Law and Blockchains

Stephen McKeon and Derek Edward Schloss

1 Introduction

The emergence of blockchain-based assets and systems of record have spurred numerous, and sometimes differing, interpretations within segments of the legal code. The decentralized nature of the technology is not always congruent with existing laws and precedent, which typically contemplates an environment with a higher degree of centralized control. In this chapter, we review various aspects of the legal environment and review how applications such as smart contracts, cryptocurrencies, tokenized securities, and decentralized autonomous organizations (DAOs) are treated with regard to tax law, intellectual property (IP) law, and securities law. We focus primarily on U.S. law, but comment on the global legal environment where applicable.

We begin with securities law because it is often unclear whether network-based assets constitute financial securities or not. We review the Howey Test and point to regulatory exemptions commonly utilized by issuers. Additionally, we briefly review the proposed benefits of issuing securities on-chain.

S. McKeon (✉)
Lundquist College of Business, University of Oregon, Eugene, OR, USA
e-mail: smckeon@uoregon.edu

D. E. Schloss
Collab+Currency, Eugene, OR, USA

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2021

R. Rau et al. (eds.), *The Palgrave Handbook of Technological Finance*,
https://doi.org/10.1007/978-3-030-65117-6_13

Smart contracts represent another area of intersection with the legal environment, specifically with contract law. A smart contract is a software code that has dominion over the value to be exchanged and executes an outcome autonomously based on a set of pre-specified conditions. They promise to reduce ambiguity, and increase speed and efficiency of the contracting environment. However, whether or not these agreements are deemed to be legally enforceable contracts has been the source of debate.

Ultimately, decentralization creates legal challenges. For example, GDPR did not contemplate data on distributed ledgers, bringing privacy questions to the fore. Illegal trade is facilitated by pseudonymous money that can be transmitted at distance without an intermediary. And the rise of decentralized autonomous organizations, where governance is executed through code, raises a host of new legal questions.

The rest of the chapter is organized as follows: Sect. 2 covers securities law, Sect. 3 examines the literature around smart contract law, Sect. 4 examines the unique challenges around decentralization, Sect. 5 reviews tax law around cryptocurrencies, Sect. 6 reviews the intersection of blockchains and intellectual property law, and Sect. 7 concludes.

2 Securities Law

The application of securities laws to blockchain tokens is the subject of considerable debate and an active segment of literature. A token is simply a digital wrapper that allows ownership of the asset to be recorded on a distributed ledger. The challenge is that this functional form can endow the holder with any number of rights, therefore, the question of whether a particular token is subject to securities laws often boils down to the specific rights associated with ownership. In this section, we review the foundational framework for securities law in the United States, synthesize literature examining tokenization and securities laws, and cover purported benefits of representing financial securities on-chain as a direction for future research.

We begin by outlining what constitutes a legal security in the United States. After the U.S. equity markets crashed in 1929, Congress began work on a regulatory cleanup that aimed to prevent some of the core problems that occurred during the lead-up to the crash—specifically, speculation and information asymmetry between issuers and investors.

As a result, Congress created the Securities Act of 1933, which defined a number of financial instruments as securities, including stocks, bonds, notes, security futures, participation in profit-sharing agreements, and investment

contracts (15 U.S. Code § 77a The Securities Act of 1933). For the first time, the Securities Act of 1933 provided clarity as to the federal classification of securities, and when securities laws would apply to the sales of these instruments (15 U.S. Code § 77a The Securities Act of 1933). Many of the instruments listed in the Securities Act of 1933 are fairly straightforward, and include clearly defined instruments like stocks and bonds. However, one area that has seen enormous legal discussion, especially as applied to blockchain-based instruments, is the investment contract.

In 1946, the U.S. Supreme Court clarified the classification of an investment contract with a four-prong analysis called the Howey Test, which continues to be utilized today (Securities and Exchange Commission v. W. J. Howey Co., 328 U.S. 293). Under the Howey Test, an investment contract is any contract, transaction, or scheme, whereby a person (1) invests money, (2) in a common enterprise, (3) and is led to reasonably expect profits, (4) derived from the efforts of others (Securities and Exchange Commission v. W. J. Howey Co., 328 U.S. 293).

In April 2019, the SEC offered guidance on the application of the Howey Test to digital assets when it published its Framework for "Investment Contract" Analysis of Digital Assets.[1] In writing the framework, the SEC wanted organizations considering the "offer, sale, or distribution" of a digital asset to apply the Howey Test framework and the SEC's digital asset framework to determine whether securities laws should apply.

However, operationalizing the Howey Test is not a straightforward exercise because tokenized networks contain features not previously contemplated in investment contracts and do not map cleanly to historical precedent and case law. For example, many tokens only endow the holder with the ability to access digital goods or services from the network, and don't contain any cash flow or governance rights. Given the large variation in design of assets on distributed ledgers, several efforts have been made to provide a framework or taxonomy for categorization, notably Rauchs et al. (2018). Additionally, Henderson and Raskin (2018) offer suggestions on how to operationalize Howey in the context of blockchain networks. One idea they advance is the creation of a "Bahamas Test" to determine the degree of decentralization. This builds on the notion that it is possible for an asset to be a *transitory* security; regulated as a security at inception, but subsequently evolve to a degree of decentralization as the network matures to where it no longer constitutes a financial security in the eyes of the SEC and regulatory jurisdiction passes to another body, such as the CFTC.

[1] Available at https://www.sec.gov/files/dlt-framework.pdf.

Drew Hinkes, an attorney focusing on blockchain, proposes four categories of security token offerings.[2] First, security-wrapped ICOs (SICOs) are network assets or utility tokens offered pursuant to registration exemptions so that their offering complies with U.S. or other securities frameworks. Second, tokenized equity or debt securities (TEDs) are traditional securities, like equity or debt securities, issued in digital token form. Third, tokenized asset-backed securities (TABS) are digital tokens that represent an ownership claim against, or ownership share in, an asset such as gold or pool of assets such as a venture capital fund. Finally, Transactional Security Instruments (TSIs) are securities that could be redeemed directly by the issuer for goods and services.

Decentralized network assets are often sold through an Initial Coin Offering (ICO) and existing regulatory approaches to ICOs are covered in Chapter 20 of this handbook, as well as Gurrea-Martínez and Remolina (2018), Park (2018), and Maas (2019). While the debate over applicable law for decentralized networks will likely persist for some time, we note that the legal environment is clearer for the second and third categories in Hinke's taxonomy, where the token is simply a new digital representation of financial securities with which we are already familiar.

In the United States today, securities offerings made to U.S. residents must either be registered with the SEC or exempt under the Securities Act of 1933. Registration with the SEC means the issuer creates a public offering for the security, and the issuer can raise money from both accredited and unaccredited investors. Public registration also carries a number of other benefits, including the ability to publicly advertise the offering, along with immediate trading and liquidity of the registered securities.

Alternatively, issuers can also raise money through a private placement by filing for an exemption under the Securities Act of 1933. Before the JOBS Act was signed into law in 2012 by then-U.S. President Barack Obama, private placement issuers could only raise money from accredited investors. As it relates to natural persons, accredited investors are defined under U.S. securities laws as any natural person whose individual net worth, or joint net worth with that person's spouse, exceeds $1.0M (17 CFR § 230.501). The accredited investor label can also be satisfied by any individual who generated $200k in each of the two most recent years, or enjoys joint income with that person's spouse in excess of $300k in each of the two most recent years, and has a reasonable expectation of reaching that same income level in the current year.

[2] See https://www.coindesk.com/the-security-token-market-needs-better-lingo.

Both the private placement rules and accreditation standards were largely constructed to protect unsophisticated individuals from predatory investment opportunities. In 2012, the JOBS Act created the ability for non-accredited "retail" investors to participate in certain exempt private offerings under Reg D, Reg A+, and Reg CF. While these private exemptions have created new wealth-generating opportunities for nonaccredited investors, in June 2019, the SEC requested public comment on ways to "simplify, harmonize, and improve" the private offering securities exemption framework in the United States ("SEC Seeks Public Comment on Ways to Harmonize Private Securities Offering Exemptions," https://www.sec.gov/news/press-release/2019-97?hootPostID=7526bcf08a34ed3da2c1f335c8e39d1f).

Today, the most common types of private placement exemptions used in digital asset issuances, along with a brief description of their features, are listed below. A more thorough discussion of the exemptions used in tokenized security offerings can be found in Goforth (2019).

Regulation D Rule 506(c) is a registration exemption that provides for an unlimited capital raise, the ability to solicit, along with an exemption from the state "blue sky" securities laws (17 CFR § 230.506(c)). However, the use of this exemption limits the pool of potential investors to accredited investors only, and the issuer must take reasonable steps to verify each investor's accreditation status. In addition, securities offered and sold under Reg D Rule 506(c) cannot be transferred for twelve months, with limited exceptions.

Regulation D Rule 506(b) has similar features to Reg D Rule 506(c) (i.e. unlimited capital raise, twelve-month transfer restrictions), except no general solicitation is allowed to market or advertise the offering, and no accredited investor verification is required, as long as the company has no reason to believe that any investor is not an accredited investor (17 CFR § 230.506(b)). However, Reg D Rule 506(b) does allow up to 35 unaccredited investors to participate in the offering.

Regulation A+, often referred to as the "mini IPO," allows issuers to offer and sell securities pursuant to general solicitation, with no minimum investment, that will be immediately transferable once delivered to the investor (17 CFR § 230.251). Here, securities can be offered and sold to both accredited and unaccredited investors, and the issuer's capital raise can be as much as $20.0M under Reg A + Tier 1 and $50.0M under Reg A + Tier 2. However, drawbacks include a lengthy SEC review and process, audited financial statements in the offering statement, and ongoing annual financial reporting. The first two token-based Reg A + s were approved in July 2019: Blockstack and Props.

Regulation CF, also known as the "crowdfunding exemption," also allows for issuers to offer and sell securities to both accredited and unaccredited investors (17 CFR § 227.100). However, while Reg CF does feature the ability to raise from a diverse investor pool, the issuer's capital raise is capped at $1.07M, securities transfers are restricted for twelve months, and issuers face reporting obligations.

As described above, there are numerous regulatory paths to issue securities on blockchains. A related question is why an issuer would wish to do so. The answer is that utilizing a digital wrapper that allows the asset to trade "on-chain" enables various features that we don't observe in securities today, and raises numerous questions about how securities will evolve. We summarize these briefly below and a more thorough review can be found in McKeon (2018).

24/7 Markets: Today, the major U.S. stock market exchanges open at 9:30 a.m. and close at 4:00 p.m. (EST) on weekdays. Electronic communication networks (ECNs) allow expanded trading hours, but are not accessible by most retail investors. However, the vast majority of trading venues for digital assets like bitcoin operate 24 hours per day, seven days a week. As traditional financial assets like stock and bonds begin to be issued in the form of tokens, a question is whether around-the-clock trading will be the norm, and further, whether that is an optimal outcome. Barclay and Hendershott (2004) report that stock prices after-hours are less efficient than prices during the day and are characterized by large bid-ask spreads. However, Barclay and Hendershott (2003) find that the low trading volume observed during off-hours can facilitate price discovery.

Rapid Settlement: Exchanges like NASDAQ and NYSE can execute trades very quickly, but settling these transfers takes time. In 2017, the SEC adopted a shortened settlement cycle for most broker–dealer transactions to T + 2.[3] Settling transfers of private securities, like LP and LLC interests, can take even longer. When ownership claims are tokenized on a distributed ledger, settlement can occur nearly instantaneously. Standardizing settlement has numerous implications, one of which is cross-border flows. Bekaert (1995) finds that inefficient settlement systems are a friction that creates an indirect barrier to investment, suggesting that tokenization may enhance cross-border investment flows.

Cost Reduction: Ritter (1987) outlines two categories of costs when firms go public—direct costs such as legal and underwriting, and indirect costs such as underpricing. A commonly cited benefit of security tokens are reductions in

[3] See https://www.sec.gov/news/press-release/2017-68-0.

back-office costs associated in the issuance of securities through automation. Additionally, we may see higher utilization of auction processes instead of traditional book building, potentially reducing both underwriting fees and underpricing.

Servicing: After issuance there are ongoing costs around servicing securities that may be reduced through automation. For example, when startups are acquired, reconciling the capitalization table to the underlying purchase agreements and option grants is costly. This problem is exacerbated as companies grow. In 2015, a court ruling required Dole to pay all shareholders, and while 36M shares were outstanding, claims for payments exceeded over 45M shares (Solomon 2017). When ownership claims are tokenized, cap tables can be reconciled in real time by code. In addition, contractual features like liquidation preferences and drag-along rights can be programmed into the security token, allowing managers to more easily run scenario analysis to calculate payoffs under different assumptions.

Looking forward: Eventually, digitally wrapped securities will allow us to build in contractual features that have previously been impossible or costly to execute manually, but become feasible through automated referencing. For example, features that tie voting rights to the duration of ownership could be useful in shaping corporate governance and mitigating managerial myopia. Smart securities will also facilitate bundling additional rights, such as early access rights to products or services for investors.

Further, they will allow unbundling of rights. Voting rights could be sold to activists while retaining cash flow rights. Dividend rights could be unbundled like Treasury STRIPS. And companies will unbundle specific revenue streams and finance them independently. Finally, we will see automated referencing between different layers in the capital stack as complex revenue sharing and payment waterfall agreements become much simpler in this environment (Lippiatt and Oved 2018).

Many of these features are dependent on the ability of computer systems and software to exchange and make use of information (i.e. interoperability). The Internet is a stack of protocols that standardize information (i.e. TCP/IP, SMTP, FTP, SSH, HTTP), however, the systems that regulate the transfer of value in our financial infrastructure lack compatibility. The great promise of applying blockchain protocols to securities and financial infrastructure generally, is that they will impose a set of standards that facilitate greater interoperability across asset classes, across borders, and across investor types.

3 (Smart) Contract Law

A contract is an enforceable agreement that, when violated, allows an injured party to access legal remedies. Building on this, traditional contract law is a remedial institution. Its purpose is not to ensure performance ex ante, but to resolve the wrongs that might arise ex post (Werbach and Cornell 2017).

Traditionally, it's been assumed that contractual agreements must always require the backing of a legal system. However, recent developments in technology have led some to speculate that smart contracts could one day displace contract law (Tapscott and Tapscott 2016), while others argue that smart contracts have little to do with legal contracts (Werbach and Cornell 2017), and/or represent an alternative to the legal system (Savelyev 2017). In this section, we examine the intersection of smart contracts and contract law.

A contract's terms and conditions are interpreted by each party to the contract, however, if a disagreement arises, third parties can be utilized to interpret and enforce the contract's terms. For example, a judge can interpret a disputed contract's conditions, and a local sheriff can enforce the judge's interpretation. Smart contracts are different because execution is automated. The smart contract itself has dominion and control over the physical or digital objects needed to effect execution (Raskin 2017).

The term "smart contract" was coined by Szabo (1996) who defines them as "a set of promises, specified in digital form, including protocols within which the parties perform on these promises." He points to a vending machine as a legacy example of a smart contract, in that it has control over the objects in the transaction and can effect the transaction automatically by issuing an unopened drink, so long as money is inserted into the machine.

Recently, automatic execution is often ensured through a computer running code that has translated legal prose into an executable program. A more advanced example might be a car that has a program installed to prevent ignition if the terms of a debt contract are not satisfied (Raskin 2017).

Although smart contracts were functioning prior to blockchains, they have gained substantial awareness in recent years as blockchains such as Ethereum have emerged as "smart contract platforms." There are three features of blockchains that have led to this rise in smart contracts: (i) acting as a source of truth, (ii) dominion over payment mechanisms, and (iii) ease of deployment through interoperability.

"A blockchain is a general-purpose technology for trusted transactions" (Werbach and Cornell 2017). Blockchains aim to solve the problem of establishing a consensus of information without relying on a single party. How might blockchains and smart contracts work together? The terms of a

contract, and the state of facts relating to the performance of a contract, can be programmed as information within a blockchain to leverage these same truth-verifying benefits (Raskin 2017).

Automation ensures performance, for better or worse, by removing human discretion from contract execution. In addition, blockchains can trustlessly verify that contract's execution. For example, if thousands of nodes on a decentralized network verify that Derek paid Steve $50 on August 13th at 3:30 PM, one can assume this occurred with a high degree of certainty (Raskin 2017). This is the power of smart contracts and blockchains working in concert, and these smart contracts can be executed with astonishing speed (Wright and De Filippi 2015).

Szabo (1997) points to the cost of breach as a defining feature of smart contracts. Strong smart contracts have prohibitive costs of revocation and modification, while weak smart contracts do not. This extends not only to the parties engaged in the transaction, but to third parties as well. For example, if a court is able to alter a smart contract after it has been executed with relative ease, then it's a weak smart contract. But if the cost of modifying the contract is so high so as to prevent third-party interference, then it's considered a strong smart contract (Raskin 2017). The cost of breach and modification is an important consideration because smart contracts lose some of their core benefits and efficiency if they can be changed easily by an outside third party.

With traditional contracts, executing a contract can be a rigorous process involving numerous intermediaries, which increases the inefficiency of execution. For example, when you buy or sell real property, you might have brokers, attorneys, deed companies, and lenders. In these types of scenarios, the interests of all involved parties must be efficiently organized through contractual agreements.

Smart contracts aim to eliminate some of these inefficiencies by embedding contracted conditions into code. Algorithmic enforcement of a smart contract allows conditions to be executed as quickly and cheaply as other computer code (Werbach and Cornell 2017). Cost savings occur at each stage, from negotiation to enforcement, and potentially replace judicial enforcement with an automated mechanism (Werbach and Cornell 2017).

In the context of a debt instrument like a bond, a smart contract can automate the payment of interest to each investor on pre-specified due dates. In addition, the bond can service itself automatically when triggered by the borrower sending funds to the smart contract. Smart contracts give both the promisor and promisee the ability to encode finality so that parties can organize their behaviors around a bargained-for certainty.

In traditional contracts, ambiguity causes problems. This is observed as far back as Raffles v. Wichelhaus, where a controversy arose over a cotton shipment contract because two different ships named "Peerless" were sailing similar routes but at different times of the year (Raffles v. Wichelhaus, 2 H. & C. 906 (1864)). The contract was deemed unenforceable due to ambiguity. Unlike traditional contract formation, smart contracts that utilize blockchains have the potential to mitigate misunderstandings and mistakes over the terms of an agreement because they explicitly reference a single source of truth.

Although smart contracts enable some desirable features, their enforceability as legal contracts is in question. A variety of challenges exist that we highlight below.

The intent that matters is objective, not subjective, as intent is manifested by the actions of the parties. Thus, a legal contract will exist for a smart contract only if the actions of the parties, judged objectively, manifest an intention that the smart contract is to be legally enforceable (Werbach and Cornell 2017).

Under common law, to objectively demonstrate that a contract has been formed, there must be offer, acceptance, and bargained-for consideration. To constitute a legal offer, smart contract code could simply be posted to a blockchain's ledger, verifiable by any downstream party who attempts to engage with the smart contract's code. To evidence counterparty acceptance of the smart contract, action must be taken to initiate acceptance of that smart contract, such as ceding control over a certain amount of money to the code (Raskin 2017). One question that remains unsettled is whether follow-on contracts that are established autonomously by the first contract are enforceable, as it is not clear that legal intent can be presumed (Giancaspro 2017).

The third element required to constitute a legally enforceable contract is consideration. Courts believe that the mutuality of obligation by both parties, or consideration, distinguishes contracts from gifts, for which parties do not have the same rights of legal enforcement (Raskin p. 322). In the case of smart contracts, consideration can be presented unilaterally, like a vending machine, or bargained-for as in the terms of a loan agreement (Raskin, p. 323).

Once a legally enforceable contract has been formed, a common law contract can either be performed, modified, or breached by a party to the contract. Because smart contracts have the ability to automate execution of agreed-upon conditions, some might argue that the risk of smart contract breach is significantly mitigated. In this way, performance of a smart contract's conditionals can be relied upon with greater certainty than traditional contracts due to its automated status.

However, one potential problem that could arise is imperfect, but substantial, performance of a smart contract. In the United States, the common law doctrine of substantial performance permits a contract to be recognized even if the performance does not fully comply with the express terms laid out. (RESTATEMENT (SECOND) OF CONTRACTS 237 cmt. D (1981)). However, execution within smart contracts is often binary and incompatible with partial performance where the outcome was not contemplated and specified by the parties during formation of the smart contract (Raskin 2017).

Assuming a risk of imperfect performance exists, what can parties to a smart contract do in order to fall inside the lines of a legally enforceable contract? One way is by baking in a certain degree of discretion into the terms of the smart contract, or by simply not using a smart contract if discretion is required. Alternatively, the smart contract could be structured to permit arbitration. However, incorporating flexible features into the smart contract will inevitably take away from the decentralization and efficiency that make smart contracts an attractive option to begin with (Werbach and Cornell 2017).

Another potential challenge to smart contract performance is modification of the contract before full performance occurs. Under common law, parties to a contract can modify an otherwise enforceable contract's terms, or be absolved from performance entirely, under certain scenarios. The common law doctrines of impossibility and impracticability are two examples of legal excuse from performance. For example, if a contract becomes illegal after it is formed, parties are typically excused from performance with no remedy for aggrieved parties. With smart contracts, however, automation will typically frustrate any potential for post-formation modification (Raskin 2017).

Another potential issue that might accompany smart contracts is the misalignment of contract performance and contract intent. What happens when the outcomes of a smart contract diverge from the outcomes that contract law demands? In the United States and other common law systems, ex post enforcement is the preferred system of enforcement. An ex post enforcement analysis of smart contract breach might be complicated by examples where smart contracts are followed by the letter of the code, but not necessarily by the spirit of the code.

Smart contracts often operate in tandem. For example, a Decentralized Autonomous Organization (DAO), is a type of firm that utilizes smart contracts to execute its corporate governance. DAOs are discussed in more detail in Section IV.c. of this chapter, but we note here that in DAOs, the rules of management are typically predetermined. In 2016, a smart contract called "The DAO" was formed on Ethereum, a public blockchain and funded with $150 million by numerous participants. The intention was to function

as a venture capital fund. However, shortly after the money was raised, $40 million was siphoned from the pool by a hacker who used the smart contract in an unanticipated way.

In the case of The DAO, the thief's engagement with the smart contract was orthogonal to the intent of the contract. If legal remedies were pursued, the common law requirement that each party demonstrate an "objective intent" to enter into an agreement would likely not be satisfied, as the terms being agreed upon by the thief were materially different than the terms being offered by The DAO. As a result, The DAO's smart contract would fall outside of contract law, and The DAO would have no access to legal remedies through a breach of contract argument.

A related issue highlighted by The DAO is that the parties were anonymous. This raises the question as to whether they had the legal capacity to enter a contract. For example, in the United States and numerous other countries, individuals under the age of 18 lack the legal capacity to enter contracts (Giancaspro 2017). This suggests some form of digital ID validating capacity will need to be tied to smart contracts in order for them to be legally enforceable.

Smart contracts are just one piece of a larger trend of technology disrupting human engagement and decision-making. However, as might be clear by the summary above, the introduction of automation into historically judgment-laden fields will create challenges for legal and practical accountability. These challenges notwithstanding, contract law is resilient, and it may evolve as a result of these new technological challenges (Werbach and Cornell 2017).

4 Decentralization Poses Unique Legal Challenges

Although there is little new legislation that addresses distributed ledgers directly, their use raises a variety of challenges and potential sources of liability under existing laws (Zetzsche et al. 2018). For example, Walch (2019) examines whether software developers should be treated as fiduciaries. In this section, we review two areas where substantial questions remain unanswered: data privacy and decentralized autonomous organizations.

4.1 Blockchains and Laws Around Data Privacy

As the world becomes increasingly awash in data, a burgeoning segment of law addresses data privacy. Of particular note is the European Union's

General Data Protection Regulation (GDPR). Finck (2018) addresses how blockchains present a challenge to GDPR as they are currently constructed, and what solutions to the challenge might look like moving forward.

GDPR contains four principles with respect to personal data:

1. Data minimization
2. The right to amendment
3. The right to access
4. The right to be forgotten

Each of these principles is challenging in the context of blockchains in part because resistance to censorship and immutability of data is a defining feature of blockchains.

The GDPR requires full anonymization before data is no longer considered to be personal data. With regard to blockchains, Finck notes that this means that pseudonymous data, even if it is encrypted or subject to a hashing process, continues to be classified as personal data and therefore subject to GDPR.

If data on blockchains is personal data and therefore subject to GDPR, then data controllers are compelled to comply. In centralized systems, which is what the authors of GDPR had in mind, data controllers are easy to identify and hold accountable. Examples include companies such as Facebook or Google.

However, in blockchain networks, there is no centralized data controller. Rather, data is processed by all nodes on the network, which can number in the thousands. Further, even if all the owners of nodes could be identified (a near impossibility for large networks), they are typically spread out across the globe. Processing of personal data in foreign countries is potentially a further violation of GDPR, however, enforcing compliance on a decentralized network of nodes is infeasible. Finck therefore concludes that many blockchain networks that exist today are fundamentally at odds with GDPR.

Although blockchains and GDPR appear to be incompatible, Finck points to a number of possible solutions. For example, courts could declare that hashed data is adequately anonymized. However, the more likely near term solutions are technical in nature. Cryptocurrencies focused on privacy such as Z-cash and Monero have pioneered application of zero-knowledge proofs and ring signatures, respectively. Zero-knowledge proofs allow verification of transactions without revealing details of the transaction. Ring signatures obfuscate transaction details by tying multiple keys together making it impossible to determine which one was used by the sender. In sum, blockchains

have great promise for portability and although they are currently incompatible with privacy, there is hope that this challenge is surmountable in time.

4.2 Illegal Trade

The pseudonymous feature of Bitcoin and other cryptocurrencies gives rise to their use in illegal transactions. While most of this chapter focuses on legal interpretation of blockchains, we briefly review the literature on the use of blockchain-based assets for illegal trade.

Perhaps the first large-scale use case for Bitcoin was as a payment method on Silk Road, a marketplace for black market goods. Prior to 2013, when the U.S. government shut down Silk Road, some (disputed) reports suggest it accounted for up to half of all Bitcoin transactions (Yermack 2017).

More recently, as Bitcoin has gained mainstream adoption, the proportion of illegal trade has declined. Moreover, Rogoff (2016) and Harvey (2014) both point out that cash, particularly the US $100 bill, is used much more commonly in illegal trade and Harvey suggests that the idea that Bitcoin is mainly used for criminal activity is a myth.

One of the obvious differences between cash and cryptocurrencies is that cash requires physical delivery while cryptocurrency can be transacted at distance. Most regulated forms of electronic cash such as PayPal require real word identification and are therefore less than ideal for illegal transactions. Marketplaces for contraband exist on the darknet, which is beyond the scope of this chapter, but we point the reader to Van Slobbe (2016) for a more detailed description.

Foley et al. (2019) offer a comprehensive account of the methods and scale of cryptocurrency use in illicit trade. The authors use two methods, network cluster analysis (SLM) and detection controlled estimation (DCE), to classify bitcoin users into primarily legal/illegal activity. Using these classifications, they report that illicit users account for about one-quarter of total users and account for approximately 20% of the U.S. dollar volume of transactions. The figures reported in Foley et al. (2019) are substantially higher than those found in other studies such as Soska and Christin (2015) and Meiklejohn et al. (2013).

Bad actors engaging in illegal trade and money laundering using bitcoin impose a negative externality on law abiding members of the cryptocurrency community. For example, obtaining a banking relationship is notoriously

difficult for many firms in the ecosystem.[4] One of the primary concerns for banks is identifying the source of funds for the depositor, which can prove challenging for firms that trade in Bitcoin, for example, a spot exchange. However, the transparency offered by the Bitcoin ledger allows some analysis to be done on the wallets through which the coins have passed. Firms such as Chainalysis, Elliptic, and Elementus offer products to financial institutions that look back through the ledger history of coins that are deposited to create a risk assessment of nefarious activities. We note that this type of analysis is impossible with cash, and illustrates why distributed transaction ledgers may ultimately be one of the most potent tools available to regulators.

4.3 Legal Considerations Around Decentralized Autonomous Organizations (DAOs)

> It is important to recognize that most organizations are simply legal fictions which serve as a nexus for a set of contracting relationships among individuals.—Jensen and Meckling (1976)

One of the more fascinating concepts that blockchain enables is that of a decentralized autonomous organization (DAO). A DAO is an organization where the firm's resources are controlled through the use of one or more smart contracts. Ownership, actions, and value flows in a DAO are strictly dictated by the terms set forth in code. A DAO is a nexus of smart contracts.

This organizational form raises a number of legal questions, for example: jurisdiction. If the organization lives entirely in the cloud, where all interactions are executed peer-to-peer by software, it is not clear what set of laws may apply. Many observers point to the location of the owners, which means many different sets of laws may apply simultaneously, but also gives rise to the problem that identity may be shielded, so enforcement becomes very difficult.

The most famous DAO was simply called "The DAO." It was to function as a decentralized venture capital fund, where investors could contribute value in the form of ether to a pool, nominate recipients, and vote on the deployment of funds. The pool grew to over USD$150 million is less than a month. Before The DAO became operational, a bug in the software allowed hackers to drain a meaningful portion of the fund, resulting in a hard fork to roll back the transactions and recover the assets. Detailed discussion of the

[4] See https://www.wsj.com/articles/lack-of-banking-options-a-big-problem-for-crypto-businesses-11558092600.

fork is outside the scope of this chapter, but the relevant fact is that The DAO never went live. From a legal perspective, the SEC later went on to advise that if it had gone live, The DAO tokens would have constituted securities under U.S. law. The question is: upon whom can the SEC impose enforcement? The DAO itself is simply computer code, with no physical address and it did not register with regulators in any nation. This raises the question of how U.S. courts would view the legal organization form of a DAO.

Metjahic (2017) holds that the most appropriate legal form that would have been applied to The DAO is a general partnership, as defined by the Uniform Partnership Act (UPA). When the investors purchased the tokens, in exchange for ether, the tokens granted them proportional cash flow and voting rights, indicating the intention to carry on a business for profit. The transparency of the smart contracts suggests that the investors knew or should have known that they shared a common interest with other investors. Of note is the fact that if all token holders are general partners, they do not have the limitation in liability afforded by other forms of legal organization.

If The DAO was not deemed to be a general partnership, Metjahic (2017) points to a Joint Venture as the next most likely determination. Joint ventures share many attributes with partnerships, but are often interpreted as more limited in duration and purpose. As with partnerships, the existence of a formal agreement is not required as one of the tests that determines this legal status.

Ultimately, DAOs fit somewhere "between an informal online group and a more formalized corporate entity" (Wright and De Filippi 2015, p. 32). Membership may be as fluid as an online group of content creators, and DAO participants will likely include machines in addition to humans. These new dynamics raise new legal questions and may generate a new body of law specific to this new ecosystem. Just as the customs and practices of merchants in Europe developed into *Lex Mercatoria* several centuries ago, and ground rules established at the advent of the Internet formed the basis of *Lex Informatica*, Wright and De Filippi (2015) posit that we are at the dawn of *Lex Cryptographia*.

5 Tax Law and Cryptocurrencies

How cryptocurrencies should be taxed has generated substantial debate and uncertainty for market participants (Lerer 2019). In this section, we review relevant literature on blockchains and tax law.

5.1 Bitcoin as Property

In 2014, the Internal Revenue Service (IRS) in the United States issued Notice 2014–21 providing guidance that virtual currencies should be treated as property, not currency, for the purposes of tax reporting.[5] This treatment has important implications for economic transactions. Weekley (2018) states "The Commissioner's Treatment of Bitcoin as property will discourage people from using them in a trade or business." The friction most often cited is reporting of capital gains and losses. When bitcoin is used to purchase goods and services, the transaction is effectively treated as selling property. Since the exchange rate between fiat currencies like the U.S. Dollar and virtual currencies, like bitcoin, are constantly fluctuating, it means that the price at which one acquired the virtual currency is almost certain to be different than the prevailing market price at the moment of a subsequent transaction. The implication is that purchasing items as trivial as a cup of coffee will trigger a taxable gain or loss. To complicate the matter further, bitcoins are divisible to eight decimal places, so a transaction could contain fractions of many different bitcoins, each with a different basis.

One solution is a *de minimis* exception, which relieves the taxpayer from reporting gains on small transactions. This exception already exists in the U.S. tax code for small gains on foreign fiat currencies. In 2017, Rep. David Schweikert introduced H.R. 3708: "To amend the Internal Revenue Code of 1986 to exclude from gross income de minimis gains from certain sales or exchanges of virtual currency, and for other purposes." It was referred to the House Ways and Means Committee, but has not been voted on as of this writing. An alternative solution is proposed by Weekley (2018), who suggests cryptocurrencies should be treated like frequent flyer miles.

Finally, while the de minimis exemption addresses taxation issues around the purchase of goods and services, a related but separate tax issue arises when one cryptocurrency is exchanged for another, for example, trading bitcoin for ether. Currently, this triggers a gain or loss, which is taxable. However, some observers suggest it should be treated similarly to when an investor sells a piece of real estate and rolls the capital into another real estate investment, that is, it should be treated as a 1031 like-kind exchange. In December 2018, Rep. Ted Budd introduced H.R 7361 (Virtual Value Tax Fix of 2018). As per this bill, gains on crypto to crypto exchanges can be tax deferred as per the Section 1031 of the "Internal Revenue Code Tax Cuts and Jobs Act." Since a

[5] IRS guidance: https://www.irs.gov/pub/irs-drop/n-14-21.pdf.

token can represent any asset, a challenge that remains with this approach is determining with more specificity what assets would be eligible.

5.2 Hard Forks

One of the most interesting aspects of cryptocurrency tax law from an academic standpoint is the treatment of "hard forks." A hard fork refers to instances where a group of developers creates a new version of a virtual currency by making a change to an existing protocol. The result is that the owner now has the asset on the original chain, as well as rights to assets on the new chain. These events are also known as chain splits. An example is that of Bitcoin and Bitcoin Cash. A segment of the Bitcoin community felt that certain changes were needed to the Bitcoin protocol, but they were unable to rally enough support to make the changes. Therefore, they created a new asset, called "Bitcoin Cash," through a hard fork. A user's wallet that held 3.5 bitcoin prior to the fork still has 3.5 bitcoin after the fork, but now also contains 3.5 bitcoin cash.

Many readers will immediately recognize the similarities to corporate spin-offs, which are not taxable events, however, there are some important differences. First, a fork requires no consent from participants on the original blockchain or the taxpayer, it is created independently and unilaterally by a third party. That said, relevant case law around "treasure troves," which are sudden and unexpected windfalls for which the taxpayer bears no responsibility, suggests that taxpayers could be responsible for income taxes on forks even if their receipt is completely passive. Second, a public market may not exist for the new asset on the day it is created—an exchange must be convinced to list it—and therefore there is no price discovery to use for tax reporting.

Several recent papers examine the tax treatment of hard forks including Landoni and Pieters (2019), Webb (2018), and Xu (2018). Webb points to the 1955 Supreme Court case *Commissioner v. Glenshaw Glass Co*. where the court defined income to include:

1. instances of undeniable accessions to wealth,
2. clearly realized,
3. over which taxpayers have complete dominion.

Glenshaw does not provide clarity on cryptocurrency hard forks, because each of these three points is in question. Extreme price volatility and illiquidity may impact the degree to which accession to wealth is undeniable. Further,

clear realization and dominion are affected by where the user stores the assets. For example, many exchanges did not support the Bitcoin Cash hard fork, so there was no way for their clients to claim the new assets even if they held bitcoin in their account at the time of the fork.

Xu (2018) points toward some proposals on how to treat hard forks. The American Bar Association (ABA) submitted a comment letter suggesting a safe harbor for 2017 whereby the fork is treated as a taxable event, but with a basis of 0, thereby deferring any tax payments until the asset is sold. This is similar to the way Japan treats hard forks. The Association of International Certified Professional Accountants (AICPA) suggests that taxpayers be allowed to make an election within 30 days of the fork, pay income taxes on the value in the election, and capital gains taxes would be applicable thereafter. Alternatively, if no election is made, all gains would be subject to income taxes when the asset is sold.

One of the most thorough analyses of the tax implications of chain splits to date is Landoni and Pieters (2019), in part because it went to press following the IRS Revenue Ruling 19–24 in October 2019. They identify several tax-related challenges that chain splits impose: parent/child designation (uncertainty regarding which is the continuation of the "original" chain), token access, and issues around fair market value. The challenges impact both determination of basis and timing of income. Landoni and Pieters assess the pros and cons of three frameworks to address chain splits: treasure trove, asset split, and calving. They conclude that calving, whereby the new coin is considered an offspring of the existing coin, assigned zero basis, and taxed upon sale, is the least problematic.

6 Intellectual Property Law

Regulators and legislators have long attempted to balance fairness, efficiency, social benefit, and commerciality as it relates to the ownership interests of individuals. A common legal theme throughout history has been to reward people for creating novel work by providing them a right to exclude others from deriving benefits without approval. As it relates to intangible property, intellectual property law emerged as a legal framework designed to prevent the dissemination of unauthorized reproduction that has the potential to erode a work's commerciality (Zeilinger 2018).

6.1 Efficient Global Registration

In civil law, while copyright is typically granted upon the creation of work, other IP rights like patents or trademarks must be codified through a registration process. The process of registration for a right in intellectual property is typically complex, costly, requires a number of intermediaries, and only enables the IP holder to the rights in the registered country. Blockchains, and the technological benefits that come with using distributed ledger technology, has the potential to unlock a number of new benefits by making the registration process easier, faster, and cost-effective. In addition, the global nature of blockchain may also help overcome the issues surrounding different registration requirements across the world (Gürkaynak et al. 2018).

6.2 Provenance

Today, works in digital form are easy to download, copy, modify, and recirculate—potentially diminishing the commercial value of the intellectual property. Using an asset-aware blockchain like the open-source Ravencoin (RVN) project, intangible work could simply be ascribed to a blockchain's ledger, immutably recording its existence along with details of its provenance, value, and history. Once written to a blockchain, an authorized copy of the work could be identified as the original, and all other copies could be approved or prevented by the IP holder to circulate (Zeilinger 2018).

6.3 Preventing Counterfeit

For a work's commercial benefits to flow efficiently to a rights holder, the rights holder must be able to enforce his or her rights effectively (Gürkaynak et al. 2018). Since blockchains store all transactions across a shared database, distributed ledger technology has been identified as a promising solution in the prevention of counterfeit. The complex cryptography powering a blockchain empowers its immutability, irreversibility, and permanency. These benefits better allow individuals to track the ownership rights of their intangible property. In fact, there are several initiatives being developed today from firms like IBM that aim to better prevent counterfeiting (Pun et al. 2018). These blockchain-based solutions could play a critical role in enforcing IP rights in the future.

6.4 Challenges—First-Sale Doctrine

Implementing a blockchain-based system for IP law won't come without its challenges. It will require legislators and regulators to grant legal status to blockchains, develop acceptable legal standards for blockchain-based IP, and create efficient technological environments that best empower tracking and managing blockchain-based IP.

In addition, there are also a number of inherent conflicts that exist between existing laws and a new blockchain-based paradigm. For example, 17 USC §109(a), called the "first sale doctrine," provides that the owner of a physical copy is entitled, without the authority of the copyright owner, to sell or otherwise dispose of the possession of that physical copy (17 USC §109(a)). Under this doctrine, a lawful owner of paintings, books, music albums, and memorabilia would be permitted to sell that physical copy without the express permission of the copyright owner (Fisher 2019).

However, digital copies are typically treated differently than physical copies under U.S. copyright's first-sale doctrine. In 2001, the U.S. Copyright Office published an opinion stating that a digital first sale right could not exist. In *Capitol Records LLC v. ReDigi Inc.*, the Second Circuit affirmed the U.S. Copyright Office's opinion and found that because it was impossible to transfer a digital file without making a copy, a transfer would be subject to a copyright owner's ongoing commercial reproduction right of digital work, as opposed to a copyright owner's distribution right of physical work (Fisher 2019). Under current U.S. law, the first-sale doctrine maintains that a work be tangible or physical in order to be relied upon.

Blockchain-based copyrights have the potential to blur these legal lines. NFTs, or non-fungible tokens, represent unique, authenticated, digitally scarce blockchain tokens. In addition to these digitally scarce tokens, smart contracts have the potential to create transferability controls on public blockchains like Ethereum. Under a blockchain paradigm, a digitally unique and scarce blockchain NFT has the potential to be transferred without resulting in a new copy, raising important new legal questions as to the legal definitions of "digital" and "physical" (Fisher 2019). This is one example of the types of legal issues that may arise as IP laws intersect with distributed ledger technology.

7 Concluding Remarks

At the most fundamental level, blockchains are a ledger of time-stamped transactions. Since there exist myriad types of transactions, or events, that might be recorded, there are numerous intersections with the legal and regulatory environment.

In this chapter, we scratch the surface of several of these intersections such as securities law, contract law, IP law, and tax law. However, as the types of information recorded on-chain expands, one could imagine an expansion of the law literature on this topic as well to areas like employment law, estate law, bankruptcy law, and perhaps even medical malpractice law. Ultimately, we expect the norms and customs that are being developed in these ecosystems to build the foundation of a new body of body, which Wright and De Filippi (2015) term *Lex Cryptographia*.

Although Bitcoin just passed 10 years old, we are still in the infancy of distributed ledgers. As the technology continues to advance, new use cases will emerge and adoption will continue to increase. While this unfolds, there will be substantial opportunities for additional scholarship at the intersection of blockchains and law.

Acknowledgements We thank Cameron Pfiffer and Clayton McDonald for research assistance.

References

Barclay, Michael J., and Terrence Hendershott. 2003. Price discovery and trading after hours. *The Review of Financial Studies* 16: 1041–1073.

Barclay, Michael J., and Terrence Hendershott. 2004. Liquidity externalities and adverse selection: Evidence from trading after hours. *The Journal of Finance* 59: 681–710.

Bekaert, G. 1995. Market integration and investment barriers in emerging equity markets. *World Bank Economic Review* 9: 75–107.

Finck, M. 2018. Blockchains and data protection in the European Union. *European Data Protection Law Review* 4: 17–35.

Fisher, Katya. 2019. Once Upon a Time in NFT: Blockchain, Copyright, and the Right of First Sale Doctrine. *Cardozo Arts & Entertainment Law Journal* 37: 629.

Foley, Sean, Jonathan R. Karlsen, and T.ālis J. Putniņš. 2019. Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? *The Review of Financial Studies* 32: 1798–1853.

Giancaspro, M. 2017. Is a 'smart contract' really a smart idea? Insights from a legal perspective. *Computer Law & Security Review* 33: 825–835.
Goforth, Carol R. 2019. Securities treatment of Tokenized offerings under U.S. Law. *Pepperdine Law Review* 45: 405–470.
Gürkaynak, Gönenç, İlay Yılmaz, Burak Yeşilaltay, and Berk Bengi. 2018. Intellectual property law and practice in the blockchain realm. *Computer Law and Security Review* 34: 847–862.
Gurrea-Martínez, Aurelio and Nydia Remolina. 2018. The Law and finance of initial coin offerings. Ibero-American Institute for Law and Finance Working Paper No. 4/2018.
Harvey, Campbell R. 2014. Bitcoin myths and facts. https://dx.doi.org/10.2139/ssrn.2479670.
Henderson, M. Todd, and Max Raskin. 2018. A Regulatory classification of digital assets: Towards an operational howey test for cryptocurrencies, ICOs, and other digital assets. *Columbia Business Law Review*, Forthcoming.
Jensen, M.C., and W.H. Meckling. 1976. Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics* 3: 305–360.
Landoni, Mattia, and Gina C. Pieters. 2019. Taxing Blockchain Forks. Available at SSRN: https://ssrn.com/abstract=3475598.
Lerer, M. 2019. The taxation of cryptocurrency. Virtual transactions bring real-life tax implications. *The CPA Journal*. Retrieved from https://www.cpajournal.com/2019/01/24/the-taxation-of-cryptocurrency/.
Lippiatt, Todd, and Michael Oved. 2018. The two token waterfall, Retrieved from: https://www.tokenframework.io.
Maas, Thijs. 2019. Initial coin offerings: When are tokens securities in the EU and US? (February 13, 2019). Available at SSRN: https://ssrn.com/abstract=3337514 or https://dx.doi.org/10.2139/ssrn.3337514.
McKeon, Stephen. 2018. The security token thesis. Retrieved from https://medium.com/hackernoon/the-security-token-thesis-4c5904761063.
Meiklejohn, S., M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G.M. Voelker, and S. Savage. 2013. October. A fistful of bitcoins: Characterizing payments among men with no names. In Proceedings of the 2013 conference on Internet measurement conference, 127–140.
Metjahic, L. 2017. Deconstructing the DAO: The need for legal recognition and the application of securities laws to decentralized organizations. *Cardozo Law Review* 39: 1533–1568.
Park, James J. 2018. When are tokens securities? Some questions from the perplexed. Lowell Milken Institute Policy Report (December 10); UCLA School of Law, Law-Econ Research Paper No. 18–13. Available at SSRN: https://ssrn.com/abstract=3298965.
Pun, Hubert, Jayashankar M. Swaminathan, and Pengwen Hou. 2018. Blockchain adoption for combating deceptive counterfeits. Kenan Institute of Private Enterprise Research Paper No. 18–18. Available at SSRN: https://ssrn.com/abstract=3223656.

Raskin, M. 2017. The law and legality of smart contracts. *Georgetown Law Technology Review* 1: 305–341.

Rauchs, M., A. Glidden, B. Gordon, G.C. Pieters, M. Recanatini, F. Rostand, K. Vagneur, and B.Z. Zhang. 2018. Distributed ledger technology systems: A conceptual framework.

Ritter, J.R. 1987. The costs of going public. *Journal of Financial Economics* 19: 269–281.

Rogoff, K. 2016. *The Curse of Cash*. Princeton, NJ: Princeton University Press.

Savelyev, A. 2017. Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law. *Information & Communications Technology Law* 26 (2): 116–134.

Solomon, Steven Davidoff. 2017. Dole Case Illustrates Problems in Shareholder System. *New York Times.*

Soska, K., and N. Christin. 2015. Measuring the longitudinal evolution of the online anonymous marketplace ecosystem. In 24th {USENIX} Security Symposium ({USENIX} Security 15, pp. 33–48.

Szabo, Nick. 1996. Smart contracts: Building blocks for digital markets, U. AMSTERDAM, https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.netsmartcontracts_2.html.

Szabo, Nick. 1997. Formalizing and securing relationships on public networks. *First Monday*, 2. https://firstmonday.org/ojs/index.php/fm/article/view/548/469.

Tapscott, Don, and Alex Tapscott. 2016. *Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world*. Penguin.

Van Slobbe, J. 2016. The drug trade on the deep web: A law enforcement perspective, In *Internet and Drug Markets*, EMCDDA Insights.

Walch, Angela. 2019. In Code(rs) We Trust: Software developers as fiduciaries in public Blockchains. regulating Blockchain. *Techno-Social and Legal Challenges*, edited by Philipp Hacker, Ioannis Lianos, Georgios Dimitropoulos & Stefan Eich, Oxford University Press, Forthcoming.

Webb, N. 2018. A fork in the Blockchain: Income tax and the bitcoin/bitcoin cash hard fork. *North Carolina Journal of Law & Technology* 19: 283–311.

Weekley, Roland. 2018. The Problematic Tax Treatment of Cryptocurrencies. *Florida State University Business Review* 17: 109.

Werbach, K., and N. Cornell. 2017. Contracts ex machina. *Duke Law Journal* 67: 313–381.

Wright, A., and De Filippi, P., 2015. Decentralized blockchain technology and the rise of lex cryptographia. Available at SSRN 2580664.

Xu, D. 2018. Free money, but not tax-free: A proposal for the tax treatment of cryptocurrency hard forks. *Fordham Law Review* 87: 2693.

Yermack, D. 2017. Corporate governance and blockchains. *Review of Finance* 21: 7–31.

Zeilinger, M. 2018. Digital art as 'monetised graphics': Enforcing intellectual property on the blockchain. *Philosophy & Technology* 31: 15–41.

Zetzsche, D.A., R.P. Buckley, and D.W. Arner. 2018. The distributed liability of distributed ledgers: Legal risks of blockchain. *University of Illinois Law Review*, 1361–1406.