GAP iNTERDISCIPLINARITIES
A Global Journal of Interdisciplinary Studies
(ISSN – 2581-5628)
Impact Factor: SJIF - 5.047, IIFS - 4.875
Globally peer-reviewed and open access journal.

BLOCK CHAIN TECHNOLOGY: ISSUES AND CHALLENGES

Dr. Ketan Desai, Mr. Hemang Shah

Assistant Professor
Faculty of Law
The M. S. University of Baroda

Assistant Professor
Faculty of Law
The M. S. University of Baroda

INTRODUCTION

Understanding the concept To quote: "A Block chain is a digital ledger which has irreversible entries and is distributed among users where transactions are recorded chronologically in real time." The prerequisite criterion for such subsequent transaction to be recorded on the ledger is the mutual consensus of all network users (nodes), which creates a continuous mechanism of control which checks manipulation, errors, and maintains data quality[1]."

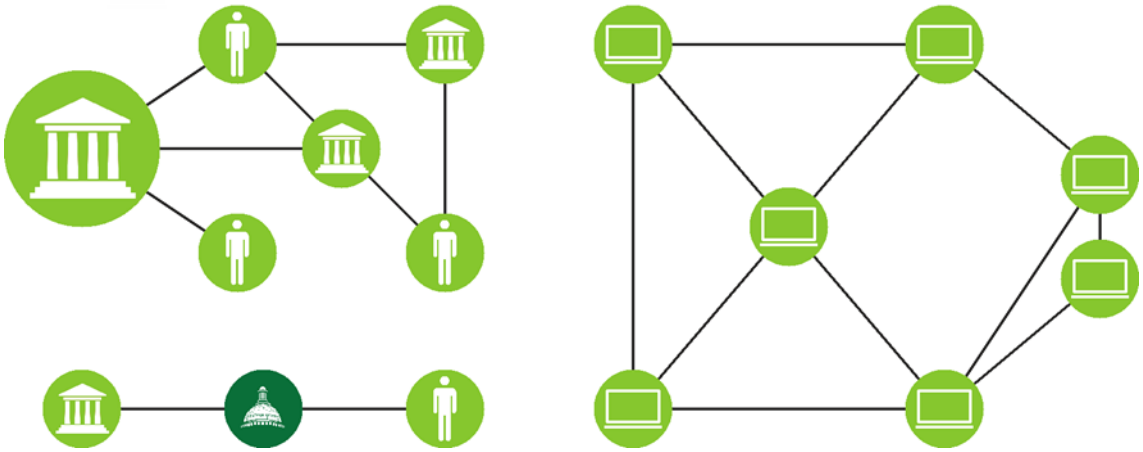

Fig1:Traditionaldatabasevs. Blockchain basedistributedledger

CurrentParadigm(*LeftChartofFigure*)

- **Centralauthorities** whichtransferactualtransactionvaluebetweentwoparties
- **Multipleintermediaries**arerequiredtofacilitateassetsfromonepartytootherandmaintain trust in system

BlockchainParadigm (*RightChart ofFigure*)

- **Distributednodes**maintainasharedandmutualsourceofinformation
- **Trust**isensuredbyacryptographicalgorithm basedsystem

Typesof Block chain

PublicBlock chain	PermissionedBlock chain	PrivateBlock chain
Fullydecentralizedand Transparent -Anyonecan	Quasi-decentralized, where consensusis	Centralized–requiresa 'hightrust'entitywhere

[1] https://www2.deloitte.com/content/dam/Deloitte/de/Documents/technology-media-telecommunications/PoV_Blockchain_Media_interaktiv.pdf

GAP iNTERDISCIPLINARITIES
A Global Journal of Interdisciplinary Studies
(ISSN – 2581-5628)
Impact Factor: SJIF - 5.047, IIFS - 4.875
Globally peer-reviewed and open access journal.

read,sendtransactions & participateinthe consensus process	controlledbya preselected set ofnodesandRead permission,isrestrictedto participants	Writepermissionsare centralizedtooneentity and Readtoall Participants

PRIVACY ISSUE

The central idea to counter legal issues surrounding pseudonymityor anonymity is the inherent feature of block chain which is partial anonymous participants and public access to distributed and mutual ledger and this is the reasons for legal implications of privacy[2].This is time and again explained that the users on block chain platform can be traced using the public key used for transaction and the IP address of the individual user along with some other identifiers, and most importantly each and every transaction is viewed and authorized by all participants on network, which is the inbuilt feature and benefit of block chain or distributed ledger technology.

In this sense particularly, as blockchain is new and emerging technology, the prevalent privacy laws in most nations along with Information Technology Act, 2000 do not recognize this type of privacy protection to users of network[3].The major aim and objective of every privacy legislation is to protect the end user against unauthorized collection of personal information by various websites and applications. For instance, the Information Technology Act lays down regulation for collection and use of private and personal sensitive data along with disclosure standard to be adopted by the entity which collects or uses such type of sensitive information. Apart from the owner of the software or app, the above regulation also applies to the entity which controls or operates upon such personal information[4].Since, decentralization is the key feature of blockchain technology, which means there is no central authority or entity which collects personal information on blockchain platform, the above inherent ordinary right of user might be obsolete and not enforceable under the space of blockchain technology. Bare reading of Information Technology Act, under Section 43A privacy for blockchain transactions will not be operative because as mentioned earlier there is no "body corporate" or "entity" which collects user personal and sensitive information and also there is no party on the platform which absolutely owns controls or operates a website or application (commonly termed as 'Computer Resource'). The network design of blockchain which consist no central body is different from the traditional web service provider. Unlike, collection and use of data by single entity on traditional network, the information of blockchain network is shared with all users or participants on the platform which results in decentralization or absence of control with one particular entity or user on the network. However, if any company or entity deploys a blockchain platform for commercial transactions, the privacy concerns may be applicable[5].In such case privacy may be incorporated in the network design of blockchain. Moreover, in deployment of blockchain based commercial platform for transactions the enterprises should also take steps to provide accountability for obvious reasons mentioned above along with other legal implications. Also, in case of centralized entity or operator on blockchain platform, policy maker should mandate such entity to incorporate dual privacy feature (one which operates between users and other between user and operator). However, this feature might not be technically feasible in inherent design of blockchain but is possible to be incorporated in particular interface modules of user and administrator.

Currently, India as a country is at a new height when it comes the standard to regulate the manner in which private and personal data is collected, processed and used. Last year, a committee of expert under the esteemed guidance of Justice Sri Krishna drafted the Personal Data Protection Bill, 2018[6]. Under the bill the parties who collect process or use personal or private data of user are referred as 'data fiduciaries'. The bill casts a mandatory duty on such 'data fiduciary' to protect the user's digital privacy. This bill also provides collection and processing of personal, private and sensitive data only for certain particular and legal purpose only provided such collection or processing of personal data is done with free consent of user. Since the above draft bill only prescribes the use of private data or the data which is attributable to a single user or individual. However, along with a deep analysis of the said bill and inherent features of blockchain technology, it may be noted that many provisions of the bill are not in accordance with the status of blockchain and the data stored on blockchain platform. However, not all but some of the regulations under the bill are explained with broader view as follows:

[2] 7http://www.lexology.com/library/detail.aspx?g=ee10aa0f-3447-4088-81dd-7521244fecb3; http://www.weblaw.co.uk/ebooks/eGuide_BlockchainTheConceptandtheLaw.pdf (last visited February 11, 2020)
[3] http://www.lexology.com/library/detail.aspx?g=ee10aa0f-3447-4088-81dd-7521244fecb3 (last visited February 11, 2020)
[4] Section 43A of Information Technology Act along with Reasonable security practices and procedures and sensitive personal data or information Rules (last visited February 11, 2020)
[5] http://www.weblaw.co.uk/ebooks/eGuide_BlockchainTheConceptandtheLaw.pdf (last visited February 12, 2020)
[6] http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf (last visited February 12, 2020)

GAP iNTERDISCIPLINARITIES
A Global Journal of Interdisciplinary Studies
(ISSN – 2581-5628)
Impact Factor: SJIF - 5.047, IIFS - 4.875
Globally peer-reviewed and open access journal.

- Deletion of Data: The bill provides for deletion of data without storing any backup once the purpose of collection or processing of data is done. This provision would not be possibly operative under blockchain space due to its inherent feature of recoding transactions in form of chain which provide immutability with security and integrity.
- In case of critical private data, the bill requires that the data should be processed in India only which is practically impossible to be applied to blockchain as it is decentralized without any regulator even at global level. Thus, it survives on internet and any blockchain designed as per this requirement to ensure all nodes or users are provided IP address of India would lead to deficiency and lack of transparency which are again inherent features of blockchain.
- The portability of sensitive data of users to allow transferability from one service to another under this bill is not practically applicable to blockchain.
- The end user has certain rights under the bill regarding modification and correction of their private information. But as blockchain is inbuilt with irreversible feature, this right of end user might be curtailed due to no scope of enforcement.

ISSUE REETING TO CYBER-SECURITY

Implementing commercial transactions on blockchain based platform would lead to enhancement of cyber security[7].Currently, breaches of data are so common, and those incidents are reported on day-to-day basis. The very recent hack of Coin Check which valued crypto assets of over USD 500 Million is a testimony of need for advanced cyber security[8].This shows that even though the technology which underlies blockchain is robust and secure and which acknowledge by experts around globe, the implementation of blockchain technology is fallible. As the private key of user is stored on private device or cloud makes it a possible target as it provides access to entire portfolio of the user. This is generally referred as single point of failure of any blockchain based program[9].This kind of risk has been already appeared on various occasions on Bitcoin based platform. Current law in India, under the Information Technology Act and Information Technology (Reasonable security practices and procedure sand sensitive personal data or information) Rules, 2011, will be applicable to blockchain transactions as it is Internet based. Moreover, the requirements under law are not practically applicable to blockchain. Also, as discussed earlier there is no central authority or entity which can be held responsible for any cyber security threat. But when there would be operators on blockchain platform they can be held responsible for cyber-attacks as per above regulations. However, this might not be the case always as mostly there are no central blockchain operators as in case of Bitcoin, the responsibility of central operator may not be always sufficient to establish cyber security. Moreover, an intensive review on standards of data protection suggest that the rules made under IS/ISO/IEC 27001 are not subject to implementation of blockchain as these have been streamlined considering a decentralized system. Every day new advanced cyber standards are being developed to ensure security of blockchain which shall influential on existing legal framework[10].

DECENTRALIZED AUTONOMOUS ORGANIZATIONS ISSUE

"Basically, Decentralized Autonomous Organization is an organization on virtual platform with full autonomy, on which operations are conducted on a software, and the terms of use and laws pertaining to this organization's operations are infused in a smart contract, which is enforceable on certain definite prerequisites conditions which needs to satisfied, and thus DAO is like a company which operates by itself without any central authority or regulator.[11]"

For instance, Ethereum blockchain which was a pool fund of crypto-currency which were valued at several million USD in form of crowd funding to be utilized for investment in form of venture capital.[12]

Since, DAO has inherent features like pseudonymity and decentralization it cannot be confined under the definitions of legal person including company, entity, body of corporate, etc.[13]. The reason for this might be the users on blockchain platform might not agree on distribution of decision making power and responsibility of operators dictated by the traditional structures of entity. Under DAO authority and decision making power is purely decentralized and is often arrived with consensus[14]. Also, due to obvious jurisdictional issues, the most

[7] http://www.lexology.com/library/detail.aspx?g=ee10aa0f-3447-4088-81dd-7521244fecb3 (last visited February 13, 2020)
[8] https://www.forbes.com/sites/forbestechcouncil/2018/09/17/why-are-crypto-exchanges-are-hacked-so-often/ (last visited February 13, 2020)
[9] See e.g., this explanation by Vitalik Buterin, a cofounder of Ethereum: https://www.youtube.com/watch?v=UFDAtStVXbc. (last visited February 13, 2020
[10] https://www.w3.org/2016/04/blockchain-workshop/report.html(last visited February 13, 2020)
[11] https://www.tractica.com/automation-robotics/blockchaindaosand-the-future-of-government/ (last visited February 13, 2020)
[12] http://fortune.com/2016/05/15/leaderless-blockchain-vcfund/ (last visited February. 13, 2020)
[13] http://www.clydeco.com/uploads/Files/CC010565_Blockchain_brochure_10-06-16_LOWRES.PDF; http://bollier.org/sites/default/files/misc-fileupload/files/DistributedNetworksandtheLaw%20report,%20Swarm-Coin%20Center-Berkman.pdf (last visited February 13, 2020)
[14] https://medium.com/@BlockChannel/what-is-a-dao-how-dotheybenefit-consumers-f7a0a862f3dc#.g8br

GAP iNTERDISCIPLINARITIES
A Global Journal of Interdisciplinary Studies
(ISSN – 2581-5628)
Impact Factor: SJIF - 5.047, IIFS - 4.875
Globally peer-reviewed and open access journal.

important question arises is about applicable law rather than how law is applicable[15]. Moreover, the nature of interest of users or participants of platform is very ambiguous in terms of share or stake. This makes it difficult to set a definite set of legal rights and duties of DAO and the users on its platform. A regulatory definition for artificial DAO cannot be simply created as this DAO is operated or governed on the basis of a computer resource and thus organizational rules for operation of such DAO can be executed in many uncountable ways. Also, the extent to which the programmers of this DAO can be held liable or accountable for actions and security defects of its design and architecture is a considerable question[16]. These theoretical implications are easily able to articulate the thought of million dollar hack of Ethereum which was mentioned earlier[17].In such situation the difficulties faced for implementation of DAO are:

A. Which law shall be applicable?
B. What are available legal remedies for DAO owner or operator?
C. Insurance considerations for blockchain space
D. Product liability and latent defect liability of DAO's computer resource
E. Whether DAO can be regulated as special vehicle for investment?
F. Responsibility and liability on blockchain platform, which is resulted due to pseudonymity and decentralization nature

Even after three years of Ethereum attack, the mastermind is untraceable. Even the users of the network including the coders of DAO software cannot be held liable as the code was available to public as it was open source which makes everyone yet no one responsible for the security and robustness of the platform. The concept of lawful association of person can be used for analysis of legal status of DAO. The Indian Law recognizes association of persons as a body of individuals or lawful entities which are associated in lieu of common object[18]. Apart from court interpretations adopted by courts of law in this regard, there are no material law statues as compared to regulation of companies, partnership, limited liability partnerships, societies, etc. This creates an ample amount of flexibility for governance of DAO as per the whims and fancies of the users of network. However, the Income tax and Competition laws in India recognize the legal concept of association of person which does not provide a way out for DAO to slip from their radar and establish as a platform for nefarious activities.

ISSUE OF IMMUTABILITY

Blockchain transactions cannot be reversed, modified or deleted like transactions on traditional ledger. Once the authorization of transaction is recorded by every participant it becomes irreversible on distributed ledger unless the users of network agree otherwise[19]. The basic parlance for the authenticity of transactions is cryptography and crowd wisdom. This might be reason why immutability or irreversibility of blockchain technology being the inherent feature, is considered on contrary as the most obvious risk which is inbuilt on blockchain technology. This might be because where on one hand the irreversibility feature of blockchain preserves transaction integrity; on other hand it might become impossible to conceal a fraud by malicious use of anonymity by any user on network due to its immutable nature. In traditional paradigm the aggrieved party may approach the third party gateway owner or banks, and if relief is not granted ultimately the courts of law and regulatory bodies. For instance in India, the aggrieved party may approach the Bank Ombudsman, RBI, court to either reverse the transaction or receive such amount to compensate the legal injury. However, under Blockchain paradigm the Grievance Redressal is flawed as the fraudulent transactions on blockchain cannot be modified, deleted or reversed by any central authority and even the court cannot trace back the defaulter on the network. Even if the court or central body is able to identify the user, the enforcement of judgment is not possible due to the reasons mentioned earlier under anonymity and legal enforcement of blockchain users. It is possible to tackle these problems by deployment of private and permission type blockchain technology by enterprises or corporate body. If this is not mandated the forerunners of blockchain technology i.e. banks and payment systems may find themselves in situation where they violate the basic and general regulations which govern them respectively. In India, the banks are regulated under Banking Regulation Act, 1949 and payment systems under Payment and Settlement System Act, 2007. Moreover, if this mandatory obligation is not regulated it may unnecessary impede innovation, compromise decentralization and avoid permanence which are unique and inherent features of blockchain technology. However, the basic design of blockchain provides for possibility of correction on the distributed ledger if certain mandatory conditions are fulfilled.

---

l9tgq (last visited February 13,2020)
[15] http://www.clydeco.com/uploads/Files/CC010565_Blockchain_brothem (last visited February 13,2020)
[16] http://www.clydeco.com/insight/article/ethereums-daoattacksmart-contracts-and-blockchain-face-their-first-big-te (last visited February 13, 2020)
[17] http://fortune.com/2016/06/18/blockchain-vc-fund-hacked/ (last visited February 13, 2020)
[18] http://www.financialexpress.com/archive/legal-concept-ofassociation-of-persons/372324/; C.I.T. v. Indira Balkrishna, 39 ITR 546. (last visited February 13, 2020)
[19] http://www.weblaw.co.uk/ebooks/eGuide_BlockchainTheConceptandtheLaw.pdf (last visited February 14, 2020)

GAP iNTERDISCIPLINARITIES
A Global Journal of Interdisciplinary Studies
(ISSN – 2581-5628)
Impact Factor: SJIF - 5.047, IIFS - 4.875
Globally peer-reviewed and open access journal.

JURISDICTIONAL ISSUES

The Internet in itself is grounded with various questions on jurisdiction issues and which law shall prevail in certain situation. For instance, in India the courts rely upon the availability of the website in our country along with the intention to operate commercial transaction for India users[20].However, in case of blockchain technology space, the difficulty to ascertain the jurisdiction is amplified to a higher extent[21].The reason for this might be the absence of any identifiable or traceable operator or host on the blockchain network as compared to traditional websites and mobile applications.

Even if the courts are able to identify an identifiable host on the network, the role of such host or operator would be very different from that of a traditional website or mobile application host or operator. This ultimately results in difficulty to identify responsibility and liability of host or operator as mentioned earlier. Moreover, when it comes to trace the servers of blockchain users, even they are scattered throughout the world and decentralized in nature which makes pinpointing of the server where security breach or failure occurred more and more difficult. Talking about Internet generally, there are various data locating tools or border controls adopted by various nations to address this issue. The forms of this control might be mandating the servers to be kept in territorial jurisdiction like in Russia or control on data flow out of territorial jurisdiction like in India and European Union. In blockchain space, the legislators might have to consider how to apply jurisdiction to their technology laws. A global approach with various stakeholders along with international rules and regulations, might seem deem fit in this situation. Along with this autonomous organizations like that of Chambers of Digital Commerce and Currency and Ledger Defence Coalition which have attracted major participation around the globe might play an influential role on multi-stakeholder global approach.

CERTAIN VIOLATIONS CONTRACT LAW

One of the key features of blockchain technology is formation and execution of smart or digital contracts[22]. This can be explained in simple terms as rights and liabilities are dictated not by natural or legal person but by software resource which are automatically executed upon satisfaction of certain conditions. This supremacy of software code may either be for certain provisions or entire of transactions. Needless to mention the contractual obligation around the globe is based on human perception and conscience. For instance free and mutual consent; expressed and implied offer or acceptance and lawful materialistic consideration are basic tenants of any contract legislation around world[23].

Hence, self-operating and automated execution of machine language creates new legal issues such as:

- Can these Smart Contracts enforceable as Contracts?
- Can parties be liable as under traditional paradigm?
- What may be the implications if the computer resource code underlying such digital or smart contracts are hacked or accessed illegally?

There have been instances which have been reported regarding the inability of users on blockchain platform seek changes in real estate transactions as all changes in ownership status of property are already recorded, verified and accessible universally. This might be the reason the aggrieved party are not able to plead duress or mistake of substantial fact[24]. It has also been noted that the volition feature of law, according to which the choice of action of party is given importance. But this might not be applicable to blockchain space as actions of party like filing of suit due to default may be executed automatically[25]. But anyone can argue that at the time of drafting smart contract volition might have occurred. Moreover, due to irreversibility of blockchain, the wrongful executed smart contracts may not be subject of traditional contract option like rescind or termination of contract[26]. For instance if in case of drought insurance the rainfall data considered may not be terminated or rescind at later stage[27]. Also, due to same reasons avoiding of contract due to situations forecasted in written contract like fraud, frustration or force majeure may not be easy to resolve on blockchain platform[28].

To overcome such ambiguities which stem into the contractual obligation of smart contract, it has been suggested to maintain standard contracts which are signed and complimentary to smart contracts. A Master

[20] Banyan Tree Holding Pvt. Ltd. v. A. Murali Krishna Reddy &Anr., 2008(38) PTC 288 (Del) (last visited February 14, 2020)
[21] http://www.clydeco.com/uploads/Files/CC010565_Blockchain_brochure_10-06-16_LOWRES.PDF
[22] http://www.lexology.com/library/detail.aspx?g=bc1e03ba-1800-4bfb-8e13-1826e9d2733f (last visited February 14, 2020)
[23] http://www.clydeco.com/uploads/Files/CC010565_Blockchain_brochure_10-06-16_LOWRES.PDF
[24] http://www.lexology.com/library/detail.aspx?g=bc1e03ba-1800-4bfb-8e13-1826e9d2733f;
http://www.lexology.com/library/detail.aspx?g=ee10aa0f-3447-4088-81dd-7521244fecb3 (last visited February 14, 2020)
[25] http://www.lexology.com/library/detail.aspx?g=ee10aa0f-3447-4088-81dd-7521244fecb3 (last visited February 14, 2020)
[26] http://www.weblaw.co.uk/ebooks/eGuide_BlockchainTheConceptandtheLaw.pdf (last visited February 15, 2020)
[27] http://www.clydeco.com/insight/article/arbitratingblockchain-disputes-will-smart-contracts-require-
Smart dispute (last visited February 153, 2020)
[28] http://www.clydeco.com/insight/article/smart-contracts-where-lawmeets-technology (last visited February 15, 2020)

Demand and Supply Agreement should be drafted to govern and control or purchase orders of smart contract. This shall enable users to resolve contractual ambiguities as under traditional contract law paradigm.

The ultimate solution that appears to be practically possible is to maintain a standard contract along with smart or digital contract at least until the legal mechanism is put into place. Also, due to earlier mentioned murky issues on legal recognition of blockchain, smart contracts have very detailed and lengthy clauses for amicable dispute mechanism; in which the major focus is to debate the counter the outcomes of this technology[29]. Smart contracts substantially question the role of lawyer changing in practice which is going forward. This question is also remarkable in new horizons achieved in field of artificial intelligence. A practical view point suggest that the need of lawyer shall paramount to draft contractual terms, or terms which are not readily in accordance with technical language; at same time interact with codes for bridging gaps between standard contracts and software resource[30]; and also solicit users about potential legal risks.

It is being slowly yet gradually established that next generation of litigants might require basic understanding of how software works[31]. Even though there are no needs to hastily implement such regulation as digital contracts are put into system, new contract rules shall govern the software code and contracts of blockchain technology[32].

CONCLUSION

Like any new technology or business model, the blockchain brings along with its benefits a host of legal, strategic, and operational challenges. From a legal point, we can foresee several legal grey areas that could arise as a result of the blockchain being deployed in the various industries that it has applications in. While it is heartening to see that some jurisdictions like Malta have taken the lead in creating regulations around blockchain, in the Indian context, it should not adopt hasty or technology-specific regulation of this technology, since it is complex and calls for time and effort to be put into understanding its implications. Further, principle-based regulation tends to be more time-proof than technology-specific regulation. A rushed job is likely to impede innovation. At the same time, left unregulated, courts, adjudicators, and commercial parties will be left trying to fit square pegs into round holes to understand how the technology fits within existing legal rules. To provide ideal solution it would be remarked to adoption of measured approach to regulation which is clear and provides clarification on ambiguities wherever necessary.

Finally, it is vital to ensure that legislators are well-informed about the technology and the immense benefits and that the public and private sectors collaborate to arrive at well-balanced policy outcomes. Such outcomes, along with education and awareness initiatives, should aid in the successful adoption of the technology in India, and in India becoming a leading player in the field, just as it has been with other information technologies over the years.

[29] http://www.clydeco.com/insight/article/arbitratingblockchain-disputes-will-smart-contracts-require-Smart dispute (last visited February 15, 2020)

[30] http://www.weblaw.co.uk/ebooks/eGuide_BlockchainTheConceptandtheLaw.pdf (last visited February 14, 2020)

[31] Richard Susskind, Tomorrow's Lawyers: An Introduction to Your Future (Oxford University Press, 2013); http://www.weblaw.co.uk/ebooks/eGuide_BlockchainTheConceptandtheLaw.pdf; http://www.lexology.com/library/detail.aspx?g=bc1e03ba-1800-4bfb-8e13-1826e9d2733f (last visited February, 2020)

[32] http://www.clydeco.com/insight/article/smart-contracts-where-lawmeets-technology (last visited February 14, 2020)