Workshop 7 June 2018 on Taxation and fight against Money Laundering: Crypto Currencies, Digitalisation and the European Semester

Additional answers in writing on cryptocurrencies

Prof.dr. R. Houben and A. Snyers

Replies to the outstanding questions of Neena Gil

1. Can we learn from national legislation, like that of Malta? Should the EU follow the Chinese example?

Our research focused on the existing and upcoming EU legal framework, leaving domestic regulations of Member States and third countries out of scope. This does not mean that existing domestic frameworks cannot be an inspiration for further progress on the EU regulatory level, on the contrary. A good approach relating to future legislation at EU level would include mapping existing domestic frameworks and analyzing what could work for the EU. This would be a research of its own, additional to that of ours.

You specifically referred to Malta. Malta positions itself as a leader in distributed ledger technology regulation. A recent consultation document on the establishment of a Malta Digital Innovation Authority, a Framework for the Certification of Distributed Ledger Technology Platforms and Related Service Providers, and a Virtual Currency Act makes this more concrete[1]. The consultation was recently closed on 9 March 2018, but the results have yet to be made public. It will be interesting to follow-up on this and assess the future framework for potential inspiration of future EU legislation.

Malta is not alone in its efforts. Also in the U.S. e.g. there are known examples of existing frameworks, such as the New York State Virtual Currency Business Activity license, which are worth exploring[2].

Contrary to the Malta and New York approach, which implies regulating crypto activity, China recently introduced a ban on cryptocurrency exchanges[3]. Our opinion is that this is not the example to follow. We advocate more punctual legislation along

[1] https://meae.gov.mt/en/Public_Consultations/OPM/Documents/PS%20FSDEI%20-%20DLT%20Regulation%20Document%20OUTPUT.PDF.

[2] https://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf

[3] https://www.investopedia.com/news/bitcoin-banned-china/; https://www.businessinsider.nl/china-eliminates-all-cryptocurrency-trading-2018-2/?international=true&r=US&_sm_au_=iVV6bs5Z45DMRVfr; https://cointelegraph.com/news/ban-complete-china-blocks-foreign-crypto-exchanges-to-counter-financial-risks; http://www.scmp.com/news/china/economy/article/2132119/beijing-bans-bitcoin-when-did-it-all-go-wrong-cryptocurrencies.

the lines of the current EU approach. This means addressing illicit use cases via money laundering and terrorist financing legislation. Over time introducing license requirements is a good option, as advocated by the EBA. Bans should be limited and focused, as elaborated in our research. We gave in our research the example of technology completely anonymizing cryptocurrency transactions, making them impossible to trace. This is especially relevant for large transactions moving value illegally.

The China approach towards crypto exchanges stands in contrast with its approach towards blockchain[4]. The Chinese IT ministry produced a report revealing that China's domestic industry would thrive on blockchain integration. An example of the use of blockchain for the Chinese good is the use of blockchain against tax fraud in the context of the partnership between Tencent and the Shenzhen national taxation bureau.

Our assessment here is that this in line with our suggested approach: whatever stance you may have on cryptocurrencies, it is important to distinguish the technology underlying it (for many coins this is blockchain technology) from the coin itself and to acknowledge the many legitimate use cases of this technology throughout society. Therefore, we suggested in our research to leave blockchain be from a money laundering, terrorist financing and tax evasion perspective and to focus on the illicit use cases of cryptocurrencies.

2. **Blockchain is about the efficient use of data, but how does one make sure it is compliant with the General Data Protection Regulation (GDPR)?**

The application of GDPR to blockchain technology is a very relevant question, yet outside the scope of our research, which focuses on the use of cryptocurrencies and blockchain for financial crime, money laundering and tax evasion.

Nevertheless, we would like to bring to your attention existing research on how GDPR relates to blockchain. Michèle Finck of the Max Planck Institute for Innovation and Competition wrote a research paper on Blockchains and Data Protection in the European Union[5]. In this paper she examines data protection on blockchains and other forms of distributed ledger technology. She analyzes that transactional data stored on a blockchain and public keys constitute personal data for the purposes of the GDPR. She suggests that in interpreting the GDPR with respect to blockchains, fundamental rights protection and the promotion of innovation must be reconciled. This is even more so, she advocates, given that, where designed appropriately, distributed ledgers have the potential to further the GDPR's objective of data sovereignty. We invite you to read this very interesting research paper.

[4] https://bitrazzi.com/blockchain-against-tax-fraud-as-tencent-partners-up-with-shenzhen-national-taxation-bureau/; https://www.coindesk.com/tencent-partners-with-city-authority-to-combat-tax-evasion-with-blockchain/.
[5] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3080322.

Furthermore, we also invite you to take note of some following (opinion) articles on GDPR and blockchain, which further elaborate the many challenges GDPR confronts blockchain technology with[6]. *Inter alia* interesting is the observation that the GDPR was first proposed by the European Commission in 2012, with an initial focus on cloud services and social networks, at a time when blockchain was not yet a known word. The suggestion is that therefore the GDPR's rationale is already outdated because of the rise of blockchain[7].

Replies to the outstanding questions of Louis Michel

1. Blockchain & digital ransom(ware)

Apart from commissioner King's remarks made at the Europol/Interpol Cybercrime conference in 2017 in The Hague[8], we are not aware of any concrete initiatives by the Commission in collaboration with Europol and Interpol to address digital ransomware.

Nevertheless, we would like to share a couple of thoughts.

Ransomware is the illegal act of restricting access to computer files until a ransom is paid. 'Hostage takers' apparently favor to be paid in Bitcoin[9], because of the anonymity attached to it. However, Bitcoin is pseudonymous rather than anonymous, as explained in our research. Hence, though difficult, it is not impossible to trace the criminals. Nowadays, there are coins that are completely anonymous. If these would be used for ransomware, the challenge for law enforcement becomes greater. A line of thought is, as suggested in our research, to ban the technology masking identities completely.

It has been suggested that blockchain technology could be an adequate defense mechanism against ransomware[10]. The idea is that through blockchain technology sensitive information can be kept in a decentralized manner instead of centralized (as it is now). Keeping information in a decentralized manner makes it harder to link the information to the person it relates to. It is then also harder to know who to address for the ransom. Moreover, there would be numerous copies of the info, making it extremely difficult for criminals to hold them all to ransom. Another deterring factor

[6] https://www.hlengage.com/_uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf?_sm_au_=iVV6bs5Z45DMRVfr; https://medium.com/wearetheledger/the-blockchain-gdpr-paradox-fc51e663d047; https://www.techzine.nl/blogs/404986/blockchain-en-gdpr-een-moeilijk-huwelijk.html?redirect=1; https://cointelegraph.com/news/gdpr-and-blockchain-is-the-new-eu-data-protection-regulation-a-threat-or-an-incentive.
[7] https://www.techzine.nl/blogs/404986/blockchain-en-gdpr-een-moeilijk-huwelijk.html?redirect=1.
[8] https://ec.europa.eu/commission/commissioners/2014-2019/king/announcements/commissioner-kings-remarks-europol-interpol-cybercrime-conference-2017-hague_en.
[9] See e.g. https://www.technologyreview.com/s/610803/true-scale-of-bitcoin-ransomware-extortion-revealed/.
[10] See e.g. https://medium.com/animal-media/2017s-ransomware-attacks-could-blockchain-technology-have-prevented-them-ed9ca6bf348b.

could be that attacking a decentralized system of information would be easily visible to its participants.

Again this is an example of a legitimate use case of blockchain technology for the greater good.

2. The Investigation of Transactions in Underground Markets (TITANIUM) project?

To our knowledge no deliverables from the TITANIUM project have been made public yet[11].

Nevertheless, we would like to share some thoughts.

We understand that the TITANIUM project will research, develop, and validate novel data-driven techniques and solutions designed to support law enforcement agencies charged with investigating criminal or terrorist activities involving virtual currencies and/or underground markets in the darknet. The expected result of the project is a set of services and forensic tools, which operate within a privacy and data protection environment that is configurable to local legal requirements, and can be used by investigators for *inter alia* analyzing transactions across different virtual currency ledgers.

It is clear that the TITANIUM project is directly relevant for the fight against money laundering, terrorist financing and tax evasion via cryptocurrencies. If successful, it will add to the toolbox of law enforcement agencies tracking down money laundering, terrorist financing and tax evasion via cryptocurrencies. Interesting will be to see whether the new techniques developed are less complex and costly than the once already available to trace criminals using pseudo-anonymous cryptocurrencies. Probably we can only speak of significant progress if the outcome would be that law enforcement agencies would have at their disposal an easy to use and relatively cheap method to trace criminals using cryptocurrencies. It will also be interesting to find out whether the new techniques can be deployed both to pseudo anonymous and fully anonymous coins.

In any event, and without prejudice to the TITANIUM project being extremely relevant and valuable, it is not something we can suffice with. The need for a more structural, regulatory approach remains valid. In this respect, the approach taken in the short term to address money laundering, terrorist financing and tax evasion via cryptocurrencies through AMLD5 is a good one, although we see room for improvement, not in the least as regards registration of users. In the longer term, a

[11] See https://www.titanium-project.eu.

more elaborate and comprehensive framework that also builds-in investor protection, as advocated by the EBA, is probably the best way forward.

It is not a story of the one or the other. Putting in place a performant regulatory framework deterring criminals from using cryptocurrencies for illicit purposes and enhancing the toolbox of law enforcement agencies on the basis of the TITANIUM project go hand in hand: to ensure compliance with the regulatory framework, law enforcement agencies must be able to adequately detect infractions (via the new techniques) and subsequently sanction them.

3. **Should we have official virtual currencies under centralised political control? Would that not be simpler and easier to trace?**

We add the following to the answer we gave at the workshop on 7 June[12].

Government backed cryptocurrencies are a topical issue. The first example is the Petro, a coin linked to the price of oil, issued by Venezuela earlier this year[13]. However, instead of being a flagship, commentators see this coin as a desperate attempt of the Venezuelan government to raise foreign currency supplies[14]. Closer to home, and more noteworthy, Sweden is exploring a state-backed cryptocurrency, the e-krona, in an attempt to further move towards a cashless society. The e-krona is conceived as a digital equivalent to the country's regular currency. The Bank of Canada is experimenting with a peer-to-peer system known as Project Jasper (CADcoin)[15]. In the U.S. the Federal Reserve System has mused the possibility of "Fedcoin" for the U.S.[16] Bank of England governor, Mark Carney, expressed that he is open-minded regarding the prospect of a central bank-issued cryptocurrency, although that would not be something for the near future[17]. A high IMF official sees central bank issued cryptocurrencies as an option for the future[18]. The Bank of International Settlements issued a report in 2017 elaborating on how central bank cryptocurrencies might look like and if they would be useful[19]. Etc.

To date, as far as we know, besides the Venezuelan example which has gone live, government-backed cryptocurrencies are still in the study phase. Hence, it is too early to measure their success; if at all these coins will ever see the light of day.

[12] Along the lines of our answer, see: https://www.forbes.com/sites/billybambrough/2018/04/24/us-fed-paper-central-bank-cryptocurrencies-are-missing-the-point/2/#4debcc49249a.
[13] More in general, commentators warn that government-backed cryptocurrencies could provide means for rogue states e.g. to bypass sanctions.
[14] https://www.raconteur.net/finance/governments-building-cryptocurrencies.
[15] https://www.jpmorgan.com/global/research/cryptocurrency.
[16] *Ibidem*; also see https://www.r3.com/wp-content/uploads/2017/06/fedcoin_central-bank_R3.pdf?_sm_au_=iVV6bs5Z45DMRVfr.
[17] https://news.bitcoin.com/central-bank-issued-cryptocurrency-round-up-imf-boe-hong-kong/.
[18] https://www.imf.org/external/pubs/ft/fandd/2018/06/central-bank-monetary-policy-and-cryptocurrencies/he.pdf.
[19] https://www.bis.org/publ/qtrpdf/r_qt1709f.pdf.

In any event, in making the decision whether or not to issue government-backed cryptocurrencies, governments and central banks will have to consider not only consumer preferences for privacy and possible efficiency gains – in terms of payments, clearing and settlement – but also the risks it may entail for the financial system and the wider economy, as well as any implications for monetary policy[20]. Some of the risks are currently hard to assess[21]. In an elaborate report of March 2018 that was fully dedicated to central bank digital currencies and which is very much worth to read, the Committee on Payments and Market Infrastructures and the Markets Committee of the Bank for International Settlements amongst others makes the observation that any steps towards the possible launch of a central bank cryptocurrency should be subject to careful and thorough consideration[22]. Further research on the possible effects on interest rates, the structure of intermediation, financial stability and financial supervision is warranted, according to the report. The effects on movements in exchange rates and other asset prices remain largely unknown and also deserve further exploration, the report states.

[20] https://www.bis.org/publ/qtrpdf/r_qt1709f.pdf.
[21] *Ibidem*.
[22] https://www.bis.org/cpmi/publ/d174.pdf