Three Potential Imminent Benefits of Blockchain for International Arbitration: Cybersecurity, Confidentiality & Efficiency

Ibrahim Mohamed Nour Shehata
PhD Candidate at Maastricht University, Lecturer Assistant at Cairo University

(A) Introduction:

According to Deloitte, the blockchain technology provides "a way of recording transactions or any digital interaction in a way that is secure, transparent, highly resistant to outages, auditable, and efficient."[1] That's maybe why the interest in the blockchain technology in 2016 alone amassed $1 billion which was invested globally by financial services and technology corporations. These investments are only expected to increase over the next five years.[2] In addition, CoinDesk estimates the annual revenue for enterprise applications of blockchain (usually takes the form of private permissioned blockchain) will increase from approximately $2.5 billion worldwide in 2016 to $19.9 billion by 2025, representing a compound annual growth rate (CAGR) of 26.2%.[3] Such interest shows how much private permissioned blockchain is expected to generate an added business value at an exponential level. As McKinsey reports, private permissioned blockchain will allow dominant players in their industries to "maintain their positions as central authorities or join forces with other industry players to capture and share value."[4] That way, such players can get the value of "securely sharing data while automating control of what is shared, with whom, and when."[5] In this regard, this article tries to determine whether there would be potential imminent benefits of using the blockchain technology in the current landscape of international arbitration. First, we start by defining the blockchain technology and its types. Second, we ask the fundamental question of whether we actually need blockchain technology at all in international arbitration. Third and finally, we explore the potential imminent benefits of blockchain technology in the field of international arbitration from our perspective; that is 1) cybersecurity; 2) confidentiality; and 3) efficiency.

(B) What is Blockchain and What are its Types?

There have been various definitions offered for the blockchain technology, however, most of them are too technical or too application-specific.[6] For example, Coinbase, the world's largest cryptocurrency exchange, defines blockchain as "a distributed, public ledger that contains the history of every bitcoin transaction."[7] This definition is, however, more suitable for bitcoin rather than the blockchain. Moreover, it is important to point out that bitcoin and cryptocurrencies are merely one type of application built on top of the blockchain. As will be discussed later, blockchain can be private and confidential and can be used with no need for bitcoin or any cryptocurrency at all. Further, the Oxford English Dictionary provides a broader definition of the blockchain as follows, "a digital ledger in which transactions made in bitcoin or another cryptocurrency are recorded chronologically and publicly"[8]. This definition also confuses the fine line between the blockchain technology and cryptocurrencies. Blockchain can be used independently in various business use cases with no need for any cryptocurrencies. Both of these definitions also "highlight the role of a blockchain as a digital ledger,"[9] nevertheless, "the ledger usage is simply a feature of the blockchain but not its essence."[10] The use of ledger feature only relates to "blockchain applications that focus on managing the exchange of value in the case of virtual assets."[11] In addition, Merriam Webster has recently added the word "blockchain" to its dictionary, defining it as a: "a digital database containing information…that can be simultaneously used and shared within a large decentralized, publicly accessible network."[12] The problem with this definition is that it also captures only one of type of blockchain; that is the public permissionless blockchain. A better definition would be a one that captures all types of the blockchain technology as follows:

A database that stores digital information in a highly secure manner through (1) using cryptographic functions to encrypt such information and (2) distributing the database across a number of networks.

This definition tries to highlight the most important feature about blockchain, namely, its extraordinary level of cybersecurity. Additionally, this definition tries to make it clear that the blockchain only concerns the realm of digital data and digital assets; there is no yet a direct connection between the blockchain and the physical world, although there are attempts to connect the digital and physical world via blockchain through the concept of the Internet of Things (IoT).

As for the types of blockchain, they are categorized on the basis of 2 main factors: **First**: Who is authorized to join and read the digital data lodged on the blockchain? This explores the distinction between public and private blockchains. **Second**: Who is authorized to write the digital data lodged on the blockchain? This explores the distinction between permissioned and permissionless blockchains. Accordingly, blockchains could be separated into 4 types as follows:[13]

Public Permissionless	Public Permissioned	Private Permissionless	Private Permissioned
Anyone Can Join & Read the Data (Anonymous Identity)	**Anyone Can Join & Read the Data (Anonymous Identity)**	**Only Participants with Known Identity Can Join & Read the Data**	**Only Participants with Known Identity Can Join & Read the Data**
All of Participants Can Write the Data	**Only Pre-Designated Participants Can Write the Data**	**All of Participants Can Write the Data**	**Only Pre-Designated Participants Can Write the Data**
Data is Transparent	**Data is Transparent**	**Data is Confidential**	**Data is Confidential**
Requires Native Assets (Cryptocurrency)	**Requires Native Assets (Cryptocurrency)**	**Does not Require Native Assets**	**Does not Require Native Assets**
Low Scalability	**Moderate Scalability**	**High Scalability**	**Very High Scalability**

In practice, the most used types of blockchains are either public permissionless blockchains or private permissioned blockchains. Currently, public-permissionless and private-permissioned blockchains are most popular in terms of the number of projects/startups involved and the greatest number of users.[14] That's why we will focus exclusively on these types throughout the remainder of this article.

Public Permissionless Blockchain: A public permissionless blockchain is a blockchain where everyone is able to access and transact with.[15] It's a blockchain where transactions are added only if they are valid. On the public permissionless blockchain, it's secured through the use of cryptography supplemented by economic incentives for the miners.[16] Anyone can be a miner who would be able to validate and publish the transactions on the blockchain.[17] In order to mine new transactions, miners have to commit software and hardware computational resources to solving a problematic cryptographic puzzle.[18] The first miner who solves such puzzle gets a monetary reward (usually a cryptocurrency).[19] Each new solution, along with the verified transactions, constitute the basis for the next puzzle to be solved.[20] Public permissionless blockchains might have the virtue of securing

transactions in a trustless manner, however, they show various limitations, especially with respect to application in business use cases. [21] That was the reason for the emergence of private permissioned blockchains that are currently widely used by business enterprises.

Private Permissioned Blockchain: A private permissioned blockchain is a "blockchain where write permissions are kept centralized to one organization." [22] As for read permissions, they are restricted to certain participants. [23] The distinction between public permissionless and private permissioned blockchains lies in the following factors: [24]

1. **Data Reversibility:** If one wants to change the data on a certain block (let's call it block (A)) on a public permissionless blockchain, she will have to change the data on all the blocks created since block (A) up till the new block. In order to do so, more than half (51%) of the participants on the public permissionless blockchain have to consent to such a change. Therefore, modifying the content of a block is almost impossible over public permissionless blockchain. [25] As for private permissioned blockchains, participants can "easily come to an agreement [off-the-chain] and modify data content."[26]

2. **Data Privacy:** Based on the type of the blockchain, the network can be public where anyone – even with anonymous identity - can access it, or private where only certain participants are allowed to join the blockchain. The restricted access on a private permissioned blockchain assures data privacy and confidentiality to its participants.[27]

3. **Data Scalability:** In public permissionless blockchains, the consensus protocol is essential to ensure the integrity and security of the data lodged on the blockchain. As mentioned above, this requires miners to commit software and hardware computational power to solve a demanding cryptographic puzzle. [28] This makes the public permissionless blockchain have low scalability as they are able to validate only tens of transactions per second.[29] On the other hand, in private permissioned blockchains, "miners or rather validators are preliminary known and trusted to some degree, this process of selection can be lowered in terms of computational power."[30] This reduction of computational complexity in the consensus protocol results directly in an increased scalability in terms of transactions validation. [31] For instance, "the first set of performance reports showing evidence that enterprise platforms such as Hyperledger Fabric, Hyperledger Sawthooth, and R3 Corda can achieve performance in the range of hundreds to thousands of transactions per second, often with sub-second response times." [32]

4. **System Responsiveness:** Technically speaking, no transaction stored on the Bitcoin blockchain (The most popular example of a public permissionless blockchain) could be considered truly final from a theoretical perspective. That's because any transaction can theoretically be deleted from the blockchain by "reorganizing it starting from the block containing the transaction in question."[33] In this regard, the longest reorganization of the Bitcoin blockchain happened in 2013 and involved 24 blocks; such incident did not relate to a malicious hack but rather a bug in the protocol.[34] Therefore, to consider a transaction to be practically final on the Bitcoin blockchain, one needs to wait for at least 36 confirmations which correspond usually to 6 hours of transaction age.[35] As for private permissioned blockchains, the use of "adapted consensus algorithm…increases the system responsiveness by shrinking waiting time for confirmations."[36]

5. **Ease of Updatability:** It's quite complicated to synchronize the software over public permissionless blockchains. [37] This is because of the vast amount of anonymous participants in such networks and how this usually result in potential disparities among them. On the other hand, it's quite

feasible to synchronize the software over private permissioned blockchains because members know each other and can quickly come to a mutual agreement off-the-chain.[38]

(C) Do We Even Need a Blockchain for International Arbitration?

An arbitration practitioner has recently claimed that: "there are cogent technological reasons which will make it difficult for the management of an arbitration reference to be conducted in a blockchain platform in the foreseeable future."[39] He reasoned by relying upon an unsubstantiated claim that it is "quite slow and expensive to store massive volumes of data on a blockchain ledger."[40] The problem here is the lack of information in the arbitration community about the various types of blockchain. It might be slow and expensive to store digital information on a public permissionless blockchain, but that is definitely not the case on a private permissioned blockchain. The arbitration practitioner was relying in his assessment upon the scalability of public permissionless blockchains such as bitcoin and did not take into consideration the very high scalable private permissioned blockchain that can allow for thousands of transactions per second at a very low cost.[41] The article goes on – and rightly so – to advocate that cloud computing might not have "adequate security protocols which can prevent major cyberattacks in the future."[42] Then, the article advocates for the use of decentralized cloud storage systems and suggests that companies such as Storj, Sia and Filecoin are currently commercializing the use of such systems.[43] This is quite confusing because if you are in the blockchain sphere, you would know that all three companies are in fact blockchain companies.

The only virtue of this article[44] is that it showed how public permissionless blockchain are not suitable to be used in international arbitration. Then, it becomes quite straightforward when it comes to choosing the most suitable blockchain type for international arbitration; that is being the private permissioned blockchain for the following reasons:

1. **Private**: To ensure the confidentiality that is usually highly regarded by participants in the arbitral process.
2. **Permissioned**: To ensure that only pre-designated participants have control over the arbitral process (i.e., the arbitral institution before the constitution of the arbitral tribunal, and then the arbitral tribunal itself when conducting the arbitral process)

Therefore, a private permissioned blockchain would be the optimal type of blockchains to be used in international arbitration. The next section will highlight the potential benefits of such type for international arbitration.

(D) Potential Imminent Benefits of the Blockchain for International Arbitration

1. Blockchain & Cybersecurity:

Cyber intrusions into the arbitral process does not imply that international arbitration is uniquely vulnerable to data breaches, but only that international arbitration proceedings are not immune to increasingly pervasive cyberattacks against corporations, law firms, government agencies and officials and other custodians of large electronic data sets of sensitive information. This was evidenced in July 2015 when the website of the Permanent Court of Arbitration in The Hague (PCA) was hacked during a hearing of a sensitive maritime border arbitration between China and the Philippines. Despite this malicious attack, arbitral institutions seem to "continue to rely upon relatively insecure storage and communication systems."[45] Evidently, institutional rules are completely silent on cybersecurity as they allow the transfer of data between the participants of the arbitral process by any electronic means.

Many arbitral institutions in fact use "unencrypted email and commercially available cloud data repositories."[46]

In *Libananco v Republic of Turkey,*[47] Turkey has admitted to intercepting Libananco's correspondence with its counsel and third parties, as part of a criminal investigation.[48] Further, in an unpublished order in *Caratube International Oil Co. LLP and Devincci Salah Hourani v. Republic of Kazakhstan*[49], the tribunal admitted into evidence certain documents obtained from the public disclosure of documents hacked from Kazakhstan's government computer network.[50] In addition, in the *Conoco Phillips* case[51], the arbitral tribunal had to deal with new evidence presented after the issuance of the award due to information available in *WikiLeaks*.[52] *WikiLeaks* were also addressed in *Opic Karimum Corporation v Venezuela* and *Kılıç v. Turkmenistan*,[53] and were also mentioned in the *Yukos* arbitration.[54]

Law firms, too, are increasingly becoming victims to cyber-attacks.[55] A 200 law firm study conducted by LogicForce (a cybersecurity consulting firm) for the first quarter of 2017 found that all of the surveyed law firms were victims of hacking attempts.[56] What is more peculiar is that that 40% of firms were not even aware of such hacking attempts.[57] In addition, 95% of the law firms were not thoroughly compliant with their cybersecurity protocols and only 23% had a cyber-attack insurance policy in place.[58] As we have seen in the above cases, hacking sensitive data may result in the acceptance of illegally obtained, or privileged evidence in a way that would undercut the integrity and legitimacy of the arbitral process.[59] Further, since the participants in the arbitral process usually live in different jurisdictions, they will accordingly be subject to different data privacy regimes.[60] Indeed, such jet-setting nature of international arbitration makes it easier to "forget about potential ways client information might be exposed."[61]

According to Deloitte, "while still nascent, there is promising innovation in blockchain towards helping enterprises tackle immutable Cyber Risk challenges such as digital identities and maintaining data integrity."[62] Blockchains could potentially help improve cybersecurity as it can impede fraudulent activities, and detect data tampering based on its underlying characteristics of immutability, data encryption and operational resilience. Accordingly, blockchains – unlike cloud computing - have no single point of failure, which highly decreases the chances of an IP-based DDoS attack disrupting the network operation.[63] If a node (i.e., a computer) is hacked, the lodged data on the blockchain is still accessible via other nodes within the network, since all of them maintain a full copy of the distributed ledger at all times. Such distributed nature of the blockchain solves the Byzantine General's problem of false consensus.[64] Even though the blockchain technology is generally considered to have no single point of failure; private permissioned blockchains with a lower number of nodes would need to make sure that their "network is sufficiently distributed globally and resilient with no single points of failure on an organization or platform level to ensure continuous operation even in the event of a natural disaster or coordinated attack."[65]

Further, blockchain technology is operationally resilient. This is because both public and private blockchain consists of multiple nodes; hence, corporations can make a node practically redundant if it comes under a cyber-attack and be able to continue to operate business as normal.[66] Therefore, even if a major part of the blockchain network is under attack, the blockchain will continue to operate normally due to the distributed nature of such technology.[67] Despite the above promises of the blockchain technology, it's still important to acknowledge that "blockchain's characteristics do not provide an impenetrable panacea to all cyber ills, to think the same would be naïve at best, instead as with other technologies blockchain implementations and roll outs must include typical system and network cyber security controls, due diligence, practice and procedures."[68]

2. Blockchain & Confidentiality

The Queen Mary University Arbitration Survey of 2018 shows how participants in the arbitral process highly value confidentiality in international arbitration. In fact, 87% of the survey respondents believe that confidentiality in international commercial arbitration is important.[69] Further, most respondents believe that confidentiality in international arbitration should be "an opt-out, rather than an opt-in, feature."[70] In this regard, private permissioned blockchains is the optimal solution to provide a higher level of confidentiality for the participants in the international arbitration process. In essence, private permissioned blockchains could be compared to "organizations intranet pages, where information is only shared and exchanged internally with those who have been authorized to access the site."[71] In any case, to ensure confidentiality, private permissioned blockchains need to be supplemented with "security controls to provide authentication, authorization, and encryption in order to properly protect data access."[72] Consequently, private permissioned blockchains would be able to provide international arbitration with a highly confidential platform and hence minimizing the risk of leaking sensitive data, either to the opposing party or to the public.

3. Blockchain & Efficiency

Judge Holtzmann has said before that: "We must not allow arbitration to be as slow as the sloth or as cumbersome – and therefore as obsolete – as the dinosaur."[73] This quote was mirrored in the most recent Queen Mary University Arbitration Survey of 2018 as it shows that respondents ranked the cost of arbitration as its worst feature (67% of respondents), and lack of speed as its fourth worst feature (34% of respondents).[74] This highlights how far the arbitral process transformed from a cost-effective and a time-efficient dispute resolution mechanism to a "monster" in terms of costs and time spent in such a process. The question is whether the blockchain technology can help with issue? The answer seems to be that it might do so. McKinsey reports that the blockchain technology initial impact will be to drive operational efficiencies.[75] In this regard, 70% of the value at stake in the short term of adopting blockchain technology is in cost reduction.[76] This is because smart contracts based on the blockchain have the potential to: "deliver costs savings by streamlining back office processes."[77] Moreover, IBM lists as one of the blockchain-based smart contracts' benefits, its ability to reduce the time consumed in dispute resolution by 75%.[78] Accordingly, smart contracts built on the private permissioned blockchain might be able to streamline the administrative and mundane tasks related to international arbitration in a timely, effective and a secure manner. To know the answer exactly to this question, we need to test the use of smart contracts based on a private permissioned blockchain in international arbitration for a period of time to see whether there will be any material efficiency gains.

(E) Conclusion

Unfortunately, arbitral proceedings are still conducted in the "same way as they were 50 years ago. Everyone shows up in one place at an appointed time, for in-person hearings before a panel reading hard-copy documents from A5 bundles."[79] It seems that the international arbitration community is underutilizing the advancements of technology, especially when it comes to securing its sensitive data against cyber-attacks. Another problem is that there are quite many misperceptions about what blockchain actually means and how it can really help the international arbitration community. That's why this article has tried to put the blockchain technology in an objective perspective showing its different types and how private permissioned blockchain would be the optimal choice as a use case in international arbitration.

In conclusion, the blockchain technology is not a panacea for all the technological dilemmas concerning international arbitration. However, the blockchain technology can certainly offer a better

platform for international arbitration, at least from a cybersecurity and a confidentiality perspective. Accordingly, it would be highly advisable if the international arbitration community takes the blockchain technology into their consideration and critically assess the potentials and pitfalls of such a nascent and a promising technology.

---

[1] Available at: https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Technology/IE_C_BlockchainandCyberPOV_0417.pdf
[2] Available at: https://www.bloomberg.com/news/articles/2016-06-23/finance-firms-seen-investing-1-billion-in-blockchain-this-year
[3] Available at: https://www.coindesk.com/research/state-blockchain-2018/
[4] Available at: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value
[5] *Ibid*
[6] Conceptualizing Blockchains: Characteristics & Applications: Karim Sultan, Umar Ruhi and Rubina Lakhani 11th IADIS International Conference Information Systems 2018
[7] Coinbase (2017) What is the bitcoin blockchain?
[8] Oxford Dictionaries (2018) blockchain | Definition of blockchain in English by Oxford Dictionaries.
[9] *Supra* en (6)
[10] *Ibid*
[11] *Ibid*
[12] Available at: https://www.merriam-webster.com/dictionary/blockchain
[13] *Supra* en (4)
[14] Available at: https://www2.deloitte.com/insights/us/en/focus/tech-trends/2018/blockchain-integration-smart-contracts.html?id=us:2ps:3gl:confidence:eng:cons:120617:em:dup1157:f5ByYZ1E:1083233419:244804533104:b:RLSA_Tech_Trends:Blockchain_BMM:nb
[15] Bambara, Blockchain: A Practical Guide to Developing Business, Law, and Technology Solutions (2017), pp. 30
[16] *Ibid*
[17] *Ibid*
[18] *Ibid*
[19] *Ibid*
[20] *Ibid*
[21] Elyes Ben Hamida, Kei Leo Brousmiche, Hugo Levard, Eric Thea. Blockchain for Enterprise: Overview, Opportunities and Challenges. The Thirteenth International Conference on Wireless and Mobile Communications (ICWMC 2017), Jul 2017, Nice, France. <https://www.iaria.org/conferences2017/ICWMC17.html>. <hal-01591859>
[22] *Supra* en (15) at pp. 31
[23] *Ibid*
[24] Supra en (21)
[25] *Ibid*
[26] *Ibid*
[27] *Ibid*
[28] *Ibid*
[29] Available at: https://www.ibm.com/blogs/blockchain/2018/05/understanding-blockchain-debunking-the-myths-of-enterprise-blockchain/
[30] *Supra* en (21)
[31] *Ibid*
[32] *Supra* en (29)
[33] Public versus Private Blockchains Part 2: Permissionless Blockchains White Paper BitFury Group in collaboration with Jeff Garzik
[34] Gavin Andresen (2013). March 2013 chain fork post-mortem (BIP 50) URL: https://github.com/bitcoin/bips/blob/master/bip-0050.mediawiki
[35] *Supra* en (33)
[36] *Supra* en (21)
[37] *Ibid*
[38] *Ibid*
[39] Ashish Chugh, 'Why We Don't Need Blockchain to Manage Cases in International Arbitration', Kluwer Arbitration Blog, May 13 2018, http://arbitrationblog.kluwerarbitration.com/2018/05/13/dont-need-blockchain-manage-cases-internati onal-arbitration/
[40] *Ibid*
[41] Available at: https://www.ibm.com/blogs/blockchain/2018/05/understanding-blockchain-debunking-the-myths-of-enterprise-blockchain/
[42] *Supra* en (14)
[43] *Ibid*
[44] *Ibid*
[45] Claire Morel de Westgaver, 'Cybersecurity In International Arbitration – A Necessity And An Opportunity For Arbitral Institutions', Kluwer Arbitration Blog, October 6 2017, http://arbitrationblog.kluwerarbitration.com/2017/10/06/cyber-security/

[46] *Ibid*
[47] (ICSID ARB/06/8)
[48] I*bid*
[49] ICSID Case No. ARB/13/13
[50] *See* Alison Ross, *Tribunal Rules on Admissibility of Hacked Kazakh Emails*, GAR (Sept. 22, 2015).
[51] ConocoPhillips Petrozuata BV, ConocoPhillips Hamaca BV and ConocoPhillips Gulf of Paria BV v Bolivarian Republic of Venezuela, ICSID Case No ARB/07/30, decision on Jurisdiction and the Merits (3 September 2013)
[52] Jessica O. Ireton, The Admissibility of evidence in ICSID Arbitration: considering the validity of WikiLeaks Cables as Evidence. ICSID Review, Vol. 30, No. 1 (2015) p. 2. For a general overview, see W. Michael Reisman, and Eric E. Freedman, "The Plaintiff's Dilemma: Illegally obtained Evidence and admissibility in international Adjudication" (1982). Faculty Scholarship Series Paper 730. http://digitalcommons.law.yale.edu/fss_papers/730, p. 742. See also, "Admissibility of Hacked Emails as Evidence in Arbitration" https://blogs.law.nyu.edu/transnational/2018/05/admissibility-of-hacked-emails-as-evidence-in-arbitration/.
[53] Brigitta John, 'Admissibility of Improperly Obtained Data as Evidence in International Arbitration Proceedings', Kluwer Arbitration Blog, September 28 2016, http://arbitrationblog.kluwerarbitration.com/2016/09/28/admissibility-of-improperly-obtained-data-as-evidence-in-international-arbitration-proceedings/
[54] *Ibid*
[55] *See, e.g.,* Nate Raymond, *U.S. Accuses Chinese Citizens of Hacking Law Firms*, INSIDER TRADING (Dec. 28, 2016), http://www.reuters.com/article/us-cyber-insidertrading- idUSKBN14G1D5; Michael Schmidt and Steven Lee Myers, *Panama Law Firm's Leaked Files Detail Offshore Accounts Tied to World Leaders*, N.Y. TIMES (Apr. 3, 2016), https://www.nytimes.com/2016/04/04/us/politics/leaked-documents-offshore-accounts- putin.html (reporting that 11.5 million documents leaked from Panama law firm exposed the offshore accounts of 140 politicians and public officials). *See also* New York State Bar Ass'n Ethics Opinion 1019 (Aug. 2014) ("Cyber-security issues have continued to be a major concern for lawyers, as cyber-criminals have begun to target lawyers to access client information, including trade secrets, business plans and personal data. Lawyers can no longer assume that their document systems are of no interest to cyber-crooks.").
[56] *See,* https://www.logicforce.com/e-book/law-firm-cyber-security-scorecard/
[57] *Ibid*
[58] *Ibid*
[59] Stephanie Cohen and Mark Morril, *A Call To Cyberarms: The International Arbitrator's Duty To Avoid Digital Intrusion*, 40 FORDHAM INT'L L.J. 981, 988 (2017). Available at: https://ir.lawnet.fordham.edu/ilj/vol40/iss3/11 ,
[60] *See Cybersecurity and Arbitration: Protecting Your Documents and Ensuring Confidentiality*, NYSBA INSIDE (2016).
[61] *See*, "Why Int'l Arbitration Presents A Tempting Target For Hackers". Available at https://www.law360.com/articles/948812/why-int-l-arbitration-presents-a-tempting-target-for-hackers
[62] https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Technology/IE_C_BlockchainandCyberPOV_0417.pdf
[63] https://blog.ethereum.org/2016/09/22/transaction-spam-attack-next-steps/
[64] https://ice3x.co.za/byzantine-generals-problem/
[65] *Supra* en (36)
[66] *Ibid*
[67] *Ibid*
[68] *Ibid*
[69] http://www.arbitration.qmul.ac.uk/research/2018/
[70] *Ibid*
[71] *Ibid*
[72] *Ibid*
[73] Howard M. Holtzmann, Streamlining Arbitral Proceedings: Some Techniques of the Iran-United States Claims Tribunal, 11(1) ARB. INT'L 39 (1995).
[74]*Supra* en (43)
[75] Supra en (4)
[76] *Ibid*
[77] Available at: http://www.nortonrosefulbright.com/knowledge/publications/137955/smart-contracts-coding-the-fine-print
[78]Available at: https://www.ibm.com/developerworks/community/files/basic/anonymous/api/library/4830497b-09f4-42c9-940f-bdd9054fcdd0/document/887cfd8f-2a2c-4f57-96df-c3be08116602/media/Blockchain%20Solutions%20v2.07.pdf
[79] Sophie Nappert & Paul Cohen, *Case Study*, *in* ARBITRATION IN THE DIGITAL AGE: THE BRAVE NEW WORLD OF ARBITRATION 126–148, at page 126 (Maud Piers & Christian Aschauer eds., 2018).