. Paper presented at International Congress on Blockchain and Applications, Guimaraes, Portugal, July 12–14.

Mololoth, Vidya Krishnan, Saguna Saguna, and Christer Åhlund. 2023. Blockchain and Machine Learning for Future Smart Grids: A Review. *Energies* 16: 528. [CrossRef]

Mondoh, Brian Sanya, Sara M. Johnson, Matthew Green, and Aris Georgopoulos. 2022. Decentralised Autonomous Organisations: The Future of Corporate Governance or an Illusion? Aris (Aristeidis), Decentralised Autonomous Organisations: The Future of Corporate Governance or an Illusion. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4144753 (accessed on 27 February 2023).

Moore, Simon. 2021. Towards a functioning legal framework for emerging DAO technologies in Australia. *ANU Journal of Law and Technology* 2: 109–19.

Nadler, Matthias, and Fabian Schär. 2023. Tornado Cash and Blockchain Privacy: A Primer for Economists and Policymakers. Available online: https://research.stlouisfed.org/publications/review/2023/02/03/tornado-cash-and-blockchain-privacy-a-primer-for-economists-and-policymakers (accessed on 27 February 2023).

Náñez Alonso, Sergio Luis. 2019. Activities and Operations with Cryptocurrencies and Their Taxation Implications: The Spanish Case. *Laws* 8: 16. Available online: https://www.mdpi.com/2075-471X/8/3/16 (accessed on 27 February 2023).

Neti, Lavanya V. 2022. Exploring the Implications of Cryptocurrencies in Selected Developing Countries. Working Paper, University of Pennsylvania Scholarly Commons. Available online: https://repository.upenn.edu/cgi/viewcontent.cgi?article=1044&context=spur (accessed on 27 February 2023).

Nickerson, Mark A. 2019. Fraud in a world of advanced technologies: The possibilities are (unfortunately) endless. *The CPA Journal* 89: 28–34.

Noked, Noam. 2018. Tax Evasion and Incomplete Tax Transparency. *Laws* 7: 31. Available online: https://www.mdpi.com/2075-471X/7/3/31 (accessed on 27 February 2023). [CrossRef]

Novak, Mikayla. 2020. Crypto-friendliness: Understanding blockchain public policy. *Journal of Entrepreneurship and Public Policy* 9: 165–84. [CrossRef]

Osmanollaj, Rinesë. 2023. The Action of Criminal Law in Time, in Space and to Persons. *International Journal of Social Science Research and Review* 6: 398–407.

Parrish, Austen. 2008. The Effects Test: Extraterritoriality's Fifth Business. *Vanderbilt Law Review* 61: 1455.

Pecharsky, Nicole, and Moin A. Yahya. 2022. Crypto-Litigation: An Empirical Overview for 2020–Present. SMU Science & Technology Law Review, Forthcoming. Available online: https://scholar.smu.edu/scitech/vol25/iss2/4/ (accessed on 27 February 2023).

Phelps, Amy, and Allan Watt. 2014. I shop online–recreationally! Internet anonymity and Silk Road enabling drug use in Australia. *Digital Investigation* 11: 261–72. [CrossRef]

Pinto, Filipe, Catarina Ferreira da Silva, and Sergio Moro. 2022. People-centered distributed ledger technology-IoT architectures: A systematic literature review. *Telematics and Informatics* 70: 101812. [CrossRef]

Pradeep, Mullekyal Devadasan. 2019. Legal Research-Descriptive Analysis on Doctrinal Methodology. *International Journal of Management, Technology, and Social Sciences (IJMTS)* 4: 95–103.

Rudd, Murray A. 2023. 100 Important Questions about Bitcoin's Energy Use and ESG Impacts. *Challenges* 14: 1. Available online: https://www.mdpi.com/2078-1547/14/1/1 (accessed on 27 February 2023). [CrossRef]

Saghir, Wael, and Dimitrios Kafteranis. 2022. The Applicable Law on Digital Fraud. In *Finance, Law, and the Crisis of COVID-19: An Interdisciplinary Perspective*. Berlin/Heidelberg: Springer, pp. 221–35.

Sanz-Bas, David, Carlos del Rosal, Sergio Luis Náñez Alonso, and Miguel Ángel Echarte Fernández. 2021. Cryptocurrencies and Fraudulent Transactions: Risks, Practices, and Legislation for Their Prevention in Europe and Spain. *Laws* 10: 57. Available online: https://www.mdpi.com/2075-471X/10/3/57 (accessed on 27 February 2023).

Scharfman, Jason. 2023a. Additional Case Studies in Cryptocurrency Fraud. In *The Cryptocurrency and Digital Asset Fraud Casebook*. Berlin/Heidelberg: Springer, pp. 161–72.

Scharfman, Jason. 2023b. *The Cryptocurrency and Digital Asset Fraud Casebook*. Cham: Springer Nature.

Scharfman, Jason. 2023c. Cryptocurrency Ponzi, Pyramid, and MLM Schemes: Part 1. In *The Cryptocurrency and Digital Asset Fraud Casebook*. Berlin/Heidelberg: Springer, pp. 35–53.

Schauer, Frederick. 2021. Normative Legal Positivism. In *Cambridge Companion to Legal Positivism*. Cambridge: Cambridge UP, pp. 61–78.

Schickler, Jack. 2022a. Tornado Cash Developer Alexey Pertsev to Remain in Jail Until at Least Late Februrary. *CoinDesk*, February 20.

Schickler, Jack. 2022b. Tornado Cash Developer's Arrest in The Netherlands Draws Community Protest. *CoinDesk*, August 22.

Shovkhalov, Shamil, and Hussein Idrisov. 2021. Economic and Legal Analysis of Cryptocurrency: Scientific Views from Russia and the Muslim World. *Laws* 10: 32. Available online: https://www.mdpi.com/2075-471X/10/2/32 (accessed on 27 February 2023). [CrossRef]

Soltani, Reza, Marzia Zaman, Rohit Joshi, and Srinivas Sampalli. 2022. Distributed Ledger Technologies and Their Applications: A Review. *Applied Sciences* 12: 7898. [CrossRef]

Soria Ruiz-Ogarrio, Jorge Jesús. 2022. *Mining Incentives in Proof-of-Work Blockchain Protocols*. Helsinki: Publications of the Faculty of Social Sciences/Department of Political and Economic Studies, University of Helsinki.

Sparkes, Matthew. 2022. *El Salvador Revamps Bitcoin System*. Amsterdam: Elsevier.

Sun, Nigang, Yuanyi Zhang, and Yining Liu. 2022. A Privacy-Preserving KYC-Compliant Identity Scheme for Accounts on All Public Blockchains. *Sustainability* 14: 14584. [CrossRef]

Suratkar, Saurabh, Mahesh Shirole, and Sunil Bhirud. 2020. Cryptocurrency wallet: A review. Paper presented at 2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP), Chennai, India, September 28–29.

Tao, Zhijie, Bo Peng, and Lina Ma. 2023. Optimal initial coin offering under speculative token trading. *European Journal of Operational Research* 306: 632–44. [CrossRef]

Taylor, Luke. 2022. *The World's First Bitcoin Republic*. Amsterdam: Elsevier.

Thomas, A. Jean. 2023. Exceeding Authorized Access Under the CFAA. In *The Open World, Hackbacks and Global Justice*. Berlin/Heidelberg: Springer, pp. 211–61.

Truby, Jon. 2018. Decarbonizing Bitcoin: Law and policy choices for reducing the energy consumption of Blockchain technologies and digital currencies. *Energy Research & Social Science* 44: 399–410.

United States v Ruja Ignatova. 2018. S4 17 Cr. 630 (Indictment). Available online: https://www.justice.gov/usao-sdny/press-release/file/1141981/download (accessed on 27 February 2023).

van Dam, Gijs, and Rabiah Abdul Kadir. 2022. Hiding payments in lightning network with approximate differentially private payment channels. *Computers & Security* 115: 102623.

Velasco, Gian Carlo B. 2015. Dungo v. People and the Classification of Crimes Mala Prohibit A. *Philippine Law Journal* 89: 627.

Wendl, Moritz, My Hanh Doan, and Remmer Sassen. 2023. The environmental impact of cryptocurrencies using proof of work and proof of stake consensus algorithms: A systematic review. *Journal of Environmental Management* 326: 116530. [CrossRef] [PubMed]

Wenhua, Zhang, Faizan Qamar, Taj-Aldeen Naser Abdali, Rosilah Hassan, Syed Talib Abbas Jafri, and Quang Ngoc Nguyen. 2023. Blockchain Technology: Security Issues, Healthcare Applications, Challenges and Future Trends. *Electronics* 12: 546. [CrossRef]

Wezza, May, M. M. El-Gayar, and Ahmed AboElfetoh. 2022. A Novel Model for Securing Seals Using Blockchain and Digital Signature Based on QR Codes. Available online: https://assets.researchsquare.com/files/rs-2031413/v1_covered.pdf?c=1662660250 (accessed on 27 February 2023).

Wronka, Christoph. 2023. Financial crime in the decentralized finance ecosystem: New challenges for compliance. *Journal of Financial Crime* 30: 97–113. [CrossRef]

Wu, Jiajing, Kaixin Lin, Dan Lin, Ziye Zheng, Huawei Huang, and Zibin Zheng. 2023. Financial Crimes in Web3-empowered Metaverse: Taxonomy, Countermeasures, and Opportunities. *IEEE Open Journal of the Computer Society*. [CrossRef]

Yang, Alex Yueh-Ping. 2022. When Jurisdiction Rules Meet Blockchain: Can the Old Bottle Contain the New Wine? Available online: https://stanford-jblp.pubpub.org/pub/jurisdiction-rules-blockchain/release/1 (accessed on 27 February 2023).

Young, Robert. 2009. Douglas Husak on dispensing with the malum prohibitum offense of money laundering. *Criminal Justice Ethics* 28: 108–18. [CrossRef]

Zajac, Dominik. 2019. Criminal Jurisdiction over the Internet: Jurisdictional Links in the Cyber Era. *Cambridge Law Review* 4: 1–28.

Zanghi, Eric, Milton Brown Do Coutto Filho, and Julio Cesar Stacchini de Souza. 2023. Collaborative smart energy metering system inspired by blockchain technology. *International Journal of Innovation Science*. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.