II.4

Towards an alternative to territorial jurisdiction to face criminality committed through or facilitated by the use of blockchains

SUMMARY: 1. Introduction. – 2. The territoriality principle to determine State jurisdiction. – 3. The development of cybercrime and its consequences on the territoriality principle. – 4. The development of blockchains and its consequences on the territoriality principle. – 5. The applicability of the targeted public theory to establish jurisdiction over offences enabled or facilitated by the use of blockchains. – 6. Towards an alternative to State jurisdiction based on territoriality. – 7. Conclusions.

1. According to Christopher Pierson, « States occupy an increasingly clearly defined physical space over which they claim sole legitimate authority[421]». The territoriality principle supposes that a State has authority to exercise jurisdiction over conducts taking place within its own territory[422]. At the birth of the modern State, the territoriality principle was subject to almost no doubt or question. However, the globalisation of the world, especially through the development of technological means and through the Internet, marked a real change of society and raised new legal questions. In a society which is built globally, jurisdiction based on national borders does not make sense anymore. According to Darrel C. Menthe « [...] cyberspace takes all of the traditional principles of conflicts-of-law and reduces them to absurdity[423] ». After the launch of Bitcoins, ten years after this quotation, Darrel C. Menthe could have said the exact same thing about blockchains[424].

The objective of this article will be to assess whether the territoriality principle in its current form may be used in order to tackle offences facilitated by or committed through a blockchain. The developments to the territoriality principle resulting from the raise of cybercrime will be used as a background. Finally, some of the proposals that have been made by scholars will be assessed in order to imagine an alternative to State jurisdiction based on territoriality to overtake criminality committed through or facilitated by the use of blockchains.

In order to do this, the concept of territoriality as it is used in order to determine State jurisdiction over an offence will be studied (2), then the consequences of the development of the Internet and cybercrime on State jurisdiction established through the territoriality principle will be assessed (3). The fourth part of this article will study the development of blockchains and its

421 C. PIERSON, *The modern State*, London, 2002, II ed., p. 9, http://psi424.cankaya.edu.tr/uploads/files/Pierson,%20The%20Modern%20State,%202nd%20ed.PDF.

422 D. IRELAND-PIPER, *Extraterritorial criminal jurisdiction: Does the long arm of the law undermine the rule of law*, in *MJIL*, 2012, p. 130.

423 D. C. MENTHE, *Jurisdiction in cyberspace: a theory of international spaces*, in *MTLR*, 1998, p. 71.

424 For more clarity, within this article, Blockchain should be understood as a transparent, secure information storage and transmission technology that operates without a central control body (the "Blockchain"). By extension, a blockchain is a database that contains the history of all exchanges between its users since its creation. This database is secure and distributed: it is shared by its various users, without intermediaries, which allows everyone to check the validity of the chain.
(a "**blockchain**") – definition provided by Blockchain France, https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/.

consequences on the territoriality principle (4) before studying the applicability of the targeted public theory to establish jurisdiction over offences enabled or facilitated by the use of blockchains (5) and finally, it will move on to review some of the proposals made in order to better respond to cybercrime and analyse their applicability to criminality enabled or facilitated by the use of blockchains (6).

2. Sovereignty constitutes one of the founding principles of the modern State. The Peace of Westphalia, which constitutes for scholars the beginning of the modern international system, implied the concept of Westphalian sovereignty. This concept supposes the inviolability of borders, the equality between all sovereign States and above all, the non-interference in the affairs of foreign States[425]. The principle of national sovereignty supposes that « within the limits of its jurisdiction (set by the division of the world into a series of similarly sovereign nation-states), no other actor may gainsay the will of the sovereign State[426] ». This Westphalian sovereignty principle is stated in article 2(4) of the United Charter, according to which « Members thus, shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations ». No limitation to the power of the State can be brought by another. The right to punish (*ius puniendi*) expresses the Sovereign's authority throughout its population and territory. This means that only the State should have a right to punish individuals on its own territory[427]. Therefore, criminal law constitutes the core of the State's Sovereignty[428]. The principle of territoriality in criminal law confirms the sole authority and jurisdiction of the States and the right to punish it has on its citizen and within its territory.

The territoriality principle – to be understood as the right for a sovereign State to prosecute offences committed within its territory – is recognised by public international law. Public international law makes a distinction between subjective and objective territoriality[429]. Subjective territoriality should be understood as the right to prosecute offences committed – or at least initiated – within the territory of the State when objective territoriality gives the right to prosecute offences initiated within the territory of another State but that are completed[430] or whose effects are to be felt

425 B. TESCHKE, *La théorisation du système étatique westphalien: les relations internationales de l'absolutisme au capitalisme*, in *CRS*, 2012, p. 31; W. BERGE, *Criminal jurisdiction and the territorial principl*e, in *MLR*, 1931, p. 240; S. GARIBIAN, *Souveraineté et légalité en droit pénal international: le concept de crime contre l'humanité dans le discours des juges à Nuremberg*, in M. HENZELIN, R. ROTH (eds.), *Le droit pénal à l'épreuve de l'internationalisation,* Paris-Genève-Bruxelles, 2002, p. 2, https://archive-ouverte.unige.ch/unige:23564.

426 C. PIERSON, *The modern State*, cit., p. 11.

427 S. GARIBIAN, *Souveraineté et légalité en droit pénal international: le concept de crime contre l'humanité dans le discours des juges à Nuremberg*, in M. HENZELIN, R. ROTH (eds.), cit., p. 2.

428 On the role of criminal law as the core of the State's sovereignty, see for example B. MATHIEU, M. VERPEAUX, *Droit constitutionnel*, Paris, 2004, paragraph 384.

429 J. B. MAILLART, *The limits of subjective territorial jurisdiction in the context of cybercrime*, in *ERA Forum*, 2018, p. 3, https://link.springer.com/article/10.1007/s12027-018-0527-2#Fn7.

430 The objective territoriality has been recognised at an international level in the Lotus Case, Permanent Court of International Justice, *S.S. Lotus (Fr. v. Turk.)*, 7 September 1927, series A, no. 10, https://www.icj-cij.org/files/permanent-court-of-international-justice/serie_A/A_10/30_Lotus_Arret.pdf.

within the territory of the State[431]. This extensive comprehension of the territorial principle follows the ubiquity theory, which recognises the possibility for an offence to be present in more than one place. The ubiquity theory supposes that an offence may be located where any of its constituent element are located – this may be the place where the offence itself took place but also the place where the effects of the offence took place[432].

We find similar rules of jurisdiction at the national levels. Therefore, it does make more sense to refer to the objective and passive territoriality as they result from international law than to refer to specific national jurisdiction rules that would echo these principles. For example, French criminal law is applicable to offences committed within the territory of the Republic[433]. However, since it is not that easy in practice and since offences are often committed only partly in a certain State, the notion of offence committed within the territory is viewed in an extensive way. Thus, the concept includes all of the offences whose only one of the constituent elements took place in France[434]. German criminal law is also applicable to all offences that were committed in Germany[435]. An offence is to be understood as committed on the German territory either when the agent acted or when the effects of the offence are to be felt in Germany[436]. Additionally, an offence is considered as committed within the territory of Italy when the constituent element to the offence happened entirely or in part in Italy or if the consequence of the constituent element to the offence happened in Italy[437].

The globalisation of the world that we perceive tends to enable the development of social relations beyond territorial constraints. Because of the global character of the social relations of our era, of course, such a conception of territoriality accepts the risk that different jurisdictions may be established over a same offence, whose constituent elements are located in different countries that may all have jurisdiction over the conduct[438]. It is sometimes argued that, even though the Internet was first referred as a lawless area[439], the ubiquity theory finally renders it an overflow of repressive powers[440].

431 C. RYNGAERT, *The concept of jurisdiction in international law*, Oxford, 2015, II ed., p. 5, https://unijuris.sites.uu.nl/wp-content/uploads/sites/9/2014/12/The-Concept-of-Jurisdiction-in-International-Law.pdf; D. IRELAND-PIPER, *Extraterritorial criminal jurisdiction: Does the long arm of the law undermine the rule of law*, cit., p. 130.

432 H. ASCENSIO, L'*extraterritorialité comme instrument*, in *Travaux du Représentant spécial du Secrétaire général des Nations Unies sur les droits de l'homme et entreprises transnationales et autres entreprises*, 2010, p. 5, https://www.rse-et-ped.info/IMG/pdf/10-12-10_Ascencio_extraterritorialite-1.pdf.

433 French penal code (*Code pénal*), article 113-2-1 and French code of criminal procedure (Code de procédure pénale), article 693.

434 French penal code (*Code pénal*), article 113-2-2.

435 German penal code (*Strafgesetzbuch*), section 3.

436 German penal code (*Strafgesetzbuch*), section 9 paragraph 1.

437 Italian penal code (*Codice penale*), article 6.

438 L. DESESSARD, *France, les compétences criminelles concurrentes nationales et internationales et le principe ne bis in idem*, in *RIDA*, 2002, p. 917.

439 T. SCASSA, R. J. CURRIE, *New first principles – assessing the Internet's challenges to jurisdiction*, in *Geo. J. Int'l L.*, 2011, p. 1037; A. C. YEN, *Western Frontier or Feudal Society?: Metaphors and perceptions of cyberspace*, in *Berkeley Tech. L.J.*, 2002, p. 1037.

440 R. BOOS, *La lutte contre la cybercriminalité au regard de l'action des État,* 2016, p. 162, https://tel.archives-ouvertes.fr/tel-01470150/document.

3. While the Council of Europe Convention on cybercrime (the "Convention")[441] does provide for examples of what should be considered a cybercrime and thus, should be tackled by national substantive criminal law, the Convention does not provide for a general definition of cybercrime. However, the doctrine seems to agree on a rather large definition of cybercrime: Majid Yar defines cybercrime as any illegal activities facilitated by a computer[442] while Sarah Gordon and Richard Ford define it as any crime committed through or facilitated by the use of electronic devices or IT networks[443]. Thus, any offence enabled or facilitated by the use of a blockchain may also fall under this definition and it should therefore make sense to use the legislation on cybercrime as a background in order to try to apply it to criminality committed through or facilitated by a blockchain.

Throughout the last decades, we observed a global integration of the world which enhanced the interactions among people at a global level. This enhanced integration at a global level has been the consequence of, amongst others, the development of technology and of the Internet. The development of the Internet has been accompanied by the one of criminality facilitated by the use of the Internet and the law had therefore needed to respond to such a phenomenon. However, the particularity of cybercrimes raised certain difficulties that the territoriality of criminal law has to face. We should recall that the Internet is a network; the communications it contains are not limited to a specific territory. « Material published on the internet can be uploaded in one state, downloaded in another, and viewed in a large number of other states[444] ». What raises some difficulties is the fact that the jurisdiction is based on delimited territorial rules while the Internet is, on the contrary, characterised by its universality[445]. Conducts on the Internet happen at once anywhere and nowhere: it seems thus difficult to decide which jurisdiction is more entitled to have jurisdiction over an offence than another one[446]. « Unlike traditional jurisdictional problems that might involve two, three, or more conflicting jurisdictions, the set of laws which could apply to a simple homespun webpage is all of them[447] ». For an offence committed online, any State may be competent[448]. This can be explained by the fact that, through the use of the Internet, an illegal content may be made available by an agent in a foreign country, through the use of a foreign server for data storage, but

441 Council of Europe, *Convention on cybercrime*, Budapest, 2001, ETS 185, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

442 M. YAR, *Cybercrime And Society*, 2006, London, p. 10.

443 S. GORDON, R. FORD, *On The Definition And Classification Of Cybercrime*, in *J. Comput. Virol.*, 2006, p. 2, https://download.adamas.ai/dlbase/ebooks/VX_related/On%20the%20definition%20and%20classification%20of%20cybercrime.pdf.

444 S. NILOUFER, *The proper basis for exercising jurisdiction in internet disputes: strengthening state boundaries or moving towards unification?*, in *JTLP*, 2013, p. 1, https://tlp.law.pitt.edu/ojs/index.php/tlp/article/view/124/127.

445 J. FRANCILLON, *Cybercriminalité, aspect de droit pénal international*, 2014, http://www.penal.org/sites/default/files/files/RH-7.pdf.

446 S. P. BEATTY, *Litigation in cyberspace: the current and future state of Internet jurisdiction*, in *U. Balt. Intell. Prop. L.J.*, 1999, p. 139; D. R. JOHNSON, D. POST, *Law and borders – the rise of law in cyberspace*, in *Stanford L. Rev.*, 996, p. 1375.

447 D. C. MENTHE, *Jurisdiction in cyberspace: a theory of international spaces*, cit., p. 71.

448 D. C. MENTHE, *Jurisdiction in cyberspace: a theory of international spaces*, cit., p. 70.

still making the illegal content available to any person benefiting of an Internet access in any State[449]. Therefore, we understand that the principles that we developed in the first part of the article, that are used to establish jurisdiction, may be difficult to apply to the cyberspace.

Regarding the subjective territoriality: first, we understand that, because of the global character of the Internet and the multiplicity of its actors, it may be difficult to determine where an offence took place. The complexity related to the localisation of the causal event has been highlighted by the Advocate General Wathelet in the case Concurrence SARL v. Samsung Electronics France SAS and Amazon Service Europe Sàrl[450]. In order to respond to this, it should be determined in which territory is located an offence on the Internet? There are many possibilities to decide what constitutes the location of the offence: the location of the author or creator of the illegal content may be one but it would however face the risk of forum shopping to choose the most clement jurisdiction to commit an offence. We could also quote some others such as the location of the viewer of the illegal content, but it would not prevent positive conflicts of jurisdiction[451]. Therefore, regarding cybercrime, Lord Denning said that « a well-advised plaintiff is likely to commence proceedings in the most favourable forum[452] ». This is particularly relevant since a similar conduct on the Internet may be tackled in a complete different manner according to the competent jurisdiction. The location of the server giving access to the Internet and enabling the upload of illegal content may also be a solution. The location of the server may be difficult to determine because of technical issues and because of the possible use of multiple sub-servers. We could finally think about the first location of the website containing the illegal content to establish jurisdiction[453]. So far, we have no consensus on what constitutes the place of location of an offence on the Internet, this is why positive conflicts of jurisdiction may therefore not be solved by the use of subjective territoriality.

Regarding the objective territoriality: since the Internet is available almost everywhere, the constituent elements to a crime occurring on such an Internet page, may be located anywhere; in fact, in any jurisdiction that provides for access to the website. If this was the case, the territorial principle would not make sense anymore since by using it, it would give jurisdiction to any State. Therefore, the competence would tend to be a universal one[454]. Finally, the consequence would be

449 M. D. DUBBER, T. HÖRNLE, *Criminal law a comparative approach*, Oxford, p. 149.
450 Advocate General WATHELET, 9 November 2016, *Opinion on Concurrence SARL v Samsung Electronics France SAS and Amazon Service Europe Sàrl*, Case C-618/15, ECLI: EU:C:2016:843, paragraph 2.
451 S. NILOUFER, *The proper basis for exercising jurisdiction in internet disputes: strengthening state boundaries or moving towards unification?*, cit., p. 2; H. VAN LITH, *International jurisdiction and commercial litigation: uniform rules for contract disputes*, The Hague, 2009, p. 5 ss. Also see a similar theory for copyrights law on the internet in T. SOLLEY, *The problem and the solution: using the Internet to resolve Internet copyright disputes*, in *Ga. St. U. L. Rev.*, 2008, p. 818.
452 S. NILOUFER, *The proper basis for exercising jurisdiction in internet disputes: strengthening state boundaries or moving towards unification?*, cit., p. 2; *Forum Shopping reconsidered*, in *Harvard L. R.*, 1990, https://www.jstor.org/stable/pdf/1341283.pdf.
453 For more information on the pro and contra arguments related to these different possibilities, see S. F. MILLER, Bloomingtom, 2003, p. 235 ss, https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1270&context=ijgls.
454 J. FRANCILLON, *Cybercriminalité, aspect de droit pénal international*, cit.

constant positive conflicts of jurisdiction[455]. So, using the objective territoriality does not solve the problem of positive conflicts of jurisdiction[456].

If the traditional rules of jurisdiction are used without taking into account the specificity of the Internet, this would lead not only to incoherencies but also to a lack of legal certainty[457]. While criminal law should respect the principle of legality which supposes that it should be not only clear but also predictable[458] and that « punishment, coercive measures, prosecution and sentencing of criminals should be predictable and be applied uniformly and in a systematic order[459] » these uncertainties constitute a problem if they lead to as many different solutions as the number of potential competent States (which, as we have seen before, is extremely high). The fact of being potentially subject to all of the criminal law systems of the world may constitute a threat vis-à-vis of fundamental principles of criminal law – especially vis-à-vis the legality principle. This could also endanger the principle of *ne bis in idem* if more than one jurisdiction is competent and decide to prosecute the same offence committed online. As a consequence, legal certainty – which encompasses both the legality and the *ne bid in idem* principles[460] – may be weakened by the inadequacy of traditional jurisdiction rules to face cybercrime and this may endanger the rule of law in the information society, which reposes on principles including, amongst others, the certainty and predictability of the legal environment[461].

In 2001, the Council of Europe published a Convention on cybercrime. In its explanatory report regarding the Convention, the Council of Europe explained that it was aware of the necessity to use international law in order to address such a form of criminality that produces effects regardless of borders and regardless of the location of the offender[462]. The challenge that constituted the global character of the Internet was taken into account by the Council of Europe, which distinguished the creation of a common space – the cyberspace – which may be used to commit offences at a transnational level[463]. In its explanatory report, the Council of Europe recognised the fact that criminals using the Internet may be located in places different to those where the offences they commit produce their effects[464]. This was notably the reason why the Council of Europe argued

455 M. DELMAS-MARTY, *Le relatif et l'universel. Les forces imaginantes du droit*, tome 1, Paris, 2004, p. 342.
456 J. FRANCILLON, *Cybercriminalité, aspect de droit pénal international*, cit.; K. N. EDWIN, J. SHILILU, *Jurisdictional challenge of the Internet ; a focus on electronic contracts*, p. 3, http://www.academia.edu/27265774/JURISDICTIONAL_CHALLENGE_OF_THE_INTERNET_A_FOCUS_ON_ELECTRONIC_CONTRACTS.
457 Z. D. CLOPTON, *Territoriality, technology, and national security*, in *U. Chi. L. Rev.*, 2016, p. 49.
458 On the exigence of quality of the law according to the European convention on human rights, see for example, European Court of Human Rights, *Cantoni c. France*, no. 17862/91, 15 November 1996.
459 A. SUOMINEN, *What Role for Legal Certainty in Criminal Law Within the Area of Freedom, Security and Justice in the EU?*, in *BJCLCJ*, 2014, p. 7.
460 A. SUOMINEN, What Role for Legal Certainty in Criminal Law Within the Area of Freedom, Security and Justice in the EU?, cit., p. 9.
461 S. NILOUFER, *The proper basis for exercising jurisdiction in internet disputes: strengthening state boundaries or moving towards unification?*, cit., p. 2.
462 Council of Europe, *Explanatory report to the Convention on cybercrime*, ETS 185, Budapest, 2001, paragraph 6, https://rm.coe.int/16800cce5b.
463 Council of Europe, *Explanatory report to the Convention on cybercrime,* cit., paragraph 8.
464 Council of Europe, *Explanatory report to the Convention on cybercrime*, cit., paragraph 6.

for the necessity to tackle the challenge of cybercrime at an international level[465]. Therefore, the Council of Europe decided to tackle the question of jurisdiction and more precisely the issues regarding the determination of the place of commission of the offence[466]. However, even if the Convention provides for State parties to exercise jurisdiction when an offence is committed on their territory, it does not give specific rules on what should be considered an offence committed in a State's territory. The only way provided for by the Convention in order to deal with positive conflicts of jurisdiction is that it provides for States to consult to determine among them which State constitutes the most appropriate jurisdiction for prosecution, when more than one State has jurisdiction over an offence according to the jurisdiction rules provided for by the Convention[467]. This should be done in order to « avoid duplication of effort, unnecessary inconvenience for witnesses, or competition among law enforcement officials of the States concerned, or to otherwise facilitate the efficiency or fairness of the proceedings[468] ». It is a big step to focus on the regional level in order to find solutions to a global problem instead of focusing on national rules. However, the Convention and the rules it provides on jurisdiction, even if they can help because of the cooperation that they provide for, do not really give clear rules on territoriality that would permit to prevent positive conflicts of jurisdiction.

At a national level, judges confronted to jurisdiction issues within cybercrime cases, often relied on the objective territoriality principle. In the Töben case, the German court held that jurisdiction of German courts may be established solely because Internet users located in Germany could have access to the content that constituted a criminal offence, even if this content had been created and stored in foreign States. The Court considered that the offence had consequences (if not only, at least also) in Germany and the objective territoriality principle should thus give jurisdiction to Germany. Before 2008, the French jurisprudence also considered that the French jurisdictions were competent as soon as illicit content were available on the Internet and were accessible from France: thus, as soon as the website containing the criminal offence was accessible from France, jurisdiction was established[469]. This view was taken in the Yahoo! case in which the French jurisdictions declared themselves competent to hear the case because the website was available in France, even if it was not supposed to be intended for the French public[470]. However, conscious of the risks that the application of the objective territoriality principle means in terms of positive conflicts of jurisdiction, a French court in 2008[471] took a different view regarding cybercrimes. The French jurisdiction decided that it is not sufficient that the content on the website which constitutes

465 Council of Europe, *Explanatory report to the Convention on cybercrime*, cit., paragraph 6.
466 Council of Europe, *Explanatory report to the Convention on cybercrime*, cit., paragraph 11(v).
467 Council of Europe, *Convention on cybercrime*, Budapest, 2001, ETS 185, art 22(5), https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561.
468 Council of Europe, *Explanatory report to the Convention on cybercrime*, cit., paragraph 239.
469 Groupe de travail CECyF – Cyberlex, *La procédure pénale face aux évolutions de la cybercriminalité et du traitement de la preuve numérique : propositions pour une efficacité juridique renforcée*, 24 janvier 2018, p. 6 ; Tribunal de grande instance de Paris, CCE 2002/5. Comm. 77, 26 February 2002.
470 A. CAMARD, C*ommentaire des arrêts Yahoo v. La ligue contre le Racisme*, in *MBDE/Société de l'information, droits et médias*, 2011.
471 Cour de Cassation, chambre criminelle, no. 07-87.281, 9 September 2008, https://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000019570259&fastReqId=850465415&fastPos=1.

the criminal offence is accessible on the French territory, but it should also be proved that the website in question is dedicated to the French public. Certain advices may help in order to decide whether a website is dedicated to the French public: these include, for instance, the language of the website or also the fact that the products sold on the website are available to French citizens[472]. This view was confirmed by the French Court of cassation in 2010[473]. This trend can also be distinguished in other national laws[474]. Especially, the United States introduced such jurisdiction rules based on the targeting of a specific public by making a distinction between active and passive websites[475]. A passive website should be considered insufficient to establish jurisdiction when an active website may give jurisdiction to the State's courts. The principal criteria to be taken into account in order to determine whether a website is to be considered as active in a State is: the fact that the website is interactive, that it conducts business in the State and that it is advertised to potential customers in that State.[476]

4. What we distinguished with the development of the Internet was a simultaneous development of criminality facilitated by it. Even though this phenomenon had to be tackled by law enforcement authorities, this did not become a reason to over regulate the Internet or to diabolise it. The same approach should be taken with regard to blockchains. While certain authors consider blockchains and cryptocurrencies as too risky and plead for very strict rules[477] and while some countries decided to completely ban the use of cryptocurrencies[478] because of the possible threats it contains, many scholars stress the fact that these potential risks should in no way be used in order to reject the advancements in technology and innovation[479]. A distinction should always be made between the positive and the negative effects of the technology and the existence of negative effects should not have consequences that would detriment the positive ones. However, this should not be a reason to ignore the criminal activities taking place within the Blockchain ecosystem. The objective of the article is not to highlight the phenomenon of criminality committed through or facilitated by the use of blockchains or cryptocurrencies, but just to raise awareness regarding its existence: Interpol identified amongst others, the use of blockchains for sharing illegal data such as child pornography while Europol highlighted the risk of money laundering facilitated by the use of cryptocurrencies[480]. There are two different ways blockchains may be used for criminal purposes:

472 See for example, Cour de Cassation, chambre criminelle, no. 15-86645, 12 July 2016, https://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000032900131.
473 Cour de Cassation, chambre criminelle, no. 10-80.088, 14 December 2010, https://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000023433809.
474 T. SCASSA, R. J. CURRIE, *New first principles – assessing the Internet's challenges to jurisdiction*, cit., p. 1049.
475 R. BOOS, *La lutte contre la cybercriminalité au regard de l'action des État,* cit., p. 175 ss.
476 See for example *Zippo Mfg. Co. v. Zippo Dot Com, Inc.*, 952 F. Supp. 1119, W.D. Pa, 1997, https://law.justia.com/cases/federal/district-courts/FSupp/952/1119/1432344/; *Cybersell Inc v. Cybersell Inc.*, 130 F.3d 414, 9th Cir., 1997, https://www.courtlistener.com/opinion/748638/cybersell-inc-v-cybersell-inc/.
477 See for example E. ENGLE, I*s Bitcoin rat poison? Cryptocurrency, crime and counterfeiting*, in *JHTL*, 2016.
478 M. DI GIUDA, *Countries where the cryptocurrencies are banned: busted for Bitcoin*, 2018, https://bitnewstoday.com/market/bitcoin/countries-where-the-cryptocurrencies-are-banned-busted-for-bitcoin/.
479 R. ANDERSON, *Risk and Privacy Implications of Consumer Payment Innovation in the Connected Age*, in *Consumer Payment Innovation*, 2012, p. 99.
480 *Report of the Commonwealth Working Group on virtual currencies*, in *Commonwealth Law Bulletin*, 2016, p. 292.

either as instrumentality of the crime – in this case the offence would just be facilitated by the use of blockchain but could have been conducted in other ways also (one could for instance think about money laundering or the selling or buying of illicit products with cryptocurrencies) or the blockchain may be the object of the crime which could not have been committed without the existence of blockchains[481]. For example, one could think about the theft of cryptocurrency or broadcast of child pornography pictures through blockchains.

Thus, criminality committed through or facilitated by the use of blockchains – and especially the jurisdiction dilemma – constitutes an issue for the criminal justice systems that they should be able to tackle.

In the third section of this article, when trying to deduce what may constitute the place of location of an offence committed on the cyberspace, we highlighted the multiplicity of the actors within the Internet ecosystem. Especially, we developed the possibility to focus on the location of the viewer of the illegal content, the location of the creator of the illegal content, the one of the server enabling the publication of the content and finally the first location of the website in order to establish jurisdiction. We distinguish a similar – if not worse – multiplicity and transnationality of the actors on a blockchain. The first actor to mention is the creator(s) of the blockchain. Then, we should mention the different users of the blockchain – also called nodes. The system has been designed as an open one: this means that it is, by its very nature, open to anyone (in the case of a public blockchain) and thus also internationally open since any individual who wishes to participate to the public blockchain may be given a pair of keys randomly by the system. The existence of miners should also be highlighted. Miners should be understood as special nodes whose role is to verify the transactions by performing a proof-of-work or any similar consensus mechanism in order to accept the valid transactions in a block that will then be added to the blockchain. Finally, even though the functioning of a blockchain only requires the participation of nodes and miners, some other actors exist around the ecosystem. They render its use easier for non-technicians and as a consequence, more accessible. The ones mentioned in this paragraph do not constitute an exhaustive list of the actors existing around the Blockchain ecosystem: the purpose is only to focus on some of them, which are commonly used by participants. One could think about exchange platforms (whose activities consist in providing people with exchange services between fiat currency and cryptocurrency for example) and we could also mention digital wallets (whose activities consist in storing the users' information on the blockchain including their public and private keys).

Blockchains are also known as distributed ledgers. This supposes that the data within the blockchain is distributed to all of the nodes of the system instead of being concentrated into one as it is the case for centralised ledgers. Therefore, all of the participants to the network gets a copy of the blockchain as it currently is. Each block that is added to the blockchain is also added at the nodes' level so that there is a consensus between the nodes on the state of the register[482]. Distributed ledgers require the consensus of these nodes rather than just the confirmation by one central authority in order to add information on the blockchain. This means that, even though a miner

481 *Report of the Commonwealth Working Group on virtual currencies*, in *Commonwealth Law Bulletin*, cit., p. 292.
482 G. MARIN-DAGANNAUD, *Le fonctionnement de la blockchain*, in A*nnales des mines: réalités industrielles*, 2017, p. 43.

validates a block, it still needs to be accepted and reused by the other nodes of the system to be integrated to the blockchain: a consensus of a majority of the nodes is needed. « Each resulting block is forwarded to all users in the network, who can then check its correctness by verifying the hash computation. If the block is deemed to be "valid", then the users append it to their previously accepted blocks, thus growing the [...] blockchain[483] ». Because of this consensus mechanism, we distinguish a joint control of the blockchain.

According to international law, the competent jurisdiction is usually either the State where the offence has been initiated (subjective territoriality) or the State where the offence is completed or its effects are to be seen (objective territoriality and ubiquity theory); in the specific case of a criminal conduct taking place on a blockchain, these States may be difficult to identify. This can be explained by the fact that the activities taking place on blockchains operate themselves without any particular spatial linkage since blockchains are developed in a global way and the localisation of the actors does not have a strong importance[484].

Regarding the subjective territoriality, it may be difficult to determine the State where the offence has been committed and what the competent jurisdiction should be. The multiplicity and global character of the actors to the blockchain – either essential or not to the functioning of the system – and also, the fact that the conducting of a transaction result from the actions of many different actors – possibly located in different jurisdictions – complicates the determination of the place of commission of the offence. It may be difficult to decide on which territory such an offence has been committed if we try to distinguish a single jurisdiction that could tackle the offence. On the contrary, we could argue that many countries may have jurisdiction over such an offence if not all of them – because of the multiplicity and internationality of the different nodes to the blockchain[485]. The subjective territoriality aims at finding some links and thus a jurisdiction that would have more legitimacy to be declared competent. As we realise the global character to a transaction happening on a blockchain, it may be questioned whether there is such a State that would have more legitimacy than another one to conduct investigations.[486]

Regarding the objective territoriality, it may also be difficult to determine where an offence committed through or facilitated by the use of blockchains is completed or where it has effects. As a blockchain is distributed to all of its nodes, the effects may be felt in any jurisdiction which gives access to the blockchain and permits individuals to join the network. As a consequence, if the Internet was seen (rightly) as a transnational technology that enabled to make content available in any State simultaneously, distributed ledgers share also this transnational characteristic but in a

483 A. MALLARD, C. MÉADEL, F. MUSIANI, *The paradoxes of distributed trust: peer-to-peer architecture and user confidence in bitcoin*, in *Journal of peer production*, 2014, p. 6, https://hal-mines-paristech.archives-ouvertes.fr/hal-00985707/document.

484 For a similar reasoning regarding the financial economy, see J. B. AUBY, *La globalisation, le droit et l'Etat,* IIe ed., Paris, 2010, p. 20.

485 On top of the fact that determining the location of an offence on a blockchain may be difficult because of the multiplicity of its nodes and the fact that they all contribute to the functioning of the system, this distribution of the blockchain and the consensus mechanism raise additional issues regarding criminal responsibility. This comes from the fact that the addition of a block to the blockchain results from the acts of many different nodes and that, the behaviour of one only node is not sufficient to modify the blockchain.

486 Private blockchains may however raise different issues, notably because of the fact that certain activities, such as mining, may be limited to certain actors.

more developed way, because of the fact that they are (as their name supposes it) distributed and thus, that any node to the network is provided with an accurate version of the blockchain.[487]

5. Blockchains function without the intervention of any central authority or third party. The functioning of the system is ensured only through the participation of the nodes and through the work of the miners. Thus, the participants to the blockchain only need to have confidence in the system and its protocol: the participants do not need to trust themselves in order to transact or to make sure that the person they plan to transact with is trustworthy. Therefore, a third party or central authority, whose role would be to ensure that the participants are well-intentioned and that the transactions are feasible, is not needed. However, these characteristics correspond in reality to only a subgroup of the Blockchain ecosystem: public blockchains, also known as permissionless blockchains. On the contrary, private blockchains (also known as permissioned blockchains) do not share all of these characteristics. Their functioning in a technological way is similar to the one of public blockchains but there is a considerable difference: a kind of central authority does exist and exercises a certain control. The authority is in charge of deciding who should be given a right to participation to the blockchain. This means that these private blockchains are, contrary to public blockchains, not open to anyone but only to those who got provided with an access right to the system by the authority[488]. The development of private blockchains can be at least partly explained by the inadequacy of public blockchains to tackle the need of regulated activities (such as the activities of the financial sector).

A private blockchain, contrary to a public blockchain, often has a Constitution (or other similar documents) that should have some legal effects[489]. This document which may for instance be a whitepaper and Terms and Conditions in the case of ICOs - should contain classical elements to a contract, including the governing law and jurisdiction[490]. Of course, from a legal perspective, this Constitution or any similar document are private contracts. Criminal jurisdiction is not subject to the individuals' disposition and may therefore not be chosen by the parties to a contract. Thus, it would make no sense to introduce a clause that would provide for the competence of a specific jurisdiction that would be competent over an offence in such a document. However, these documents may provide for some advices regarding the targeted public of the private blockchain.

We should recall the French jurisprudence tackling cybercrime and which considers that to establish competence of the French jurisdictions, it is not sufficient to demonstrate that the website was available in France but it should also be demonstrated that the website was dedicated to the French public. The advices that could help to deduce to which public the website was targeting

487 Private blockchains may also raise different issues, notably because of the fact that reading the blockchain may be limited to certain actors.

488 P. WAELBROECK, *Les enjeux économiques de la blockchain*, in *Annales des Mines - Réalités industrielles,* 2017, p. 10.

489 A. SANITT, I. GRIGG, Norton rose Fulbright, *Legal analysis of the governed blockchain*, 2018, http://www.nortonrosefulbright.com/knowledge/publications/167968/legal-analysis-of-the-governed-blockchain.

490 For instance, the Booking Token Unit's whitepaper specifies that any contract relationship relating to the tokens' protocol are governed by French law, V. CHRIQUI, H. HABABOU, *Whitepaper Booking Token Unit (BTU) Protocol*, 2018, p. 21, https://www.btu-protocol.com/pdf/whitepaper.pdf, also, the Crypto20 Token terms and conditions provides for the applicability of English law as the governing law, Crypto20, Terms and conditions, https://crypto20.com/en/legal/.

include the language of the website or also its content. A similar reasoning could be made regarding private blockchains. Thus, we could argue that the Constitution of a private blockchain targets also a specific public (that may not be limited to a certain country but that may be limited to a certain number of States) such as the Whitepaper of an ICO by selling its tokens to a specific public and by describing the legal statute of blockchains in certain countries[491]. Also, the language of publication of the documents of the blockchain may be taken into consideration[492]. As a consequence, if we stick to the advices distinguished by the French jurisprudence that may be useful in order to deduce the targeted public of a specific website, a similar reasoning could be made with regards to private blockchain: the targeted public may be deduced from the documents to the blockchain and may help to establish jurisdiction.

This targeted public theory, even though it may be useful in the context of private blockchains may be insufficient to establish jurisdiction over offences committed through or facilitated by a public blockchain because these networks are, by nature, open to anyone. If we take the example of the Bitcoin blockchain, we can see that it is used worldwide and it is in no case targeting a special public located in a certain country. Therefore, we understand that the national rules permitting to establish criminal jurisdiction according to the territoriality principle may not be sufficient in order to tackle the phenomenon of criminality facilitated or committed through the use of blockchains or cryptocurrencies – as they were not sufficient to tackle the issue of cybercrime. While private blockchains may give some pieces of advice in order to decide which jurisdiction should be competent, public blockchains do not propose such tools. Thus, the same consequences that we highlighted from the uncertainties about jurisdiction rules regarding cybercrime can be made regarding blockchains: they may result in numerous positive conflicts of jurisdiction. This may weaken the principle of legal certainty and the principles of the rule of law.

6. According to Amartya Sen, the indispensable response to the doubts about globalisation resides in its construction[493]. This supposes that globalisation in terms of criminal matters and more specifically in our case, in terms of territoriality, should be built. In order to do so, it should be accepted that the territoriality of criminal law should be rethought because of its inability to fit with the globalisation permitted by technology.

491 For instance, the 'Legal' part of the MaxiMine whitepaper describes the legal status of blockchains, cryptocurrencies and ICO tokens for certain jurisdictions (China, United States, European Union, Australia and Singapore), *Maximine Whitepaper*, p. 37 ss, https://maximine.io/whitepaper/whitepaper_en.pdf; the Booking token Unit whitepaper's section on disclaimer provides for some legal information regarding the statute of cryptocurrency and ICO tokens according to European and French laws. It also submits the purchaser of the tokens to some obligations of French law, including some obligations whose breach is to be considered a criminal offence according to French law, V. CHRIQUI, H. HABABOU, *Whitepaper Booking Token Unit (BTU) Protocol*, cit., p. 21. See also, for example The Tokes platform whitepaper launching tokens related to the Cannabis industry limits the selling of tokens to jurisdictions where a legal cannabis industry exists and, it only provides for exchange of the tokens in exchange of cryptocurrency or U.S. Dollars, Tokes Platform, Whitepaper version 3.1, 2018, p. 27, https://tokesplatform.org/TokesPlatform_WhitePaper.pdf, which provides that « Tokes may not be resold to purchasers who are citizens or permanent resident of China, Singapore, New York or any other jurisdiction where the purchase of Tokes may be in violation of applicable laws (including but not limited to laws regulating controlled substances, such as cannabis) »

492 For instance, the MaxiMine Whitepaper has been published in several languages, including English and Chinese, *Maximine Whitepaper*, cit.

493 A. SEN, *Dix vérités sur la mondialisation*, in *Le Monde,* 2001, p. 1.

II.4

Seen the insufficiency of the regional response provided for by the Council of Europe Convention and its rules on jurisdiction, conscious of the difficulties faced by national jurisdiction rules, and above all conscious of the necessity for States to coordinate in order to prevent numerous positive conflicts of jurisdiction, scholars kept on looking for alternatives to territoriality. Some of the proposals made by scholars in order to develop jurisdiction rules that would better fit the cyberspace than the territoriality principle currently does will be reviewed in this paragraph. Most of those have been only made with regard to cybercrime and as a result, authors were not aware of the issues raised by blockchains (especially because most of the opinions were made before the quick and recent development of blockchains). While it is not the aim of this article to provide for a unique solution in order to tackle the issue of jurisdiction on blockchains, we will review some of the solutions proposed by scholars and see whether they might be applicable and desirable for the Blockchain environment.

One proposal would suppose that, even though the new challenges brought by the global character of the Internet cannot be denied, it is unlikely that it will lead to special jurisdictional rules if the Internet could adapt itself in order to impose fictional territorial borders within the cyberspace[494]. Thus, traditional jurisdiction rules based on territoriality may be adequate and sufficient to solve jurisdictional issues[495]. In the context of blockchains, we distinguished a beginning of such a development for private blockchains in the third section of the article when we analysed the possibility to apply the targeted public theory to private blockchains in order to establish jurisdiction. However, this may be more difficult when dealing with public blockchains which are by nature globally open and not subject to any restrictions that could be applied by any authority or third party.

In the context of jurisdiction in Internet disputes, a proposal was made in order to consider the cyberspace as a separate international space (such as it is the case for the high seas, the international space or the Antartica). According to this proposal, jurisdiction should be based on the nationality principle irrespective of the geographic location as it is already the case for the other international spaces, mentioned above[496]. This may be hardly manageable regarding blockchains, especially because it may be difficult to determine which person committed the offence. We should recall that a blockchain is by nature distributed. Since the approval of an additional transaction on a blockchain results from the actions of many actors, it may be difficult to isolate one person that would be responsible for an offence. Even if this proposal argued for the so called active nationality principle to establish jurisdiction (which refers to jurisdiction established according to the nationality of the offender), we could make a link between this proposal and the modifications made to the French criminal code in 2016 in order to solve the territorial issue of cybercrime[497] by adding article 113-2-1 according to which any crime realised by means of an electronic communication network which is committed against a person living in France, is to be considered as committed

494 T. SOLLEY, *The problem and the solution: using the Internet to resolve Internet copyright disputes*, cit., p. 834.
495 S. NILOUFER, *The proper basis for exercising jurisdiction in internet disputes: strengthening state boundaries or moving towards unification?*, cit., p. 17 ss.
496 Proposal made in D. C. MENTHE, *Jurisdiction in cyberspace: a theory of international spaces*, cit.
497 Loi no. 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, JORF n°0129, 4 June 2016, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032627231&categorieLien=id.

within the territory of France. So, even if the offence had been committed somewhere else, if the victim is located in France, the offence should be considered as having been committed in France and thus, the French jurisdictions should be competent. This competence echoes the passive nationality principle (according to which a State may have jurisdiction over offences committed abroad when the victims are its nationals). This modification to the criminal code has been admitted by the French Council of State which considers that it responds to the Government's objective to secure and legally reinforce the proceedings in terms of cybercrime[498].

With regard to blockchains, if this passive nationality theory enables to overcome the difficulties that reside in the determination of the place of commission of the offence that are faced with active nationality theory, it may not solve all of the difficulties. As we already saw, the distributed character of the blockchains supposes that the effects of an offence, and the victim may be located in any jurisdiction where the blockchain is available.

Some scholars pleaded for a unification of national jurisdiction rules[499] that would consist in the introduction of a transnational criminal law, specific to the era of Internet[500]. In this respect, it is argued that the cyberspace should be considered a sovereign jurisdiction[501]. In this case, it would be necessary to take into consideration the characteristics of the cyberspace, especially the transnationality of the offences[502], in order to establish new rules that would correspond better to the global character of the Internet. In other areas of law, amongst other regarding Internet dispute resolution, some share this view and call for a Convention on Internet jurisdiction, which should be an effective strategy for ensuring legal certainty[503], predictability and enforceability. However, even though a common approach may be beneficial, it may not happen because of States' reluctance to do so and to abandon their sovereignty and jurisdictional claim over the Internet[504]. This reluctance has been highlighted in the area of copyrights law on the Internet[505] and it is even more important in the area of criminal law given the nature of the area and the sovereignty principle to which States are strongly attached.

498 Conseil d'Etat, *Avis sur un projet de loi renforçant la lutte contre le crime organisé et son financement*, l'efficacité et les garanties de la procédure pénale, N° 391004, 28 January 2016, http://www.conseil-etat.fr/content/download/54700/484379/version/1/file/391004%20EXTRAIT%20AG%20AVIS.pdf.

499 A. HUET, *Droit pénal international et internet*, Travaux du centre de recherche sur le droit des marchés et des investissements internationaux (eds.), *Souveraineté étatique et marchés internationaux à la fin du 20e siècle, Mélanges en l'honneur de Philippe Kahn*, Paris, 2000, p. 675 ss; L. XIAOBING, Q. YONGFENF, *Research on criminal jurisdiction of computer cybercrime*, in *Procedia Comput. Sci.*, 2018, p. 795; S. NILOUFER, *The proper basis for exercising jurisdiction in internet disputes: strengthening state boundaries or moving towards unification?*, cit., p. 2.

500 See for example A. HUET, *Droit pénal international et internet*, Travaux du centre de recherche sur le droit des marchés et des investissements internationaux (eds.), cit., p. 675 ss.

501 S. P. BEATTY, *Litigation in cyberspace: the current and future state of Internet jurisdiction*, cit., p. 139.

502 C. MEIER, *Vers un système judiciaire mieux adapté à la cybercriminalité*, p. 6, http://www.lecreis.org/colloques%20creis/2001/is01_actes_colloque/meier.htm.

503 S. NILOUFER, *The proper basis for exercising jurisdiction in internet disputes: strengthening state boundaries or moving towards unification?*, cit., p. 19; R. DAVID, *The methods of unification*, in *AJCL*, p. 25, 1968, http://www.imeryurdaneta.com/archivos/clases/art_382__DAVID%20-%20The%20Methods%20of%20Unification.pdf.

504 See for example, J. FRANCILLON, *Cybercriminalité, aspect de droit pénal international*, cit.; D. J. B. SVANTESSON, *Borders on, or border around – The future of the Internet*, in *Alb. L.J. Sci. & Tech.*, 2006, p. 352.

505 T. SOLLEY, *The problem and the solution: using the Internet to resolve Internet copyright disputes*, cit., p. 834.

Other scholars rather argue for a harmonisation of national jurisdiction rules[506]. While unification would consist in a unique set of rules, directly applicable for State parties, harmonisation would focus more on developing more coherence between the different national jurisdiction rules by reducing the differences among them but while respecting their particularities. This may constitute a more reasonable solution because it would be more respectful of national sovereignty and States may therefore be less reluctant to such a proposal.

7. In criminal matters, the territoriality principle is used in order to determine that a State has jurisdiction over offences committed on its territory. The territoriality is strongly linked to the principle of national sovereignty which supposes that no State should interfere with the competence of another for offences committed on its territory. According to the ubiquity theory, the territorial principle is extended and it enables a State to prosecute any offence whose, at least, one of its constituent elements is located on its territory – including the effects of such an offence.

However, territoriality was challenged by the development of the Internet and by the phenomenon of cybercrime which accompanied it. Because of the multiplicity of its actors and because of the fact that the Internet makes content available simultaneously at an international level, it seems difficult to determine on which territory a cybercrime has been committed – either through the use of the subjective or objective territoriality principle and national jurisdiction rules that follow those principles. At the regional level, the Council of Europe published a Convention, providing for basic jurisdiction rules based on territoriality. Even if the Convention was a progress because of its regional character, it did not solve the issue of positive conflicts of jurisdiction and let State parties discuss among them in order to choose the most adequate jurisdiction when more than one has jurisdiction over an offence.

We saw that the development of blockchains and of the criminality that accompanies it raise similar questions to those that accompanied the development of the Internet. To determine which jurisdiction is competent over an offence committed through or facilitated by the use of a blockchain may be particularly difficult for public blockchains because of the multiplicity and global character of its actors but also because of the joint control the nodes exercise over the blockchain. This may be less complicated for private blockchains where the applicability of the jurisprudence focusing on the targeted public that had been developed to tackle cybercrime, could be envisaged. However, a global response in order to determine with certainty a competent jurisdiction is lacking and, since the consequence is constant positive conflicts of jurisdiction, this may endanger the principle of legal certainty and the principles of the rule of law.

Most scholars have different views on what the best option is to tackle the issue of jurisdiction over cybercrime. Some would rely on technology itself to reinstall national borders and keep the territorial principle the way it is. This may be feasible for private blockchains but could be more difficult for public ones. Some would give up jurisdiction based on territoriality and would rely solely on the nationality principle to establish jurisdiction over offences on the cyberspace. This may also involve difficulties because of the multiplicity of the actors and the joint control exercised

506 S. NILOUFER, *The proper basis for exercising jurisdiction in internet disputes: strengthening state boundaries or moving towards unification?*, cit., p. 25; Y. A. TIMOFEEVA, *Worldwide prescriptive jurisdiction in Internet content controversies: a comparative analysis*, in *Conn. J. Int'l L.*, 2005, p. 214.

by nodes over the system. Some others argued for unification or harmonisation of national rules of jurisdiction even though States may be reluctant to such proposals.

So far, we should stress the inadequacy of national jurisdiction rules to tackle the issue of criminality on blockchains and the need to rethink the territoriality principle. The response should be discussed at a global level in order to prevent positive conflicts of jurisdiction and thus, reinforce legal certainty and the principles of the rule of law. However, the form of this response should still be discussed and thought about.

LOREN JOLLY