Modernizing Contracts Across Industries: A Review of Smart Contract Applications and the Evolving Legal Landscape

Kiran Bohyer[1], Thaier Hayajneh[2,*]

[1, 2] Fordham University, 113 W 60th Street, New York, NY 10023, USA

Abstract

We provide (1) an overview of various present and future applications of smart contracts across various industries including real estate, finance, and healthcare and (2) an assessment of the efficacy of smart contracts as a means of replacing or supplementing traditional contracts. Disclosed in this paper are (1) present and future applications of smart contracts and potential risks and downsides, and (2) legal considerations when using smart contracts to replace or supplement traditional contracts. Aspects of blockchain technologies can be applied to traditional contracts, in part or in whole, to reduce common challenges associated with contracts. Specifically, smart contracts can be integrated with or replace traditional contracts with the benefit of ensuring reciprocal obligations are enforced and aid in ensuring mutual consent, offer and acceptance, consideration and legal purpose.

Received on 30 April 2023; accepted on 06 July 2023; published on 10 July 2023

Keywords: Blockchain; Cryptocurrency; Smart contracts; Ethereum; Contract law; Web3

doi:10.4108/eetsis.3299

1. Introduction

Contracts can be costly to create and expensive to enforce. Creating them often requires many parties including the contracting parties, legal advisors, subject matter experts, or third-party service providers to ensure the proper development and execution of a contract.

This requires the contracting parties to place trust in various external parties (e.g., escrow providers, attorneys and subject matter experts). Third-parties provide additional assurances including increased trustworthiness and objectivity, however, these assurances come at a high cost. The additional cost for one or more of the contracting parties may be prohibitive in certain applications. Additionally, if the contracting parties entrust contracts or finances to a 3rd-party with lackluster security policies, there could be a breach of confidentiality, integrity, or availability.

When holding funds in escrow, the third party is responsible for the timely and accurate distribution of funds. Instead of relying on a third party, smart contracts can ensure funds are safe and transmitted only once parties meet the necessary conditions. Smart contracts offer a solution to cut out many 3rd-party intermediaries typically necessary in contract negotiations. There are many benefits to using a smart contract over traditional contracts, including increased security, full transparency, precision of terms and conditions, increased savings, and increased efficiency. These benefits stem from the way that blockchains are designed.

Escrow providers perform 2 primary functions (1) verification of contract conditions: The escrow provider will verify that all the conditions outlined in the contract have been met, (2) distribution of funds: once the escrow provider has verified that all conditions have been met, they will distribute the funds to the appropriate party or parties. Typically, distributing funds involves wiring funds to a bank account or issuing a check. Smart contracts can be used to automate the contract condition verification and ensure

* Corresponding Author. Email: thayajneh@fordham.edu

the distribution of funds in the form of cryptocurrency, USD or other currency. Problems that can occur when entrusting an escrow provider stem largely from human error. For example, when a person is responsible for reviewing the contract, it is possible that the person does not carefully or adequately review the contract which could lead to errors in disbursement.

Various industries can integrate or replace traditional contracts with smart contracts, to combat the inefficiencies, high cost and lack of trust associated with third-parties. Smart contracts can be intricate pieces of code however, traditional contracts can have intricacies that are exceedingly difficult to hard code into a smart contract. Thus, the traditional contracts that should be replaced with smart contracts are not the intricate situation specific contracts (e.g., mergers and acquisitions agreements, joint venture agreements, or international trade agreements) but rather standard boilerplate contracts for common occurrences (e.g., non-disclosure agreements, employment contracts, lease agreements, sales agreements, service agreements, or terms of service agreements). As the World Wide Web evolves, and we begin to see adaptations and coexistence of web2 and web3 technologies, smart contracts will become more commonplace.

There are still challenges with smart contracts that prevent them from being adapted into the mainstream workflow of various industries. These challenges include (1) bugs in code, (2) trustworthiness of data sources, (3) efficiency according to [29]. The reluctance to integrate smart contracts into business processes are not unfounded. Some contracts, if mismanaged, can have serious repercussions for the contracting parties. Furthermore, the lack of legal precedent surrounding smart contracts leaves the enforceability and prospect of adjudication ambiguous. Therefore, starting with "simple contracts" which are contracts that have simple straightforward terms and conditions that are easily comprehensible by all contracting parties, few provisions and minimal legal review or negation will pave the way for regulations to be implemented, and the education and familiarization of the public with blockchain technologies. Implementing simple contracts will serve as a proof of concept for future more complex adaptations of smart contracts across industries. This paper will go over the background and history of blockchain, briefly explaining the core tenets of the technology and how it relates to contracts. An additional primer on smart contracts will be included. After we provide a foundational explanation of blockchain and smart contracts, we will present a few current fields that we argue are well oriented for adapting smart contracts. By no means is this an exhaustive list of industries: merely, it is a starting point from which to build. These fields include: (1) Real Estate, (2) Finance, and (3) Healthcare. We will then provide pseudocode for certain sample contracts. Finally, after we explore these smart contract adaptations, we will address one important issue that is restraining the mass adaptation of smart contracts: legal enforceability.

2. Blockchain History

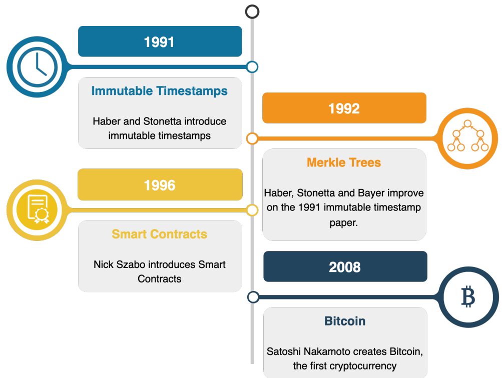

Figure 1. Visual depiction of the history of blockchain development.

2.1. Blockchain

Figure 1 is a visual timeline of the history of blockchain development. The foundational technology for blockchain was developed in 1991 and today there are various use cases for blockchain technology that improve efficiency and reduce cost. Blockchain is a technology that validates blocks of information by using a complex problem that miners need to solve and a hash of the previous block. This is a robust way to store data with a slew of benefits over other traditional methods of storage. [7], "Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets" additionally, nearly anything valuable "can be tracked and traded on a blockchain network." Blockchain has various applications today, but the technology had humble beginnings.

In 1991, Stuart Haber and W. Scott Stornetta introduced the concept of Blockchain to the world with their paper introducing a new way to ensure the authenticity of timestamped documents [18]. In the following year Haber, Stornetta and Bayer improved upon their paper covering record timestamping in a second paper [12]. These papers provided the foundational technology required to implement a blockchain. Haber, Stornetta, and Bayer's initial research allowed Nick Szabo to introduce the concept of a smart contract in 1996 [26].

Smart contracts were difficult to implement and scale, as there wasn't a digital incentive for the network to process contracts. Then, in 2008 Satoshi

Nakamoto introduced the first cryptocurrency: Bitcoin. The prior work of Haber, Stonetta, Bayer and Szabo was essential in creating the cryptocurrency now synonymous with the word “Blockchain”. The Bitcoin whitepaper, [23], detailed the intricacies of creating a form of decentralized currency and built on technology introduced in 1992 by Haber and Stornetta. Satoshi Nakamoto designed Bitcoin as a cryptocurrency: it was not designed to handle transactions like Smart Contracts.

To allow for applications beyond cryptocurrencies, Vitalik Buterin introduced the Ethereum in blockchain in 2013 [13]. Buterin discusses various limitations to the Bitcoin blockchain for applications outside cryptocurrencies, specifically a lack of turing-completeness (loops) which is essential for implementing more complex smart contracts [13]. Additionally, Buterin calls attention to "value-blindness" which is the lack of granular control of funds [13]; this makes smaller transactions difficult to implement. Buterin mentions “lack of state” which makes multiple stages of smart contract difficult to implement [13]; this would make developing more complex smart contracts difficult. He claims that Ethereum is the solution to these problems: it is “a blockchain with a built-in Turing-complete programming language, allowing anyone to write smart contracts and decentralized applications where they can create their own arbitrary rules of ownership, transaction formats and state transaction functions" [13].

A blockchain is a ledger that records transactions. It requires the input of the previous transaction to ensure immutability and protect the integrity of the blockchain. While there are many intricacies of blockchain technology, the important characteristics for this paper is that blockchains offer [11]:

1. A **decentralized** and trustless model which ensures no reliance on third parties and no central authorities for public blockchains.

2. A **resilient** network that resists breaches to integrity as only when “a consensus among the peers” is reached can the ledger record a transaction; once recorded it “cannot be altered or deleted.”

3. A **scalable** ledger that can expand as more miners join the network (*This is dependent on a variety of factors, and Bitcoin is notoriously not scalable and scalability in terms of transactions processed is typically an issue)

4. An **auditable** ledger because it is publically accessible by all parties of a transaction and anybody interested, this provides high levels of transparency

5. An **autonomous** means of transacting in that various applications can operate without a third party of human interaction (e.g., various smart contract applications)

While there are many advantages to implementing blockchain in certain applications, there are drawbacks as well. [11] discusses many challenges with widespread adaptation of blockchain including:

1. A **lack of awareness** of the technology outside the mainstream applications like Bitcoin

2. A **lack of regulation**, specifically, regulations for decentralized blockchains like Bitcoin as well as "a need to ensure legal enforceability of smart contracts to avoid disputes"

3. A **lack of privacy** as anyone can view the transactions (although this can be viewed as a positive as well depending on the application)

4. A **lack of efficiency** in proof-of-work protocols

Various consensus protocols exits within the Blockchain realm. Two primary consensus protocols are proof-of-stake and proof-of-work. While the intricacies of these methods are not relevant for this paper, it is important to note that proof-of-stake systems are generally accepted as a better alternative to proof-of-work systems due to improvements in efficiency, and reduced risk of various proof-of-work associated attacks [6]. Ethereum, in 2022, introduced proof-of-stake as the underlying consensus mechanism [6]. Proof-of-stake allows for far greater scalability in terms of faster block verification as well as a reduction in energy consumption. This reduction in energy consumption is especially important for the Ethereum blockchain, as it is designed for many applications outside of simple cryptocurrency transactions, like smart contracts and decentralized autonomous organizations.

2.2. Web 3.0

Finally, there is a buzzword in the blockchain industry, Web3.0. It is often misunderstood as a final solution to many problems with the internet today. In reality, many experts suggest organizations will slowly update their websites to be Web3 compatible and likely Web2 and Web3 websites will coexist. [14], Web 3.0 is the third in a series of versions of the internet: Web 1.0 and Web 2.0. The term Web 3.0 was coined by Gavin Wood, one founder of Ethereum [14]. Web 1.0 is regarded as an era of passivity: low bandwidths, primary websites hosted information to be referenced [14]. Web 2.0 is the internet as we know it: content producers create engaging content that consumers consume, e.g., “tweeting, blogging, liking, reviewing, and posting” [14]. Web 3.0 aims to solve problems present in Web

2.0. Opponents of Web 2.0 believe it has a power problem: oligopolies in the tech sphere – like YouTube, Amazon, Google, and Meta – can gate keep platforms and adjudicate disputes with no checks or balances from 3rd-parties or the community they serve[14]. Web 3.0 proposes the solution in the form of a “blockchain-oriented structuring of the internet” [14].

[21] specifically calls out the “preliminary” and “fancy word” riddled nature of current Web 3.0 definitions. In their paper, they define a novel definition for Web 3.0 that is both “generic” and “measurable” meaning that it is not bound to any applications or infrastructures and all members can see the “application’s eligibility for the Web3.0 era” [21].

2.3. Smart Contracts

Nick Szabo published his paper prior to the development of Bitcoin, but the concepts Szabo introduced are applicable today and can be implemented across various industries replacing existing contracts [26]. Szabo succinctly defines smart contracts as, "a set of promises, specified in digital form, including protocols within which the parties perform on these promises" [26].

Szabo introduced the concept of smart contracts. At the time of its introduction, smart contracts were theorized as contracts that executed autonomously with code. It wasn’t until blockchain technology was refined and cryptocurrencies were introduced that smart contracts became more prominent. After Szabo’s paper, Satoshi Nakamoto developed the Bitcoin Blockchain, which created the first cryptocurrency, but it had difficulties with scalability. Vitalik Buterin created Ethereum in 2014, 6 years after Nakamoto, as a response to the various applications of blockchain extending far beyond cryptocurrencies that the Bitcoin blockchain could not handle.

Smart contracts alone can accomplish rudimentary tasks, if you add additional data sources as well as the ability to convert physical items to a digitally tradable asset there are many applications that are unlocked. To connect real world data sources to smart contracts, we can use an oracle. There are various types of oracles, the intricacies of which are not relevant for this paper; essentially, an oracle connects "outside data feeds" to smart contracts [28]. The combination of tokenization and oracles allows for a much wider scope of applications for smart contracts.

2.4. Future of Blockchain

Bitcoin introduced the public to the concept of a cryptocurrency and blockchain however, there are problems associated with Bitcoin; problems with Bitcoin include scalability challenges and high energy consumption. Blockchain is being used for much more than digital currencies, and new applications of the technology are constantly being implemented. Therefore, it is not sustainable to use the Bitcoin network to process all these different types of applications.

This paper focuses on the Ethereum network, as it is a primary blockchain for smart contracts. Ethereum has an associated cryptocurrency, Ether. Ethereum also operates as a proof-of-work system but, as mentioned earlier, it is shifting to a proof-of-stake system, which will make it more sustainable and scalable in the long term [6].

Overall, the benefits of blockchain situate the technology to neatly integrate and replace certain aspects of more traditional approaches. These benefits are organized in Table 1.

Table 1. Table explaining the benefits to Confidentiality, Integrity, and Availability of Blockchain over traditional methods

	Traditional Approach	Blockchain Approach
Confidentiality	Data Security and Privacy are heavily dependent on the organization managing the data: healthcare organizations are HIPAA-compliant, but there are industries with less regulatory oversight	Blockchain has security built in by ensuring the has of previous blocks is used to validate new blocks, thereby creating an immutable and verifiable record keeping system. Privacy can be added by keeping addresses private.
Integrity	Centralized – one organization has full control over data which is problematic if the organization is breached or the data is corrupted or not stored properly	Due to the decentralized nature of public blockchains there is not a single entity that can be targeted by attackers, if one node on the network disappears the network is still intact.
Availability	If the system loses power, fails to ensure adequate backups, or a number of other incidents occur, data can be irrevocably lost	The decentralized nature of blockchain ensures that even if certain nodes are compromised the blockchain and data remain intact

3. Current Fields Suited for Smart Contracts

There are various applications of smart contracts throughout various industries. Additionally, there are new applications adapted daily for various industries. Many smart contract applications overlap between industries. The fields discussed in this paper are not exhaustive, but serve as an entry point to real-world smart contract applications. The industries in this paper include: real estate, finance, healthcare, supply chain management and mobility as a service.

3.1. Real Estate

Within the field of real estate, there are various contractual agreements that are required for the industry to operate. Two examples are Purchase Agreements and Lease Agreements.

Purchase Agreement. As [15] notes, purchase agreements typically involve the following boilerplate information:

1. Seller/Owner
2. Buyer/New Owner
3. Property Description
4. Purchase price
5. Payment Details: when and how

These 5 pieces of information can be hard coded in a smart contract. Specifically, the seller and buyer become addresses associated with cryptocurrency based wallets. The property description can be posted by the seller and adapted into the smart contract as a description that can later be used to identify the asset sold should arbitration ensue. The purchase price can be specified in the respective cryptocurrency. The date of the transaction can be coded as a deadline and the "how" regarding payment becomes obsolete as all payments with smart contracts use a blockchain.

Lease Agreements. Lease agreements are typically more complicated than a purchase agreement. Broadly, they enumerate the duties of the landlord and a tenant. More specifically, [20], a lease agreement involves:

1. "Terms and Rent Conditions"
2. "Important Dates and Periods"

These agreements are very difficult to translate into code for a smart contract. For example, suppose a lease agreement included the following condition, "tenants cannot use the rented apartment as a place of business." It would be very difficult to hard code what a "place of business" entails, or to have a way for the program to detect the misuse of a space. this condition into a smart contract. Much more difficult than a purchase agreement that simply transfers ownership upon a transfer of funds.

Challenges Implementing Smart Contracts in Real Estate. Real Estate requires the storage and transmittance of sensitive data. This data can include personally identifiable information (PII) like financial information, Social Security Numbers, credit card information, addresses, and full names. It is important that smart contracts are implemented in a manner that reduces the risk of exposure of PII of either party.

An additional challenge in implementing smart contracts in real estate includes the blending of a physical asset with a digital blockchain. Certain real estate functions, such as a walkthrough of an apartment, are difficult to represent on a blockchain or in a smart contract. It is therefore important to recognize the limited use case of smart contracts for more complex operations in real estate.

3.2. Finance

Finance is an industry that is often associated with Blockchain. The association stems from one of the first practical applications of Blockchain: cryptocurrencies. Finance is a hugely broad category encompassing everything from accounting, to corporate finance, to economics and more; it is not feasible to attempt and cover the applications of smart contracts for all the subcategories of finance, however there are certain contracts from various fields in finance that are well suited for smart contract adaptation.

[27], among the benefits of blockchain for use in finance are "decentralization" and "replication" which together provide audit trails that are verified by inbuilt cryptographic integrity checks. A transparent audit trail and cryptographic integrity ensures financial transactions remain transparent and secure. Additionally, by shifting to a blockchain model, the reliance on central hubs for things like integrity checking becomes obsolete [27].

Another benefit is that blockchains are "partition resistant" meaning that due to the structure of a blockchain "a copy of all the data" is preserved, and thus the blockchain can continue operating despite a node disconnecting from the network [27]. The robust design of a blockchain can help alleviate many issues with current methods of data storage and processing in various financial fields.

Smart contracts are another benefit cited by [27]. The ability for smart contracts to improve efficiency is hugely important in an industry where profits derive in part to the efficiency of operation: the quicker and cheaper the phases of a contract can be completed, the more profit the financial entity will make.

Among the fields in finance that are suited to smart contract integration are:

Stock trading. There are various entities that trade stocks. To trade a stock, regardless of volume or price, an investor is reliant on various third parties to help facilitate the transaction, including a stock exchange. Humans are rarely manually executing trades, now complex algorithms "decide to buy or sell based on price signals and other publicly available information" [27]. As it stands, humans do not have to interact to facilitate a stock trade, however, trading is still reliant on a stock exchange to facilitate the transaction [27].

An over-the-counter market (OTC market) is a stock exchange that allows participants to trade unencumbered by the third party, such as a broker or exchange [27]. Assuming an OTC market, it is possible to structure a smart contract such that stock trades can be executed without an intermediary between two market participants [27]. Obviously, without the third parties, trades become more risky. There is an international governing body, International Swaps and Derivatives Association (ISDA), that has created a document called an ISDA Master Agreement to provide protections for both parties involved [3]. They have considered the legal impacts smart contracts will have within the realm of finance.

Micropayments. Another application of smart contracts in finance concern micropayments. Micropayments are a relatively new concept and are typically used to make small payments of less than one dollar online [16]. Examples of micropayments include, "immediate distribution of digital rights, royalties, in-game purchases, online tipping, and even to coordinate devices connected via the internet of things (IoT)" [16].

Using a smart contract, it could be possible to pay fractionally to allow access to a website behind a paywall, an example used in [27]. The smart contract could be situated such that when a set sum of cryptocurrency is sent to a specified address, the password to access the article (or a more passive method of access like granting access rights to an account on the service).

Figure 2 is pseudocode that demonstrates a micropayment to access a news article behind a paywall.

```
new Smart Contract
{
   store walletID of the news organization variable called newsOrg;
   store walletID of customer in variable called customer;

   store the amount to unlock the article in variable called amount;

   if the customer send newsOrg the amount specified
   {
      use the walletID of the customer to unlock the associated article on their account
   }
   else
   {
      refund the money if sent and terminate smart contract
   }
}
```

Figure 2. Pseudocode demonstrating micropayments to access content behind a paywall.

By using this method of access, organizations could facilitate seamless transactions with clients, reducing some of the ordinary friction associated with online payments and increasing the trust and transparency of the transaction.

Challenges Implementing Smart Contracts in Finance. [27] notes two primary concerns with integrating smart contracts into the financial field: 1) difficulties in connecting real world assets to the digital blockchain and 2) the need for regulatory compliance on day one is contingent on adequate regulation provided as well as the willingness of an organization to comply with the regulations.

[27] introduces the concept of tokenizing fiat money to allow real world assets to be represented on the blockchain. There are three primary ways tokenization of fiat money can be accomplished: 1) "the central bank itself could issue digital money that lives on a blockchain," 2) "a large trusted institution could issue cryptocoins fully convertible into fiat money with promise backed by a 100 per cent reserve of fiat money," and 3) "decentralized smart contracts can be used to create a token that is pegged to a fiat currency" [27]. The first two solutions proposed rely on a third party intermediary, which partially defeats the purpose of implementing a smart contract. Additionally, the third solution is logical but difficult, as the price of cryptocurrencies can fluctuate.

Ultimately, these challenges may slow the process of integrating smart contracts, as well as require limitations to the level of complexity surrounding smart contracts. However, neither of these complications prohibit smart contracts from being integrated in some capacity to trade stocks or use micropayments.

3.3. Healthcare

In healthcare, there are a variety of applications of smart contracts. There are unique benefits to adapting blockchain in healthcare, discussed in [10] including:

- The decentralized nature of blockchain ensures that "stakeholders can have controlled access to the same health records" without a central authority.
- Blockchain relies on immutability, which "greatly improves the security of the health data store on it." Furthermore, since cryptographic keys are used to identify patients, the public nature of a blockchain does not breach patient privacy.
- Robustness of the data due to the distributed nature of a blockchain provides reliable availability of patient records.
- Blockchain ensures the integrity of data by design, which leads to improvements in "pharmaceutical supply chain management and insurance claim processing."

Electronic Health Record Requests. [19] provides an overview of the benefits of using blockchain for electronic health records (EHR). The categories cited by [19] concern traditional EHRs as well. Table 2 assesses each of the categories from [19] in a traditional EHR and the proposed blockchain based EHR.

Blockchain-based EHRs provide ample opportunity for smart contract integration. One application directly tied to the Blockchain based EHR is accessing patient records as a physician, insurance provider, or patient. This smart contract could simply transfer a key to decrypt patient records to an entity upon authorization from a physician or patient.

[17] provides an additional application of blockchain technology in healthcare. [17] discusses using IoT connected medical devices to remotely monitor patients in a hospital environment. Specifically, [17] notes that using blockchain over other traditional methods of patient monitoring which often require the physical presence of a medical professional allows for "secure analysis and management of medical sensors" which is vital in ensuring HIPAA compliance as well as preserving patient privacy and the confidentiality of medical data. [17] includes using smart contracts to bridge the communication between the IoT enabled medical monitoring equipment with doctors, EHRs, and actuator nodes.

A practical example discussed in [17] is an insulin pump and continuous glucose monitor (CGM) provided for a patient with diabetes. The insulin pump and the CGM are connected IoT devices. A smart contract takes as input the data measured by the CGM. The smart contract is programmed to include doctor's instructions or threshold values that, when exceeded, prompt one or more actions. For example, if the CGM measures a patient's glucose levels as exceeding a threshold set by a doctor, the smart contract generates a notification to a doctor and instructs the insulin pump to release a predetermined about of insulin. By using blockchain, an immutable record of the actions is stored; This is vital for preserving a history of patient care. Furthermore, since the process is automated, the patient is less likely to experience complications from a glucose level that exceeds the threshold set by the doctor if the doctor cannot be physically present to administer the insulin. Additionally, programming a smart contract to release the precise amount of insulin may reduce the likelihood of a dosing error.

Adjudicating Insurance Claims. One primary use case for a smart contract in healthcare is in insurance. Blockchain technology is well suited for use cases in insurance, as adjustments are somewhat formulaic. [30] provides a comprehensive implementation of a system to store insurance information called MIStore.

The system proposed in [30] provides various benefits over traditional means of storage including: a lack of third party intermediaries, data security, preservation of confidentiality, verifiably and efficiency [30]. The implementation covered in [30] is a good

Table 2. Contrasting attributes from [19] in traditional EHRs and blockchain based EHRs

Attribute	Traditional EHR	Blockchain EHR
Location	Centralized and therefore any requests to transfer data must go through a third party. This can be a difficult and time-consuming process for consumers.	Decentralized management allowing patients to manage their own healthcare records (i.e., patients are able to transfer healthcare information across providers) [19].
Immutability	Records stored in traditional EHRs are not immutable: physicians as well as bad actors can alter the record, which can cause life-threatening consequences for the patient. Additionally, corrupted files can lead to missing patient data if records are not backed up	A blockchain based EHR has immutable audit trails to ensure that patient records are not only traceable but once recorded cannot be changed. This ensures accuracy of patient records that can save lives [19].
Data Prove-nance	It is possible that traditional EHRs lose track of the source of data for certain patient records. This could lead to complications for the patient.	Data provenance allows anyone accessing patient records to see the source, which ensures a high level of trust can be placed in medical records [19].
Robustness and Avail-ability	Typically traditional EHRs are maintained by a single entity. If the entity managing the patient records is compromised the patient records are at risk	A blockchain based EHR helps ensure robustness and availability of records ensures that data cannot be compromised by attacking a single entity, which is not the case with current methods of data storage. [19]
Security and Privacy	HIPAA regulation helps ensure there are safeguards in place for patient data. It does not make EHRs invincible to attacks, rather reduces the likelihood of a breach of confidentiality, integrity, or availability.	Security and privacy ensure that confidentiality and integrity of patient records are maintained similar to a traditional EHR [19]. Blockchain has these features built-in, which ensures that an EHR on a Blockchain is by default secure and aides in maintaining patient privacy

use case for blockchain technology generally, but on a more granular scale, a smart contract can be used in conjunction with this type of system to improve the efficiency of processing insurance claims.

[19] notes additional benefits of using blockchain for insurance claims including quick claim processing, fraud protection because of immutability, verifiably of records, distributed nature of blockchain permit better access to patient data and finally blockchain maintains the security and privacy of patient data. Since blockchain improves upon the traditional method of insurance adjudication, it makes sense to apply smart contracts to insurance.

Suppose an insurance organization develops a smart contract that assesses the medical expenditures of a patient to a hospital on a blockchain and cross-references them with crash sensors in a vehicle and pays the patient based on the likelihood of a crash. This could be an automated process and alleviate the need to contact an insurance adjuster in an already stressful time. While this isn't a comprehensive method for ensuring appropriate compensation for clients, especially as there could be a crash that requires medical attention that may not trigger the sensor, it is beneficial to implement the smart contract regardless. With the crash detection smart contract deployed, the adjusters at an insurance organization have more time to spend adjusting claims for other, more complicated, insurance claims. This is a great example of how traditional contracts and smart contracts can coexist. Figure 3 is pseudocode for a smart contract that can automatically adjust a claim for a car crash.

```
new Smart Contract
{
   store walletID of the hospital variable called hospital;
   store walletID of customer in variable called customer;
   create a boolean variable called crashSensor, that stores the status of the crash sensor in a vehicle;

   if the customer sent currency to hospital and crashSensor is true
   {
      reimburse customer from the insurance wallet
   }
   else
   {
      send the case to an insurance adjuster for further review
      terminate smart contract
   }
}
```

Figure 3. Pseudocode demonstrating automatic vehicle incident adjustments.

It would even be possible to set up a smart contract to monitor the wallet of a client and automatically reach out to see if they want to file a claim in the event of a payment to an in network provider.

4. Overview of Contract Law

As shown, there are a wide variety of smart contract applications across various industries. There are many more industries that are suited to smart contract integration as well as more applications in real estate, finance, and healthcare. The purpose of providing pseudocode for certain applications as well as discussing various benefits of transitioning and supplementing current paradigms with blockchain based technologies is to demonstrate the importance of taking smart contract integration seriously, drafting regulations and attempting to consider additional use cases as web3.0 becomes more widespread.

Legal enforceability of a contract is important for widespread adaptation and integration with traditional contracts. Without the option to be legally enforceable, certain applications – like real estate, financial and healthcare transactions – won't be able to integrate smart contracts.

There are different ways to construct a smart contract that result in different assessments of enforceability. If the smart contract is embedded in a traditional contract, there is no concern with ensuring the contract is legally binding. However, if a smart contract is designed to be legally binding on its own, it is important to make careful considerations when designing the contract.

4.1. What does it take for a contract to be legally binding?

The question of legal enforceability depends largely on jurisdiction. In the United States, a contract must satisfy 5 requirements to be considered legally enforceable [2]:

1. Mutual Assent – meaning both parties have to agree to a contract [5]
2. Offer and Acceptance – meaning the value of the item exchanged must be agreed upon, and are two essential components of mutual assent [8]
3. Consideration – meaning the contract must be mutually beneficial [2]
4. Capacity – meaning anyone signing the contract must be legally capable (minimum age, soundness of mind, etc.) [1]
5. Legality – meaning nothing unlawful can be included in the contract [4]

4.2. Smart Contracts and Contract Law

Table 3 assesses how the attributes that make a contract legally enforceable apply to the development of a smart contract. Most of the attributes necessary for legal enforcement of a traditional contract easily implemented in a smart contract. However, the challenge in making a smart contract enforceable is not ensuring smart contracts include the elements of a legally enforceable contract, but rather it is ensuring proper communication between the multitude of parties involved in the process. If attorneys have

Table 3. Legal enforceability of smart contracts.

Requirement	Smart Contract Fulfills?
Mutual Assent	Both parties must agree to the smart contract through the use of offer and acceptance. This can be accomplished by using digital signatures to ensure that both parties agree to the terms of the smart contract.
Offer and Acceptance	Smart contracts cannot be altered after they are signed. Therefore, it is important to completely understand the offer prior to digitally signing the document. This can be difficult if the syntax of the smart contract is complicated, as it would require interpretation from either an attorney or a programmer.
Consideration	A smart contract can be mutually beneficial. There isn't any technical restriction that would prohibit both parties from getting something out of the contract.
Capacity	Smart contracts can be integrated with certain databases to automatically assess eligibility, or there can be a clause written that consults oracles to determine eligibility.
Legality	Smart contracts can be lawfully programmed. If no laws are violated in the terms of the smart contract, the contract can remain enforceable.

trouble understanding the smart contract they will not be able to adequately describe it to their client which means the elements that comprise a legally enforceable contract could be compromised. Similarly, if the smart contract developer doesn't understand the legal concepts necessary to implement the smart contract according to the wishes of both parties and attorneys cannot ensure the accuracy of the program, there may be a dispute over the outcome of a mutually agreed upon smart contract. The divergence of understanding between developers, attorneys, and clients is discussed in [9].

In addition to fulfilling the elements that comprise a contract, smart contracts need to be well-designed. Szabo discussed the "four basic objectives of contract design" [26]:

1. "Observability" which is transparency of each party's actions surrounding the smart contract

2. "Verifiability" which is the ability to prove "that a contract has been performed or breached"

3. "Privity" which is the concept that contents of the contract should be explicitly limited to the parties involved: no unnecessary third-parties

4. "Enforceability" which entails code being designed to minimize the need for external enforcement.

The success of smart contract is directly linked to the ability of the developer to account for the four objectives Szabo cited and fulfill the five requirements for a legally binding contract. Assuming these conditions are met, there are benefits to using a smart contract over a traditional contract. As opposed to traditional contracts, smart contracts can be cheaper and more efficient by "automating one or more of the key contractual phases of search, negotiation, commitment, performance, and adjudication" [27]. Assuming a smart contract can be developed in the manner above: in a way that is legally binding, the next question is how to adapt and integrate smart contracts with traditional contracts. As shown in [9] there are two ways to implement smart contracts in the current legal realm (1) externally and (2) internally.

In the external model, smart contracts are smart contracts that are integrated with traditional contracts [9]. In contrast, in the internal model, smart contract exists in isolation, with legal doctrine transcribed to code and necessary clauses added in comments [9]. Importantly, [9] notes that without portions of "natural human language" it would be difficult to ensure the enforceability of a smart contract. There are benefits and downsides to each of the approaches. However, the external model may be more applicable for current adaptations of smart contracts as attorneys are familiar with some automated functions already, so making the leap to a smart contract is doable [9].

To reap the maximal benefit from adapting smart contracts, an internal model is ideal. The difficulty in adapting an internal model is communication. [9] cites two reasons for this difficulty:

1. "Multiplicity of programming languages" would mean nothing is standardized, and therefore attorneys would have trouble deciphering the code in a smart contract.

2. Current programming languages don't cater specifically for a legal application.

To ensure that smart contracts can be integrated as seamlessly as possible, [9] proposes developing a novel programming language. The language would be designed to "intuitively follow the flow and terms of legal drafting" however, there would still be a learning curve for attorneys and programmers [9].

Externally facing smart contracts allow for those in the legal realm to choose what to automate and ensure the non-smart code portion of the contract allows the entire contract to be legally enforceable. It provides flexibility for the client and the attorney when drafting the code and relies less on the expertise of an individual

Table 4. Internal Model vs. External Model

Internal Model	External Model
Relies only on smart contract	Smart contract is integrated with traditional contract
Can be legally enforceable but can be difficult	Enforceable as the traditional contract is enforceable
Difficult for attorneys to adapt	Easier for attorneys to adapt

with the programming skills necessary to construct a smart contract.

Alternatively, internally facing smart contracts provide a way for a contract to be hosted entirely on a blockchain. There would be a higher reliance on programmers to implement and test the smart contracts.[9] recommended developing a language to bridge the gap between legal terminology and phrasing and computer code. This would help attorneys better understand the contracts and subsequently explain the contract to their clients. Table 4 provides a high level overview about the advantages of each approach.

Likely, in the future, smart contracts will coexist with traditional contracts, an external model. Additionally, some contracts may be better suited towards an internal model. Some applications, complex ones especially, will require diligent effort in drafting from an attorney for intricate details particular to the contract. For other applications that are more simple in the terms of the contract, an internal model may suffice. Regardless, both internal and external models of smart contracts can be legally enforceable.

5. Discussion

The application of smart contracts to various industries is not obvious. There are limitations of the technology as well as other factors to consider surrounding the ethics of replacing traditional contracts with blockchain based smart contracts. Ideally, a future can exist such that smart contracts and traditional contracts coexist, pulling the benefits from each to form a more secure and streamlined process for everything ranging from filing an insurance claim to buying a house.

The ramifications of implementing this type of technology could be huge economic benefits for the fields that choose to adapt smart contracts. It is important to lay the framework now for web3.0 technologies and more widespread adaptation of blockchain technologies like smart contracts.

6. Conclusions

The applications of smart contracts extend far beyond what was discussed in this paper. Real Estate, Finance, and Healthcare are three examples of areas with simple contracts that can be executed with smart contracts. Additional areas can include education as discussed in [24], media [22], and supply chain [25]. Each of these fields require contracts to be legally enforceable.

Smart contracts are a solution to the bloated nature of certain contracts today. They can streamline the contract process and save organizations time and money. They provide additional security for all parties involved and are transparent. The limitations come when formulating complex contracts as a smart contract. Work still needs to be done to connect the legal aspects of contract law to the technical aspects of smart contract creation. Bridging the gap between programmers and lawyers will dictate how easy it is to adapt this technology across industries, but it is achievable.

6.1. Bibliography

References

[1] Capacity. Available: https://www.law.cornell.edu/wex/capacity, *Cornell Law School Legal Information Institute*

[2] Contract. Available: https://www.law.cornell.edu/wex/contract, *Cornell Law School Legal Information Institute*

[3] International swaps and derivatives association, inc. 2002 master agreement, https://www.sec.gov/Archives/edgar/data/1065696/000119312511118050/dex101.htm

[4] Legality. Available: https://www.law.cornell.edu/wex/legality, *Cornell Law School Legal Information Institute*

[5] Mutual assent. Available: https://www.law.cornell.edu/wex/mutual_assent, *Cornell Law School Legal Information Institute*

[6] Proof-of-stake (pos), https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/

[7] What is blockchain technology? - ibm blockchain, https://www.ibm.com/topics/what-is-blockchain

[8] Section 2-206 offer and acceptance in formation of contract. Available: https://www.nysenate.gov/legislation/laws/UCC/2-206 (Sep 2014), *Cornell Law School Legal Information Institute*

[9] Smart contracts and distributed ledger – a legal perspective. International Swaps and Derivatives Association (Aug 2017), https://www.isda.org/a/6EKDE/smart-contracts-and

[10] Agbo, C., Mahmoud, Q., Eklund, J.: Blockchain technology in healthcare: A systematic review. Healthcare **7**(2), 56 (Apr 2019). doi:10.3390/healthcare7020056

[11] Bahga, A., Madisetti, V.K.: Blockchain platform for industrial internet of things. Journal of Software Engineering and Applications **09**(10), 533–546 (2016). doi:10.4236/jsea.2016.910036

[12] Bayer, D., Haber, S., Stornetta, W.S.: Improving the Efficiency and Reliability of Digital Time-Stamping, p. 329–334. Springer New York (1992). doi:10.1007/978-1-4613-9323-8_24, http://link.springer.com/10.1007/978-1-4613-9323-8_24

[13] Buterin, V.: Ethereum: A next-generation smart contract and decentralized application platform (2014)

[14] Chohan, U.W.: Web 3.0: The future architecture of the internet? SSRN Electronic Journal (2022). doi:10.2139/ssrn.4037693, https://www.ssrn.com/abstract=4037693
[15] Crowley, E.: What is a purchase agreement? all you need to know (Sep 2021), https://legaltemplates.net/resources/real-estate/what-is-a-purchase-agreement/
[16] Frankenfield, J.: Micropayment (Feb 2022), https://www.investopedia.com/terms/m/micropayment.asp
[17] Griggs, K.N., Ossipova, O., Kohlios, C.P., Baccarini, A.N., Howson, E.A., Hayajneh, T.: Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. Journal of medical systems **42**, 1–7 (2018)
[18] Haber, S., Stornetta, W.S.: How to time-stamp a digital document. Journal of Cryptology **3**(2), 99–111 (Jan 1991). doi:10.1007/BF00196791
[19] Kuo, T.T., Kim, H.E., Ohno-Machado, L.: Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association **24**(6), 1211–1220 (Nov 2017). doi:10.1093/jamia/ocx068
[20] Leivaditi, S., Rossi, J., Kanoulas, E.: A benchmark for lease contract review. arXiv:2010.10386 [cs] (Oct 2020), http://arxiv.org/abs/2010.10386, arXiv: 2010.10386
[21] Liu, Z., Xiang, Y., Shi, J., Gao, P., Wang, H., Xiao, X., Wen, B., Li, Q., Hu, Y.C.: Make web3.0 connected. IEEE Transactions on Dependable and Secure Computing p. 1–1 (2021). doi:10.1109/TDSC.2021.3079315
[22] Madu, B.C.: Protecting intellectual property using blockchain in the entertainment industry: Creating economic value
[23] Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review p. 21260 (2008)
[24] Nouman, M., Ullah, K., Azam, M.: Secure digital transactions in the education sector using blockchain. EAI Endorsed Transactions on Scalable Information Systems **9**(35) (2021)
[25] Saberi, S., Kouhizadeh, M., Sarkis, J., Shen, L.: Blockchain technology and its relationships to sustainable supply chain management. International Journal of Production Research **57**, 2117 – 2135 (2018)
[26] Szabo, N.: Smart contracts: building blocks for digital markets **18**(2), 28 (1996)
[27] Varma, J.R.: Blockchain in finance. Vikalpa: The Journal for Decision Makers **44**(1), 1–11 (Mar 2019). doi:10.1177/0256090919839897
[28] Voshmgir, S.: Token economy: how the Web3 reinvents the internet. BlockchainHub, second edition edn. (2020)
[29] Zheng, Z., Xie, S., Dai, H.N., Chen, W., Chen, X., Weng, J., Imran, M.: An overview on smart contracts: Challenges, advances and platforms. Future Generation Computer Systems **105**, 475–491 (Apr 2020). doi:10.1016/j.future.2019.12.019
[30] Zhou, L., Wang, L., Sun, Y.: Mistore: a blockchain-based medical insurance storage system. Journal of Medical Systems **42**(8), 149 (Aug 2018). doi:10.1007/s10916-018-0996-4

7. Copyright statement

Please be aware that the use of this LaTeX 2_ε class file is governed by the following conditions.

7.1. Copyright

Acknowledgement. This class file was developed by Sunrise Setting Ltd, Torquay, Devon, UK. Website: www.sunrise-setting.co.uk