THE BLOCKCHAINS AND REGULATIONS: PAMPERING OR SLAPPING?

A Study of privacy and data protection regulations in European Union and India

Garima Agrawal
Student
O. P. Jindal Global University

INTRODUCTION

"Getting information from the Internet is like taking a drink from a hydrant."
-Mitchell Kapor (Personal Computing Pioneer and Investor)

Is it the same for blockchain technology, the horse behind the Bitcoin protocol? Privacy is a pre-requisite to a healthy life of any individual. With the advent of technologies and exploitation of the same leads to the question of regularizing them as then they start affecting individuals privately and publicly. The country of India under its Constitution has declared right to privacy to be a fundament right[1]. Under Article 21of the Constitution of India, this right to privacy includes the right to data protection and privacy. Similarly, on 25th May 2018, The General Data Protection Regulation ("GDPR") governing the European Union ("EU") came into force to strengthen individuals' data protection rights. The launch of Bitcoin in January 2009 by Satoshi Nakamoto brought life to an 18-year-old technology, designed by Stuart Haber and W. Scott Stornetta then. It is known for its "tamper proof", decentralized and transparent structure which is total opposite of what internet is. But can we really conclude that it is the better than internet?

The blockchain technology or distributed ledger technology has widespread use that includes Food Trust blockchain created by IBM[2], healthcare, records of property, smart contracts, voting and in other such sectors along with in cryptocurrencies. Companies like Walmart, Pfizer, AIG, Siemens, Unilever and others have already incorporated blockchain[3]. This technology can be foreseen to be the future of the world. The increasingly hype of the blockchain technology pushed the Commission Nationale de l'Informatique et des Libertés ("CNIL"), the French Data Protection authority to issue a guidance report for GDPR in regards with the blockchain technology. The author in this paper will reflect on whether the regulations of EU and India will try to support the growth of the blockchain technology or inhibit them keeping in view the long run of the same. This reflection will be drawn by support of the internet and blockchain comparison and by drawing inferences from CNIL report.

---

[1] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1
[2] https://www.ibm.com/products/food-trust.
[3] Luke Conway, *Blockchain Explained*, INVESTOPEDIA (Sept. 23, 2021, 9:00 AM)

1. WHICH IS BETTER: BLOCKCHAIN OR INTERNET?

Internet is supposed to be thriving on the personal data of users while blockchain relies on the shared information. The blockchain technology in comparison to internet is a "tamper proof" one. The blockchain vests its hype on its unique and novel method of storing and transferring data which entails facilitating peer-to-peer transaction without need of a central or third party. The former is known to be truth machine while latter is termed to be an information machine[4]. The accounting method of two is different as of blockchain is decentralized one while that of internet is a centralized one. Transparency in the case of blockchain is commendable as in the network of public blockchain every transaction of bitcoin can be publicly available. Despite the praise, a 15-year-old boy in United Kingdom in the March of 2018 demonstrated the proof-of-concept code that allowed him to get authorizations for a hardware wallet, Ledger Nano S[5]. In his personal blog he had explained the process depicting that how easily attackers can penetrate these ledgers. Therefore, in matter concerning privacy of an individual, it is stake in either of them.

However, I believe that the two cannot be completely compared in the present day due to the period of time they have been subjected to use. Blockchain is a ledger to maintain records while internet entails social media, information and many other such things. The experience with blockchain has been maximum in the field of cryptocurrencies and gradually increasing in others as well. So as of now, the amount of private information of extreme personal nature of an individual can be found more on an internet than blockchain. In contrary, details with respect to finance, location and with the expand in use to that of health and other would be available in blockchain as well. For the crypto exchange, blockchain has proved to be a boon but with incidents of cyber-attack it is no more the same. Also, transaction settlement time is an issue with blockchain. The bitcoin blockchain can process about 8 to 10 transactions per second only while visa and the master cards can process about 40 thousand transactions per second[6]. This is due to de-regulation and transparency often leading to loss of efficiency. The notion of 'private' and 'permissioned' blockchains was brought up because of the same reason of efficiency, but as rightly criticized to be nothing more than 'shared databases' by computer science researchers like Arvind Narayanan and Jeremy Clark[7].

The comparison depicts that both have their own pros and cons. Some researchers claim the blockchain to be the new internet in the future, but I am not sure of that. According to me both internet and blockchain in the future would be parallel instruments with blockchain being used for more sophisticated regimes like banking, locating things in various industries and reducing the paperwork of maintain the records while internet will go on with providing information. The blockchain technology if studied more and algorithms be changed with same decentralization but with increased efficiency would lead to betterment of future with a guarantee of more privacy. Internet and blockchain working parallelly will be a sustainable growth in the digital sector for the world ensuring privacy.

2. THE NEED FOR REGULATIONS

In the 21st century there is no doubt that people are willing to exploit their privacy and internet has become means for it, expediating the growth of internet applications, especially social media websites and Google. However, the exploitation has not been constrained within the walls of willing individuals but extended to the 'sensitive information' and non-willing individuals leading to violation of privacy. Similarly, as has been mentioned above the blockchain technology is not immune of cyber-attacks. The decentralization allows different nodes to be attacked separately just like the boy in UK did. In some cases, where certain nodes carry out all activities, then identifying and attacking those will compromise the blockchain severely. Another way is when an attacker attacks node with high computing power[8]. Therefore, just like internet, blockchain must be regulated.

---

[4] Dr.Xiao Feng, *A Comparison between Blockchain and Internet*, WANXIANG BLOCKCHAIN (Sept. 23,2021, 10:00 AM).

[5] Dan Goodin, *A "tamper-proof" currency wallet just got backdoored by a 15-year-old*, ARS TECHNICA (Sept. 23,2021, 10:05 AM).

[6] Dharmin Dave, Shalin Parikh, Reema Patel and Nishant Joshi, *A Survey on Blockchain Technology and its Proposed Solutions,* PROCEDIA COMPUTER SCIENCE 740, 744 (2019).

[7] Nishith Desai Associates, *The Blockchain: Industry Applications and Legal Perspectives*, NISITH DESAI 1,7 (2018).

[8] John Salmon and Gordon Myers, *Blockchain and Associated Legal Issues for Emerging Markets,* IFC 1,4-5 (2019).

In India, long with the Article 21 of the Constitution of India, The Information Technology Act, 2000 ("IT Act") and the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("SPDI Rules") govern data protection and privacy[9]. Later, in 2019 the Personal Data Protection Bill ("the Bill") was tabled before the Parliament to ensure the protection of privacy of personal data of individuals. It was inspired by EU's GDPR and is in many ways' replica of it. In EU, GDPR governs data protection since 2018. The debate whether these regulations support the upcoming technology with a different database system is a long drawn one. In fact, the blockchain technology is considered to be not in compliance with the rules laid down under the two jurisdictions. The CNIL's report, in contradiction pushes towards filling the gap between the regulations and the blockchain technology.

3. DOES REGULATIONS GIVE A WARM WELCOME TO BLOCKCHAIN?

Multiple points of tension have always been observed between the blockchain technology and common data privacy requirements. The following are some of them along with how CNIL has tried to address them: -

3.1 Jurisdictional Issue

In India, Section 1(2) read with Section 75 of the IT Act allows for limited extra-territorial applicability of the Act. On 24th August 2011 a clarification to the SPDI Rules by the Ministry of Electronics and Information Technology was issued restricting the applicability of the SPDI Rules to body corporates or persons located within India. Therefore, the blockchain technology will be required to comply with IT Act till a certain extent and only nodes and miners operating from India will fall under the ambit of SPDI Rules, leaving the network participants operating outside India unregulated. Section 2 of the Bill allows extra-territorial application but in certain limited circumstances like "where the processing which takes place outside India is in connection with any business in India, or which involves the profiling of individuals within India"[10]. The Indian commercial-civil courts also devised an 'interactive website' test wherein wherever a website facilitates to conduct trade and cause of action arises, then despite not having a physical establishment would be considered as jurisdiction for governing purposes. However, the test and Section 2 of the Bill cannot be narrowed down to be applicable to blockchain technology because of the complex nature of process and identification of individuals and nodes cannot be ascertained due to anonymity.

Similarly, GDPR has also broadened its territorial scope to include data processing carried out by data controllers or data processors established within the territory of the EU and also those have no physical presence in EU, but process data of subjects located in EU territory[11]. It basically is concerned till the various behaviors happen within EU. According to me EU took faces similar problem as to India due to structure of blockchain.

3.2 Issue of Anonymity

In order to determine whether GDPR and Indian data protection laws would be applicable, we have to determine if the data being processed by blockchain technology falls under the ambit of 'personal data'. GDPR has defined 'personal data' broad enough to drop the identification threshold very low. In the case of *Breyer v. Germany*[12], European Court of Justice ("ECJ"), included dynamic IP addresses in realm of personal data. Similarly, in India, the Bill defined 'personal data' to include data of natural persons which can be traced to be a natural person but dropped the threshold of identification to not identifiable. Both the regulations require traceability without assurance of identification, allowing existence of pseudonymity. However, blockchain technology functions on anonymity. Due to decentralization of blockchain database, the identity of individuals stays anonymous, restricted to nodes only. One of the primary advantages of using this technology for cryptocurrency but on the other side, the heavy cash flow cannot be regulated due to anonymous identity and

---

[9] Anish Jaipuriar, Ashutosh Nagar, Varun Kalway and Sayantika Ganguly, *Blockchain And Data Privacy: An India Perspective*, MONDAQ (Sept. 23, 11:00 PM).

[10] Anish Jaipuriar, Ashutosh Nagar, Varun Kalway and Sayantika Ganguly, *Blockchain And Data Privacy: An India Perspective*, MONDAQ (Sept. 23, 11:15 PM).

[11] Sonia Daoui, Thomas Fleinert-Jensen and Marc Lempérière, *GDPR, Blockchain and the French Data Protection Authority: Many Answers but Some Remaining Questions,* STANFORD JOURNAL OF BLOCKCHAIN LAW AND POLICY (2019) (Sept. 23, 12:00 PM).

[12] Case 582/14

problem of who to make liable occurs. Therefore, the organizations operating and using blockchain must try for compatibility with pseudonymity in the existing structure which will be beneficial for all.

3.3 Stakeholders: Who can be Data Controller?

GDPR identifies two categories of stakeholders, data controllers and data processors. The bill in India identifies three categories of stakeholder, Data Principals, Data Fiduciary and Data Processor while the SPDI Rules provide for data controllers and processors. EU data protection laws is based on the assumption that in relation to each data point, one or many legal or natural person exist who are data controllers and to whom data subjects can address to enforce their rights[13]. In contrary, the blockchains which believe in decentralization, replaces the unitary actor with many different players. According to GDPR and the Bill, nodes that process personal data are data processors as they facilitate the blockchain networks operation[14]. This is cannot be applied to all blockchains since they have different structures. Also, because of this there cannot be demarcation between the three categories as per the Bill. In the guidelines, CNIL considers this difficulty in respect of data processor but mentions that it requires more investigation to be addressed thoroughly. However, the concern is for data controllers as they hold the power to be deemed liable in case of discrepancy. CNIL addressed this issue by drawing from Article 2(2)(c) of GDPR which allows application of GDPR to go beyond purely personal or household activity while processing of personal data by a natural person. The CNIL report redefined controllers to be one who processes data for purpose of business or anyone who is a legal entity, writing personal data on blockchain like the bank registering client data on blockchain[15]. This can be applicable to India as well under SPDI Rules which is replica of GDPR and under the Bill, Data principals will fall under the ambit of data controller.

3.4 Cross-Border Transfer issue

GDPR sets out various means like binding corporate rules, standard data protection clauses adopted by the European commission as mentioned under Article 93(2) of GDPR, an approved code of conduct[16] and other such measures in case a data is transferred outside the territory of EU. In India, chapter VII of the Bill mandates that a copy of the Sensitive Personal Data should be stored domestically and restricting the Critical Personal Data to be stored in India only. Under Rule 7 of SPDI Rules, cross border transfer of data is constrained to the condition that the country receiving it provides for the same level of protection to the data. CNIL on this has rightly suggested the use of permissioned blockchain for transfer of data as it can be observed that these measure by EU and India can only be effective by seeking permission which otherwise would go blur in the complexity. This again aligns with the idea of pseudonymity which has been stated earlier.

3.5 Immutability issue

GDPR under Article 16 and 17 makes 'right to erasure', a legal requirement and believes that data can be modified or erased. It is usually put in action once the use of data is over. Similar to this, the Bill in India has introduced 'right to be forgotten' which includes, erasure, data anonymization, destruction of hardware and putting data beyond use[17]. The blockchain in contrast works on immutability principle which entails that information can be added block by block but can never be deleted. Therefore, CNIL considered storing of data in blockchain by hashing or any form of state-of-the-art encryption which includes a private key that can be subjected to deletion[18]. Thereby, securing confidentiality of the personal data, the ultimate goal of both the rights, erasure and forgotten. However, CNIL report states that it amounting to erasure is left be examined. It reinforces the privacy by principle of design as under Article 25 of GDPR which requires personal data to be uploaded only with encryption otherwise try not to. Other alternatives can be programming chameleon hashes,

---

[13] Dr Michèle Finck, *'Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?'*, EUROPARL I, II (2019).

[14] John Salmon and Gordon Myers, *Blockchain and Associated Legal Issues for Emerging Markets,* IFC 1,3(2019).

[15] Sonia Daoui, Thomas Fleinert-Jensen and Marc Lempérière, *GDPR, Blockchain and the French Data Protection Authority: Many Answers but Some Remaining Questions,* STANFORD JOURNAL OF BLOCKCHAIN LAW AND POLICY (2019).

[16] Article 40 of GDPR.

[17] Anish Jaipuriar, Ashutosh Nagar, Varun Kalway and Sayantika Ganguly, *Blockchain And Data Privacy: An India Perspective*, MONDAQ (Sept. 24, 9:00 AM).

[18] Sonia Daoui, Thomas Fleinert-Jensen and Marc Lempérière, *GDPR, Blockchain and the French Data Protection Authority: Many Answers but Some Remaining Questions,* STANFORD JOURNAL OF BLOCKCHAIN LAW AND POLICY (2019).

zero knowledge proofs or a censorable blockchain as suggested in the paper, "Redactable Blockchain or Rewriting History in Bitcoin and Friends"[19]. This issue is important as well as complicated, but a close erasure can work effectively. Also, since no tribunal or legal authority has declared that the blockchains is immutable in nature, one can expect such an advancement in technology which allows for complete erasure. CNIL's report leave a grey area and a space to continue with experimentation on same and also with a diligent idea.

The above issues being put to scrutiny under EU's and India's Data protection law and some them being addressed by CNIL depicts that despite the issues currently being non-compliant of the regulations can be brought in compliance with the regulations. CNIL's guidance reports analysis shows that it has tried to bring the existing regulation in square with the blockchain technology's structure. So, it was indeed a warm welcome by regulations to the blockchain.

CONCLUSION

The century we live in is one of the most dynamic and digitalized of all the times. The COVID-19 pandemic has pushed the masses either to rely on technology for their sustainability or incur immense loss in a human life as a whole. This went to such an extent that it gave a boom in crypto dealing across the world making the blockchain technology the 'knight in shining armor'. This knight so then was subjected to privacy and data protection, the first and most important thing when one enters cloud industry. Due to the complex structure of the blockchain technology it does not comply with the regulations completely. However, by amending the regulations a bit and certain changes in the blockchain and a better combination of permissioned and standard blockchain can make it more sustainable. Researchers are still studying and have been successful in deriving a "Trustworthy Management in Decentralized IoT Application using Blockchain"[20]. The CNIL guidance report and above analysis clearly depict that in the long run, the regulator authorities of EU and India view blockchain technology to be a part of future and so works towards enhancing it and bridging the gap. It can also be said that the existing regulations on privacy and data protection merely acts as band aid and more research and experimentation is required in the same for both internet and blockchains. From a top-bottom view, the blockchain technology coupled with proper regulations would prove to be better than internet but from a bottom-top view as analyzed above a parallel working of internet and blockchain properly regulated would prove to be a revolution in the digitalized world.

REFERENCES

1. Dharmin Dave, Shalin Parikh, Reema Patel and Nishant Joshi, *A Survey on Blockchain Technology and its Proposed Solutions,* PROCEDIA COMPUTER SCIENCE 740, 744 (2019).

2. Nishith Desai Associates, *The Blockchain: Industry Applications and Legal Perspectives*, NISITH DESAI 1,7 (2018), http://www.nishithdesai.com/fileadmin/user_upload/pdfs/Research%20Papers/The_Blockchain.pdf .

3. John Salmon and Gordon Myers, *Blockchain and Associated Legal Issues for Emerging Markets,* IFC 1,3-5 (2019), https://www.ifc.org/wps/wcm/connect/da7da0dd-2068-4728-b846-7cffcd1fd24a/EMCompass-Note-63-Blockchain-and-Legal-Issues-in-Emerging-Markets.pdf?MOD=AJPERES&CVID=mxocw9F.

4. Sonia Daoui, Thomas Fleinert-Jensen and Marc Lempérière, *GDPR, Blockchain and the French Data Protection Authority: Many Answers but Some Remaining Questions,* STANFORD JOURNAL OF BLOCKCHAIN LAW AND POLICY (2019), https://stanford-jblp.pubpub.org/pub/gdpr-blockchain-france/release/1.

---

[19] Giuseppe Ateniese, Bernardo Magri, Daniele Venturi, and Ewerton Andrade, *Redactable Blockchain - or - Rewriting History in Bitcoin and Friends*, EURO S&P (2017).
[20]
Bhabendu K. Mohanta, Soumyashree S. Panda, Utkalika Satapathy, Debasish Jena, Debasis Gounti, *Trustworthy Management in Decentralized IoT Application using Blockchain*, RESEARCH GATE (Sept. 24, 2021, 10:00 AM).

5. Dr Michèle Finck, *'Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?'*, EUROPARL I, II (2019), https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf.

6. Giuseppe Ateniese, Bernardo Magri, Daniele Venturi, and Ewerton Andrade, *Redactable Blockchain - or - Rewriting History in Bitcoin and Friends*, EURO S&P (2017), https://eprint.iacr.org/2016/757.pdf.

7. Pritesh Shah and Daniel Forester, *Blockchain Technology: Data Privacy Issues and Potential Mitigation Strategies*, DAVIS POLK (Sept. 22, 2021, 5:00 PM), https://www.davispolk.com/sites/default/files/blockchain_technology_data_privacy_issues_and_potential_mitigation_strategies_w-021-8235.pdf.

8. Luke Conway, *Blockchain Explained*, INVESTOPEDIA (Sept. 23, 2021, 9:00 AM), https://www.investopedia.com/terms/b/blockchain.asp#citation-23.

9. Dr.Xiao Feng, *A Comparison between Blockchain and Internet*, WANXIANG BLOCKCHAIN (Sept. 23,2021, 10:00 AM), https://wxblockchain.medium.com/a-comparison-between-blockchain-and-internet-85a78099613a.

10. Dan Goodin, *A "tamper-proof" currency wallet just got backdoored by a 15-year-old*, ARS TECHNICA (Sept. 23,2021, 10:05 AM), https://arstechnica.com/information-technology/2018/03/a-tamper-proof-currency-wallet-just-got-trivially-backdoored-by-a-15-year-old/.

11. Anish Jaipuriar, Ashutosh Nagar, Varun Kalway and Sayantika Ganguly, *Blockchain And Data Privacy: An India Perspective*, MONDAQ (Sept. 23, 11:00 AM), https://www.mondaq.com/india/fin-tech/978488/blockchain-and-data-privacy-an-india-perspective.

12. Bhabendu K. Mohanta, Soumyashree S. Panda, Utkalika Satapathy, Debasish Jena, Debasis Gounti, *Trustworthy Management in Decentralized IoT Application using Blockchain*, RESEARCH GATE (Sept. 24, 2021, 10:00 AM), https://www.researchgate.net/profile/Bhabendu-Mohanta/publication/338371383_Trustworthy_Management_in_Decentralized_IoT_Application_using_Blockchain/links/5e0f6f17a6fdcc283756148d/Trustworthy-Management-in-Decentralized-IoT-Application-using-Blockchain.pdf.