DECENTRALISING THE INTERNET: THE TECHNICALITY AND LEGALITY BEHIND SMART CONTRACTS

Aditi Vinzanekar, Shashank Venkat[93]

ABSTRACT

A new, popular and rapidly arising technology known as "Smart Contracts" have gained popularity in the recent years. These Smart Contracts, based on blockchain technology, take the form of legal agreements that are executed automatically and do not require any middlemen or intermediaries. This paper examines and explains the technical, legal, and economic significance of these Smart Contracts. In essence, the research conducted for this paper is a study of the position and applicability of smart contracts in the existing purview of Contract Law. The issue of legal significance arises due to the fact that Smart Contracts are regulated entirely by users alone, without any formal central authority to oversee them.

The authors focus on explaining the basics of what smart contracts are and believe that for a comprehensive understanding of the topic, the study of its technicalities, history and evolution are pivotal. After delving into the origins of smart contracts and their advantages and disadvantages, the authors would then move on to the core principle on which blockchain technology and smart contracts are based, decentralisation, and further explain how this leads to effective cost cutting as well as eradication of the middleman, which in the long run would lead to mutual benefits to transacting parties. The authors will then move on to discuss the legal implications that accompany this technology, the issues that stem from it, and possible solutions to ensure that the positives do outweigh the negatives. Conclusively, the authors examine to what extent this technology can be used today.

INTRODUCTION

Over the last few years, innovators and computer experts, have been formulating various technologies that can bring about a "self-help"[94] approach to the world of contracts. Due to their self-executory nature, these contracts have come to be known as smart contracts[95]. To understand smart contracts, we must first understand the technology[96] that forms the basis for smart contracts.

---

[93] Students, 2nd Year, B.A LL.B (Hons.), Symbiosis Law School, Pune.

[94] Max Raskin, *"The Law and Legality of Smart Contracts"*, Georgetown Law Technology Review, Volume 1: Issue 2, 1 GEO. L. TECH. REV. 305 (2017)
"Self-help is nothing new. Whether building walls to stymie trespassers or changing locks to evict squatters, individuals regularly act on their own before invoking the formal legal system."

[95] Nick Szabo, *"Smart Contracts: Building Blocks for Digital Markets", 1996,* available at - http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html , last seen on 29/07/2017, wherein Nick Szabo coined the term "Smart Contracts" as follows:
"New institutions, and new ways to formalize the relationships that make up these institutions, are now made possible by the digital revolution. I call these new contracts "smart", because they are far more functional than their inanimate paper-based ancestors. No use of artificial intelligence is implied. A smart contract is a set of promises, specified in digital form, including protocols within which the parties perform on these promises."

[96] Blockchain Technology helps Smart Contracts maintain their decentralised chain, thus reducing need to depend on central authority, and allows two exchanging parties to directly interact and deal with one another.

Blockchain Technologies have been considered a technological revolution and have begun changing the very face of common financial interactions, such as property purchases, and, as mentioned earlier, contracts. Blockchain, the underpinned technology for Bitcoin, seeing as how each of the blockchain databases are shared by all participants in the system. Just like Bitcoin, other blockchains based implementations aren't regulated by any central authority throughout the world, and is regulated exclusively by users.

A "blockchain" is basically a public ledger of all cryptocurrency transactions, put forth in a digitised and decentralised fashion. Blockchain refers to the storage of digital information, in blocks of data. These "blocks"[97] store/record a few current/recent transactions, after which, the block goes into the blockchain into chronologically arranged, permanent, databases. It thus, allows all participants in market transactions, to keep a track of all transactions made on a digital currency basis without a centralised mechanism of information storage. Therefore, there is no central authority through which these databases are regulated and hence remaining entirely in the hands of those participating in such contracts[98].

When A pays B for any good or service, only A and B are party to this transaction, and there is no middleman/ third party required to process the said transaction.

However, due to the lack of central authority oversight into the processes of entering into Smart Contracts, the question of formal legal intervention arises. The legality of these contracts must be assessed, and it is required to formulate a few simple rules to form a framework for even the most complex of situations[99].

Smart Contracts have a mechanism that can be represented by that of a vending machine[100]. You can simply drop a unit of cryptocurrency into the vending machine, and whatever you purchase will appear in your account. Smart contracts, generally conform to almost all the rules and regulations that are part of a traditional contract, and can also automatically enforce whatever relevant, mentioned obligations.

Due to the decentralised nature of the blockchains, a legal scholar/cryptographer, by the name of Nick Szabo, realised that the technology had the potential to be used for the formation of self-executing contracts. For this, contracts had to be converted to code, and that code was to be replicated onto the systems.

---

[97] Ben Yuan, Wendy Lin, and Colin McDonnell, *"Blockchain and Electronic Health Records",* available at http://mcdonnell.mit.edu/blockchain_ehr.pdf last seen on 27/12/2017

[98] Satoshi Nakamoto, *"Bitcoin: A Peer-to-Peer Electronic Cash System"*, Bitcoin Project, 31/10/2008, available at - https://bitcoin.org/bitcoin.pdf last seen on 21/12/2017

[99] Donald Skull, and Kathleen M. Eisenhardt, *"Simple Rules for a Complex World",* Harvard Business Review, September 2012 Issue available at - https://hbr.org/2012/09/simple-rules-for-a-complex-world last seen on 23/12/2017

[100] The comparison of Smart Contracts to a Vending Machine was given by Nick Szabo in his "Vending Machine Model", and a brief description of the concept of vending machines has also been given by Max Raskin, (Supra 1)

Thus, smart contracts are a mechanism that help you exchange money, property, or shares, and help you carry out monetary transactions, effectively without the use of middlemen, thus transforming the role of lawyers, bankers and brokers all over the world[101].

SMART CONTRACTS

A) Smart Contracts Defined

Simply speaking, a Smart Contract is an agreement whose execution is automated[102]. The principle characteristic of a "Smart Contract" is its self-executory and automated nature[103]. However, if we need to investigate a broader, more detailed definition of the term, we can look to the definitions proposed by Josh Stark. Josh Stark, is a lawyer, and was previously the head of the legal and operations teams at a former blockchain consulting and development firm known as Ledger Labs[104].

Various definitions of the term 'smart contract', have been proposed such as: "*contracts between parties that are stored on a blockchain"* or even, *"any computation that takes place on a blockchain".*

Josh Stark also clarified, that while there is no well settled definition of what a smart contract really is, there have been countless definitions proposed and most of them fall under one of two categories. One, which focuses on defining a smart contract as a specific technology, i.e. a code that is stored, verified and executed on a block chain; and the second, which focuses on the application of blockchain technology, as a complement or substitute for legal contracts.

We already have the understanding that blockchain was mainly incentivized by the termination of a middleman and having peer-to-peer transparent transactions. In simple terms, a blockchain will effectively give users access to a database which can be modified and simultaneously updated for multiple users at once. A blockchain effectively creates digital cash which can be transferred without an intermediary. This digital cash is valued on the basis of the trust that humans assign to it.[105].

---

[101] Arthur Piper, *"Blockchain and Smart Contracts"*, 25/08/2017, available at - https://www.ibanet.org/Article/NewDetail.aspx?ArticleUid=e64618b4-02bc-4e57-a5a6-3167027de3f9 last seen on 21/12/2017

[102]More detailed definitions of Smart Contracts are discussed further, but from a legal perspective, the relevant fact to be mentioned within the definition is the one regarding the elimination of human intervention to contracts.

[103] Christopher D. Clack, Vikram A. Bakshi, Lee Braine, *"Smart Contract Templates: Foundations, Design Landscape and Research Directions",* 2/08/2016 (Unpublished Manuscript), available at - https://arxiv.org/pdf/1608.00771.pdf last seen on 24/12/2017

"A smart contract is an agreement whose execution is both automatable and enforceable. Automatable by computer, although some parts may require human input and control. Enforceable by either legal enforcement of rights and obligations or tamper-proof execution."

[104] Ledger Labs was a Canada based firm, specialising in blockchain services and solutions for clients all over the world. However, recently they have decided to cease their provision of consultancy services, and to now focus on developing their own product, by partnering with BlockGeeksLab.

[105] Josh Stark, *"Making Sense of Blockchain Smart Contracts",* 4/6/2016, available at - https://www.coindesk.com/making-sense-smart-contracts/ last seen on 12/12/2017

Creator of Ethereum[106], Vitalik Buterin, at a DC Blockchain Summit[107], held at Georgetown University, explained that in a smart contract approach; an asset or currency is transferred into a program, *"and the program runs this code and at some point it automatically validates a condition and it automatically determines whether the asset should go to one person or to the other person, or whether it should be immediately refunded to the person who sent it or some combination thereof."*

The decentralised ledger also stores/replicates the document which provides to the process, a certain degree of security and immutability. Thus, the applications of blockchain technology accompanied with coded conditions can have a multitude of use-cases in our world today whether it be in the field of transfer of property, transparent transactions or to simplify[108] tasks of contract drafting; all this while also terminating the role of an intermediary and reducing costs overall. The nuances that however need to be addressed are with respect to legal culpability and responsibility and will be delved into in later sections of the paper.

B) Advantages and Disadvantages of Smart Contract Technology

Just like every other creation in the world, the practice of entering into smart contracts has proved to have its pros as well as its cons.

The issuance of smart contracts into the world of finance, insurance, and now even auditing/taxation processes, can imply a lot of positive progress, but at the same time could do as much harm as good. Due to its unregulated nature, these choices and decisions lie solely with the users, and only they can decide for themselves whether the weight of advantages is lighter or heavier than the weight of the disadvantages of smart contracts.

Advantages-

- ***Speed and Time Saving Quality****- As experience has proven, technology will always be able to work faster than human beings. An invention as simple as a calculator can save so much time and human effort. Just so, it has been realised that digital contracts are much faster and far more accurate than the processing of physical documents and*

[106] Vitalik Buterin, Ethereum: A Next-Generation Cryptocurrency and Decentralized Application Platform, Bitcoin Magazine, 24/01/2014, available at- https://bitcoinmagazine.com/articles/ethereum-next-generation-cryptocurrency-decentralized-application-platform-1390528211/ last seen on 24/12/2017

[107] The Chamber of Digital Commerce, partnering with Georgetown University held the Inaugural Blockchain Conference, where companies such as Microsoft, Deloitte, IBM, Bloq, Nasdaq etc had attended.

[108]David Yermack, *"Corporate Governance and Blockchains",* Review Of Finance, Volume 21, Issue 5, 19/01/2017, available at - http://revfin.org/corporate-governance-and-blockchains-by-david-yermack/ last seen on 23/12/2017

"A firm could post all of its business transactions on a blockchain, allowing anyone to aggregate them into an income statement and balance sheet at any time. This may significantly reduce the need for of auditors, deter accruals earnings management, and deter related party transactions."

paperwork. Time, is probably one of the most valuable of human resources, and the automated processes on which smart contracts operate, saves a lot of this valuable time.

- ***Accuracy****- Technology has also proven to be far more effective and accurate, due to the fact that it leaves no room for human error. Smart contracts are thus exceedingly accurate due to the lack of human involvement in its technical processes.*
- ***Independence from Intermediaries***[109]*- As one of the main objectives that were meant to be achieved with the invention of smart contracts, the elimination of middlemen has certainly saved money, time and effort on the part of the users. This technology, as mentioned before, brings about an environment of self-help, thus enabling users to handle their contractual agreements independently and effectively without forced reliance on third parties..*
- ***Security and Reliability****- One of the most attractive qualities of the Blockchain, is that its data cannot by altered or removed. The parties to a contract are protected by these unchangeable conditions, since they remain protected in the event of breach by the opposite party. The fact that middlemen are eliminated also increases security.*[110]

Disadvantages-

- ***Unregulated****- Though some people may see this as an advantage, the unregulated nature of these contracts may make it difficult for the world to ascertain the legality of these contracts. It has been suggested that there needs to be some presiding authority that investigates the matters of ongoing smart contracts as a regulatory system.*
- ***Implementation problems****- Since the world of blockchain is so vastly separate from the traditional way of operating as of now, it may be difficult to implement some of the contracts in the real world due to development and acceptance of such contracts, thus causing the users a certain degree of time, money and effort.*
- ***Rigid security****- As mentioned before, the data in blockchains cannot be altered or modified. While being one of the top advantages of smart contracts, this can also prove as a disadvantage in situations where the parties want to make urgent changes to the contract. It has thus been proposed, that the technology for supplementary contracts to be added should be looked into.*

C) Distinction Between Strong and Weak Smart Contracts

---

[109] Supra 14,
"A smart contract is an automatic way to execute a contract: for example, a self-driving car could drive to the bank if the borrower defaults on a car loan. The blockchain can implement smart contracts cheaply, for example changing the title of collateral upon a default, substantially reducing enforcement costs. Finance professors might not be able to write papers in the future about difficulties in seizing collateral!"

[110] BitFury Group, *"Smart Contracts on Bitcoin Blockchain"*, Version 1.1, 4/09/2015, available at - http://bitfury.com/content/5-white-papers-research/contracts-1.1.1.pdf last seen on 27/12/2017
"One of the advantages in using Bitcoin as a medium for smart contracts is the inherent low trust approach. Built-in Bitcoin mechanisms let users minimize counterparty risks by utilizing mathematical and algorithmic tools, not by relying on a mediator's authority, as it is often the case in the traditional approach."

It has come to be understood that some smart contracts are legally enforceable while others may not be. However, the vending machine mechanism of smart contracts may enforce all agreements, even if *ex post* the law finds the agreement legally unenforceable. To understand the distinctions between a strong and a weak smart contract, we must keep in mind the traditional and the non-traditional[111] methods of enforceability:

- ***Traditional Method***- The traditional methods of enforcing any contract are with the power of any established legal authority, which uses a variety of dispute resolution techniques. In certain situations, one can approach a court of law, and in other situations can seek arbitrators. The courts have the power to award damages, or provide other appropriate reliefs, as per the degree of wrong-performance/non-performance of the contract.

- ***Non Traditional Method***- There exists discussion and experimentation on what actions can be taken in case of needing to enforce a smart contract code, without needing to seek recourse from formal legal authorities. This effort/method of enforcement however, becomes questionable due to the existence of "tamper-proof" technology. Tamper proof technology refers to code that is unstoppable in its execution, foul play, or natural/mechanical disruptions. Thus, traditional methods of enforcing a contract are preferred, because no overrides or variations can be made to an agreement launched code that is "tamper-proof".

On the basis of the degree of effort and method of enforcing a smart contract, Max Raskin[112] has proposed a distinction between strong and weak smart contracts. In his article, he defines strong smart contracts as those that require large costs and efforts to altering or changing them, while explaining that weak contracts are those that courts can alter with relative ease even after they are executed.

The legal issue to be addressed exists mainly in case of strong smart contracts. The fact that any legal authority would be rendered helpless post execution of a "tamper-proof" contract, brings us to question the legality behind such an unstoppable agreement. The point of a "smart" contract is that as soon as it has been initiated, it will execute itself, by definition.

HISTORY AND EVOLUTION OF THE CONCEPT

[111] Ibid, at 4.

[112] Supra 1, at 310

"..For legal purposes, I will further differentiate between strong and weak smart contracts. Strong smart contracts have prohibitive costs of revocation and modification, while weak smart contracts do not. This means that if a court is able to alter a contract after it has been executed with relative ease, then it will be defined as a weak smart contract. If there is some large cost to altering the contract in a way that it would not make sense for a court to do so, then the contract will be defined as strong."

The first ever definition of a "Smart Contract" was proposed[113] in 1997, by the American cryptographer/programmer Nick Szabo, who has been one of the leading authorities on blockchain and smart contracts for nearly the last two decades. As previously mentioned, his first definition was proposed at a time, when the idea and concept of a smart contract could only exist in theory, due to the lack of adequate technology to implement something so complex. The reasoning behind this proposition by Nick Szabo was for two fundamental reasons. Firstly, he worked on the basic psychology of every human being that wants to reduce costs. Nick Szabo conceived the idea on the basis of the need to eliminate the cost of middlemen from the process of contractual agreements. Secondly, he realised the ability of smart contracts, to be able to cause a shift from paper to digital databases, due to which these processes become a lot more effective and serve as a more reliable form of data storage.

Nick Szabo, along with others began trying to formulate cryptocurrencies (such as Bit Gold) using encrypted, secured online ledgers. However, on 31st October 2008 a paper was published with the heading "Bitcoin: A Peer-to-Peer Electronic Cash System"[114], authored by an unknown identity using the alias "Satoshi Nakamoto". On 8th January 2009, the first version of Bitcoin was announced, and soon after that Bitcoin Mining evolved.

Soon after the mining of bitcoin began, it proved successful as the first ever instance of mass usage of digital ledgers[115], thereafter creating an effective foundation for the implementation of smart contracts. Thus the proposition that was made by Nick Szabo more than two decades before, was implemented on the basis of Blockchain Technology.

DECENTRALISED NATURE OF BLOCKCHAIN

From Richard Hendricks in the American comedy series 'Silicon Valley' to Sir Tim Berners Lee, 'the father of the world wide web'; there are countless individuals who believe that the problems we face in the world today with respect to monetisation of sensitive data, hacking, censoring or prioritising of data due to biased interests and lack of access to vital functionality, to mention a few, *can all be resolved by decentralising the internet*. As of today, no single entity owns the internet, but there are large centralised services that support critical components such as web hosting, cloud computing, DNS servers, social media, search engines etc. All these services require all their data to be on a limited number of physical and virtual servers.

---

[113] Nick Szabo, *Formalizing and Securing Relationships on Public Networks*, 1/09/1997, available at http://ojphi.org/ojs/index.php/fm/article/view/548/469 last seen on 26/12/2017

[114] Supra 5

[115] Max Raskin, *"Realm of the Coin: Bitcoin and Civil Procedure"*, 20 Fordham Journal of Corporate & Financial Law, Volume 20 Issue Number 4, (2015) available at - http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1418&context=jcfl last seen on 25/12/2017

We have however, given these companies too much power as the aforementioned problems can potentially have a drastic effect on the end users of these services. Blockchain technology has to this end achieved to a decent extent the decentralising of powers with respect to monetary transactions among other things. Blockchain technology, at its core, is a distributed ledger that allows the sharing of transactional information among parties *without trusting an information broker or any intermediary*. Countless companies today are using this technology to create decentralised versions of vital services to ensure minimum inconvenience and disruptions to the end user.

A decentralised internet may have its own obstacles[116] as well as challenges but if robust , uncompromised services are going to be offered Blockchain technology will most likely be an integral part of this. [117]

A) Decentralised Web Hosting

Hacking has in the 21st Century caused many companies that provide a multitude of internet services millions of dollars, and this continues to occur every year. Distributed Denial of Service attacks have become a favourable tool of hackers and cyber criminals who want to shut down websites. This is fairly easy to do in a centralised system, with enough firepower directed at the targetted website the company has to spend millions on servers to stay online, and this in the past as well in the world today been of great detriment.

Blockchain technology replaces centralised servers with thousands of nodes that act as separate parts of the website, thus, even if cyber criminals have enough firepower to take down a centralised server of the target website, the nodes which are now acting as separate entities and with no central server to hit renders the efforts futile regardless of the magnitude. This process could save millions of dollars in the world today and countless companies are already implementing networks like this to ensure that their server capacities are not concentrated in one place.

Gladius is an example of such a company which created a decentralised content delivery system and has "*DDoS"* mitigation system. Gladius uses blockchain technology to distribute assets and files across thousands of computers that share a network. Users rent out a computer's idle time, storage and bandwith when they sign up with this company[118]. By decentralising storage locations, they are less

---

[116] Securities and Exchange Commission v. Trendon T. Shavers and Bitcoin Savings and Trust, 416, U.S., 1469, (2014, United States District Court, Eastern District of Texas) stated:
"Bitcoin is a decentralized digital currency that may be used to purchase goods and services online, or traded on online exchanges for conventional currencies, including the U.S. dollar. Bitcoin was created by the pseudonymous developer (or developers) Satoshi Nakamoto; it has no single administrator, or central authority or repository."

[117] Ben Dickson, *"Can blockchain decentralize the internet?"*, available at https://venturebeat.com/2017/10/08/can-blockchain-decentralize-the-internet/, last seen on 21/12/17

[118] Hunaln Naseer, Gladius ICO – *"Can a Blockchain-powered Anti-DDoS Solution Save the Internet?"*, available at- https://cryptovest.com/reviews/gladius-ico--can-a-blockchain-powered-anti-ddos-solution-save-the-internet/ last seen on 10/12/17

prone to hacking and also by using the blockchain technology they provide faster services as they bring cached content closer to the user. It also incentives people to share their idle network and computing resources.

B) Decentralised DNS

DNS services are indispensable when it comes to accessing the internet. While trying to access a site, the DNS service converts that domain name to an IP address which then provides access to the host. Many companies have now adopted a distributed alternative to the centralised web server system to prevent hacking or other cybercrime. One infamous instance was when the servers of the company *"Dyn"* were hacked and users lost access to vital services such as Paypal, Github etc[119]. Nebulis is a company that uses the Ethereum blockchain to store, update and resolve domain records. A decentralised DNS on the blockchain would exponentially increase the difficulty of staging man-in-the-middle attacks or to manipulate DNS records for domain redirection.[120]

C) Decentralised Data Storage

One of the most important reasons for decentralising internet services is to prevent hackers to manipulate sensitive data of countless users. But decentralising data storage mitigates more than just hackers. Many private companies have access to your data which may they might use in their own business interests, share with the government, or sell off to third parties without your consent. The greatest benefit that Blockchain technology provides you is the access to all vital services while retaining ownership of your data. To use centralised internet services today, the respective company must be trusted with sensitive data, but this is giving them too much power and many things can potentially go wrong in this model. In 2013, Yahoo was breached by hackers and data of three million accounts were leaked[121]. More recently, a credit reporting agency Equifax was breached and sensitive information belonging to a hundred and forty-three million people was leaked[122]. There are countless other examples as well which point out that data decentralisation can ensure that sensitive information as in the above examples isn't leaked.

Google Drive and Dropbox provide a centralised storage service. Storj, however provides a decentralised storage system by using blockchain technology to split the files into small bits and further

---

[119] Scott Hilton, *"Analysis of Friday 21st October Attack"*, Vantage Point, available at https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/ last seen on 15/12/17

[120] Ben Dickson, *"How blockchain can help fight cyber attacks"*, available at https://techcrunch.com/2016/12/05/how-blockchain-can-help-fight-cyberattacks/ last seen on 15/12/17

"One of the main characteristics of the blockchain is its immutability. The use of sequential hashing and cryptography, combined with the decentralized structure, make it virtually impossible for any party to unilaterally alter data on the ledger."

[121] *"Yahoo data breach hits all three billion accounts"*, BBC News, 3/10/2017 available at http://www.bbc.com/news/business-41493494 , last seen on 17/12/17

[122] Equifax Hack, Fox Business, 27/12/2017 available at http://www.foxbusiness.com/markets/2017/12/27/equifax-hack-what-learned.html, last seen on 30/12/17

encrypting them and distributing them to different participating nodes all over the network. The people that provide their own storage are remunerated in cryptocurrency. Storj not only prevents hackers from having access to centralised sensitive information, it also speeds up the access to the files on the storage system as it enables users to download the files at very fast speeds from different locations all at once[123]. Other examples of companies that use blockchain technology to distribute and encrypt their data range from email service providers such as Cryptamail and Swiftmail[124]; which encrypt the data on an email and provide the decryption key only to the receiver of the email, to social networking sites such as Indorse which store their data on a blockchain and run their services through a smart contract to ensure user privacy. Users are also given cryptocurrency rewards if they add value to the network and get to choose how they want to show their data with the network.

Legal Aspect and Significance

Before delving into the legal issues that arise out of the use of blockchain technology and smart contracts, we have to understand that, the rate of innovation in the world today is exponentially on the rise, while the legislative backing that is supposed to accompany it, lags helplessly behind.

But it isn't enough to say, that bringing in accompanying legislation is a long drawn out process, because there are countless socio-economic changes that the legislation isn't able to keep up with. With Blockchain technology and smart contracts, there are involved laws and jurisdictions of multiple territories, and thus the task at hand which initially bordered on herculean, now borders on impossible. There are a multitude of issues that the authors wish to focus on, which they believe need to be looked into before this technology can be used to its full, desired extent.

A) Comparison between Smart Contracts and Traditional Contracts

Now, prior to begin with the comparisons in the characteristics and legal implications of traditional and smart contracts, it is important to elucidate on the concept of a contract. A legally binding contract is one which formalises an agreement between parties, for performance of any particular act for a consideration.[125] Similar to a traditional contract, even smart contracts include a consideration for intended performance of terms of the contract to be carried out.

---

[123] Digital income, "*Storj Open Source Blockchain Review",* Icoin Blog, 27/09/2017, available at https://icoinblog.com/storj-open-source-blockchain-storage-review/ last seen on 21/12/17

[124] Julio Gil-Pulgar, *"Its time to switch to decentralized email"*, 18/12/2016, available at https://news.bitcoin.com/blockchain-based-email-systems/, last seen on 22/12/17.

[125] Tara Naughter, *"Smart Contracts v Traditional Contracts"*, ContractWorks Blog, 17/03/2017, available at-https://www.contractworks.com/blog/smart-contracts-vs.-traditional-contracts , last seen on 30/12/2017

"The core of a contract is that it formalizes an agreement between one or more parties. The parties to the agreement usually commit to performing some action in exchange for something of value, which in contract language, is called consideration."

One of the primary differences between a traditional contract and a smart contract is the lack of paperwork involved in smart contracts. Usually, when two parties enter into contracts with one another, there is involvement of attorneys and paperwork. Smart contracts however, operate using online databases, thus eliminating the use of paper, due to their sole reliance on information stored on the Blockchain.

As defined by Nick Szabo in 1996, "Smart contracts are digital protocols for information transfer that use mathematical algorithms to automatically execute a transaction once the established conditions are met and that fully control the process"[126]

Hence, due to the fact that smart contracts are automated through the use of coding, there is far less ambiguity[127] in their wordings as compared to traditional contracts, which are written using human languages. When contracts are written into code, there is far less chance of ambiguity than in natural human language because natural human language is infinite, while computer codes are by definition, absolute and predefined.[128]

When we talk about voidable nature of certain smart contracts, the conditions are quite similar to those that render a traditional contract void or voidable. For example, entering into a contract whose object or consideration is unlawful. For instance, the sale of alcohol or cigarettes to minors.[129]

In the case of traditional contracts, an express or implied acceptance is required, however, in a smart contract, the acceptance of the contract is given by initiating performance of the terms of the contract. This is since the contract is carried out by an automated system. Technically speaking, the issue of non-performance of the terms of a contract is avoided when entered into a smart contract, due to the fact that smart contracts can rarely be altered or deleted. However, this can become a disadvantage in a situation where a legal authority wishes to alter or modify the contract.

Traditionally, a contract can always be modified, if a governing legal authority issues the relevant orders. However, a smart contract, is one which may to allow modifications even under orders from legal authorities. Here, the question of legality arises. If the performance or non-performance of a smart contract cannot be intervened into by any formal legal authority, how can the legal legitimacy of a smart contract be established?

---

[126] Supra 2

[127] Supra 1

"Ambiguity is celebrated in human language. It is a central feature of literature, poetry, and humor. Ambiguity is anathema to computer language. An ambiguous computer language is a nonsensical concept because the predictability of computers is what gives part of their value."

[128] C.A. Gunter, *Semantics of Programming Languages,* 4, (1992)

"Perhaps the most basic characteristic of the distinction is the fact that an artificial language can be fully circumscribed and studied in its entirety"

[129] Modern Cigarette, Inc. v. Town of Orange, 774, 969, 970–71 (Supreme Court of Connecticut, 2001)

There may be numerous situations in which a smart contract may be required to be modified. For instance, if circumstances render the performance of a contract impossible or impractical, or if the performance of the terms of the contract are established as illegal after the creation of the contract.

The authors feel that to cater to such situations, smart contracts need a way to be modified. However, programmers would argue that such a change in the working of smart contracts could decrease security, since one of the most attractive features of a smart contract is its very ability to remain un altered. Thus, the most viable solution for such a problem would be to allow modifications to be made to smart contracts, only under the issuance of orders from governing legal authorities.

At this point, due to their increasing popularity, it feels as though smart contracts will gradually replace their traditional counterparts. However, due to the unclear nature of legal intervention into smart contracts, it seems unlikely that large firms would be willing to risk putting their faith in smart contracts while forgoing the "legal recourse" that traditional contracts make available to them. However, having said that, it could be possible for smart contracts to gradually adopt certain characters of their traditional counterparts, hence providing a digital approach to contract making while retaining the opportunity for legal and judicial intervention.[130]

Lack of a Regulatory FrameworkLaw has just begun to accept the use of the Bitcoin in select territories, the use of Blockchain or the use of other crypto currencies has not been explicitly spoken about. This could, again, be potentially problematic for someone who is not as well versed with the technology. There exists, plenty of ambiguity with respect to application of laws to these transactions. When a transaction takes place between two individuals from different parts of the world, there is no clarity about which country's law should prevail. A potential solution to this must be a universal regulating authority and framework which could adjudicate on the matters, but since we have absolutely no hindsight as to the working of this technology, and the potential impact and problems it could lead to in the future, the formulation of such a framework is a bit arduous. There is also a question of who will frame this set of rules and how many countries' views and opinions will be taken into consideration. The authors believe that a drafting committee with zonal representation is the most viable solution, but as this concern potentially millions of individuals in the future, this representation may not be adequate and hence the authors are sceptical about even the most viable solution.

In status quo most people have taken a 'wait and see' approach as to how to resolve disputes that may arise out of this. Although this does not stifle innovation and allows the regulators to see how this

[130] Supra 33,
"It would not be surprising to see some kind of melding of the two agreements, allowing for faster, simpler arrangements to be established digitally, yet also providing an avenue for judicial review."

technology would potentially affect us, it leaves a lot unsaid and presents a grey area of uncertainty and ambiguity for businesses looking to invest in this and to the blockchain innovators.[131]

B) A Smart Contract Cannot Account for Subjectivity

C) The first question that needs to be answered is whether all the essential elements of a traditional contract can be fulfilled. Coders who encode these smart contracts will have a great deal of difficulty trying to account for subjectivity and unforeseen circumstances such as force majeur events.[132]

As a smart contract is self-executing, the next question we need to ask ourselves, is whether a contract which becomes illegal to execute or against common business sense, will automatically be executed by this technology. Programming this code into a contract will again be a very arduous task as an exhaustive list of events, that may potentially happen or not happen, is infinitely large. There are also several contracts that are required to be in written form (for example, transfer of land), and computer code does not fall within the ambit of a written contract. Thus, the issue of legislation not keeping up with socio economic change comes up yet again.

D) Compliance with Data Protection

The distributed nature of the data which Blockchain technology uses, is what ensures privacy and protection of the users'. However, different territories have different data compliance laws in force. This is potentially problematic as a lot of interaction between users occurs between different countries. There needs to be a mechanism to ensure that cross-border transfers of data are compliant. For example, the Europe-United States Privacy shield ensures that all transfers are compliant to laws of both countries and similar such framework must be implemented with other countries as well.

The New General Data Protection Regulation will formalise on obligation on data processors to pseudonymise data[133] and a right to request erasure of their personal data. Pseudonymisation seems like

---

131 Hayley McDowell, **"***ESMA takes 'wait and see' regulatory approach to blockchain"*, 24/01/2017 available at- https://www.thetradenews.com/FinTechQ/ESMA-takes--wait-and-see--regulatory-approach-to-blockchain/ last seen on 24/12/17
"The European Securities and Market Authority (ESMA) has stated blockchain technology has not reached a point where regulatory action is needed, so has taken a 'wait and see' approach towards it."
132 Antony Lewis, "*A gentle introduction to smart contracts", 1/02/2016,* available at- https://bitsonblocks.net/2016/02/01/a-gentle-introduction-to-smart-contracts/, last seen on 24/12/17
"Force majeure is present in many contracts to allow for wiggle-room for the parties involved. In a smart contract environment, how does one party call that without abusing it or referring to a human arbitrator. So many grey areas, so many things to figure out."
133 '*Anonymisation and Pseudonymisation*', available at - https://www.dataprotection.ie/docs/Anonymisation-and-pseudonymisation/1594.htm last seen on 25/12/17
"it is important for organisations which process personal data to be cognisant of this right. When carried out effectively, anonymisation and pseudonymisation can be used to protect the privacy rights of individual data subjects and allow organisations to balance this right to privacy against their legitimate goals."

a very viable option as it goes hand in hand with blockchain technology whereas, the right to be forgotten presents more of a challenge considering the immutability of records on a block chain.[134]

E) Liability and Responsibility

Another poignant question right at the crux of Blockchain technology is whether a self-programmed, self-executing code without human intervention is considered to be a legal entity. If there is an ambiguity in the nature of the Decentralized Autonomous Organisation (DAO)[135], does unlimited liability fall upon the Blockchain operators?

It is difficult to determine the nature of a DAO and this difficulty brings about other issues about ownership and liability. If the nature of the DAO cannot be determined then ownership and control cannot be determined. A viable option is contribution of crypto currency can be deemed to be an ownership stake similar to shares in a company, but it has to be noted here that most crypto currencies do not attach ownership rights to their tokens. DAO's, as they have no legal personality, cannot enter into contracts. Here, the DAO members contracting in their own name, or setting up a business entity to operate the system and deal with customers and supplies is a viable solution.

Legal culpability at times of fault has also raised many eye brows as there is no concrete solution as to how deal with the faults in a smart contract. Whether the culpability would fall on the coder or the manager of the DAO is still uncertain, and with no legal hindsight, only experience can guide how to handle these situations from a legal standpoint. But the authors feel, that culpability can be interchangeable based on a number of factors (such as, how the code is used or the reason for the establishment of the DAO etc.), and on a case to case basis.

F) Litigation, Dispute Resolution and Issues of Jurisdiction

Jurisdiction in the cases of cross border transactions and in the case of an adjudication requirement, poses many questions. Assuming that it isn't explicitly stated in advance, there is an ambiguity as to what laws will prevail at times of adjudication. Assuming there occurs a transaction with conflicting laws, adjudication on such a matter will become very tedious. The authors feel a viable solution to this is pre determining which laws would apply to the transaction, but this leaves great scope for

---

[134] Antony Lewis, *"Immutability of block chains"*, 29/02/2016, available at- https://bitsonblocks.net/2016/02/29/a-gentle-introduction-to-immutability-of-blockchains/ last seen on 25/12/17

"once data has been written to a Blockchain no one, not even a system administrator, can change it."

[135] Toshendra, *"What are Decentralized Autonomous Organizations DAO in Blockchain"*, 10/05/2017, available at - https://www.toshblocks.com/solidity/decentralized-autonomous-organization-dao-blockchain/ last seen on 25/12/2017

"DAO are just the digital version of the above arrangement(organization structure) where all rules & regulation are written in the source code rather than the piece of paper. They are executed by thousands of people/computers together through some consensus-based algorithm. The platform where the DAO runs is called Blockchain."

manipulation and exploitation. Other than this considering other forms of remedies, such as arbitral awards instead of court awards can prevent issues regarding jurisdiction from coming up.[136] Making the users of this crypto currency sign a 'terms of use' clause while signing up can also prevent a great deal of confusion, but this solution works better on paper than in a pragmatic situation.[137]

Can the courts in the present day with technical matters of this sort? In England as well as other countries, courts can cater to technological disputes, but with reference to blockchain technology, the judges would require a lot of time to adjust and completely understand the working of this technology to able to appropriately adjudicate on the matter. Another issue at hand is the recovery of stolen cryptocurrency. There are legal theories that could help recover stolen cryptocurrency such as unjust enrichment, but this isn't a tried and tested system. When courts can adjudicate on these matters, big questions as to whether crypto currency is actual property that can be 'owned' will be answered. But as of right now, speculation and anticipatory formulation seems like the only solution that can be viable.

It a known fact, that public law will always override private law. For example, a minor may enter into a contract for buying alcohol from a vendor. In this example, both parties would be satisfied with the terms of the contract. However, public law calls for review of such a contract, since alcohol should not be permitted for use by minors.

Similarly, smart contracts require legal regulation to be able to be formally accepted into contract law.

But as of now, as mentioned before, very few countries had a legitimate legal framework in place for the use of blockchain technology, and smart contracts.

Maltese Law, now governs a few aspects of smart contracts under the "Electronic Commerce Act".[138]

The issue arises of jurisdiction arises however, because one jurisdiction may recognise a particular law or statute, which another jurisdiction does not, for example in the case of property laws.

This serves a problem to blockchain users, since the implication here is that any transaction occurring within the blockchain community, must conform to a ridiculous number of regulations from the various jurisdictions it may concern.[139] If this happens, all Blockchain transactions would more or less come to an abrupt halt, simply due to the impracticality of this proposition.

CONCLUSION

Nick Szabo had a vision, and an idea, all the way back in 1996, for the implementation of Smart Contracts, however, at the time the required technology had not been invented. Now, although the

---

136 Jean Murray, "*Arbitration vs. Litigation - What is the Difference?*", 17/09/2017, available at- https://www.thebalance.com/arbitration-vs-litigation-what-is-the-difference-398747 , last seen on 25/12/17,
"Arbitration, on the other hand, involves two parties in a dispute who agree to work with a disinterested third party in an attempt to resolve the dispute. In arbitration, there may be one or more arbitrators who hear both sides of the issue and who make a decision."

137 Supra 33

138 Chapter 426, of the Laws of Malta

139 Camilleri Preziosi, "Blockchain: Dissecting the Legal Issues", Lexology, 30/09/2017, available at- https://www.lexology.com/library/detail.aspx?g=710a9468-fbe5-4d90-ba5e-411697269828 last seen on 14/12/2017

supporting technology for smart contracts exists, its implementation should be as gradual and deliberate as possible, so as to ensure that it can be put to its full use all over the world.

As of now, sufficient legislative support does not exist around the realm of smart contracts due to the fact that the concept is so new. To avoid issues of different jurisdiction, in an ideal scenario, there should be one single, central, international authority, which could govern and cater to the needs of these smart contracts. However, this is possible only sometime in the future, since it will require time for countries all over the world to come together to form this singular authority.

Smart Contracts have the potential to facilitate orderly, efficient, and affordable transactions. Their goal is facilitate contractual agreements between businesses, or even individuals, without a large cost or any of the formality. Having said that, these qualities can only be enjoyed across the world if the concept is applied gradually alongside the formulation of adequate legislative backing.

The future for smart contracts looks promising, provided they can retain certain qualities that traditional contracts have. If smart contracts are to be successful in everything they hope to achieve, adaptation is of utmost importance. Adaptation of the legislature, the judiciary, the executive, and most importantly, - the people.