Nihad Mukhtarli,

II study year, International and European Law Programme Student

Master's Thesis

The Use of Blokchain Technology in The Formation and Enforcement of Contracts

Blokų grandinės technologijos naudojimas sudarant ir vykdant sutartis

Supervisor: Asist. dr. Victor Terekhov

Reviewer: Lekt. dr. Stasys Drazdauskas

Vilnius

2024

Abstract and Key Words

Today, the development of technologies creates a certain level of impact in every sector that comes into contact with humans. With the widespread use of Information and Communication Technologies (ICT), it has become possible to process data quickly, efficiently and store it for a long time through automated systems. New computer technologies have initiated digitalization processes in many areas of life. Every field of law has begun to get its share of these innovations. Over the past few years, there have been numerous advancements in the subject of blockchain and the law, and it is likely that these changes will continue. However, the core of the subject the legal ramifications and effects of the increasing adoption of blockchain-based technologies and their applications, like crypto and smart contracts runs the risk of being somewhat lost due to the seemingly endless stream of publications and ongoing developments in the blockchain and crypto markets. It examines the key characteristics of both the blockchain and the law, examining their relationships and how new developments should be implemented while remaining true to the promise and capabilities of the technology and the role of the law as the primary instrument for social order.

Key Words: Blokchain and Contracts, Technology Law, Digital Contracts, Decentralzied Systems, Legal Recognition of Blockchain Contracts.

Table of Contents

Introduction

In the initial quarter of 2021, Bitcoin, Ethereum, and nearly all other cryptocurrency assets achieved unprecedented price levels, signaling the onset of a new bull market. Proponents praised the price increase, crediting it to the increasing adoption of cryptocurrency and blockchain technologies by a diverse range of entities, including firms like Tesla and MicroStrategy, traditional financial institutions such as banks, and even nations like Ethiopia. Approximately four years following the previous bull market and the conclusion of the "hype cycle" surrounding blockchain, 2021 appeared to be the year when the technology would begin to thrive. Proponents assert that its achievement would signify the onset of a new era in the digitalization of value exchanges.(Kapasi 2021; Spilka 2021.)

Paradoxically, another cryptocurrency-related phenomenon reached its zenith during the challenging years of the bear market, approximately from early 2018 to late 2020, assuming one delineates the historical boundaries accurately. The emergence of the crypto-economy has prompted a vigorous and focused domain of publishing and study concerning cryptocurrencies and blockchain technology. Legal academia was similarly affected. A multitude of articles, books, theses, reports, and working papers were produced on the subject. Extensive and well-attended blockchain conferences were conducted, and new specialist publications were established. "Observatories and working groups were founded, research projects initiated, alliances formed, and courses launched at prominent universities. Within around three years, the subject of blockchain and the law had a substantial surge, evolving into a distinct domain of legal education and scholarship.(The EU Blockchain Observatory and Forum)

It is common for legal scholars and attorneys to follow technological advancements anytime they are sufficiently novel to significantly alter human interactions. But none could have foreseen how rapidly and intensely the field of blockchain and legal studies would expand. With great enthusiasm, legal experts embraced and began studying blockchain, a new technology that offers a new way to establish communities, organizations, and economies. Based on sound and thought-provoking ideas like decentralization, smart contracts, and digital currency, blockchain and distributed ledger technology appeared to usher in a new era of societal disruption. Even though adoption was slow, the promise of blockchain technology to digitize value and its allure were so compelling that two of the movement's most well-known authors chose to create a term to characterize the new legal system that would address the advancements of blockchain technology developments that, in their opinion, "traditional" law was unable to address. The new, "revolutionary" law known as "Lex cryptographica" was supposed to address autonomous organizations (idem), automated contracts (whatever they were), and the nascent token economy.(De Fillipi and Wright 2018, 5–9.)

it always appeared that the justifications for blockchain's uniqueness as a social phenomena and its "revolutionary" legal nature veered more toward philosophical conjecture than logic. It is undeniable that the blockchain phenomenon presents difficulties for the way the law

operates, notwithstanding its intricacies and ambiguities.(EU Blockchain Observatory and Forum.) It's also true that conventional legal remedies might not be the best or even the only way to address blockchain and its problems.

Nonetheless, the law constitutes a multifaceted reality, comprising regulations and their enforcement, values, and societal perceptions, as well as its political dimensions. The principles and concepts regulating legal relations, along with its methodology and ideology, are as ancient as human existence. The law is, in this context, the fundamental legacy institution. Legal terminology and principles have developed in tandem with our technological advancements. The law is an inescapable phenomena of social order and authority. Therefore, I contend that the legal difficulties posed by blockchain technology are neither entirely "revolutionary" nor "innovative" from a legal and philosophical standpoint, and most can be summarized and addressed within the frameworks of contract and responsibility. Other circumstances must be addressed with imaginative solutions that honor the technology's purpose and structure, as well as its beneficial advancements. Another inquiry pertains to the ability of state-created legislation and national agencies to successfully implement the regulation of this market.

Aim, Object, and Tasks:

Aim:
The main aim of this research is to explore and provide a comprehensive understanding of the role and impact of blockchain technology in the formation and enforcement of contracts within the global legal framework. The research will focus on how blockchain can transform traditional contract practices, address challenges in enforcement, and analyze the legal implications of its application.

Objectives:
The objectives of this research are as follows:

1. To identify key features of blockchain technology that influence its use in contract formation and enforcement.
2. To conduct a historical overview of contract formation methods and assess how blockchain has reshaped these practices.
3. To review existing blockchain-based contract enforcement systems, examining the legal, technical, and practical challenges they face.
4. To forecast potential future developments in blockchain technology that could further enhance the efficiency and security of contract formation and enforcement.

Tasks:
The following questions will guide the research tasks:

1. How does blockchain technology facilitate the formation and enforcement of contracts?
2. What legal frameworks currently govern the use of blockchain in contract formation and enforcement?

3. What challenges and uncertainties exist in the legal recognition of blockchain-based contracts?

Relevance of the Topic:

The use of blockchain technology has emerged as a revolutionary development in various sectors, including contract law. With its ability to provide transparent, immutable, and secure transaction records, blockchain is changing how contracts are formed, executed, and enforced. In today's digital age, the demand for efficiency, security, and automation in legal processes is increasing. Blockchain technology, especially through the use of smart contracts, offers solutions that can reduce human error, increase trust between parties, and automate complex legal processes. This trend is particularly relevant as the world continues to digitize, and legal professionals seek innovative ways to streamline contract practices. The significance of blockchain in transforming the legal landscape is undeniable, and understanding its application in contracts is crucial for the future of legal processes.

Originality of the Research:

Blockchain technology represents a significant shift in how contracts are formed and executed. While traditional contract law has been based on physical documentation and human intermediaries, blockchain offers a decentralized, automated, and secure alternative. What sets this study apart is its focus not only on the challenges posed by blockchain in legal contexts but also on its potential for driving legal innovation. Unlike previous research that has mainly focused on theoretical aspects of blockchain, this study also aims to propose practical solutions for overcoming the barriers to its full integration into the contract law domain.

Methods of the Research:

This study uses a combination of methods to investigate the role of blockchain technology in contract formation and enforcement:

1. Comparative Historical Method:
   This method will be employed to trace the historical evolution of contract law and how technological advancements like blockchain have influenced its development. This analysis will provide insight into the shift from traditional contract methods to blockchain-based solutions.
2. Statistical Analysis Method:
   Statistical data related to blockchain adoption in contract law, including usage rates, industry adoption, and case studies, will be analyzed to identify trends and patterns in the development of blockchain-based contracts.

3. Analytical Method:
   The analytical method will be applied to identify key challenges and uncertainties in the legal recognition and enforcement of blockchain-based contracts. This will include issues such as jurisdiction, data privacy, and regulatory gaps that hinder the widespread adoption of blockchain in contract law. The research will also explore the potential future trajectory of blockchain integration in the legal field, particularly concerning contract formation and enforcement.

   The most important sources:

   In order to achieve the established objectives, the author relies on regional regulatory legal acts and international recommendations. These serve as potential models for globally recognized documents in the future. Notable documents in this context include European Commission, Proposal for a Regulation of The European Parliament and of the Council on Markets in Crypto-assets, and amending Directive. To conduct a thorough investigation and draw specific conclusions, the author examines the works of primary contributors such as De Fillipi and Wright, Hughes, Arvind Narayanan, Joseph Bonneau.

1. The Definition and Characteristics of the Blockchain Technology

Blockchain is primarily a technology: a practical application of scientific findings for human advancement, particularly in industrial contexts. It is a digital technology founded on computer technology, designed for the communication of information or data: “a multi-party system wherein participants achieve consensus regarding a set of shared data and its validity, without a central coordinator.” (Rauchs) Blockchain is a technique for structuring and processing digital data inside a decentralized network of computers.

The most well-known blockchain protocol is Bitcoin. The technological and ideological significance of the Bitcoin protocol should not be overlooked. The majority of what is characterized as blockchain, including its ideas, benefits, issues, and hazards, refers to the characteristics of the Bitcoin protocol. The core premise is well understood: Bitcoin created a method for exchanging value between people via a decentralized peer-to-peer network. The word "decentralized" refers to the fact that there is no middleman between the transaction parties: the process is controlled by the network and its users. Two participants in the network with cryptographic identities agree to trade tokens and broadcast their intentions to the network by signing off on the transaction using their respective cryptographic identities. When a user solves an automatically created puzzle, the network creates a new block and inserts the transaction, which is timestamped and chronologically ordered. When people validate the block inside the chain, the transaction is sealed, and anybody may view the block and verify the contents but not modify it.(Narayanan)

The assertion of decentralization in Bitcoin carries a further, crucial implication: the absence of a governing authority, such as a board of directors. The obscurity of its founder, Satoshi Nakamoto, facilitated the proliferation of Bitcoin and entrusted its governance to the community. This indicates that protocol governance is very contentious, as seen by events such as the SegWit upgrade and the "blocksize wars." This can result in hard forks, a division of the protocol into two segments, where one adheres to the existing rules while the other stays unaltered. Blockchain subsequently evolved to represent a distributed system characterized by decentralization, both in its technological framework and governance structure.

The bulk of subsequent blockchain systems were designed distinctively, despite drawing technical and ideological influence from Bitcoin and Nakamoto. A standardized terminology is employed to differentiate first-generation protocols (mostly Bitcoin) from second-generation (Ethereum) and third-generation (e.g., Cardano, Algorand) protocols.

The second generation of protocols gave rise to the age of "smart contracts," which are programmable digital scripts facilitating the development of applications including programs, protocols, and tokens. The third generation introduced staking, a modification to the consensus method that eliminates reliance on computing energy (as in Bitcoin, the proof of work consensus mechanism) but instead on the quantity of tokens held by network users.

There are more protocols that are accessible through private (anyone can download the protocol and run it, as long as it has sufficient computing power to do so) rather than public channels. (people need permission from the protocol's creators to join the network)

Only the first definition of decentralization applies to protocols of the second and third generations. Its presence is less clear in the second interpretation. The inventors of the protocols are "public" individuals, typically with a strong internet presence and significant business goals, despite the protocols' purported lack of a central formal authority. Private organizations having the financial and human resources to intervene and have an impact on how the protocol is implemented occasionally support protocols. Examples of this impact include the way Justin Sun acquired the Steem protocol and the way the Ethereum foundation backed a hard fork to fix a fault in the code. (Copeland 2020) Therefore, it is unclear that they are as decentralized as aspired from a ruling perspective.
The token, a digital representation of value kept in a user's wallet and registered with the network, was created by the Bitcoin protocol as an incentive. Since the token was intended to be used as a money and a payment method, all protocol tokens were referred to as cryptocurrencies. The token in the crypto economy is both a product that is, the component that adds value to the protocol and an economic incentive for the decentralized consensus process to function.

The value of Bitcoin derives from its function as a currency serving as a payment method, a store of wealth, or a unit of account.Nonetheless, some tokens have distinct purposes. Ether is utilized for storage space and transaction fees inside the Ethereum network; Filecoin allows users to store data via its protocol; Tezos permits holders to participate in governance voting; Ada, when staked in a pool, yields dividends for its holders. Certain tokens signify securities utilized as collateral, provided via public offerings. In summary, tokens signify several value categories, including rights, currencies, contracts, and property. Considering cryptocurrencies just as currencies is insufficient; so, the most appropriate word is crypto assets, due to their diverse utility.

Nonetheless, market practice categorized tokens according on their functionality. This classification has now been embraced by public organizations, notably EU authorities, in implementing the planned Market in Crypto Assets Regulation (MiCA).(European Commission, Proposal for a Regulation of The European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM/2020/593) The traditional functional classification consists of currency tokens (tokens that resemble currencies), security tokens (tokens that resemble securities), and utility tokens (essentially, all other tokens). The classification is very simple and artificial, as many symbols might readily belong to multiple categories. A cryptocurrency designed to serve as a currency while offering dividends to users when staked should be regarded only as a currency token. Is a utility token, issued via a public sale, only a utility token? These categories were effective for illustrative reasons when the market emerged in 2017; however, by 2021, as several protocols operated at full capacity and an increasing number of users engaged with decentralized finance (DeFi) protocols and tokens, maintaining such classification seemed complex.

Tokens are undoubtedly the most recognized aspect of the blockchain phenomena. They serve as the fundamental components for the operation of the protocols and have emerged as a readily accessible source of liquidity. Tokens may be traded instantaneously between individuals, with minimal or no involvement from middlemen, hence diminishing transaction costs. Nonetheless, despite their utility, they exhibit a speculative inclination, creating an alternative (and less sophisticated) financial market that is increasingly appealing to more conventional institutional participants such as banks and corporations. A significant aspect of the cryptocurrency market, highlighting an amusing contradiction to the decentralized promise of distributed ledger technology, is that several components of the token economy are centrally administered, including wallet providers, exchanges, and custodians. The extent to which the focus on the economic value of tokens detracts from interest in protocol development and adoption remains ambiguous.

1.1 The Law in Blockchain

Blockchain is a technology and an economic reality. As a communication technology, it is used to progress human interaction; as an economic reality, it is a production of value. In both ways, blockchain is a social phenomenon and, therefore, a legal one too.

Where in blockchain is the law? In other words: if two or more persons come to an agreement. Individuals agree to take part in a joint venture by downloading and running the protocol. They agree to abide by the governance and operation protocol standards by joining the company. They have the right to sue individuals who have harmed them for damages if their reasonable expectations are violated by malicious intent. Assume that they were not harmed and that there were reasonable expectations that they were engaging in a dangerous activity by downloading the protocol. If they don't have strong legal protection, they are at risk.

Network users engage in transactions with each other. Transactions are governed by legal regulations and standards. A smart contract facilitates transaction execution but does not constitute a legal agreement governed by special "alegal" standards. Ultimately, programmable code is a human-created language that may signify declarations and agreements. In relation to engagements with individuals, acquiring a wallet, establishing an account on an exchange, and installing a mobile application for the management of their tokens represent legal agreements governed by contractual regulations. Tokens serve as digital representations of value that, akin to other recognized legal categories of value (such as securities, property titles, and identity marks), are required to adhere to the relevant regulatory frameworks. With the exception of El Salvador and the Central African Republic, no other jurisdiction grants crypto-assets the status of legal tender. Nonetheless, this does not inherently render them prohibited payment methods; legally, they are akin to casual conversation. If individuals consent to transact in cryptocurrency, there are typically no repercussions.

if a miner neglects to mine a block and include a transaction from a user, can the user seek damages from the miner for lost profits? In the event that a protocol's code contains a bug that

facilitates illegal transactions, the question arises as to who bears responsibility. The entity responsible for the creation and maintenance of the protocol. The freelance programmers and developers who allocate their time? What is the significance of voting and participation? Am I entitled to transparency through staking and participating in protocol governance? In the event of a hard fork with which I disagreed, am I entitled to seek damages from those who supported it? Additionally, what are the applicable rules (contractual and corporate) in this situation?

The determination of applicable law and jurisdiction constitutes a fundamental aspect of international private law, providing a critical framework for identifying the governing law and the appropriate forum for the enforcement of rights. An article by Andrew Dickinson effectively demonstrates that, despite challenges, it is feasible to identify the rules applicable to situations involving blockchain technology. (Dickinson 2019, 94–136) The legal issues concerning the rights and responsibilities of all participants in the protocol miners, holders, and members of decentralized autonomous organizations (DAOs) should be analyzed within the context of the relevant jurisdictional regulations. This includes considerations of contractual private and legitimate expectations, as well as the rights and responsibilities associated with joint ventures and other informal or irregular associations. Considering the differences between protocols is essential when assessing the legal implications of users' rights and duties. For instance, regarding expectations and agreements, most of the highest-valued protocols by market capitalization are supported by enterprises or corporations and possess established marketing frameworks. Individual users typically do not interact directly with the protocol; rather, they engage with third-party companies that are directly linked to the protocol through agreements established with service providers. Users wishing to participate in the protocol are protected as they engage directly with the protocol's backers, including the foundations and companies that developed it and have a vested interest in its success. Expectations are established and legally defined in advance, with a clear identification of the parties involved and their respective contractual obligations. Consequently, the risks associated with governance decentralization are partially alleviated.

In the end, the problems of "decentralization" and automatic processing (or smart contracts) are not as hard to solve as first thought when they are properly understood in terms of what they mean and how they affect real life. Law and decentralization don't go against each other; they've been around for a long time, especially in government systems like feudalism and federalism. It means that the ability to decide, order, or rule is not (or not fully) held by one central group or organization, but is spread out among many places. (Dickinson) .What's important is the agreement, pact, covenant, or ritual that sets up the foundation and structure of power. As soon as this is clear and agreed upon, legal links will be made to create rights, duties, and liability.

Despite the fact that blockchain is a digital platform with automated mechanisms of interaction, it is a private endeavor, a market that was created and is managed by people. The norms are established by individuals through agreement and within the autonomy that the law grants them. It is necessary to amend the code if there is an issue with the way in which something is impossible to attain (for example, data privacy), as this can occur. The circumstance regarding Bitcoin is the most challenging from this viewpoint. Nakamoto's

anonymity, coupled with the absence of a centralized framework governing the protocol and the diverse stakeholders involved, complicates the pursuit of sufficient legal safeguards for users and obscures the rights and responsibilities of each participant within the network. A legal practice, referred to as a digital-community custom, is seen in the methods set by Bitcoin community members for updating the network. The method remains rather unpredictable and unstructured. Nonetheless, considering that the majority of individuals engage with intermediaries rather than connecting directly to the network, and acknowledging the liability between the user and the intermediary, I do not perceive the situation as particularly problematic from a pragmatic perspective.

1.2 The Law for Blockchain

Blockchain is a legal phenomenon as it is governed and regulated by law, encompassing its developments and interactions. Another inquiry pertains to the adequacy of this "coverage" (or regulation). The law encompasses social and technical issues within its framework. The operation of law is intricate, heavily reliant on hermeneutics and interpretation. The broader the interpretation of norms, the greater the law's ability to adapt to new circumstances. An exemplary instance is the definition of security under EU law, which is sufficiently broad to encompass any manifestation of value that functions as an investment vehicle.

Is the law sufficiently flexible to address blockchain and its advancements? Private law regulations can address many scenarios involving blockchain technology. Nevertheless, the scope of private law autonomy is limited, and certain factors that hinder the further implementation of blockchain are prohibited. Establishing a negotiating system for financial products on a decentralized blockchain is generally illegal. Representing a property title for a house, automobile, or corporate store as a cryptographic token is illegal or lacks legal validity; such transactions must be conducted through a legally prescribed form, such as a public deed for real estate acquisitions. While certain regulations delineate incorporation conditions for individuals engaging in economic activities involving "virtual assets" to mitigate money laundering, it remains ambiguous if credit institutions are permitted to include tokens in their portfolios. (Directive (EU) 2018/843 of the European Parliament and of the Council) The artificial tripartite split of token classification complicates the comprehension of tax law treatment regarding gains from the sale of crypto assets. Moreover, it remains ambiguous whether blockchain can function as a reliable mechanism for identity verification.

The primary legal difficulty of blockchain is practical rather than dogmatic: Distributed Ledger Technologies (DLTs) are global protocols managed by numerous individuals across various jurisdictions, facilitating peer-to-peer transactions. Identities are cryptographically generated, and pseudonyms are employed, complicating the processes of identification and enforcement. International collaboration and specialized knowledge among law enforcement agencies and judicial systems are essential. The global acknowledgment of cryptocurrency as a legal category could facilitate financial and tax regulation.

In conclusion, for the blockchain revolution to be successful (and for value to be digitalized), legal regulations must permit digitalization. Rules governing automated decision-making and

processing already exist, but there aren't many governing the digitization of public deeds, identities, certificates, or other types of verified data. Furthermore, public organizations or authorized actors, such notaries, issue the majority of these property certificates. From a technical perspective, the idea of a "decentralized" state apparatus is intriguing. Even though it can be separated into departments or several administrations (such as regional, local, and federal), public administration is the most centralized social institution in the world. Even though a blockchain can increase efficiency and transparency, the protocol is ultimately controlled by the public sector.

2. Blokchain and Contracts

As the Great Recession worsened, Alistair Darling, the United Kingdom's Chancellor of the Exchequer, faced a difficult decision. Because of a worldwide financial crisis partly caused by risky and exotic derivatives, he had to decide whether to inject £37 billion into British banks to keep the country's credit flowing.(Francis Elliot and Gary Duncan) Should he sanction another bailout for the banks for the short-term benefit of the economy, or should he let them fail as a punishment for their speculative behavior?

As he pondered this option, a new experiment was ready to begin in an obscure part of the Internet. On January 3, 2009, an individual or group of individuals known as Satoshi Nakamoto ran the code required to construct the Bitcoin blockchain, along with an express political message: "The Times 03 / Jan / 2009 Chancellor on brink of second bailout for banks.(This message can be viewed through a “blockchain explorer” like the one provided by Blockchian.Info and viewing the block’s “coinbase.”) This message, likely a criticism of the centrally controlled banking system, was linked to the action that launched the world's first decentralized digital money, resulting in a new type of "crypto-currency" that is native to the Internet and free of central control.

Salt, tobacco, dried fish logs, rice, cotton, and cocoa beans have all been used as payment at different times. Barley was used by the ancient Babylonians and Assyrians. Medieval Norwegians utilized butter. Chinese, North African, and Mediterranean traders traded enormous slabs of salt.(Jack Weatherford, The History of Money) Coins eventually superseded these early forms of payment, beginning in the eleventh century BC.(Christopher Howgego) Paper and banknotes appeared next, migrating from China to the West via the Silk Road.(Thomas Francis) Over the last century, credit cards and digital payments have begun to supplant these older systems.(Oren Bar-Gill) Payment systems, whether based on commodities or digital currencies, facilitate trade and transactions, making them a complex yet fundamental element of our daily lives. These rules govern value exchange and promote global economic activity.(Wayne K. Lewis)

Contemporary payment systems comprise a collection of diverse services that enable credit card transactions, interbank transfers, remittance mechanisms, and online payments.8 These

interconnected networks guarantee the optimal operation of markets.(Henry H. Perritt) If a payment system entails high transaction costs, potential benefits from trade may never materialize. Consequently, and as acknowledged by the European Central Bank, payment networks are essential for most economic activities; without adequate payment systems, trade would be nonexistent.(Tom Kokkola)

Payment systems do more than facilitate trade, however. By facilitating remittances, they address humanitarian requirements, ensuring that essential monies from immigrant populations residing and working abroad are transmitted home, thereby assisting families in alleviating poverty.(Ezra Rosser) In 2014, Pew Research reported that worldwide remittances exceeded $500 billion, surpassing three times the total of international aid.(Pew Research Center)

Notwithstanding its essential function, the existing payment infrastructure possesses specific constraints. Transferring money globally in a seamless and cost-effective manner remains unfeasible. Transferring money electronically frequently requires more time than physically transporting cash to another state or country.(Benjamin M. Lawsky) Financial organizations, including banks, may require up to one week to process fund transfers. Online payment companies, such as PayPal, facilitate electronic transactions but impose substantial fees and lack broad accessibility.

Remittance mechanisms are also unreliable. Transferring cash internationally is frequently costly, protracted, and unwieldy. Fees imposed by banks or other money transmitters, such as Western Union, can be substantial, averaging over 7 percent,(World Bank Group, Finance and Markets, Remittance Prices Worldwide) and payment may take several days, consequently delaying assistance to relatives and other beneficiaries.

Payment and Remittance Systems

Decentralized digital currencies such as Bitcoin provide novel solutions to address some deficiencies. Bitcoin addressed a significant issue that compromised previous efforts to establish a functional and enduring decentralized digital currency: the double spending dilemma. Bitcoin facilitated the transfer of digital currency among participants using a robust and tamper-proof database, a peer-to-peer network, and a consensus mechanism based on proof of work, eliminating the necessity for a centralized coordinating entity and mitigating the risk of double spending. The Bitcoin network is pseudonymous and permissionless, lacking territorial limitations.(Bitcoin differs from e-mail in one critical respect: sending Bitcoin is not free for the user. As with traditional paper mail, if you send a large Bitcoin transaction, you may need to pay a small fee (as low as 0.0001 bitcoin) to miners for maintaining the database and processing. (Bitcoin transactions)

Because of these features, digital currencies like Bitcoin have a certain appeal for emerging and developed nations alike. They serve as a novel kind of infrastructure that could be beneficial for nations with weak or underdeveloped financial systems.(Joshua Baron, Angela O'Mahony, David Manheim, and Cynthia Dion- Schwarz) For example, in nations like Argentina, Venezuela, or Zimbabwe that lack stable currencies, Bitcoin may be used in addition to or even in place of conventional payment methods. Citizens can opt to store their savings in bitcoin or exchange bitcoin into other more stable currencies, potentially reducing country-specific inflationary risks or devaluations, because Bitcoin is protected from national economic problems or instabilities.(Karen Maley)

Blockchain technology is being investigated to quickly and securely exchange popular fiat currencies, even in nations like the US, which have stable currencies and easy ways to make payments. For depository institutions and central banks to perform interbank transfers and exchange money between currencies, the technology is seen as a new technological backbone.(Gareth W. Peters and Efstathios Panayi) For instance, banks can now swap money between currencies in a matter of seconds and for little to no cost thanks to Ripple, which uses a blockchain. The Ripple protocol initiates a sequence of transactions between foreign exchange traders who are part of the Ripple network in order to make an exchange. After determining the most economical method of converting money across currencies, the Ripple protocol generates a sequence of deals that are instantly resolved via a blockchain. With the Ripple protocol, an exchange of U.S. dollars to Japanese yen would necessitate two distinct trades: a first trade of U.S. dollars to euros with one party and a second trade from euros to yen with another, rather than a straightforward transaction converting one currency to another.

Because Ripple allows virtually instantaneous access to widely used currencies, an increasing number of financial institutions in the United States, Germany, and Australia have begun to integrate Ripple's protocol into their respective payment infrastructures on an experimental basis. Twenty-four customers of these banks now benefit from the efficiencies of blockchain technology, enabling them to exchange currencies at reduced fees without the necessity of converting existing deposits held in either U.S. dollars or euros into digital money. Blockchain technology functions discreetly in the background, frequently without the awareness of the end user.

Blockchains are starting to introduce comparable efficiencies to remittance markets. Certain blockchains facilitate global fund transfers at minimal or no cost, thereby underpinning new services that allow immigrants to swiftly and affordably remit money to their families overseas, independent of traditional services like Western Union and MoneyGram. Blockchain technology enables international money transfers without the necessity of visiting a teller or physical institution, making the process as simple as sending a text message. Services such as Abra enable immigrants to participate in a peer-to-peer remittance network using their mobile devices, allowing them to easily transfer or receive payments globally through a straightforward application.(Abra) These services operate without an intermediary,

such as a bank or other depository institution, to enable a transaction. A blockchain-based remittance network, such as Abra, circumvents centralized intermediaries by utilizing the Bitcoin blockchain to facilitate transactions, thus transforming numerous smartphone users into local bank tellers.

There are, nevertheless, substantial hurdles for blockchain-based remittance services. Although these services aim to supplant physical establishments such as kiosks and retail stores these tangible locations are frequently crucial for establishing a presence in a local area and for engaging with existing payment systems. Currently, the majority of products and services cannot be purchased with bitcoin, and the digital currency's volatility frequently renders it an impractical medium of exchange. (Stephanie Lo and J. Christina Wang,) Users of blockchain-based remittance services predominantly depend on conventional fiat currency for their daily living expenditures.

Building out local and regional remittance networks is a long and often hard process that Abra and other blockchain-based services must go through in order to completely change the remittance industry. Because of this, the prices of these new blockchain-powered services are currently the same as those of their traditional peers. But in the long run, Abra and other new blockchain-based payment systems may be better than old cross-border payment services. If more people use these networks, network effects could happen that build trust and make things more visible. This could help these new services replace current payment options without the need for physical locations.

2.1 Digital Currencies and Existing Laws

Because blockchains are distributed, cross-border, and anonymous, they often run into problems with current laws and rules. However, they hold the promise of new and better payment systems. In order to stop foreign tax havens, money laundering, drug trafficking, and terrorist activity, many countries have passed anti-money laundering (AML) and money transmission laws that require financial institutions to closely watch all financial transactions. Different places have different rules, but many of them say that controlled businesses must "know their customers" and report any strange behavior. (Kevin Tu and Michael Meredith)

On the other hand, the federal Bank Secrecy Act (BSA) and similar state money transmission laws in the United States have made it so that financial services that handle the transfer of value must follow a complex web of anti-money laundering rules. The BSA tries to stop people from laundering money by making regulated "money services businesses" keep records of all transactions or linked transactions involving large amounts of money being sent.(Tu and Meredith, Regulation) The law also says that businesses must keep track of their

customers' identities and report to the government any activities that seem fishy and might be linked to illegal activity.

Companies that move money or monetary equivalents must follow a patchwork of state money transfer rules in 47 states, the District of Columbia, and Puerto Rico. They also have to apply for separate licenses, which makes things even more complicated. At first, state licensing programs were made to protect consumers. Now, these rules require AML compliance more and more. High fines and even jail time are common consequences for not getting the right license and following the rules set by the state.

Even though there are laws and rules in place, most of the blockchain-based systems that control digital currencies have not been programmed to follow them. Because it was made that way, the Bitcoin network is a public, anonymous network that anyone can join. You don't have to go to a bank, open an account, and give basic personal information in order to trade bitcoin or any other digital currency. This is what most anti-money laundering laws require. Anyone can receive a Bitcoin transaction at any time, and because they happen automatically, it's hard to stop or undo them once they've happened.

Because of this, bitcoin and other digital currencies have become popular among people who want to avoid following the rules and laws that are already in place. Bitcoin was the most popular way for sellers on the renowned drug market Silk Road to accept payments. The Silk Road helped people sell drugs worth an estimated $200 million.(Joshuah Bearman) Terrorist groups used Bitcoin to send money they had earned in the United States, or at least they looked into it. Some people have even said that Bitcoin makes it easier for people to avoid paying taxes because it doesn't go through regulated middle men.(Omri Y. Marian,) New "mixing" services make digital currencies even less legal because they make it hard for governments to track blockchain-based transactions. These services act like banks in places with strict bank-secrecy rules, like the Cayman Islands or Panama (Darkwallet,), by combining transactions that have nothing to do with each other. This makes it harder for a third party to figure out who is sending money to whom.

Bitcoin, on the other hand, was just the start. New digital currencies are making it easier to avoid AML and other financial rules about payment systems by acting like cash and coins, which are hard to track. These new currencies build on the ideas that make up the Bitcoin blockchain. More advanced cryptographic methods, like zero-knowledge proofs and ring signatures, are used by these anonymous digital currencies to hide the source, location, and amount of every transaction that a blockchain handles.(Eli Ben Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza,) For instance, Zcash is a project by Israeli and American cryptographers that lets people in the Zcash network send a digital currency called a "z-coin" without being tracked using a blockchain. Zero-knowledge proofs make Zcash transactions almost impossible to track by allowing private transactions on a blockchain that is both open and available to only one person at a time. Users of the Zcash network can hide the amount of their transactions and the identities

of the people sending and getting z-coin by using advanced cryptographic algorithms and zero-knowledge proofs. It is possible to use zero-knowledge proofs to make sure that the sender has enough z-coin to complete a transaction without giving the network any information about the transaction.Zcash makes it hard to connect a Zcash account to a real-life name on purpose. On the Z-cash network, accounts are anonymous, and the Zcash blockchain doesn't keep track of where "private" Zcash transfers come from or go to. If anonymous digital currencies like Zcash become popular, they will make it easier for bad people to do bad things without being caught. This is because governments, regulators, and law enforcement would not be able to use financial
monitoring to stop crime, threats, or other illegal activity.

In the long run, this means that truly anonymous "digital cash" may make it harder for states to control the flow of money around the world. As this trend continues, one way to look at it is that currencies are breaking away from both their actual form and centralized control.(Meghan E. Griffiths) The Internet split creative content from physical media like newspapers, CDs, and VHS tapes, making the flow of information harder to control. We are now starting to see a similar trend in the way money and payments are made. Money can now move outside of a tightly controlled banking system, which makes things more complicated with the laws that are already in place.

Cryptocurrencies and Reduced Privacy in Financial Transactions

However, most popular blockchain-based digital currencies today, such as Bitcoin, do not offer strong privacy rights. As we already said, digital currencies are not private; they just use fake names. Blockchains are open and allow anyone to see every transaction that an account has made. Blockchain technology lets groups that handle digital currencies like governments, exchanges, and other services that accept, store, or send them learn about the habits of many account users. Third parties can make a map of blockchain-based activities and then combine that with personal information to figure out not only who owns these accounts but also what they've done with their money in the past.

This knowledge could be beneficial, but it may also facilitate new types of mass monitoring, as governments and companies utilize these tracing tools to regulate and oversee the circulation of blockchain-based digital currencies globally. Upon the advent of the Internet, it was characterized by some as an unregulatable domain a novel realm devoid of boundaries.(John Perry Barlow) Nonetheless, this vision proved to be illusory, partly due to the traceable characteristics of IP addresses. With the widespread use of the Internet, China established its "Great Firewall," blocking anything considered disruptive to the Chinese socialist system, along with pornographic and violent material. The firewall limits the information accessible to Chinese residents by targeting the IP addresses of websites and online services that do not meet state censorship criteria. Blockchain-based digital currency accounts, characterized by a public-private key pair utilized for receiving and transferring digital money on a blockchain network, exhibit numerous parallels with conventional IP addresses. Similar to IP addresses, they serve as permanent reference points that may be identified and tracked. If digital currencies emulate the trajectory of the Internet, it may

increasingly facilitate the ability of China or another authoritarian regime to establish a blacklist of digital currency accounts, so excluding specific individuals from participating in commercial transactions.

The proliferation of digital currency may facilitate governmental supervision and regulation over both the online communications of the populace and the economic activities in which citizens participate. The consolidation of payment information and financial transactions in a singular, collaboratively managed repository significantly enhances the rewards for effectively deanonymizing transactions, since it provides parties with access to the transaction history of a whole network of users rather than merely that of an individual.
If unregulated, this may pose a new threat to fundamental liberties, since governments may opt to intervene by filtering financial transactions and ordinary business activities. These hazards have been recognized for decades. In late October 1971, a consortium of scholars and technologists convened at a symposium at Georgetown University. They were assigned the responsibility of developing the most extensive (but imperceptible) monitoring program conceivable for the KGB, the Soviet secret police.
They envisioned not a network that intercepts every phone conversation, message, and email, nor a network of cameras throughout a city; instead, they conceptualized a "electronic funds transfer system" capable of identifying and tracking payments. These researchers asserted that it was the most effective surveillance method due to its unobtrusiveness.

The transparent characteristics of blockchains may ultimately hinder the extensive adoption of bitcoin and other decentralized digital currencies. Due to the traceable and transparent nature of existing blockchains, individuals can monitor the flow of digital currency transactions and evaluate the extent of "affiliation" between each new transaction and others, including those linked to illicit activities such as criminal financing, money laundering, or the acquisition of illegal goods. If transactions associated with illicit activities are classified as "tainted" and subjected to distinct legal or market treatment, it would compromise the fungibility of these emerging digital currencies.

Although laws and regulations cannot entirely inhibit individuals from engaging in transactions involving blockchain-based digital currencies, they can effectively deter parties from accepting digital currencies linked to criminal behavior. Governments could establish secondary liability for holders of compromised digital currencies, thereby extending their authority beyond transaction monitoring to prohibit individuals from engaging in transactions with purportedly criminal account holders or other entities deemed troublesome by the government. The implementation of such policies would diminish the apparent economic worth
of any compromised digital money.

Although this prospect may seem unlikely, analogous methods have already been employed in the private sector in response to criminal behavior. In 2012, the web-hosting firm Linode experienced a security breach, leading to the theft of 43,000 bitcoins (exceeding $755 million as of December 2017).(Dan Goodin,) In response, Mt. Gox formerly one of the largest

Bitcoin exchanges suspended all accounts with transactions that could be somewhat linked to the crime. The exchange released frozen accounts just after individuals confirmed their accounts were not implicated in the theft.(Vitalik Buterin) With the broader acceptance of Bitcoin, there have been escalating demands for the Bitcoin protocol to implement new capabilities enabling the establishment of a blacklist for tainted transactions. Researchers have proposed that this strategy could be a "promising" method to combat crime by making any illicit behavior linked to Bitcoin ineffective.(Malte Möser, Rainer Böhme, and Dominic Breuker,)

If Bitcoin or another digital currency addresses fungibility and privacy issues, they might potentially destabilize the current financial system and its dependence on central banks. A disintermediated, transnational, and pseudonymous digital currency may reduce individuals' reliance on existing financial intermediaries for the storage and management of their cash.(Bank of International Settlements, Committee on Payments and Market Infrastructures,) The extensive use of blockchain-based digital currencies may, theoretically, result in a reduction of central banks' authority over monetary policy. In nearly all market economies, central banks are tasked with adjusting the monetary base to manage inflation and stimulate economic growth. However, if decentralized digital currencies such as Bitcoin achieve widespread acceptance, a central bank may forfeit its capacity to regulate a nation's economy through control of the money supply, as the parameters for the issuance of these digital currencies are predetermined and governed solely by code.

The widespread adoption of blockchain-based digital currencies will diminish banks' balance sheets, resulting in a loss of essential revenue. If a sufficient number of individuals depend on decentralized digital currencies rather than conventional fiat currencies, it may affect the revenue that central banks derive from lending their deposits. The widespread use of blockchain-based digital currencies may lead to central banks failing to produce sufficient interest from their holdings to cover operational expenses,(IMF report) necessitating a modification in their
operations to compensate for the revenue shortfall.

A potential strategy involves central banks issuing and regulating one or many digital currencies.(Benjamin M. Friedman,) Similar to how Napster altered the dynamics of the music industry, leading to the establishment of regulated, industry-backed platforms like Spotify, one or more central banks may introduce a centrally governed digital currency to effectively rival blockchain-based options. This strategy allows central banks to leverage the advantages of digital currencies, such as cost efficiency and scalability, while retaining authority over money supply and the capacity to implement restrictions to combat crime and other illicit activities.
This method, however, would not inevitably result in the extinction of Bitcoin and other decentralized digital currencies. Timothy May's predictions have materialized, as blockchains

and enhanced access to cryptographic tools have unleashed significant changes.(Timothy May,)

As long as there is a demand for decentralized digital currency, blockchain networks will persist in their operation. Due to the non-compliance of blockchain-based digital currencies with jurisdictional norms, these currencies may facilitate persons in evading laws governing the
transfer and storage of funds.

Blockchain-based digital currencies demonstrate multiple, competing qualities through the reliance on code and lex cryptographica. Blockchains may augment and improve present, increasingly outdated, cross-border payment systems. Conversely, they may support decentralized, autonomous, and anonymous digital currencies, like to untraceable digital currency, which do not align with existing laws and hinder initiatives to utilize payment systems in combating crime.

3. Smart Contracts

Payment systems are merely one domain possibly affected by blockchain technology, where blockchains may encourage illicit activities. Decentralized blockchain-based platforms and lex cryptographica are transforming the manner in which parties document commercial agreements. Blockchain technology facilitates a new era of digital contracts that are robust, modular, dynamic, and, in certain instances, less ambiguous than those articulated in conventional legal language, by leveraging the capacity of blockchains to execute resilient, tamper-resistant, and autonomous smart contract code.

Nevertheless, the utilization of smart contracts to document all or portions of legal agreements introduces novel obstacles and disadvantages. They offer less privacy than contemporary written contracts and, if their code is not publicly disclosed and articulated in a comprehensible manner, they may enable the formation of standardized contractual frameworks that are mostly incomprehensible to the general populace. The autonomous and disintermediated characteristics of blockchain-based smart contracts raise significant concerns over their potential to enable criminal activities. Blockchain technology can influence legal agreements both beneficially and detrimentally and parties may utilize lex cryptographica to establish smart contracts that enable illicit activities.

The narrative of digital contracts commenced in June 1948, when the Soviet Union severed road, rail, and barge access to western Germany and sections of Berlin. In response, the United States and its allies initiated the Berlin Airlift, delivering over 2 million tons of food and various supplies to the partitioned city. U.S. Army Master Sergeant Edward Guilbert devised a manifest system for the systematic organization and monitoring of the extensive

cargo dispatched to West Berlin daily, which could be communicated via telex, radio-teletype, or telephone.(Frank Hayes)

Insights from the Berlin Airlift permeated the commercial sector following the conclusion of the conflict with the Soviet Union. In 1965, Guilbert, then employed by DuPont, devised a system for electronic data interchange (EDI), establishing a standardized set of electronic signals for transmitting cargo information between DuPont and its carrier, Chemical Lehman Tank Lines.Guilbert's invention enabled DuPont to transmit trans-Atlantic shipping manifests as telex messages, which were then transformed into paper tape and entered into company computers.

In the late 1990s, computer scientist and cypherpunk Nick Szabo recognized these limits and devised a novel method of conducting electronic contracts. In a paper titled "Formalizing and Securing Relationships on Public Networks," Szabo described how relying on more robust cryptographic protocols would allow for the creation of computer software that resembled "contractual clauses" and bound parties together in a way that would limit either party's ability to terminate its performance obligations. Since then, scholars have investigated computer-based contractual languages. For example, shortly after Szabo's work was published, Mark Miller, Chip Morningstar, and Bill Frantz used an object-oriented programming language to represent option contracts.(Mark S. Miller, Chip Morningstar, and Bill Frantz) In the late 1990s, Microsoft and University of Glasgow academics experimented with computerized financial contracts. (Simon Peyton Jones, Jean-Marc Eber, and Julian Seward,)

In 2004, financial cryptographer Ian Grigg introduced the concept of a "Ricardian Contract" a contract that can be read by both machines and humans.(Ian Grigg, “) More recently, in 2012, Harry Surden, a law professor at the University of Colorado, researched the concept of data-oriented contracts and how representing contractual responsibilities as data can result in the construction of "computable" contract terms.(Harry Surden,)

3.1 Smart Contracts and Legal Contracts

With the increasing acceptance of Bitcoin and other blockchain-based systems, there has been renewed interest in and experimentation with converting legal agreements into code. Advanced blockchain-based protocols, such as Ethereum, give the technology required to put some of Nick Szabo's ideas into action more than two decades later. Using blockchain-based smart contracts, parties can enter into a legally enforceable economic relationship, either totally or partially codified, and utilize software to govern contractual performance.

In many aspects, smart contracts are identical to today's written agreements. To carry out a smart contract, the parties must first negotiate the parameters of the agreement until they reach a "meeting of the minds."(Stephen J. Choi and Mitu Gulati,) Once agreed upon, parties memorialize all or part of their agreement in smart contract code, which is activated by digitally signed blockchain transactions. In the event of a dispute, parties have the option of

renegotiating the underlying agreement or seeking remedy from a court or arbitration panel to undo the smart contract's consequences.

Where regular legal agreements and smart contracts differ is in their capacity to enforce obligations through autonomous code. Smart contracts do not use normal legal language to express performance responsibilities. Rather, these commitments are formalized in the code of a smart contract written in a precise and formal programming language (such as Ethereum's Solidity). Smart contract code is executed in a distributed way by all nodes supporting the underlying blockchain-based network, without the need for an intermediary operator or trusted mediator. Because smart contracts are autonomous, promises inscribed in them are, by definition, more difficult to terminate than those commemorated in a natural-language legal agreement. Because no single party controls a blockchain, there may be no way to stop the execution of a smart contract after it has been activated by the appropriate parties. Once the wheels of a smart contract are set in motion, the terms represented in the code will be executed, and they cannot be stopped unless the parties have included logic to halt the program's execution.(Kevin D. Werbach and Nicolas Cornell)

Smart contracts are also more dynamic than standard paper-based contracts because they can be designed to alter performance requirements during the period of an agreement by relying on a trusted third-party source, known as an oracle among programmers.(Alec Liu) Oracles are individuals or programs that store and communicate information from the outside world, allowing blockchain-based systems to interact with real-world people and potentially respond to external events. Oracles, for example, can be linked to a third-party data stream that contains the most recent London Interbank Offered Rate (LIBOR), or to sensors that send outside temperature, humidity, or other pertinent information about a specific place. More experimentally, an oracle can be used to impart human insights or to support private conflict settlement and arbitration systems.(Michael,) Smart contracts are also more dynamic than standard paper-based contracts because they can be designed to alter performance requirements during the period of an agreement by relying on a trusted third-party source, known as an oracle among programmers. Oracles are individuals or programs that store and communicate information from the outside world, allowing blockchain-based systems to interact with real-world people and potentially respond to external events. Oracles, for example, can be linked to a third-party data stream that contains the most recent London Interbank Offered Rate (LIBOR), or to sensors that send outside temperature, humidity, or other pertinent information about a specific place. More experimentally, an oracle can be used to impart human insights or to support private confilct settlement and arbitration systems.

Oracles allow smart contracts to respond to changing situations in near real time.(M. Ethan Katsh) Contracting parties can use an oracle to modify payment flows or encoded rights and responsibilities in response to new information. Oracles also allow for the determination or updating of specific performance obligations based on individual subjective and arbitrary judgments. In this way, parties may rely on smart contracts' predictable and guaranteed execution to make objective commitments that can be easily translated into code. Simultaneously, they can delegate the work of assessing promises that cannot be easily encoded into a smart contract, either because they are too ambiguous or because they necessitate a subjective judgment of real-world occurrences.(Pietro Ortolani) Since

Ethereum's inception, we've seen an increase in the number of smart contracts used to manage business arrangements. Smart contracts are being developed to manage the transfer of digital currencies or tokens representing tangible or intangible assets, as well as to control access to data or other informational resources stored on a blockchain network.(Joshua Fairfield) For example, Ujo Music's initiative uses a smart contract to ease the selling of digital music files featuring Imogen Heap's song "Tiny Humans." The smart contract is activated whenever someone pays $0.60 to download the music from Ujo Music's website. Once paid, a smart contract splits the proceeds between Imogen (who earns 91.25% of the sale price) and seven other collaborators who helped create the song (each receiving 1.25%). Payment is not administered by a centralized party, such as a music label or performance rights organization. The exchange takes place on a peer-to-peer basis, between the consumer and the song's authors. Unlike a typical agreement, the smart contract allows for microtransactions at little to no cost, and payment is divided virtually instantaneously per the rigorous logic of the smart contract code and quickly dispersed to the musicians in amounts of less than $0.01.

Smart contracts are also enabling peer-to-peer transactions in decentralized e-commerce marketplaces that do not rely on a centralized intermediary such as eBay or Craigslist to support and coordinate the sale of items (Open Bazaar).

These services handle payment for commodities using blockchain technology and smart contracts, and they use human-based oracles to potential isues that may arrise during trade.

In these decentralized markets, merchants can offer a product for sale by recording information to a blockchain, such as a product description and pricing. Interested buyers can transfer monies to a virtual escrow account supported by a smart contract (also known as a multisignature account), which autonomously controls and manages any submitted funds.(Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder) If everything goes as planned and the buyer obtains the item in question, the buyer sends a digitally signed blockchain-based message to the escrow account, which releases the purchase price to the seller. In contrast, if a dispute occurs over the quality of the thing or if the product is simply never delivered, a human-based oracle comes in to examine the facts of the case and determine who should receive the escrow monies.

3.2 Hybrid Agreements

Contracts establish rights and obligations for each contracting party, which are formalized in context-sensitive legal prose. These promises include not just individual obligations, but also time- and sequence dependent activities that may result in contractual responsibilities. Some rights and duties are easily translated into the rigid logic of code, particularly those involving the exchange of money or the transfer of title to a digitally represented asset. These promises are frequently binary in nature and hence easily translatable into software.

Other contractual provisions, however, are less clear-cut. Legal agreements typically include open-ended phrases that describe performance duties. For example, a contracting party may promise to act in "good faith" because it is difficult to precisely define what constitutes appropriate performance, whereas another party may promise to use "best efforts" to fulfill his or her obligations because the most cost-effective or efficient method of performance is not yet predictable. Keeping contracts open-ended or ambiguous is generally beneficial since it allows parties to be more flexible while also reducing discussion time and money. In many circumstances, vagueness can result in more efficient contracts.(George G. Triantis,)

Standard legal agreements also include representations and warranties, which cannot be met only by referring to data stored or controlled on a blockchain network. While these representations and warranties encompass the full range of legal agreements, contractual parties frequently assert ownership interests, agree to keep material confidential, or guarantee that they will follow applicable laws. Smart contracts, at least in the short term, will be unable to account for these more open-ended rights and duties that are neither binary nor highly formulaic. These unstructured phrases are difficult to forecast at the time of contracting, making them unsuitable for memorialization in the rigid logic of code. Law firms are already considering the limitations of smart contracts in the context of legal agreements. For example, the prominent international law firm Hogan & Lovells developed a "smart" earthquake insurance agreement. They created a digital term sheet defining essential aspects of the agreement and used it to model an Ethereum-based smart contract that governs relevant payouts. However, after running the trial, the firm immediately recognized that a solely code-based algorithm could not account for the standard conditions seen in a basic earthquake insurance agreement. They discovered significant disparities between the smart contract and a comparable natural-language agreement, as well as other legal and technological flaws.(Steven Norton) Given these constraints, it is likely that the deployment of smart contracts will follow a similar route as EDI agreements. With EDI, parties elected not to rely solely on code-based arrangements, instead signing master agreements that contextualize the use of electronic communications within the context of a larger contractual relationship.(Robert A. Wittie and Jane K. Winn)

If smart contracts are used to model legal agreements, parties can establish hybrid arrangements that combine natural-language contracts and smart contracts written in code. These agreements could be written mostly in traditional legal writing while simultaneously referencing a smart contract and explaining how the program fits into a bigger business transaction. This approach allows natural-language agreements and smart contracts to work together to commemorate the parties' intentions. By merging the two, the benefits of both formal agreements and code-based regulations are available simultaneously, without a party having to choose between the two.

3.3 Legal Enforceability of Agreements Relying on Smart Contracts

Even when smart contracts completely replace conventional legal agreements, these programs do not function in a vacuum. While smart contracts can automate payment

responsibilities and the transfer of valuable assets, they do not eliminate the requirement for parties to agree to these terms. Promises must first be negotiated and then translated into code, and for a contractual relationship to form via a smart contract, parties must still demonstrate approval to defined terms through the use of a digital signature. If there is a disagreement regarding whether a smart contract adequately memorializes the parties' intent or whether one party broke the agreement, the contracting parties retain the right to pursue legal action or engage in private dispute settlement. Courts ultimately have jurisdiction over the legal consequences of a smart contract. They will read the underlying code in accordance with long-standing contract law principles, with the assistance of specialists as needed. If a court determines that a party breached its contractual responsibilities, it retains the authority to award damages to compensate the affected parties. Even if a smart contract allows for an alternative dispute resolution system based on a third-party oracle, the court may invalidate any adjudication rendered by the oracle, such as if the arbitrator failed to comply with the arbitration provision memorialized in the agreement or manifestly disregarded the law. The fact that a contract memorializes promises in code rather than legal words will have little impact, at least in the United States. Contracts can be expressed or implied under US common law, and there are often no formal criteria for the manner in which a contract is drafted in order for a court to discover adequate evidence of a binding contract.The main issue is not the wording of the agreement, but whether a judge can infer the parties' desire to be contractually bound.

Under these ideas, smart contracts that memorialize legal commitments are likely to be considered enforceable under US law. Parties can record their intent in code just as they might in paper, and if they include recurrent performance requirements, smart contracts may even establish a course of performance or dealing. For example, in Bibb v. Allen (1893), the United States Supreme Court upheld an agreement communicated electronically via enciphered telegraph communications based on the Shepperson Cotton Code. Despite the unconventional manner in which the arrangement was memorialized, the Supreme Court determined that the parties entered into a contract involving the sale of 10,000 bales of cotton because they "agree[d] upon the terms in which the business should be transacted" via a series of telegraph messages.(Bibb.)

Today, federal and state regulations protect parties from disputing the validity of a contract just because it is in an electronic or code-based format. Under the Uniform Electronic Transactions Act (UETA) and the federal Electronic Signatures in Global and National Commerce Act (the "E-Sign Act"), a court cannot deny legal effect to an electronic contract (with certain exceptions) if the parties express an intent to be bound by it.(Electronic Signatures in Global and National Commerce Act) Indeed, wide definitions in both the E-Sign Act and the UETA include blockchain technologies, smart contracts, and digital signatures created with public-private key encryption. For example, under the UETA, a "record of signature" and a "electronic record" may not be denied legal effect or enforceability if they are utilized in contract formation. Electronic signatures and electronic records are loosely defined as any "record created, generated, sent, communicated, received, or stored by electronic means," and a digital signature created using public-private key cryptography will fall within the scope of the statute if it is "executed or adopted by a person with [an] intent to sign the record." The UETA even considered the use of automated software, such as smart contracts,

to bind participants to an agreement. The law contemplated the execution of "computer programs or . . . other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part, without review or action by an individual." The UETA's drafters provided that agreements entered into by parties utilizing automated software, referred to by the act as "electronic agents," could not be denied legal effect unless the underlying program included an error.

When parties use hybrid smart contract arrangements, such as those discussed earlier, the risks of enforceability decrease. As with EDI, parties can construct master agreements in traditional legal text that incorporate terms stating that smart contract code is considered genuine writing. They can also incorporate normal severability provisions, which provide courts the flexibility to interpret an agreement as needed. When combined with the UETA and E-Sign Act, these hybrid agreements limit the ability of parties to contest the validity of a legal agreement only because it is based, in whole or in part, on smart contract code.

A. The Benefits of Code

Smart contracts, like other technologies, offer similar advantages in terms of clarity, precision, and adaptability. Despite the best intentions, legal contracts can suffer from bad drafting. Inconsistent phrases seep into complex agreements particularly those prepared under tight deadlines obscuring the parties' true meaning.(Richard A. Posner,)

When faced with contract interpretation issues, courts have struggled to apply consistent criteria. According to Allan Farnsworth, one of America's most well-known legal scholars on contracts, the use of contractual interpretation canons is "often more ceremonial (as decorative rationalizations of decisions already reached on other grounds) than persuasive.(Allan E. Farnsworth,) For decades, researchers have understood that symbolic logic, such as software code, can reduce contractual ambiguity by transforming commitments into objectively provable technological norms.(Symbolic Logic: A Razor-Edged Tool for Drafting and Interpreting Legal Documents,") Because smart contracts are simply bits of logic implemented deterministically, they can reduce the chance of misinterpretation in situations where parties can reliably identify objectively verifiable performance commitments.(John W. L. Ogilvie)

Smart contracts, like other types of programming, are naturally modular and can be divided into separate sections and chunks that can be easily created and disassembled.(Henry E. Smith) Programmers and lawyers can construct smart contract code libraries that are specifically designed to implement certain functionalities that are commonly found in legal contracts. For example, libraries of smart contract code might be created to manage the transfer of payments over specific time periods, with or without interest. These libraries may be incorporated into a variety of agreements, including as promissory notes, employment, services, contractor, and severance agreements. If smart contract code libraries be distributed under open source licenses, as many software libraries are, a community of legal professionals may develop them.Ultimately, this could result in the establishment of a collection of standard smart contract-based provisions that can be used, reused, and continuously updated in response to public scrutiny and criticism.(George S Automating) Smart contract code, like the growth of programming languages, which has proliferated and simplified since the

introduction of computing, may become easier to modify and include into a variety of contractual agreements over time. As blockchain technology advances, these libraries may become more complex, allowing parties to draft smart contracts similarly to how Lego blocks are assembled, with chunks of smart contract code appended together to account for a variety of potential contingencies, resulting in more complex, comprehensive, and sophisticated legal agreements. Smart contracts, which are machine readable, could be employed by autonomous devices and artificial intelligence (AI). As we'll see later, smart contracts enable Internet-connected devices to conduct "machine-to-machine" activities, such as controlling digital currency accounts and engaging into agreements to purchase products or services. For example, a vending machine may detect when it has run out of drink or candy bars and use a smart contract to request that a supplier resupply the machine in exchange for a small charge. Similarly, a self-driving car might pay for gas or electricity using a smart contract, eliminating the need for human participation.

B. Privacy Concerns

However, the degree of openness that smart contracts demonstrate may not be desirable to the parties that are entering into the contract. Generally speaking, when parties engage into an agreement that is written in legal writing, they have the option to keep the terms of their agreement private. On the other hand, due to the fact that blockchains are transparent, all transactions that are carried out through the use of a smart contract, in addition to the code for the smart contract, are transmitted throughout a peer-to-peer network, making them available to network nodes in the public eye. This is a threat to individuals' privacy, particularly in situations when the accounts of the parties involved in a transaction on a blockchain are linked to well-known entities.

However, the degree of openness that smart contracts demonstrate may not be desirable to the parties that are entering into the contract. Generally speaking, when parties engage into an agreement that is written in legal writing, they have the option to keep the terms of their agreement private. On the other hand, due to the fact that blockchains are transparent, all transactions that are carried out through the use of a smart contract, in addition to the code for the smart contract, are transmitted throughout a peer-to-peer network, making them available to network nodes in the public eye. This is a threat to individuals' privacy, particularly in situations when the accounts of the parties involved in a transaction on a blockchain are linked to wellknotines.

It is possible that the potential for smart contracts to replace traditional legal contracts in many commercial settings will be limited because to the privacy concerns that have been raised. The absence of robust privacy safeguards makes it highly probable that smart contracts will not be suited for use in legal agreements where confidentiality is of the utmost importance. This is a subject that will be revisited in the context of derivatives and securities deals. When a smart contract covers a sensitive financial transaction, a payment to a critical supplier, or a settlement payment to a former employee, the terms of these arrangements run the risk of being disclosed. There is also the possibility that the details will be disclosed. Despite the fact that blockchains that protect users' anonymity, such as Zcash and Monero, have arisen over the course of the past few years, these networks do not yet support the

deployment of powerful smart contracts, such as those that are available on Ethereum. Privacy concerns thus cloud smart contracts and may ultimately function as a barrier to the widespread implementation of the technology.

C. Formalization of Legal Obligations

In addition, because smart contracts are dependent on formal programming languages, it is highly unlikely that they will be helpful for agreements that have a hazy or open-ended vision. Designed to make it easier to create contractual obligations that are governed by stringent and inflexible code-based regulations, smart contracts are designed to enable the development of such obligations. They are especially well-suited for memorializing agreements in which the parties are able to outline performance responsibilities in a manner that is objective and predictable. On the other hand, they are not suitable for agreements in which performance obligations are not exactly defined or determinable at the time of contracting.

In point of fact, not all contracts apply to economic relationships that have been meticulously described. Contractual arrangements frequently stay open-ended because the parties involved are unable to anticipate or define their performance duties at the time that the agreement is being drafted. Under what has become known as the "relational theory of contracts," legal academics have long acknowledged that many contracts function more like long-term marriages as opposed to one-night encounters. This is because the relationship between the parties involved is more similar.(Karen E. C. Levy) Agreements are frequently executed by the parties, and they typically contain open-ended terms that are continuously changed to take into account unanticipated occurrences or the evolving relationship between the parties.(Robert W. Gordon) It is possible that these contracts will not be carefully negotiated before they are signed, and they frequently indicate a commitment to work together in the future.In order to enable legal arrangements that are relational in nature, smart contracts are not particularly well adapted to support such arrangements.(Levy) For a smart contract to be put into effect, the parties involved need to carefully describe their performance duties and, if they rely on human-based oracles, the situations in which human insight is absolutely necessary. In the case of particular legal structures, this might be immediately evident. Smart contracts, on the other hand, will not be able to give parties with the flexibility to structure their ongoing contractual relationships. This is because duties will likely prove to be unpredictable in many commercial transactions.

Even if smart contracts are used to model legal duties that are foreseeable and can be objectively verified, there are still difficulties over the extent to which smart contracts can accurately commemorate the intent of the parties involved. In order to properly create a smart contract, it will be necessary to make significant decisions regarding the meaning, content, and applicability of the arrangements that the parties to the contract have made. During the process of developing code for smart contracts, programmers will be required to make subjective judgments, interpretations, and substantive decisions regarding possibly unpredictable future events. This may result in the parties' intentions being obscured or distorted.

D. Contracts Among Pseudonymous Individuals

When it comes to commercial deals that involve pseudonymous parties, the autonomous nature of smart contracts also causes issues. Pseudonymous parties will have little capacity to impact a smart contract transaction once it has been triggered. This is true even if there is a mistake or error in the code that is underpinning the smart contract. If a smart contract is used to regulate an arrangement between parties whose identities are known, then the performance obligations that are embodied in the smart contract can be modified by participating in a second transaction to unwind or change the effects of any code that was previously executed. As is the case with any other type of legal agreement, these parties also have the option of asserting their contractual rights in a court or other decision-making tribunal, which could result in the recovery of damages.(Danielle Keats Citron,) In the case of smart contract-based arrangements, which involve parties who are not aware of each other's identities, it is possible that such opportunities will not be available. A party that has been wronged will be required to be aware of the identification of the other party in order to fulfill the requirements for service in order to be able to launch a lawsuit. Even in the event that a party were to get a default judgment (for instance, against a "John Doe"), the default judgment would have limited practical effect unless it was possible to identify the identity of the other party to a contract in some way.

Due to the difficulties associated with enforcement, it is quite probable that agreements based on smart contracts that involve pseudonymous parties will have internal dynamics that are distinct from those of the agreements that are already in place. For example, solid common law and civil law concepts, such as incapacitation and unconscionability, help to mitigate the impact of contracts that contain provisions that are unfavorable or imbalanced.: However, in the context of smart contracts that are used to govern transactions between pseudonymous parties, it is highly likely that injured parties will not be able to rely on these defenses. This could potentially encourage the deployment of smart contract–based agreements that favor parties with greater bargaining power in a disproportionate manner.

3.4 Contractual Standardization

The extensive implementation of smart contracts may expedite transformations in the provision of legal services, leading to a fundamental alteration in the legal profession. As smart contracts advance in complexity, individuals may increasingly depend less on legal counsel, choosing instead to utilize standardized agreements that integrate smart contract code.

For instance, rather than engaging a seasoned copyright attorney, a collective of musicians might opt to implement a meticulously scrutinized and widely trusted hybrid royalty agreement (such as an advanced iteration of the Ujo Music smart contract previously mentioned) that amalgamates conventional natural-language legal stipulations with smart contract code. A digital platform might be developed to guide the group through a sequence of inquiries, assisting the musicians in formulating a tailored agreement that aligns with their

specific requirements. This service could generate a hybrid agreement that encompassed pertinent intellectual property licenses and functioned cohesively with a smart contract to enable royalty payments without requiring a third-party middleman. Should such a service be initiated and smart contract-based agreements gain prevalence, individuals requiring legal assistance may progressively bypass direct counsel from a practicing attorney, therefore diminishing transactional legal work. Currently, we increasingly exhibit greater faith in computer-generated recommendation systems compared to alternative information sources, a phenomenon referred to as automation bias. Rather of critically evaluating information, we adhere to recommendations from computers and machines, regardless of whether the guidance is erroneous or leads to mistakes.

The increased accessibility of common libraries for smart contract code or hybrid agreements may result in the loss of some nuances in transactional legal activity. Due to the improbability of these libraries aligning precisely with the particulars of each commercial and legal agreement, contracting parties may opt to document their obligations through default provisions, without thoroughly assessing whether these provisions adequately address their legal requirements.(Kevin E. Davis) As we transitioned from a previous period of costly, custom-tailored apparel to mass-produced clothing with minimal personalization, the increasing utilization of blockchain technology and other contract automation tools may herald a shift from expensive, bespoke contracts to inexpensive, highly standardized legal agreements with restricted options for customization.

Criminal or Immoral Contracts

Smart contracts may attract malicious individuals seeking to partake in unlawful activity. Criminals cannot depend on conventional institutions such as courts or insurance to rectify deception or fraud.(Klaus Von Lampe and Per Ole Johansen) Instead, they depend on reputation, honesty, and honor to regulate behavior and deter cheating by harsh consequences, including physical harm or even death.(Bill McCarthy, John Hagan, and Lawrence E. Cohen)

Criminals now possess new instruments to orchestrate illicit activities using blockchains and related smart contracts. Smart contracts can establish legal systems that depend mostly or solely on lex cryptographica. Similar to digital currencies, nefarious entities might exploit this technology to establish illicit economic frameworks that deliberately circumvent current laws and regulations. The disintermediated, resilient, and tamper-resistant characteristics of a blockchain render commitments embodied in smart contract agreements difficult to terminate or modify once commenced. Smart contracts enable parties to engage in business transactions including the sale or acquisition of illegal things, such drugs, firearms, or Nazi memorabilia. Decentralized marketplaces could function independently of centralized authorities by utilizing lex cryptographica to monitor illicit activities within the network. Consequently, these markets may enable the extensive trade of items prohibited in specific jurisdictions.

Smart contracts can be utilized to facilitate gambling and various games of chance. Smart contracts can be utilized to establish the conditions of gambling agreements, eliminating the need for a centralized casino. Consider the Pokereum project, which utilizes smart contracts to facilitate poker gameplay on a blockchain network. In contrast to the

majority of current online poker games that rely on trusted third parties, Pokereum functions atop a blockchain-based peer-to-peer network, utilizing a set of smart contracts to manage tasks such as shuffling cards and conducting ether transfers after each hand.(Pokerium)

These instances may merely signify the inception of a more extensive trend. Researchers at Cornell University and the University of Maryland have indicated that blockchain technology might potentially permit more intricate crimes, such as the killing of a public figure, via a bounty governed by a smart contract.(Ari Juels, Ahmed Kosba, and Elaine Shi)

Researchers indicate that entities intending to assassinate a senator, president, or prime minister may deposit digital currency into an escrow account established and administered by a smart contract. Individuals seeking to claim the bounty may submit information to the governing smart contract (via a digitally signed message), including fundamental aspects regarding the date and location of the assassination. To ascertain the appropriate timing for disbursing the bounty's award, the smart contract may consult one or more reliable oracles such as a feed from the New York Times to evaluate the victim's death status. Should an assassin's prior communication align with the data disclosed by the reliable oracle, the smart contract might autonomously deposit the bounty into the criminal's account.

This approach could potentially promote criminal activities and enable mob behavior. A smart contract that delineates the requirements for a crime and manages the associated payment would eliminate the necessity for criminals to arrange a meeting for planning or recompense. An assassin need just comprehend the bounty and carry out the act in accordance with the stipulated conditions of the smart contract. The assassin could conceal their identify by use mixing services or more anonymous cryptocurrencies like Zcash. Smart contracts facilitate the coordination of unidentified parties, enabling participants in criminal activities to participate in unlawful conduct without the necessity of communication.

Ultimately, in the context of legal and commercial agreements, blockchains facilitate both legitimate and unlawful conduct. They may facilitate and underpin novel digital agreements that function autonomously, reducing monitoring expenses and hazards associated with opportunistic conduct potentially heralding an era of machine-to-machine transactions and AI-generated agreements. Simultaneously, akin to digital currencies, malevolent entities could exploit this technology to establish illicit economic frameworks that are difficult to trace and may deliberately circumvent existing laws and regulations. Entities may depend on lex cryptographica to complicate governmental and public authority intervention, hence fostering black markets, gambling, and illicit activities, including crimes orchestrated by untrustworthy parties.

4. Methods of Governance

Blockchain technology reduces the necessity for intermediaries, allowing parties to participate in economic and social interactions on a more peer-to-peer basis, and promotes the development and implementation of autonomous systems or devices. Nonetheless, despite

these prospects, governments continue to possess the authority to regulate the utilization of these technology.

Multiple intermediates are essential for sustaining blockchain-based networks, particularly Internet Service Providers and other entities that function or assist protocols situated lower in the TCP/IP stack. Blockchains are fundamentally governed by individuals and miners, who are predominantly driven by economic incentives. They depend on software developers and hardware manufacturers, which function inside a certain jurisdiction and can therefore be governed by municipal, state, or national authorities. In his analysis of Internet regulation, Lawrence Lessig articulated a theory commonly known as the "pathetic dot theory,"(Cade Metz) which delineates how an individual's behavior can be influenced or governed through four distinct mechanisms: state-enacted laws, societal norms, market dynamics stemming from supply and demand, and the architecture that defines both physical and digital environments. A government can most effectively affect individual behavior by enacting rules that either authorize or forbid specific actions.3 Individuals, under the prospect of legal action, must either alter their behavior or incur a penalty for non compliance.A government can most effectively affect individual behavior by enacting rules that either authorize or forbid specific actions.Individuals, under the prospect of legal action, must either alter their behavior or incur a penalty for noncompliance.

Governments, meanwhile, can also affect individual behavior in more nuanced manners. They can not only enact legislation that delineates acceptable conduct but also apply indirect pressure on persons and organizations. For instance, governments can employ taxation to manage markets and their participants or to establish new societal standards gradually. They can formulate policies that influence the structure of both the physical and digital realms—from implementing speed bumps near educational institutions to reduce vehicular speed, to establishing regulations about data gathering to improve online privacy.(Ruben Lee) In considering methods to affect individual behavior, governments may opt to utilize any or all of these many policy instruments. (Donald MacKenzie and Yuval Millo)

The advent of lex cryptographica and blockchain technology introduces a novel array of issues for regulators. Given that blockchains enable decentralized, disintermediated, tamper-resistant, resilient, and potentially autonomous code-based systems, inquiries arise regarding the applicability of the four regulatory forces defined by Lessig within the blockchain environment. Indeed, due to the autonomous characteristics of certain systems, the "pathetic dot" that serves as the regulatory object seems to be vanishing, supplanted by autonomous code-based systems that function independently of any natural or legal entity. At first glance, it appears that governments may forfeit their capacity to regulate these blockchain-based networks and the applications and services built upon them. Nonetheless, appearances may be misleading. Similar to the Internet, legislation can continually evolve to govern, limit, and shape the advancement of blockchain technology. Ultimately, blockchains are merely a decentralized network, akin to the Internet.

Even the most independent systems are influenced by certain pressures and constraints. Although blockchain-based systems may be constructed to circumvent legal frameworks, they rely on new intermediaries that facilitate the underlying blockchain network,

which are subject to regulation. Furthermore, these systems inherently depend on code (or architecture), and their functions are ultimately governed by market dynamics and influenced by societal standards. Legislation can affect all three of these factors to govern the technology.

Governments may most effectively regulate blockchain technology by enacting laws and regulations that directly target end users.(Richard Squire) The intrinsic transparency of most blockchain networks, along with their predominantly pseudonymous nature, leaves parties involved in blockchain transactions vulnerable to governmental demands. Indeed, advanced data mining techniques and big data analytics enable law enforcement agencies to detect individuals utilizing blockchain technology for questionable or illegal activities.Deanonymization strategies might possibly disclose the names of individuals engaged in blockchain transactions by analyzing the relationships of recorded transactions and integrating this information with contextual data.(Jeremy C. Kress,)As data accumulation increases and data mining techniques advance, individuals may have difficulties in maintaining the confidentiality of financial transactions or other activities conducted on a blockchain network.(Mills)

Although feasible in practice, regulating end users is onerous and time-intensive. As previously established about online copyright infringement, pursuing actions against end users offers an inadequate resolution because to the challenges associated with identifying and prosecuting individuals.(Arthur E. Wilmarth Jr.,) These issues are expected to be intensified inside the realm of blockchains due to the technology's significant dependence on encryption and various data-protection methods.

Rather than explicitly attributing responsibility to individuals for utilizing a blockchain-based system, governments could impose vicarious liability on end users for engaging with unwanted blockchain applications. Entities utilizing and compensating for a blockchain-based application are ultimately accountable for maintaining the service's functionality, justifying the imposition of both direct and vicarious liability on these users for enabling unlawful activities arising from that platform. Users engaging with a fraudulent blockchain-based gambling platform derive subjective benefits from their interactions while simultaneously supporting the platform by remitting fees to miners, thereby ensuring the continued availability of the illicit service for others. The potential for vicarious liability may enhance the deterrent effect: awareness of the possibility of being apprehended is one aspect; understanding that such apprehension could result in accountability for the acts of others is another. In certain instances, individuals may fail to understand the harm that a blockchain-based system could inflict, leading to potential causality issues. Imposing accountability on persons for activities that are unforeseeable or unexpected would be inherently unjust and unfair. Prior to implementing regulations aimed at individuals facilitating blockchain operations, governments should establish a clear causal nexus between a person's transaction and any unlawful act (or the unlawful acts of others) to confirm that such illegal activity was indeed foreseeable.

Governments may opt not to directly control end users; but, they maintain the authority to legislate intermediaries engaged with blockchain systems, mandating their assistance in monitoring these decentralized networks. Employing this technique enables

governments to exert control and indirectly regulate blockchain technology to deter unlawful or undesired activities.

Transportation Layers

The transportation layers of the Internet have been acknowledged for an extended period as sectors in need of regulation. Governments can utilize ISPs as a regulatory mechanism or as "a crude instrument of Internet discipline," as articulated by Jonathan Zittrain, by mandating the monitoring and selective disregard of data packets associated with specific addresses.(James W. Christian, Robert Shapiro, and John-Paul Whalen,) Although the Internet may be relatively decentralized, Internet Service Providers (ISPs) are typically recognizable and hence subject to regulation within certain jurisdictions, enabling governments to influence citizens' interactions with the Internet. The United States has been hesitant to enforce regulations mandating that ISPs monitor online activities, whereas countries like China have actively employed coercive measures, compelling ISPs to filter traffic and eliminate politically sensitive or pornographic content from the Internet. A blockchain-based network essentially relies on Internet connectivity and functions atop the TCP/IP protocol. This protocol transmits information among network-supporting nodes and assists them in achieving consensus on the recording of new data or code in the shared database

Internet service providers can function as a rudimentary disciplinary tool to regulate and oversee these emerging decentralized and increasingly autonomous networks.(Dominic O'Kane ") The intrinsic transparency of blockchains enables ISPs to identify which computers are linked to a blockchain network (by their IP address or hostname) and, in certain instances, to scrutinize the data being documented on the blockchain. As blockchain technology proliferates, governments may mandate that ISPs within their jurisdictions obstruct data originating from or destined for a specific blockchain, or, more specifically, differentiate among transactions executed within a particular blockchain-based application based on their respective sources or destinations. Although entities engaging with blockchain-based applications may utilize encryption and anonymization methods to obscure their identity and inhibit an ISP from scrutinizing their data, the traffic on the Bitcoin and Ethereum networks presently remains unencrypted. Moreover, although participants engaging with these blockchains may opt to conceal their browsing activities (e.g., by use the Tor browser), only a small percentage of Internet users presently employ such precautions.

The regulation of ISPs could significantly affect the traffic to blockchain-based networks or applications, thereby restricting the public accessibility of certain blockchain services and, consequently, diminishing the potential user base from which these systems could generate fees.

Information Intermediaries

In addition to transportation layers, governments possess the authority to impose rules on information intermediaries, such as search engines and social networks, mandating that they intentionally refrain from indexing or disseminating links to unwanted or illegal

blockchain-based apps. All blockchain networks require assistance from third parties, or maybe machines in the future, to compensate miners for transaction processing and network maintenance. Although one can acquire knowledge of online apps via word of mouth, these systems are more frequently identified through prominent search engines or endorsements from friends, family, or acquaintances on social networks.(European Market Infrastructure Regulation (EMIR) Information intermediaries possess the ability to obstruct individuals from discovering blockchain-based applications, hence constraining the proliferation of this technology.(Noah L. Wynkoop) This method has been progressively examined to regulate illegal or undesirable online activities and content. The European Union has recently implemented regulations for information intermediaries to safeguard privacy rights via the innovative "right to be forgotten." The Motion Picture Association of America (MPAA) has allegedly sought to coerce Google into filtering and eliminating links to copyrighted content and has lobbied Congress for legislation that would empower its members to obtain court orders to prevent internet infringement.(Robert Steigerwald,) Major information intermediaries, like Facebook and Twitter, have yielded to external pressure and now eliminate messages that could be considered to provoke or promote "abusive or hateful conduct" or that may be classified as "fake news."

Similarly, if governments consider blockchain-based networks or applications excessively hazardous or malevolent, they may enact laws or regulations mandating that information intermediaries remove blockchain-based services, aiming to significantly impede public access to these systems.

Blockchain-Specific Intermediaries

New enterprises and services leveraging blockchain technology are emerging and growing sufficiently to enforce governmental rules and regulations. Upon the Internet's initial emergence into general awareness, there were persistent assertions that this global network will result in extensive disintermediation and the elimination of all intermediaries.(John. C. Coffee,) Nonetheless, when the Internet achieved widespread acceptance, it became evident that, although it obviated the necessity for certain intermediaries, it simultaneously facilitated the rise of other intermediaries that could be subject to regulation.(Anita K. Krug, “) A comparable trend is emerging in the realm of blockchain-based applications, with new enterprises being established to function as novel intermediaries utilizing these technologies.(Coffee,) Not all blockchain-dependent services are autonomous. Certain services exclusively retrieve information from a blockchain, whereas others rely on a blockchain just to a limited extent for their functioning. For instance, substantial corporations supported by venture capital are offering "wallet" services that facilitate account creation for the transmission and reception of blockchain-based digital currencies such as Bitcoin and Ether.(Brad Smith and Elliot Ganz) Centralized exchanges are evolving, allowing anyone to transfer digital currencies into dollars, euros, or other fiat currencies.(S. A. Dennis and D. J. Mullineaux) Initially, there was uncertainty regarding the applicability of current financial laws and regulations to these services. In mid-2013, the U.S. government issued preliminary regulatory guidance indicating that digital currency exchanges may not legally operate in the United States without obtaining requisite licenses and implementing anti-money laundering (AML) compliance systems.(Michael Mackenzie and Tracy Alloway,) States like New York enacted technology-specific

legislation aimed at people who oversee or manage the transmission of digital currencies.(Josh Berkerman,) Currently, the exchange and storage of digital currencies increasingly parallel those of other currencies and assets. A significant number of services in the United States now primarily seek to enforce Anti-Money Laundering (AML) and money transmission regulations.

As emerging intermediaries proliferate across several jurisdictions, governments can exert pressure on these new chokepoints to enforce local laws and regulations. Centralized operators dependent on a blockchain or managing access to blockchain-based networks may be compelled to adhere to an expanded array of regulations, including mandates to report misconduct to law enforcement or duties to decline processing specific transactions.

Miners and Transaction Processors

Intermediaries are not only arising within blockchain-based networks; they also provide support for them. Blockchains depend on miners or alternative transaction processors to enable the transfer of digital currencies, the storage of data, and the execution of smart contracts. These miners obtain block rewards and fees for their endeavors.

In blockchain networks, miners possess the definitive authority to implement new software that alters or modifies the foundational protocol of the blockchain. By doing so, miners can alter the transaction history of the shared database or establish supplementary controls that dictate the storage, processing, and recording of information. For instance, due to Bitcoin's reliance on a proof of work consensus process, a majority of miners, as determined by their computational capacity, can collectively agree to modify the protocol's rules or disregard transactions associated with a particular Bitcoin account.(Nasdaq) In recent years, mining on prominent blockchain networks such as Bitcoin and Ethereum has become increasingly centralized, consolidating into massive mining pools (Tanaya Macheel) that combine the processing power of numerous machines to enhance the likelihood of obtaining a block reward. Currently, the level of centralization is pronounced, with four mining pools together controlling over 50 percent of the Bitcoin blockchain, while two mining pools jointly dominate more than 50 percent of the Ethereum blockchain. These mining pools could collaborate or conspire to fork a blockchain.

Through the regulation of miners and mining pools, governments can exert influence over the operations of blockchain-based systems, mitigating certain ostensibly uncontrolled traits of these novel decentralized frameworks. Should a blockchain-based network or application violate legal statutes, governments may compel mining pools to execute particular protocol modifications or potentially prohibit applications, corporations, individuals, or devices. Governments might alternatively offer miners targeted incentives, like as liability limitations or safe harbor provisions, contingent upon their adherence to legal standards and the processing of compliant smart contracts. Governments might deter miners from endorsing criminal apps by imposing taxes or penalties on them for processing transactions associated with illegitimate blockchain systems or devices. Nonetheless, overseeing miners and mining

pools is a complex endeavor. Although governments may regulate mining activities in a limited number of countries, such regulations may prove ineffective due to the global and decentralized nature of blockchain technology. Altering a blockchain's foundational protocol and functionality necessitates network consensus; if a significant number of miners or mining pools are located in jurisdictions unaffected by these regulations, the blockchain network may fork or persist in operation as though these regulations were nonexistent.

Equally concerning is the miners' potential inability to distinguish between legitimate and illegitimate uses of a blockchain-based network, particularly when the network accommodates both lawful and unlawful activities. In contrast to an ISP, which can partially monitor Internet traffic through methods like deep packet inspection, miners may be unable to discern between authorized and unlawful transactions within a blockchain network. Although miners can determine the cryptographic or technical validity of a transaction, they may lack the understanding of its intent without supplementary contextual information.

4.1 Regulating Code and Architecture

Governments can regulate parties who develop blockchain-based protocols and smart contracts. Code has historically been acknowledged as an effective instrument for implementing legal regulations. Technological systems such as the Internet lack inherent natural features associated with physical locations; therefore, they rely on code to define their structure and delineate the limitations of user actions.(Jeff Desjardins) Due to the reliance of blockchains on code for their functionality, governments may opt to restrict the manner in which developers construct blockchain-based applications and smart contracts, hence influencing the utilization and evolution of these systems. For example, new legislation could require software developers to integrate specific features, such as a government backdoor, directly into a blockchain's foundational protocol, thereby granting the government the authority to deactivate autonomous smart contracts or suspend a blockchain-based application that does not adhere to legal requirements.

Regulators could alternatively impose strict liability on developers for the creation and deployment of autonomous blockchain-based systems, incentivizing them to act with greater caution to mitigate the danger of harm. Similar to other potentially hazardous products, like as pharmaceuticals or aircraft, governments might implement a permission-based or command-and-control regulatory framework requiring parties to undergo an approval process prior to implementing a smart contract or a new blockchain. In this scenario, a central agency might meticulously evaluate prospective applications and decisively choose whether the public should be permitted to engage with emerging blockchain-based technologies.

Regulators could penalize developers or companies who deliberately produce software facilitating unlawful activities as part of this strategy. The creation of code is subject to regulation. When the "Melissa Virus" disseminated from a pornographic newsgroup in 1999, affecting over 1.2 million computers, (Houman B. Shadab,) judges and prosecutors did not abandon their efforts despite the extensive harm inflicted by the virus. The author of the virus

received criminal charges and was incarcerated. Nonetheless, a government's authority to regulate software producers is not unlimited. It is constrained by the disintermediated and pseudonymous characteristics of blockchains, together with First Amendment protections in the United States. While software has been recognized as deserving of First Amendment protection in some cases, such rights are not absolute.

If code is considered excessively hazardous or clearly illegal, courts have readily rejected a First Amendment claim. In United States v. Mendelsohn, the Ninth Circuit affirmed a ruling that deemed software developers, who created tools for recording and analyzing sports betting, guilty of unlawfully transporting "wagering paraphernalia," as the software served solely to facilitate illegal gambling.

Should governments opt to restrict blockchain developers, certain code may be safeguarded by the First Amendment, whilst other code may not be. Decentralized e-commerce marketplaces, utilized for the trade of daily things as well as potentially illicit products, such as narcotics or firearms, may be afforded First Amendment protection (provided the code is deemed as speech) due to their facilitation of both lawful and unlawful activities. In contrast, decentralized prediction markets and exchanges enabling the trade of binary options are likely to contravene existing legislation such as the Commodities Exchange Act (CEA), so exposing their inventors to potential responsibility.

In addition to First Amendment concerns, the problem of transnationality arises. Due to the global nature of blockchains, the technology limits a government's capacity to enforce regulations throughout the whole network. Unlike current online services, where centralized operators can unilaterally implement new features or restrictions in their code, the code regulating a blockchain-based network operates in a decentralized manner through distributed consensus. Modifications to a smart contract or blockchain protocol necessitate the endorsement of a majority inside the blockchain's network. Although governments may mandate that blockchain developers incorporate certain elements into their code, they cannot compel users or other private entities to embrace these features outside their jurisdictional limits. If governmental restrictions are too severe, ineffective, or unjust, miners participating in a blockchain network may repudiate these regulations by declining to install software that integrates such rules or by refusing to process transactions or smart contract code dictated by these laws.

To enhance the complexity of this regulatory framework, governments must possess the capability to identify the creators of blockchain-based applications and smart contracts in order to impose restrictions or liability on software developers. This task, while feasible, is frequently arduous due to the pseudonymous characteristics of blockchains. A government could identify pertinent parties by mandating that all developers of blockchain-based applications and their corresponding smart contracts register themselves and their creations in a searchable database, which would function as a traceable repository of existing blockchain-based applications. If any of these applications resulted in harm to a third party due to a coding flaw or operational problem, the pertinent parties could ascertain the creator and pursue appropriate measures to collect damages or assert legal rights.

This strategy is constrained by the reality that governments would have few to no options against developers in different jurisdictions who decline to register their software in this database. Furthermore, as demonstrated by Satoshi Nakamoto, anyone situated within a controlled jurisdiction might utilize anonymization techniques to implement blockchain-based apps in manners that are untraceable to their true identity.

Hardware Manufacturers

Similarly, governments possess the authority to regulate hardware manufacturers (such as Intel or Samsung), requiring them to adopt specific procedures to monitor or prevent the utilization of blockchain-based applications, smart contracts, or gadgets that enable illicit activities. Manufacturers utilize conventional trade channels, and as governments predominantly regulate the movement of commodities inside their territories, they can enforce rules and restrictions on both manufacturers and merchants. In the United States, manufacturers must adhere to safety and health, homeland security, and environmental requirements.36 Similarly, merchants engaged in international sales adhere to export regulations, and those aiming to produce pharmaceuticals or medical equipment must undergo a comprehensive regulatory approval process prior to public distribution. Through the regulation of manufacturers, governments could acquire the authority to control or deactivate a blockchain-based device, or even incapacitate an entire blockchain network if a smart contract malfunctions or if an autonomous system enables illicit activities. Governments may regulate manufactured items and oversee or authorize the selling of chips or other hardware essential for miners to sustain a blockchain-based network. They may restrict the functions that manufacturers are allowed to incorporate into a smart contract regulating a blockchain-enabled device or mandate that these devices contain backdoors or "kill switches." Similar to software developers, governments might impose strict liability on manufacturers for any harm resulting from a blockchain-enabled item. Manufacturers may be mandated to obtain government approval prior to marketing any equipment that utilizes or supports these new decentralized databases.

Nonetheless, historical evidence demonstrates that efforts to implement a technological backdoor or alternative access controls on software and hardware devices may compromise the technology's integrity. (Michael del Castillo,) In the 1990s, the U.S. government sought to require all manufacturers of encryption-enabled devices to integrate a chip developed by the NSA, known as the Clipper Chip, which would enable governmental authorities to decrypt data stored on the device. The chip was discovered to include multiple security vulnerabilities, allowing individuals to exploit the mechanism in unintended manners. (New York Stock Exchange)

Incorporating analogous access control systems into a blockchain-enabled device may diminish the advantages of utilizing blockchain technology initially. Such limitations would not only constrain the technology's unique attributes specifically autonomy, tamper resistance,

and resilience but might also render it more susceptible to exploitation by both governmental and non-governmental entities.

4.2 Regulating Blockchain-Based Markets

Governments may also utilize market intervention to affect the actions of entities who sponsor, utilize, or install apps on a blockchain, rather than adopting the previously mentioned ways. All current blockchain-based networks are fundamentally rooted in economics. To complete a transaction, participants are required to pay transaction fees to miners for the validation and addition of information to a blockchain or for executing a smart contract's computational logic. Although these fees are typically negligible for an individual transaction, such as an ether transfer, they can accumulate significantly in smart contracts with multiple logical phases.(Robert Sobel,) Consequently, for an autonomous system to operate on a blockchain, the pertinent smart contracts must acquire sufficient digital currency to offset their expenses. Due to the fees included into the technical framework of blockchains, each interaction with a blockchain is an economic transaction, with every participant in the network acting as an economic agent. The expense associated with a blockchain's operations consequently affects the actions of network members, including miners, software developers implementing smart contracts, and end users. These attributes render the regulation of a blockchain analogous to that of a conventional market. Similar to how a government can manipulate the pricing of goods or services to deter or promote specific behaviors such as imposing taxes on cigarettes or offering subsidies to certain producers altering the market dynamics of a blockchain-based network could similarly impact the conduct of all participants dependent on this collective network.

By adjusting the expenses associated with data storage or the execution of smart contracts, governments might influence the interactions among members in a blockchain-based network and potentially elevate the costs of operating and deploying smart contract code. By doing so, they can leverage the market dynamics of blockchain-based networks to motivate these systems to comply with the law by rendering it economically advantageous for them to do so. For a market-based regulatory strategy to be effective, governments must possess the capacity to alter a blockchain's foundational market dynamics. One approach to do this would include governments assuming control of the network's mining operations a process that currently necessitates acquiring a majority of a blockchain-based network's mining power, particularly in the context of a blockchain utilizing a proof of work consensus method. If governments managed transaction processing on a blockchain through a majority framework, they might initiate protocol modifications essential for transforming the fundamental economic incentives and payout structure of the blockchain. Network participants who consent to these modifications may adhere to the new protocol, while those who dissent may diverge and establish a smaller, potentially less secure blockchain. Furthermore, as they possess a majority of the network's computational power, governments could lower fees for lawful and authorized transactions while raising fees for unlawful transactions to deter potential illegal activities on a blockchain platform.

Governments might potentially affect the transaction execution costs on a blockchain by altering the value of the blockchain's native digital currency in the secondary market. A government cannot implement conventional monetary policies using a blockchain, such as increasing currency supply to induce inflation; however, it can still intervene in an open market by purchasing or selling the blockchain's native digital currency to influence its price upward or downward. This strategy is being employed by governments aiming to affect the exchange rates of various fiat currencies beyond their direct control, while avoiding domestic inflation increases. By purchasing and sustaining a reserve of foreign currency, a government can enhance the value of that currency in relation to its national currency, so augmenting the competitiveness of its exports and diminishing the incentives to import foreign goods.(Jeanne L. Schroeder,) A similar approach can be applied inside the framework of a blockchain-based digital currency. By acquiring and sustaining reserves of digital currency, governments can elevate the market price of the currency, consequently raising the expenses associated with data storage, transaction execution, or the deployment and execution of smart contract code on a blockchain network thereby affecting the degree of interaction among network participants and the market dynamics of the network itself. This strategy primarily focuses on the general utilization of a blockchain; nevertheless, governments could leverage it to influence miners or other network participants to modify the blockchain's foundational protocol. For instance, if governments threatened to raise the fees associated with Bitcoin transactions, they may compel the network to adopt protocol modifications required to impede or restrict illicit activities.

Certainly, if miners or other middlemen were aware of the government's authority, the potential for government action could inherently produce a significant deterrent effect. The knowledge that a government might alter the incentive frameworks associated with the development and implementation of blockchain systems could influence the progression of blockchain protocols and deter individuals from participating in illicit activities.

4.4 Regulation via Social Norms

The proposed methods herein are not the sole means of regulating blockchains. Governments may endeavor to preserve order on a blockchain by influencing the social norms developed inside a blockchain-based society. As blockchains are fundamentally underpinned by human involvement, societal norms can serve as a significant regulatory mechanism. Blockchains depend on distributed consensus for functionality, granting miners and other stakeholders the power to enforce legal or community regulations. Miners and other transaction processors function as adjudicators, possessing the authority to uphold the regulations or principles of a blockchain network. Network nodes can intervene to cease illegal conduct when a sufficient consensus is reached among them. The parties may jointly elect to intervene to rectify a harm by enacting requisite modifications to the protocol to censor or reverse specific transactions or to retract autonomous code. Diverse social norms have already emerged inside several blockchain-based networks. In the Bitcoin ecosystem, there is a strong emphasis on the

concept of "immutability," desiring a blockchain that remains unaltered. Nick Szabo asserts that "Bitcoin has preserved its integrity through decentralized decision-making among technological experts, coupled with a robust doctrine of immutability." Nonetheless, despite this common cultural standard, the Bitcoin network has encountered challenges in achieving consensus regarding the evolution of the Bitcoin protocol to accommodate a growing volume of transactions, as exemplified by the enduring "scalability debate" within the Bitcoin community.(Bob Hills, David Rule, Sarah Parkinson, and Chris Young,) Privacy and anonymity appear to be the primary motivators for other blockchain-based networks, such as Monero and Zcash. As previously outlined, both digital currencies are engineered to integrate robust privacy safeguards through the utilization of stealth addresses, ring signatures, and zero-knowledge proofs.(Kress) Proponents of Ethereum seem to have embraced a pragmatic approach, aiming to offer versatile tools for the development of decentralized blockchain applications. The Ethereum community has repeatedly altered the Ethereum protocol, forking the blockchain to implement supplementary features. This contrasts with the Bitcoin network, whose protocol has been modified infrequently, solely to rectify faults or tackle scalability issues. What sets Ethereum apart from other blockchain networks is that its community has modified the underlying protocol not solely for technical necessities but also to "regulate" network activities, thereby employing social norms to directly influence the network's operations. This intervention occurred in the context of the TheDAO hack. TheDAO was a blockchain-based, decentralized investment fund lacking a centralized operator, governed by an autonomous smart contract executed on the Ethereum blockchain. Due to its operation primarily by lex cryptographica, members of TheDAO had no means to recover monies siphoned by an attacker exploiting a flaw in the underlying smart contract technology. Rectifying the damage necessitated a unified effort by the entire Ethereum community to amend the protocol and condition of the Ethereum blockchain.(Bank for International Settlements, “Principles for Financial Market Infratructers) Executing such concerted action though technically as straightforward as installing a new software application was, nonetheless, a challenging endeavor. Altering the status of the Ethereum blockchain necessitated consensus among a majority of miners, as well as the broader Ethereum community, comprising digital currency exchanges and other commercial entities. Despite the occurrence of goal theft, the Ethereum community deliberated for nearly a month before reaching a consensus on whether and how to address the damage. Ultimately, key stakeholders in the Ethereum community resolved to execute a protocol modification via forking the Ethereum network. All proponents of the fork consented to transfer the funds back into TheDAO's account and substitute the existing smart contract code with a basic withdrawal contract, allowing stakeholders to reclaim the ether deposited in the fund. By altering the Ethereum protocol to recuperate the assets, the Ethereum community exhibited a readiness to intervene to rectify a perceived injustice.(Bank for International Settlements) The TheDAO event illustrates that societal norms may significantly influence the regulation of blockchain networks. Governments may influence the social norms of communities surrounding these

networks to indirectly regulate their functioning. Governments could influence societal norms by disseminating information regarding the risks and benefits of emerging technology, enabling individuals to make more informed judgments about engaging with specific blockchain-based systems. They could also initiate enforcement actions or prohibit certain activities, attempting to influence individuals' actions. Governments might actively participate in a blockchain-based network by acting as miners, thus acquiring a role in the network's governance. They could also establish official working groups or other nonprofit international entities to influence the advancement and evolution of the technology.(Bilski v. Kappos,)

4.5 Regulatory Tradeoffs

All regulatory approaches, irrespective of the strategy employed, have trade-offs. Governments have the dilemma of regulating either traditional Internet intermediaries, such as ISPs, or the novel intermediaries facilitating blockchain networks, with both strategies posing the risk of stifling innovation and perhaps limiting the new opportunities offered by blockchains. (Andrew Beckerman-Rodau)

Internet researchers and technologists have consistently contended that governments ought not to control networked settings in a manner that could contravene the “end-to-end principle.”(Robert Jackson,) This principle posits that networks need to be constructed with maximal simplicity and generality, thereby allowing "intelligence" to reside at the "edges" of the network. Network operators should solely be accountable for routing data packets across the network infrastructure without prioritizing certain packets over others.(Shaun Martin and Frank Partnoy)

The end-to-end principle was primarily promoted for technical reasons; but, as noted by Lawrence Lessig and Mark Lemley, it possesses significant attributes as it "broadens the competitive landscape by allowing a greater diversity of applications to connect and utilize the network."(Shaun Martin and Frank Partnoy) The end-to-end principle is regarded by numerous authors and experts as a fundamental factor contributing to the remarkable expansion of the Internet. If the original architecture of the Internet had been executed in a more centralized fashion, with central authorities positioned at the core of the network, many contend that it would not have fostered the same level of experimentation and invention. (David Yermack,) The Internet fostered an atmosphere of "permissionless innovation," allowing individuals to initiate and implement new services or business applications without the oversight or undue influence of a limited number of gatekeepers.

The architecture of the majority of blockchain networks largely adheres to the end-to-end principle.(Jessica Erickson) Blockchains are fundamentally neutral data and computational layers that are indifferent to the type of data they store or the objectives of the applications they execute. All transactions submitted to these networks are processed uniformly at the technical level and will be approved if they comply with the requirements of

the underlying protocol. Miners on a blockchain network need just to confirm that transactions are valid according to the protocol's requirements. They do not indiscriminately censor transactions, as this could result in economic loss.(Bengt Holmstrom and Steven N. Kaplan) In regulating a blockchain, governments may either uphold the end-to-end principle or implement a more stringent regulatory framework by imposing regulations on miners or other intermediaries involved in a blockchain network, necessitating their active participation in monitoring these networks.

Some may contend that the end-to-end principle is irrelevant in the context of blockchain-based networks due to the inherent characteristics of the activities conducted on these networks. Considering that blockchain-based transactions frequently entail value transfer, the associated hazards in these networks are arguably more significant than those related to the transmission of media or communications. The utilization of blockchains for payment systems, financial exchanges, and the safeguarding of critical government documents may lead to instability and hazards due to the end-to-end concept, so undermining governments' capacity to protect significant assets and data. If governments wish to prevent permissionless innovation from disrupting established financial and governmental systems, greater centralized control may be required to maintain the functionality of these systems.

In contrast, individuals aiming to enhance innovation may endeavor to uphold the end-to-end concept within blockchain frameworks and establish new legal standards mandating that miners handle all blockchain transactions equitably. The increasing concentration of power among a limited number of telecommunications operators and online market entities has prompted demands for "network neutrality," which advocates for the prohibition of telecommunications companies and ISPs from directing Internet traffic based on data type, source, or destination. Similarly, in the realm of blockchain applications, there may arise demands for "blockchain neutrality," necessitating that miners process transactions impartially, irrespective of their origin or intent.

Secondly, governments may opt for unrestricted development or impose comprehensive regulatory limitations on software development. They may seek to obstruct innovation on blockchain networks, complicating the ability of private entities to develop or implement innovative (and legal) applications. The United States government currently regulates code across several settings to safeguard certain businesses, improve safety, and restrict the dissemination of illegal or harmful content. For instance, the Digital Millennium Copyright Act granted copyright holders the authority to deploy DRM systems and established penalties for circumventing these systems.(Jason Zweig,) Congress has enacted legislation mandating that media and broadcast firms utilize filtering software and v-chips to restrict access to television shows for the protection of children,(Cynthia A. Williams) thereby generating First Amendment issues.(Michael Jensen and William H. Mecking,) Furthermore, to improve the safety of air travel, the U.S. Federal Aviation Administration (FAA) oversees the development of public safety code, mandating that developers adhere to recognized software engineering techniques to guarantee the program functions correctly.

Regulation of blockchain-based apps may mirror existing frameworks, thus hindering innovation. If autonomous blockchain-based systems enable illegal activities, more detailed regulation of their development could mitigate unanticipated risks and prevent harm. By mandating that these applications conform to fundamental norms, governments could ultimately achieve a suitable equilibrium, safeguarding the advantages of the technology while mitigating concerns associated with autonomy. Governments might, for example, influence the types of applications utilizing blockchain technology by enforcing stricter laws on specific applications such as financial applications or those involving autonomous devices while easing the standards for less contentious applications. Third, governments may opt to utilize alternative regulatory mechanisms, such as market or social standards, to oversee a specific blockchain network or application. By affecting the market dynamics of a blockchain-based network, governments acquire the ability to disturb the natural equilibrium and alter the prevailing practices of the community of participants engaged with that network. While it may suppress innovation and impede technological advancement, it could also function as a mechanism to shape the behaviors of that network, compelling it to adopt certain policy objectives outlined above. Should the processing of transactions on a specific blockchain network become too costly or inefficient, rival blockchains may arise that are immune to governmental interference. These new networks will presumably depend on an alternative mining algorithm and necessitate a distinct array of hardware devices, thereby constraining the effect of such regulation.

As is frequently observed in regulation, all the regulatory measures examined below are partial answers. If individuals intend to develop or implement blockchain-based applications or smart contracts to cause harm or otherwise affect another party, the solutions presented here are unlikely to eliminate all illicit conduct. Similar to how governments seek to mitigate the risks associated with firearms by imposing limitations on manufacturers and increasing the costs of acquisition through licensing and other regulations, they continue to face challenges in preventing the illicit use of guns by individuals.(Troy Paredes) Unauthorized firearm possession continues. (Baruch)

In the realm of blockchain systems, there are intrinsic constraints on the extent to which governmental entities may monitor and regulate the actions of software developers, manufacturers, market participants, and other intermediaries. Similar to the inability of governments to completely monitor the Internet to eradicate all avenues for criminal or undesirable conduct, they will also be unable to prevent all illicit activities on a blockchain-based network, notwithstanding the regulatory mechanisms available to them.

4.6 Code as Law

While governments could fail to regulate blockchain technology comprehensively, they may nonetheless rely on blockchains as a means to apply their own laws and regulations in a more efficient and automatic way. Similar to how governments and corporations have progressively embraced and integrated the opportunities provided by the Internet and digital technologies into their everyday operations, both public and private actors could potentially use blockchain

technology to establish their own system of rules and regulations, implemented using selfexecuting, codebased systems. Leveraging the transparency and tamper resistance of a blockchain along with the automatic execution of smart contract code, governments have the opportunity to experiment with new means of code-based regulation to achieve specific policy goals and potentially constrain blockchain-based applications. With blockchain technology and associated smart contracts, a growing range of legal and contractual provisions can be translated into simple and deterministic code-based rules that are automatically executed by the underlying blockchain network. Thus, not only is it important to understand how blockchain-based applications can be regulated, but it is also necessary to assess how lex cryptographica can be used for regulation.

Irrespective of their intentions, all laws and regulations possess a common aim: to direct behavior in order to promote specific actions.("Distributed Ledger Technology: Beyond Block Chain,") Laws can establish a framework of incentives or rewards to encourage desired behavior, or they might enforce a system of punishment or sanctions for undesirable conduct.(Daron Acemoglu, Simon Johnson, and James A. Robinson,) Through either approach, governments actively influence individuals' intentions, functioning as either an incentive or a deterrent.(Simon Johnson,) Nevertheless, individuals retain the autonomy to select the most advantageous course of action. Like legislation, technology possesses a comparable ability to affect an individual's behavior.(Hernando De Soto,) Technology enables individuals to perform tasks that would otherwise be impossible, such as air travel or telecommunication, while also regulating the methods of execution, including the maximum velocity of an aircraft or the bandwidth of a telephone line. In contrast to the law, technology offers limited options for individuals to determine their path of action. It depends on stringent regulations and technical attributes to offer certain affordances and limitations that eventually influence human relationships. (Moussa Ouédraogo)

Until now, technology was regarded as a regulatory instrument alongside the law that shaped human conduct.(Peggy Garvin,) However, with the emergence of the Internet and digital technology, code has evolved into a significant regulatory instrument employed by both public and private entities to influence an expanding array of actions in manners that frequently surpass legal boundaries. Lawrence Lessig articulated in 1999 that "Cyberspace will primarily be regulated by... cyberspace," signifying that code will ultimately serve as the "supreme law in cyberspace." In essence, as articulated by Charles Clark, "The response to the machine is the machine."The most effective method to govern a code-based system is via the code itself.Both Lessig's and Clark's assertions resonate profoundly within the realm of blockchains. If governments find it challenging to enforce laws against autonomous blockchain systems, they can consider utilizing blockchain technology to establish a new framework of code-based legislation for individuals, corporations, and machines.

Blockchain technology and its corresponding smart contracts enable the conversion of legal and contractual stipulations into straightforward, deterministic code-based rules that are performed automatically by the underlying blockchain network. Technical regulations may progressively adopt the same role and function as legal statutes.(Timothy P. Layton,)

Transposing Law into Code

Similar to how code may encapsulate entire legal agreements or their components, governments possess the capacity to codify laws and regulations particularly those with objectively verifiable constraints or parameters and integrate them into software. Governmental authorities and public administrations have increasingly utilized code to integrate and enforce existing rules and regulations, primarily of an administrative character. These software systems encompass a wide array of applications, from evaluating individuals' eligibility for welfare benefits and public assistance ("The Biggest Security Threats") to identifying parents who may be obligated to contribute child support. Several states in the United States utilize software to determine the eligibility of low-income residents for the Supplemental Nutrition Assistance Program and to assess their entitlement to food stamps.(Melanie Swan,) The United States employs data mining and big data analytics to conduct predictive evaluations of national security hazards, automatically placing individuals on a no-fly list to safeguard against terrorism.(Michael del Castillo,) Governments aim to assure legal compliance through the development of these code-based systems. Legal provisions are automatically enforced by the underlying technological infrastructure through the translation of laws into technical norms. Rather than pursuing offenders post-violation, code-based systems might enhance legal compliance by preemptively averting infractions. Assigning the responsibility of executing these regulations to a technical system mitigates the danger of non-compliance whether accidental or intentional thereby reducing the necessity for supervision an continuesenforcement.

In certain instances, codifying laws diminishes the ambiguity regarding the interpretation or implementation of these regulations. Due to the structured nature of computer code, governments may accurately delineate, in advance, how laws should be implemented. In contrast to laws articulated in normal language, code-based regulations provide little interpretation, hence enabling more consistent and predictable implementation.(Pete Rizzo,) Certain rules and regulations are especially amenable to codification.(Laura Shin,) This is especially applicable to laws that are clear and unequivocal, such as those governing the distribution of welfare and social assistance, food stamps, or the computation of taxes and other financial obligations. Despite the intrinsic intricacy of these laws, their provisions can be transposed into code provided they can be expressed as conditionals ("if this, then that") or objectively proven. Code-based regulations can potentially be more readily adjusted to accommodate specific individuals, with varying conditions activated based on their present or historical conduct. The increasing dependence on big data analysis and machine learning methodologies enables the construction of an individual's profile by examining their behavior in both online and offline contexts.(Avi Spielman,) The utilization of such data to guide the functioning of certain software applications may result in the development of a new

generation of highly tailored rules or laws that can be automatically modified to meet the specific demands and attributes of individuals.(Martin Chuvol,)

4.7 Blockchain Technology as Regulatory Technology

Similar to other technologies, blockchains may assist governments in converting laws into code. Blockchain protocols and smart contracts can model or embody laws, embedding them directly into a blockchain network to ensure automatic execution and preemptive enforcement of these regulations. By integrating laws into a smart contract and mandating that parties engage with these contracts or embed them into their information systems, governments can automate the enforcement of particular rules or regulations without the necessity of actively monitoring every transaction. Legislation enacted by blockchain technology offers distinct advantages over conventional coding in terms of autonomy and transparency. The execution of smart contract code is redundantly performed by the blockchain network, and it cannot be unilaterally altered by any individual entity. Consequently, encoding legal rules into smart contract code, as opposed to software on a centralized server, ensures that no central authority can modify these rules or obstruct their execution. A blockchain-based platform provides the assurance that all parties engaging with it adhere to the established regulations. Governments might thus enforce adherence to regulatory criteria through the utilization of smart contracts embedded in these code-based systems. This enables the attainment of a novel form of technical accountability one governed by technology and less reliant on conventional ex-post enforcement.

Furthermore, due to the inherent transparency and tamper resistance of blockchain technology, any regulation established through a smart contract or integrated within a blockchain-based protocol can be documented and recorded on a cryptographically secure and distributed data system, thereby offering an auditable record of activities associated with a specific account or smart contract. From a regulatory standpoint, blockchains may demonstrate greater reliability than conventional reporting methods, as they are both declarative and performative; one cannot assert the execution of a transaction without having genuinely completed it. Given that information inscribed on a blockchain cannot be unilaterally altered or erased by any individual entity, a blockchain serves as reliable evidence of the occurrence of a specific transaction. By integrating legal stipulations into a blockchain protocol or smart contract, governments may ascertain the application of the law, including the timing and parties involved, while mitigating the possibility of manipulation by a centralized operator.(Andrea Tinianow and Caitlin Long,)

Governments worldwide enforce anti-money laundering (AML) legislation, mandating financial institutions to monitor value transfers (including virtual currencies) and report suspicious activities to combat money laundering, tax evasion, and terrorism financing. Utilizing blockchain technology, legislation could mandate that regulated intermediaries such as virtual currency exchanges deploy or engage with designated smart

contracts that govern transaction flows for these intermediaries, permitting transactions solely when they conform to the stringent logic of the underlying code. A blockchain may be utilized to ascertain an individual's authorization to transfer virtual currency, and based on the data obtained from the blockchain, a smart contract could restrict the quantity of virtual currency a person is rightfully permitted to transfer at any moment.
This principle may also pertain to derivatives-based smart contracts. Title VII of the Dodd-Frank Act amended the U.S. Commodities Exchange Act, instituting new reporting regulations and augmenting margin requirements for uncleared derivatives. The compliance expenses for the institutions impacted by these regulations might be substantial.("Dubai Wants All Government Documents on Blockchain by 2020) A blockchain enables margin requirements to be included within a smart contract, which governs the contractual relationship between the two parties and ensures compliance with the necessary margin calls. Should the trade's risk escalate due to an external event such as a surge in interest rates or a decline in the credit rating of one party the smart contract may autonomously augment the collateral in the relevant trading account to ensure legal compliance. Similar to money transmission laws, blockchain technology has the potential to substantially decrease the expenses associated with regulatory compliance for collateral management and margin requirements, enabling regulators to verify that parties do not engage in agreements that may introduce additional risks in the event of default.(Swan, "Blockchain.")

Tax collection might potentially be optimized by blockchain technology. Automated smart contracts may facilitate the compliance of individuals, corporations, and maybe machines utilizing blockchain systems with tax obligations. For example, rather than awaiting periodic tax returns, tax authorities could mandate that certain taxes such as value-added taxes (VAT) or personal income taxes be automatically computed and remitted immediately upon transaction completion through the utilization of specially designed smart contracts, which would be executed each time a party receives or disburses funds from a designated blockchain-based account or when one party engages with a specific smart contract. This solution would minimize the necessity for periodic tax reporting and diminish opportunities for individuals or corporations to perpetrate tax evasion or other forms of fraud. Similarly, within the framework of the Internet of Things, smart contracts may be utilized to guarantee that blockchain-enabled devices autonomously remit taxes whenever they partake in profitable economic transactions, even in instances devoid of human involvement, relying solely on machine-to-machine interactions.

These methodologies could facilitate blockchain technology in attaining particular regulatory goals more efficiently and economically than current rules and regulations. Expanding upon Lessig's examination of the dual role of computer code on the Internet as both an adjunct and an enhancement to legal frameworks, blockchain technology may play a progressively significant role in governing the conduct of persons and machines. As governments and public institutions embrace this technology, we could transition from a regulatory approach of "code is law," which utilizes code to enforce specific rules, to "code as law," where technology inherently defines and enforces state-mandated laws.(Price Waterhouse.)

For efficacy, blockchain-based solutions must be embraced by private entities, necessitating that governments not only create smart contracts and other code-driven systems but also legislate to compel regulated institutions and additional private parties to engage with these blockchain systems. Proposed legislation may mandate that banks and financial institutions engage with government-sanctioned smart contracts or similar code-based systems during monetary transfers to ensure adherence to money transmission regulations. Governments could mandate that businesses utilize a blockchain-based network for transactions involving specific goods or services to guarantee the payment of VAT.

Governments could alternatively choose to incentivize companies and organizations engaging with blockchain-based systems by easing legal constraints or reporting duties. A blockchain can function as a verified audit record of transactions, allowing governmental authorities to retrospectively confirm a private actor's legal compliance. In the event of a disagreement or public injury, a government official may utilize the information documented on the blockchain to accurately ascertain the cause and the accountable parties, and if warranted, inflict appropriate sanctions.

Limitations of Code as Law

The conversion of legislation into code is fraught with challenges. Relying on the precise language of code to govern individual behaviors poses inherent risks. Not all statutes can be readily converted into code. Legal standards are articulated in natural language, which is inherently fluid and ambiguous. Well-crafted rules and regulations typically seek to address a range of unforeseen contingencies not anticipated by the lawmaker. By formulating legal regulations in a broad and ambiguous manner, these regulations can be utilized in diverse contexts even those not explicitly considered by the legislator without necessitating further additions or modifications to the existing legislation.

The adaptability of natural language also introduces increased ambiguity. Judges interpret and reinterpret laws to ascertain, on an individual basis, the applicability of the law to specific circumstances. In certain instances, a court may be required to reinterpret the law if the application of its literal text, in light of the case's facts, would contravene the statute's original intent.(Christopher D. Hoffman,)

Codifying open-ended laws articulated in natural language may distort their intended meaning by rendering them less adaptable and incapable of responding to unforeseen circumstances. (AIan Allison) Due to their dependence on computer code, smart contracts are ill-suited for indefinite legal stipulations. Code is applicable just to a collection of objectively verifiable rules established within the foundational code. Until the emergence of increasingly sophisticated AI systems, computer code will typically be unable to adapt to and address new and unforeseen circumstances that may arise in a complex society.(Martin Ruubel) Consequently, at present, smart contracts are applicable solely in a limited range of situations.

Since it is nearly impossible to anticipate all potential applications of a specific set of rules in various situations, laws dependent on a blockchain-based system would probably

possess a more limited reach than conventional laws and regulations. Rules articulated in rigid and formal language lack the adaptability of natural language and fail to address unforeseen edge circumstances that exist in legal gray areas those not sufficiently covered by the foundational code. The formal nature of code may facilitate the manipulation of legal rules when they are converted into code-based regulations. Unless all contingencies are explicitly described in a smart contract (which is improbable), individuals may discover methods to circumvent these regulations, either due to overly exact coding or insufficiently broad parameters. Examining the smart contract code enables individuals to discern actions required (or to be avoided) to activate (or refrain from activating) specified conditions, so evading the applicability of any legislation encoded within. The hack of TheDAO serves as a valuable lesson in this context. By putting contractual stipulations typically articulated in plain language into the codified language of code, TheDAO's smart contract inadequately represented the true intents of the contracting parties.33 An attacker exploited a weakness in the smart contract, resulting in the unauthorized extraction of nearly $50 million worth of ether, an outcome unforeseen and unintended by other members of TheDAO.

If governments employed smart contracts to enforce code-based rules and regulations, analogous concerns would undoubtedly arise, thereby diminishing a government's inclination to enact laws as code. These restrictions universally affect all code types, but they are intensified inside a blockchain-based infrastructure due to the resilient, tamper-resistant, and autonomous nature of smart contract code. If a regulation is improperly executed as a smart contract, rectifying the resulting error may be challenging without engaging in subsequent court proceedings.

Automated Rules

The tamper-resistant and automated characteristics of blockchain-based systems present a dual challenge. Although the technology may diminish the expenses associated with regulatory compliance and law enforcement, it could also result in the implementation of particular laws and regulations that fail to accurately embody the original goals of the legislative body. Legal regulations depend on a framework of retrospective sanctions. Individuals have the autonomy to determine whether to adhere to these regulations, and those who contravene the law are penalized subsequently. Technical regulations establish a framework of ex-ante governance, permitting individuals to act solely in accordance with the stipulations outlined in the code.

A code-based approach ensures that regulations cannot be breached without altering the foundational technological infrastructure. However, the drawback is that, due to the constraints of software code, expansive technical regulations may inadvertently restrict chances for legitimate operations. A framework composed of inflexible, code-based regulations may restrict individuals' capacity to engage in legally allowed actions by limiting allowable behaviors to a finite array of predetermined conditions.

The automated characteristics of smart contracts, coupled with the difficulty of modifying its foundational code, may result in scenarios where a defective code segment is perpetually executed, adversely affecting all stakeholders involved. For example, returning to

the earlier illustration of taxation, if a government mandated that entities utilize a smart contract for tax payments and the smart contract contained a coding flaw either due to a software defect or an inherent limitation in the translation of conditions into code a scenario could arise in which the blockchain-based system would impose charges exceeding the actual tax liabilities of the parties involved. Since the smart contract code is implemented automatically by the underlying blockchain network, only judicial action can rectify the harm suffered by these parties.

Customized Rules

Ultimately, as blockchain-based regulations develop into personalized frameworks, they may contradict essential principles of universality, equality, and non-discriminatory practices.(Brian Forde) As blockchain technology advances, governments may opt to implement legislation that integrates smart contract code and external oracles, utilizing external data. Through the implementation of code-based regulations informed by data mining and big data analytics, regulators could differentiate among citizens, subjecting them to varying restrictions based on their identification, profile, or past and present behavior. Flecks of this planet are beginning to manifest. The Chinese government has proposed the establishment of a "social credit system" (Joshua A. Kroll, Ian C. Davey, and Edward W. Felten) designed to issue a national score (or reputation) to each Chinese citizen. The social credit system will affect how Chinese citizens engage with governmental services, particularly the legal system.38 Although there is presently no intention to implement this system on a blockchain, it is conceivable that smart contracts may be designed to interface with this system, activating the application of various rules and conditions based on the score assigned to each participant.

Progress in data mining and profiling methodologies may promote and expedite the development of algocratic systems, regulated by a framework of stringent and formalized code-based regulations, which are, however, intrinsically dynamic and adaptable. If laws are integrated into a technical framework that evolves dynamically with new information, and if these laws can be tailored to the individual interacting with the system, the adaptability of these rules may undermine the principles of universality ("all are equal before the law") and nondiscrimination.

4.8 Lex Cryptographica and Algocratic Governance

Overall, the implementation of blockchain technology as a regulatory tool could offer numerous advantages to regulators and even to society as a whole. Utilizing blockchain technology, governments could enhance societal regulation by diminishing the expenses associated with regulatory compliance and law enforcement, automating legal processes, and concurrently decreasing the inherent uncertainty in legal language. If these systems achieve widespread acceptance and governmental endorsement, they could gradually facilitate the creation of a new regulatory framework one that increasingly depends on lex cryptographica

and consequently possesses the same attributes as the majority of the previously described code-based systems, including resilience, tamper resistance, and autonomy.

A blockchain can facilitate the translation of some laws and regulations, either wholly or partially, into a framework of independent code-based rules. As rules encoded in this form are executed automatically by the underlying blockchain network, individuals will have diminished reliance on a judge to ascertain the applicability of a certain rule enshrined as a smart contract to any particular circumstance. The implementation of blockchain-based regulations necessitates no governmental action, hence its effects may only be assessed retrospectively by a court or other judicial entity.

Although this may yield significant advantages for efficiency and legal certainty, the attributes of lex cryptographica also pose risks to individual autonomy and society at large. Under the governance of a centralized and authoritative regime, the unique attributes of a blockchain such as resilience, tamper resistance, and automated execution may result in scenarios where dominant entities impose their own regulations within a blockchain-based framework, compelling all participants to conform to these stipulations in order to engage with the system. This may ultimately enhance the authority of inflexible and authoritarian governments, enabling them to exert greater control over their populace through a succession of self-executing, code-based regulations. If blockchain technology were utilized correctly, it would substantially alter contemporary law enforcement practices. The transition from a bureaucratic paper-based system to a technologically driven code-based system, which explicitly governs interpersonal and societal interactions, may restrict individual behavior in unprecedented ways, thereby altering the fundamental rules and principles of law enforcement.

Currently, governmental entities are responsible for establishing the regulations that society must follow. Certain individuals are tasked with establishing these regulations, while others are charged with their enforcement. Specifically, since laws are enforced retroactively, judicial organizations are typically tasked with interpreting and implementing the law, determining the applicability of the law to specific circumstances. In contrast to current legislation, which is enforced retroactively, laws encoded in technology are enforced automatically through the foundational technological framework. Upon the codification of legal or contractual stipulations as smart contract code, the corresponding blockchain network will autonomously execute the code and enforce the encoded rules precisely as intended eliminating any potential for alteration or influence by governmental or other authoritative entities post-triggering. An injured person may appeal to the judiciary alone in instances of erroneous application of the law to reverse the effects of these regulations.

As governmental services increasingly depend on a blockchain-based infrastructure, we may ultimately eliminate the inefficiencies of current bureaucratic systems in favor of progressively algocratic solutions. These signify novel societal frameworks regulated by lex cryptographica, with laws delineated and enforced by autonomous software code, leaving individuals with minimal to no redress against erroneous interpretations or inequitable applications of the law. If a government fails to implement protective mechanisms or opts to dismantle existing systems, the prevailing regulatory framework based on the rule of law may

ultimately be supplanted by a system of algorithmic governance, solely administered by the rule of code.

Conclusion

1. Blockchain technology is reshaping the landscape of contract formation and enforcement by offering a decentralized, secure, and transparent method of handling agreements. Through smart contracts, blockchain enables automatic execution of contract terms, reducing the need for intermediaries and mitigating the risk of human error. By providing immutable records, blockchain ensures that contract data remains secure, verifiable, and tamper-proof, enhancing trust between parties and promoting efficiency.

2. Despite the potential of blockchain, the legal landscape for blockchain-based contracts is still evolving. Existing legal frameworks are fragmented and fail to fully accommodate blockchain's unique characteristics. Current regulations often do not address key issues such as jurisdiction, contract enforcement, and the legal status of smart contracts. Some jurisdictions have started to recognize blockchain in specific contexts, but broader legal recognition remains in development, with the regulatory environment needing to catch up to blockchain’s rapid advancements.

3. A major challenge in the legal recognition of blockchain-based contracts is the lack of comprehensive legal standards. There are significant uncertainties about the enforceability of smart contracts across borders and how blockchain technology aligns with existing contract law principles. These challenges create obstacles for widespread adoption, as legal professionals and businesses seek clarity on how blockchain will be interpreted and integrated within traditional legal systems.

4. Technological advancements in blockchain scalability, interoperability, and the integration of artificial intelligence (AI) are poised to further enhance blockchain’s role in contract law. As blockchain technology continues to evolve, its ability to handle more complex contract scenarios will increase, and its integration with AI-driven tools could improve contract management, decision-making processes, dispute resolution, and compliance monitoring.

Blockchain holds significant promise for transforming contract formation and enforcement, but its full potential can only be realized through ongoing legal innovation and technological progress. Addressing current regulatory gaps and embracing future advancements will be key to unlocking blockchain’s role as a fundamental tool in modernizig contact law.

List of sources

Regulatory Legal Acts:

1. European Commission, Proposal for a Regulation (COM/2020/593)
2. Electronic Signatures in Global and National Commerce Act
3. European Market Infrastructure Regulation EMIR
4. Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directives 2009/138/EC and 2013/36/EU, PE/72/2017/REV/1

Court Jurisprudence:

1. Bibb v. Allen, 149 U.S. 481 1893
2. Bilski v. Kappos, 130 S. Ct. 3218, 3223 (2010)

Special Literature (Academic Works):

1. "Symbolic Logic: A Razor-Edged Tool"
2. Alexander 2019 and Cerar 2009
3. Allan E. Farnsworth, "Meaning in the Law of Contracts"
4. Allen, Hillary - "$=€=BITCOIN?" Maryland Law Review 76, no. 4 (2017):877–941
5. Anita K. Krug, "Investing and Pretending"
6. Ari Juels et al., "The Ring of Gyges"
7. Arthur E. Wilmarth Jr., "The Transformation of the US Financial Services Industry"
8. Arvind Narayanan et al., Bitcoin and Cryptocurrency Technologies
9. Avi Spielman, "Blockchain: Digitally Rebuilding the Real Estate Industry"
10. Bar-Gill, Oren - "Seduction by Plastic," Northwestern University Law Review 98, no. 4 (2004): 1373–1434
11. Baron, Joshua et al. - "National Security Implications of Virtual Currency: Examining the Potential for Non-state Actor Deployment," Research Report 1231 (Santa Monica, CA: RAND Corporation, 2015), http://www.rand.org/pubs/research_reports/RR1231.html
12. Baruch Lev and Meiring de Villiers, "Stock Price Crashes"
13. Bengt Holmstrom and Steven N. Kaplan, "Corporate Governance"
14. Benjamin M. Friedman, "The Future of Monetary Policy"
15. Carter, Thomas Francis - The Invention of Printing in China and Its Spread Westward (New York: Columbia University Press, 1925)
16. Choi, Stephen J. and Gulati, Mitu - "Contract as Statute," Michigan Law Review 104 (2006):1129–1173
17. Christian, James W., Shapiro, Robert, and Whalen, John-Paul - "Naked Short Selling: How Exposed Are Investors?" Houston Law Review 43 (2006): 1033–1090
18. Christopher D. Hoffman, "Encrypted Digital Cash Transfers"
19. Christopher Howgego, Ancient History from Coins
20. Coffee Jr., John C. - "Extraterritorial Financial Regulation: Why E.T. Can't Come Home," Cornell Law Review 99 (2014): 1259–1302

21. Cynthia A. Williams, "The Securities and Exchange Commission"
22. Danielle Keats Citron, "Technological Due Process"
23. Daron Acemoglu et al., "Institutions as a Fundamental Cause"
24. David Yermack, "Corporate Governance and Blockchains"
25. Davis, Kevin E. - "The Demand for Immutable Contracts: Another Look at the Law and Economics of Contract Modifications," New York University Law Review 81, no. 2 (May 2006): 487–549
26. De Fillipi and Wright 2018, 5–9
27. De Soto, Hernando - The Mystery of Capital: Why Capitalism Triumphs in the West and Fails Everywhere Else (New York: Basic Books, 2000)
28. Dennis, S. A. and Mullineaux, D. J. - "Syndicated Loans," Journal of Financial Intermediation 9 (2000):404–426
29. Dickinson 2019, 94–136
30. Dominic O'Kane, "Credit Derivatives Explained"
31. Donald MacKenzie and Yuval Millo, "Negotiating a Market"
32. Einzig, Paul - Primitive Money: In Its Ethnological, Historical and Economic Aspects (Amsterdam: Elsevier, 2014)
33. Eli Ben Sasson et al., "Zerocash: Decentralized Anonymous Payments"
34. Ezra Rosser, "Immigrant Remittances"
35. Fairfield, Joshua - "Smart Contracts, Bitcoin Bots, and Consumer Protection," Washington and Lee Law Review Online 71 (2014):35–50
36. Garvin, Peggy (ed.) - Government Information Management in the 21st Century: International Perspectives (Farnham: Ashgate, 2011)
37. Gordon, Robert W. - "Macaulay, Macneil, and the Discovery of Solidarity and Power in Contract Law," Wisconsin Law Review 1985 (1985):565–579
38. Griffiths, Meghan E. - "Virtual Currency Businesses: An Analysis of the Evolving Regulatory Landscape," Texas Technology and Administrative Law Journal 16 (2015): 303–331
39. Grigg, Ian - "The Ricardian Contract," in Proceedings of the First IEEE International Workshop on Electronic Contracting
40. Grinberg, Reuben - "Bitcoin: An Innovative Alternative Digital Currency," Hastings Science and Technology Law Journal 4 (2012): 160–208
41. Henry H. Perritt Jr., "Legal and Technological Infrastructures"
42. Hughes 1968, pp. 411–439
43. Jensen, Michael and Mecking, William H. - "Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure," Journal of Financial Economics 3, no. 4 (1976): 305–360
44. Jessica Erickson, "Corporate Governance in the Courtroom"
45. Johnson, Simon - "Unbundling Institutions," Journal of Political Economy 113, no. 5 (2005):949–995
46. Kandiah, Gajen and Gossain, Sanjiv - "Reinventing Value: The New Business Ecosystem," Strategy and Leadership 26, no. 5 (1998): 28–33
47. Kapasi 2021; Spilka 2021
48. Kelsen 1967, pp. 33–35
49. Kress, Jeremy C. - "Credit Default Swaps, Clearinghouses, and Systemic Risk: Why Centralized Counterparties Must Have Access to Central Bank Liquidity"

50. Layton, Timothy P. - Information Security: Design, Implementation, Measurement, and Compliance (Boca Raton, FL: CRC, 2016)
51. Lee, Ruben - What Is an Exchange? Automation, Management, and Regulation of Financial Markets (Oxford: Oxford University Press, 1998)
52. Levy, Karen E. C. - "Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and the Social Workings of Law," Engaging Science, Technology, and Society 3 (2017): 1–15
53. M. Ethan Katsh, Law in a Digital World
54. Malte Möser et al., "Towards Risk Scoring of Bitcoin Transactions"
55. Mangabeira Unger 1976, pp. 49–50 and 127
56. Marian, Omri Y. - "Are Cryptocurrencies Super Tax Havens?" Michigan Law Review (First Impression) 112 (2013): 38–48
57. Martin, Shaun and Partnoy, Frank - "Encumbered Shares," University of Illinois Law Review 2005 (2005):775–813
58. Miller, Mark S., Morningstar, Chip, and Frantz, Bill - "Capability-Based Financial Instruments," in International Conference on Financial Cryptography
59. Mills et al., "Distributed Ledger Technology"
60. Ogilvie, John W. L. - "Defining Computer Program Parts under Learned Hand's Abstractions Test in Software Copyright Infringement Cases," Michigan Law Review 91, no. 3 (1992):526–570
61. Ortolani, Pietro - "Self-Enforcing Online Dispute Resolution: Lessons from Bitcoin," Oxford Journal of Legal Studies 36, no. 3 (2016): 595–629
62. Ouédraogo, Moussa - "Land Tenure and Rural Development in Burkina Faso," Drylands Issue Papers 112 (2002):1–24
63. Peters, Gareth W. and Panayi, Efstathios - "Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money," In Banking beyond Banks and Money (Cham: Springer, 2016), 239–278
64. Peyton Jones, Simon, Eber, Jean-Marc, and Seward, Julian - "Composing Contracts: An Adventure in Financial Engineering (Functional Pearl)," ACM SIGPLAN Notices 35, no. 9 (2000): 280–292
65. Rauchs et al. 2018, p. 22
66. Schroeder, Jeanne L. - "Bitcoin and the Uniform Commercial Code," University of Miami Business Law Review 24 (2015):1–79
67. Shadab, Houman B. - "Regulating Bitcoin and Block Chain Derivatives," New York Law School Legal Studies Research Paper (2014)
68. Smith, Henry E. - "Modularity in Contracts: Boilerplate and Information Flow," Michigan Law Review 104 (2006): 1175–1222
69. Squire, Richard - "Clearinghouses as Liquidity Partitioning," Cornell Law Review 99 (2014):857–924
70. Steigerwald, Robert - "Transparency, Systemic Risk and OTC Derivatives," Futures & Derivatives Law Report 34, no. 7 (2014):20
71. Swan, Melanie - Blockchain: Blueprint for a New Economy (Sebastopol, CA: O'Reilly, 2015)

72. Triantis, George G. - "The Efficiency of Vague Contract Terms: A Response to the Schwartz-Scott Theory of U.C.C. Article 2," Louisiana Law Review 62 (2002): 1065–1079
73. Von Lampe, Klaus and Johansen, Per Ole - "Organized Crime and Trust: On the Conceptualization and Empirical Relevance of Trust in the Context of Criminal Networks," Global Crime 6, no. 2 (2004): 159–184
74. Weatherford, Jack - The History of Money (New York: Three Rivers Press, 1997)
75. Werbach, Kevin D. and Cornell, Nicolas - "Contracts Ex Machina," Duke Law Journal 67 (2017)
76. Wittie, Robert A. and Winn, Jane K. - "Electronic Records and Signatures under the Federal E-SIGN Legislation and the UETA," Business Lawyer 56 (2000):293–340
77. Wood, Frances - The Silk Road: Two Thousand Years in the Heart of Asia (Berkeley: University of California Press, 2002)
78. Wynkoop, Noah L. - "The Unregulables? The Perilous Confluence of Hedge Funds and Credit Derivatives," Fordham Law Review 76 (2007):3095–3099

Other Sources (News, Reports, Websites):

1. Abra (https://www.goabra.com)
2. AIan Allison, International Business Times (http://www.ibtimes.co.uk/uk-nuclear-power-plants-protected-cyberattack-by-guardtime-blockchain-technology-1533752
3. Alec Liu, Ripple blog
4. Andrea Tinianow and Caitlin Long, Harvard Law School Forum (https://corpgov.law.harvard.edu/2017/03/16/delaware-blockchain-initiative-transforming-the-foundational-infrastructure-of-corporate-finance/)
5. Bank for International Settlements reports
6. Barlow, John Perry - "Declaration of Independence of the Cyberspace" (1996)
7. Bitcoin Magazine (Buterin, Vitalik) - "MtGox: What the Largest Exchange Is Doing about the Linode Theft and the Implications," https://bitcoinmagazine.com/1323/mtgox-the-bitcoin-police-what-the-largest-exchange-is-doing-about-the-linode-theft-and-the-implications/
8. Bitcoin Magazine (Buterin, Vitalik) - "MtGox: What the Largest Exchange Is Doing about the Linode Theft and the Implications," https://bitcoinmagazine.com/1323/mtgox-the-bitcoin-police-what-the-largest-exchange-is-doing-about-the-linode-theft-and-the-implications/
9. Blockchain.Info - https://blockchain.info/tx/4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b?show_adv=true
10. Blockchain.Info - https://blockchain.info/tx/4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b?show_adv=true
11. Bob Hills et al., Financial Stability Review
12. Brad Smith and Elliot Ganz, "Syndicated Loan Market"

13. Brian Forde, Medium blog (https://medium.com/mit-media-lab-digital-currency-initiative/medrec-electronic-medical-records-on-the-blockchain-c2d7e1bc7d09#.j128mdvat)
14. Business Insider (del Castillo, Michael) - "A Huge Wall Street Firm Is Using Blockchain to Handle $11 Trillion Worth of Transactions," http://www.businessinsider.com/wall-street-firm-using-blockchain-to-handle-11-trillion-transactions-2017-1
15. Business Insider (del Castillo, Michael) - "A Huge Wall Street Firm Is Using Blockchain to Handle $11 Trillion Worth of Transactions," http://www.businessinsider.com/wall-street-firm-using-blockchain-to-handle-11-trillion-transactions-2017-1
16. CoinDesk (del Castillo, Michael) - "Illinois Unveils Blockchain Policy in Bid to Attract Industry Innovators," http://www.coindesk.com/illinois-blockchain-initiative-policy-regulation-bitcoin-blockchain/
17. CoinDesk (del Castillo, Michael) - "Illinois Unveils Blockchain Policy in Bid to Attract Industry Innovators," http://www.coindesk.com/illinois-blockchain-initiative-policy-regulation-bitcoin-blockchain/
18. CoinDesk (del Castillo, Michael) - "Lawyers Be DAMNed: Andreas Antonopoulos Takes Aim at Arbitration with DAO Proposal"
19. CoinDesk (del Castillo, Michael) - "Lawyers Be DAMNed: Andreas Antonopoulos Takes Aim at Arbitration with DAO Proposal"
20. CoinDesk (http://www.coindesk.com/dubai-government-documents-blockchain-strategy-2020/)
21. CoinDesk (Rizzo, Pete) - "Sweden Tests Blockchain Smart Contract for Land Registry," http://www.coindesk.com/sweden-blockchain-smart-contracts
22. CoinDesk (Rizzo, Pete) - "Sweden Tests Blockchain Smart Contract for Land Registry," http://www.coindesk.com/sweden-blockchain-smart-contracts
23. Computerworld (Hayes, Frank) - "The Story So Far," http://www.computerworld.com/article/2576616/e-commerce/the-story-so-far.html
24. Computerworld (Hayes, Frank) - "The Story So Far," http://www.computerworld.com/article/2576616/e-commerce/the-story-so-far.html
25. Dan Goodin, ArsTechnica (http://arstechnica.com/business/2012/03/bitcoins-worth-228000-stolen-from-customers-of-hacked-webhost/)
26. Darkwallet - https://www.darkwallet.is/
27. Darkwallet - https://www.darkwallet.is/
28. EU Blockchain Observatory and Forum - https://www.eublockchainforum.eu/
29. EU Blockchain Observatory and Forum - https://www.eublockchainforum.eu/
30. Federal Reserve Bank of Boston (Lo, Stephanie and Wang, J. Christina) - "Current Policy Perspectives: Bitcoin as Money?"
31. Federal Reserve Bank of Boston (Lo, Stephanie and Wang, J. Christina) - "Current Policy Perspectives: Bitcoin as Money?"
32. Financial Review (Maley, Karen) - "Flight from Gold to Digital Currencies," http://www.afr.com/personal-finance/flight-from-gold-to-digital-currencies-20150703-ghyuv3?stb=twt
33. Financial Review (Maley, Karen) - "Flight from Gold to Digital Currencies," http://www.afr.com/personal-finance/flight-from-gold-to-digital-currencies-20150703-ghyuv3?stb=twt

34. Financial Times (Cohn, Gary) - "Clearinghouses Reduce Risk, They Do Not Eliminate It," http://www.ft.com/cms/s/0/974c2c48-16a5-11e5-b07f-00144feabdc0.html#axzz4HchAyLja
35. Financial Times (Cohn, Gary) - "Clearinghouses Reduce Risk, They Do Not Eliminate It," http://www.ft.com/cms/s/0/974c2c48-16a5-11e5-b07f-00144feabdc0.html#axzz4HchAyLja
36. Financial Times (Mackenzie, Michael and Alloway, Tracy) - "Lengthy US Loan Settlements Prompt Liquidity Fears"
37. Financial Times (Mackenzie, Michael and Alloway, Tracy) - "Lengthy US Loan Settlements Prompt Liquidity Fears"
38. Forbes (Shin, Laura) - "The First Government to Secure Land Titles on the Bitcoin Blockchain Expands Project," https://www.forbes.com/sites/laurashin/2017/02/07/the-first-government-to-secure-land-titles-on-the-bitcoin-blockchain-expands-project/#de3b2444dcdc
39. Forbes (Shin, Laura) - "The First Government to Secure Land Titles on the Bitcoin Blockchain Expands Project," https://www.forbes.com/sites/laurashin/2017/02/07/the-first-government-to-secure-land-titles-on-the-bitcoin-blockchain-expands-project/#de3b2444dcdc
40. Goldman Sachs, "Blockchain Putting Theory into Practice"
41. Guardtime blog (Ruubel, Martin) - "Guardtime and Galois Awarded DARPA Contract," https://guardtime.com/blog/galois-and-guardtime-federal-awarded-1-8m-darpa-contract-to-formally-verify-blockchain-based-inte
42. Guardtime blog (Ruubel, Martin) - "Guardtime and Galois Awarded DARPA Contract," https://guardtime.com/blog/galois-and-guardtime-federal-awarded-1-8m-darpa-contract-to-formally-verify-blockchain-based-inte
43. https://remittanceprices.worldbank.org/sites/default/files/rpw_report_june_2015.pdf
44. Josh Berkerman, Wall Street Journa
45. Joshuah Bearman, Wired (http://www.wired.com/2015/04/silk-road-1/)
46. May, Timothy - "Crypto Anarchy and Virtual Communities" (1994), http://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-virtual-comm.html
47. May, Timothy - "Crypto Anarchy and Virtual Communities" (1994), http://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-virtual-comm.html
48. Nasdaq press release - "Nasdaq Launches Enterprisewide Blockchain Technology," http://www.nasdaq.com/press-release/nasdaq-launches-enterprisewide-blockchain-technology-initiative-20150511-00485
49. Nasdaq press release - "Nasdaq Launches Enterprisewide Blockchain Technology," http://www.nasdaq.com/press-release/nasdaq-launches-enterprisewide-blockchain-technology-initiative-20150511-00485
50. New York Stock Exchange - "One Hundredth Anniversary of the New York Stock Exchange: Brief Sketches of Wall Street of Today" (New York: J. B. Gibson, 1892)
51. New York Stock Exchange - "One Hundredth Anniversary of the New York Stock Exchange: Brief Sketches of Wall Street of Today" (New York: J. B. Gibson, 1892)
52. OpenBazaar - https://openbazaar.org/
53. OpenBazaar - https://openbazaar.org/

54. Pew Research Center - "Remittance Flows Worldwide in 2012," http://www.pewsocialtrends.org/2014/02/20/remittance-map
55. Pew Research Center - "Remittance Flows Worldwide in 2012,http://www.pewsocialtrends.org/2014/02/20/remittance-map
56. Pokereum - http://www.pokereum.io/
57. Pokereum - http://www.pokereum.io/
58. Price Waterhouse Coopers U.S. Financial Services - "Q&A: What Might Blockchain Mean for the Mortgage Industry?," http://www.pwc.com/us/en/financial-services/publications/assets/pwc-financial-services-qa-blockchain-in-mortgage.pdf
59. Price Waterhouse Coopers U.S. Financial Services - "Q&A: What Might Blockchain Mean for the Mortgage Industry?," http://www.pwc.com/us/en/financial-services/publications/assets/pwc-financial-services-qa-blockchain-in-mortgage.pdf
60. SafeMarket - https://safemarket.github.io/
61. SafeMarket - https://safemarket.github.io/
62. Sobel, Robert - The Big Board: A History of the New York Stock Market (Washington, DC: Beard, 2000)
63. The Money Project (Desjardins, Jeff) - "All of the World's Stock Exchanges by Size"
64. The Times London (Elliot, Francis and Duncan, Gary) - "Chancellor Alistair Darling on Brink of Second Bailout for Banks"
65. Wall Street Journal (Norton, Steven) - "Law Firm Hogan Lovells Learns to Grapple with Blockchain Contracts"
66. Wall Street Journal (Zweig, Jason) - "1930s Lessons: Brother, Can You Spare a Stock?"
67. Wired - "The Biggest Security Threats We'll Face in 2016"
68. World Bank Group - "Finance and Markets, Remittance Prices Worldwide,"