appg

ALL-PARTY
Parliamentary
Group on
Blockchain

Evidence Report
APPG BLOCKCHAIN
UK Parliament

DATA GOVERNANCE

Blockchain applications - regulation, policy & strategy

BLOCKCHAIN

2020 DECEMBER

BIG INNOVATION CENTRE

Sponsors of APPG Blockchain

The Group supporters – Big Innovation Centre, British Standards Institution (BSI), Capita, CMS Cameron McKenna Nabarro Olswang, INDUSTRIA, IOTA Foundation, MyNextMatch, and SAP – enable us to raise the ambition of what we can achieve

www.biginnovationcentre.com | info@biginnovationcentre.com | @BigInnovCentre
www.appg-blockchain.org | appg-blockchain@biginnovationcentre.com | @appg_blockchain

Table of Contents

1. APPG Blockchain Evidence Meeting on Data Governance & Regulatory Framework.

1.1. Purpose

The mission of the All-Party Parliamentary Group on Blockchain (APPG Blockchain) is to ensure that industry and society benefit from the full potential of blockchain and other distributed ledger technologies (DLT) making the UK a leader in Blockchain/DLT's innovation and implementation.

This Evidence Report of an APPG Blockchain Evidence Meeting explores the regulatory framework of Blockchain Technology and its Data Governance.

This report provides a summary of the takeaways from the meeting. The Video recording of the session is available on our websites APPG Blockchain *https://www.appg-blockchain.org/* and Big Innovation Centre *https://www.biginnovationcentre.com/*

1.2. Details of the Meeting

- Date, 14th July 2020
- Time, 17:30 – 18:30pm BST
- Location, House of Lords
- Participants, 97 attendees

1.3. Panellists: Evidence Givers, Chair & Secretariat

The meeting was Chaired by APPG Blockchain Chair Martin Docherty-Hughes Member of Parliament.

Parliament has appointed Big Innovation Centre as the Secretariat for the APPG on Blockchain, led by CEO, Professor Birgitte Andersen and Fernando Santiago-Cajaraville as the Rapporteur.

Blockchain industry, Academia and regulators presented their point of view at the meeting. Oral and written pieces of evidence were provided by representatives of the London School of Economics and Political Science (LSE), CMS Cameron Mckenna Nabarro Olswang LLP and Consumer Node. A piece of written evidence was also summited by a representative from the Planck Institute for Innovation and Competition.

Evidence Givers

Dr Enrico Rossi
Fellow
LSE
London School of Economics and Political Science

Muhammad Tanoli
Head of Blockchain R&D
Consumer Node

Charles Kerrigan
Partner
CMS Cameron McKenna Nabarro Olswang LLP

Dr Michèle Finck
Senior Research Fellow Max Planck Institute for Innovation and Competition

Chair

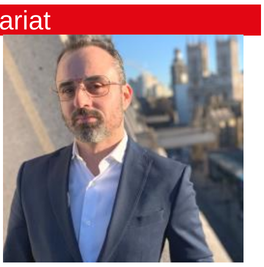
Martin Docherty-Hughes
MP

House of Commons,
UK Parliament

Secretariat

Secretariat:
Professor
Birgitte Andersen
CEO

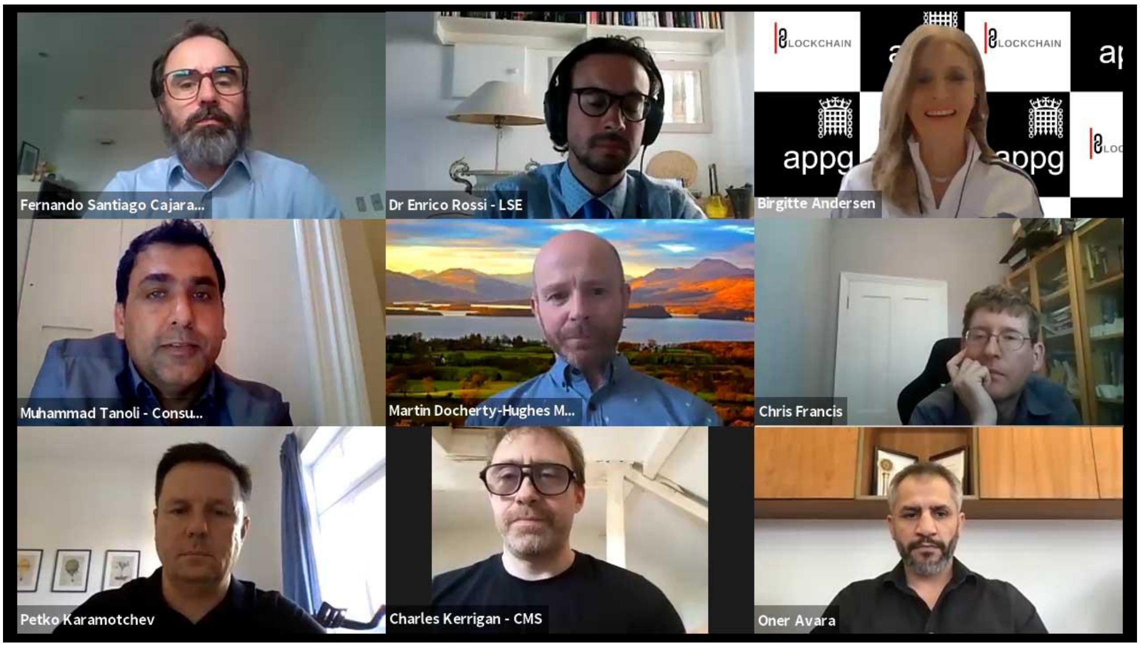
BIG INNOVATION CENTRE



Rapporteur
Fernando
Santiago-Cajaraville
Project Manager,

BIG INNOVATION CENTRE

2. Background



In recent years, Blockchain technology and its fit with the General Data Protection Regulation (GDPR) has been amply discussed as we see more and more Blockchain application in the market. Many discuss the contradiction between the use of Distributed Ledger technology and the current data protection law.

The fifteen APPG on Blockchain evidence meeting aimed to explore the Data Governance on Blockchain networks further. The APPG on Blockchain presented the following questions to the Evidence givers,

Data Governance

- How is data collected and used by Blockchain Networks? Can Blockchain make data collection auditable and transparent? And how can Transparency and Privacy find the right balance?
- Can Blockchain be the definitive tool to protect personal data privacy and security?
- How can Governments and Policymakers regulate Data Ownership on Blockchain networks?

Regulatory Framework

- What challenges do Blockchain networks (Public and Private) raise for Privacy and Data protection under GDPR? Is a new data regulation for Blockchain necessary?
- How can Governments and Policymakers regulate Blockchain networks?

3. Meeting Takeaways

1. Current Regulations do not contemplate Blockchain Technology

There are multiple contradicting points between Distributed Ledger Technology and the current data regulations:

- General Data Protection Regulation (GDPR) is based on the assumptions that there is at least one natural or legal person associated with each data point, and that personal data can be modified or erased.
- While Blockchain is a decentralised tool, GDPR is founded on the principle of centralised data processing.
- GDPR is concerned with limiting access to information. Blockchain is concerned with sharing information.

"Regulatory and Governance problems (to comply with GDPR) of the blockchain are usually linked to the decentralised nature of the blockchain." *(E. Rossi, LSE)*

"The law on data protection did not contemplate blockchain" *(C. Kerrigan, CMS)****.***

"Public Blockchain networks challenge GDPR data minimisation, data limitation, personal data protection and cross border data processing" *(M. Tanoli, Consumer Node)*

Blockchain, as a decentralised technology, replaces a unitary actor with many different players and data cannot be modified or erase in the Blockchains networks. The debate is focused on the data which is typically stored on a distributed ledger and qualifies as personal data, as per the GDPR. The regulators are regularly questioned if the personal data in an encrypted or hashed form still qualifies as personal data. The role of regulators widens in such cases.

"There is an initial role here for regulators and standards bodies perhaps more than legislators." *(C. Kerrigan, CMS).*

"Examining Blockchain technology through the lens of the GDPR highlight significant conceptual uncertainties related to the GDPR, itself*" (M. Finck, Max Planck Institute)*

2. Decentralised data governance models are more transparent than centralised models

Centralised data governance models lack transparency and do not provide individuals with control of their data. Transparency is limited to the front end and is enabled by the privacy terms and conditions in the centralised models.

Current centralised data governance models are mostly organisations collecting data, without the data subject and the knowledge of data user. The user control is thus limited.

"GDPR has not given citizens control of their data" *(C. Kerrigan, CMS)*

Decentralisation models, based on blockchain technology, will enable data subjects to be part of the governance at the collection, storage and aggregation. Decentralisation will enable accountability and user empowerment.

"The decentralised models can enable meaningful transparency by engaging user into the transaction level processing". *(M. Tanoli, Consumer Node)*

3. Blockchain is good on data privacy.

Blockchain technology has the potential to provide individuals with the control of their data. Distributed Ledger Technology has the potential to protect both business interest and users concerns around who has access to the data, where it is stored and how it is used.

Ultimately, Blockchain can provide citizens with the right to "Data Portability."

"Decentralisation will enable, accountability and user empowerment" *(M. Tanoli, Consumer Node)*

"Blockchain is good on privacy. It protects data integrity." *(C. Kerrigan, CMS).*

4. The activities should be regulated, not the technology itself

With the current regulations, the activities in Public or permissionless blockchains (e.g. Bitcoin) seem challenging to regulate. However, the government can regulate the activity around those networks. Indeed, governments can regulate the entries and exits of public Blockchain networks, similar to anti-money laundering regulations, in the part that touches the individual. Typically, this part is concerned with value; however, it could equally apply to data

The regulation focus should be more at the use of technology for a specific use-case, and not the technology itself."
(M. Tanoli, Consumer Node)

"What has to be regulated are the logical layers and their interfaces, not the single elements of a network as stand-alone elements."
(E. Rossi, LSE).

The benefits and goals of Blockchain technology should be taking into consideration at the time of the regulations are put in place. A situation where people start using distributed ledger technology in their areas, and the regulator stop the use because it does not satisfy them should be avoided. For example, the principle of immutability of the records has a great potential to audit transactions; however, it would not allow a data controller to modify or delete the records.

"It's about ensuring the regulator understands and is satisfied by the particular application of blockchain because it is always going to be content-sensitive" *(Chis Francis, SAP)*

4. Evidence Giving

4.1. Dr Michèle Finck, Senior Research Fellow, Max Planck Institute for Innovation and Competition

Blockchains and the General Data Protection Regulation (GDPR)

The relationship between blockchains and the GDPR has been amply discussed in recent years. Indeed, it has frequently been highlighted that there are significant points of tension between the technology and European data protection law. Broadly, it can be maintained that these tensions are due to two overarching factors.

First, the **GDPR** is based on the assumption that **in relation to each personal data point there is at least one natural or legal person** – the data controller – that data subjects can address to enforce their rights under EU data protection law. Blockchains, however, often seek to achieve decentralisation in replacing a unitary actor with many different players. This makes the allocation of responsibility and accountability burdensome, particularly in light of the uncertain contours of the notion of (joint)-controllership, which has been aggravated by the recent case law of the European Court of Justice.

Second, the **GDPR** is based on the assumption that **personal data can be modified or erased** where necessary in order to comply with legal requirements such as the rights to modification or erasure (the “right to be forgotten”). Blockchains, however, render such modifications of data purposefully onerous in order to ensure data integrity and to increase trust in the network. Again, the uncertainties pertaining to this area of data protection law are increased by the existing uncertainty in EU data protection law. For instance, it is presently unclear how the notion of ‘erasure’ in Article 17 GDPR ought to be interpreted, specifically what it requires at a technical level to meet the legal threshold of “erasure”.

These tensions play out in many domains. There is, for instance, an ongoing debate of whether data typically stored on a distributed ledger, such as public keys and transactional data qualify as personal data for the purposes of the GDPR. Specifically, the question is whether personal data that has been encrypted or hashed still qualifies as personal data. Another example of the tension between blockchains and the GDPR relates to the overarching principles of data minimisation and purpose limitation. Whereas the GDPR requires that the personal data that is processed is kept to a minimum and only processed for purposes that have been specified in advance, these principles can be hard to apply to blockchain technologies. Distributed ledgers are append-only databases that continuously grow as new data is added. In addition, such data is replicated on many different computers. Both aspects are problematic from the perspective of the data minimisation principle.

It follows that the very technical specificities and governance design of blockchain use cases can be hard to reconcile with the GDPR, specifically in relation to public and permissionless blockchains.

Therefore, blockchain architects need to be aware of this since the beginning and make sure that they design their respective use cases in a manner that allows compliance with European data protection law. Second, the current lack of legal certainty as to how blockchains can be designed in a manner that is compliant with the regulation is not just due to the specific features of this technology. Rather, examining this technology through the lens of the GDPR also highlight significant conceptual uncertainties related to the GDPR.

4.2. Charles Kerrigan, Partner, CMS Cameron McKenna Nabarro Olswang LLP

This is about trade-offs. Therefore, it is not a good question for a lawyer to answer. The problem with lawyers is we like telling people what the law is. That does not work here.

Existing Law in Data Protection

We have existing law on data protection. We do not yet have directly applicable law on blockchain.

The law on data protection did not contemplate blockchain.

In any questions on what the law is, the answer is all in the GDPR. On any questions of what the law should be, we do not know because we have not thought about it yet.

Everyone notes the inherent tension here. But why is there one?

GDPR is concerned with limiting access to information. Blockchain is concerned with sharing information.

In particular, the best use cases of blockchain are in multiparty transactions, a shared ledger., where everyone can see everyone else’s information.

I would suggest that we do not try to solve the problem by focusing on private blockchains because we will miss some of the greatest potential benefits of the technology.

Blockchain is good on privacy. It protects data integrity.

There is an irony in the problem because Blockchain is a decentralisation tool. GDPR's foundation is centralised data processing. Any attempt to reconcile that will lead to a headache.

That is where we are now. And that is where much of the commentary resides. There are different views on anonymity and pseudonymity and the applicability of data protection and privacy laws. Maybe it is ok because transaction data only references a public blockchain address that is mainly encrypted. Maybe it is not ok because methods still exist to link individuals to the public keys.

More broadly, the technical issues: concern identifying the processor in a distributed system, with cross-border data transfer, with applying jurisdictional rules, with applying criteria for legitimate reasons for the processing, and (famously) for dealing with consent withdrawal on immutable ledgers. That is a long list.

So, I do not think that looking for workarounds for each point is the right approach. In any event at the end of any analysis related to a public blockchain, you can find a breach, but you still do not have anyone to sanction.

It is not all a GDPR problem. Industrial use cases do not need to store personal information. So, some of the concerns are straw man arguments. But I have said that we should still be concerned with the hard problem.

How can Governments and Policymakers regulate Blockchain networks? Well, to start, they cannot regulate them away. Decentralised ledgers are here. They cannot be "un-invented" now.

How can Governments regulate Data Ownership on Blockchain networks? What are they trying to regulate? Governments can regulate the things that they own – that is easy to describe - or control, that is not easy and takes us back to the issues about jurisdictional capacity. They cannot regulate permissionless chains. But we can see in other contexts - such as anti-money laundering - that governments can regulate the entrances and exits… the part that touches the individual. That is normally concerned with value. But it could equally apply to data.

Blockchain and GDPR - do we need a new data regulation for Blockchain? I think we might. But we should also keep in mind the technical capacity to signpost centralised data on-chain while maintaining substantive data off-chain.

GDPR has not really given citizens control of their data. Because there is a low bar to define personal information, there is also a low bar defining informed consent. And cyber-security breaches expose data even where there is true informed consent.

1. Scope out the size of the problem. Do the taxonomy. Public and private blockchains. Ones with personal information and ones without. How much is in each bucket? A properly designed system will tell you if it stores personal information.
2. Move away from theoretical debates about tracing personal information from encrypted keys. That is a long way from information that is brought up by a web search. Someone who can access encrypted data is a government or a professional or a hacker. We need different protections from them than GDPR.
3. Do not ignore the trade-offs. The tax authorities want transactions to be traceable.
4. Keys are a route to the tokenisation of personal information where access control is in the hands of the individual. In an information economy that must be an important topic for policymakers. I am influenced by Dave Birch's work, including the part that identity is the new money. That is true for people. But we should not lose sight of the fact that this has been true in wholesale markets for 200 years since the issue of banknotes that were not backed by gold. The identity of the Bank of England is the old money.
5. Do the grand theory – do we require centralisation, or will we allow decentralisation? If we require centralisation is that realistic in practice? People now have a tool they can use. So, they will. I would say that we need a plan to support decentralisation by being thoughtful about the harms. Who needs protection from what?

But also do the practical bits - do not go round in circles. Do not just make work for lawyers. That is in two areas – both on the setup and on the fall out of systems.

There is an initial role here for regulators and standards bodies perhaps more than legislators.

Both system architecture and standards should be high priority. The Information Commissioners Office work on AI can be read across and extended to blockchain. The British Standards Institution work on smart contracts likewise. The Competition and Markets Authority approach to default settings is relevant here too. I would like to see some work on what positive targets can be set alongside any work we are doing on the regulatory perimeter.

4.3. Dr Enrico Rossi, Fellow, LSE, London School of Economics and Political Science

Dr Enrico Rossi
Fellow, LSE - London School of Economics and Political Science
Dr Enrico Rossi - LSE

The typical governance problems with blockchain (transparency vs privacy or transparency vs security) derive from the very well-known fact that blockchain is a decentralised technology: transparency and replication of data, together with their immutability are a result of the "decentralised nature" of blockchain.

All regulatory problems (such as the ones emerging from the application of the GDPR) and governance problems of the blockchain are usually linked to the decentralised nature of the blockchain.

> ***Regulatory and governance problems (GDPR) of the blockchain are usually linked to the decentralised nature of the blockchain.***

One way to address this problem is to understand that blockchain can be decomposed into two dimensions access vs consensus-validation, also referred to as storage vs manipulation or off-chain vs on-chain problem.

Blockchain Vs GDPR

The paradoxes and problems emerging from the blockchain technology (transparency VS privacy or transparency VS security) are usually just a reinterpretation of these two dimensions of the blockchain. For instance, the GDPR distinguishes between data controllers and data processors: control of data applies to the dimension of data access and data storage. In contrast, data processing usually applies to the dimension of consensus (data validation) happening on-chain.

One usual known way to address the trade-off between privacy (security) and transparency is to decouple the two dimensions of **access/storage** (on the one hand) and **processing/manipulation** (on the other).

It is well-known that one convenient way to deal with the tension between data privacy and transparency, and therefore with the problems emerging from a decentralised environment is to store data off-chain (asymmetric access to personal data), coupled with some encryption or hashing mechanisms so that manipulation on-chain only occurs over metadata (or derived data) at the protocol layer.

There are various solutions to this decoupling of data ownership and control & data manipulation for both dimensions: encryption – avoid identification of users & access & obscure content (ZKP, but also the novel Aztec protocol, and various other solutions). What is important is to understand (and it is usually missed in the literature) that these two dimensions are not independent, but they interact. Decentralisation (and all the issues emerging from it) is about the interaction between these two dimensions.

One way to understand how these two dimensions interact (and therefore, how to interpret decentralisation) is to map them into different logical layers of the technology stack of the digital infrastructure. Potential paradoxes, tensions or problems are usually tackled can be better identified and addressed if these two dimensions of the blockchain are studied as different layers of the technology stack.

Breaking the Paradox

Two examples can be discussed of the importance of the layered stack.

For instance, in the most basic case of a dedicated (protocol-specific), permissionless and open blockchain, there are usually three different logical layers:

1. Infrastructural or transmission layer (data are accessed and exchanged) defines the architectural dimension
2. Protocol or consensus layer (data are validated and manipulated) defines the governance dimension
3. Application or service layer (data are used, exploited, and valued) defines the service dimension

The infrastructural or transmission layer deals with storage and the architecture & distribution of data, while the protocol or consensus layer deals with data manipulation and processing. The problem of data governance then turns out to derive from an analysis of the various layers and their interaction.

These three layers are not independent as the nature of the data stored off-chain (at the infrastructural layer) is not independent from its manipulation on-chain (at the protocol or consensus layer). It is clear that the simple separation of validation through encryption from access and control (storage) of data does not necessarily work. Over a blockchain, the nature, the value and the meaning of data stored, accessed and transacted at both the infrastructural and application layers depend on and is directly affected by, the dynamics at the protocol layer (even though data sovereignty, privacy and control are not violated).

Understanding the decomposition of the two dimensions of blockchain into logical layers becomes even more useful in case of so-called private and permissioned blockchains, which is my second point.

Private & permissioned blockchains are more centralised than public and permissionless. This centralisation in digital networks is usually achieved by adding a further logical layer complementing the protocol layer (in support of it) usually called a platform layer: while data are transacted p2p over the deepest transmission layer, there is an added platform layer that in case of private & permissioned platforms represents the centralised layer. The platform layer ensures aggregation and interoperability (in this sense is centralised), and it usually contains the control points (APIs) to support alternative services and apps. The platform layer also operates as a filter. It represents the logical interface between a centralised back-end (hardware, usually a cloud) and a distributed dashboard at the data layer (consumer interface for functionalities and apps). This platform layers for private & permissioned networks is usually where smart contracts operate.

An interesting aspect is that in this multi-layer configuration, there are usually two different tokens conferred by the platform manager/back-end owner: one token defines the status of the actor (it is an identifier), another token defines some temporary condition. The former remains with the actor and is released by the platform layer. The latter is processed and manipulated by the protocol layer. The two are usually linked, and the latter usually depends on the former.

Takeaways,

In order to understand data governance over a blockchain (but any digital network), it is important to reframe the dual nature of the problem (framed in terms of control/processing but also off-chain/on-chain or privacy/transparency) as a problem occurring across logical layers of a technology stack.

The problem that must be understood is how different layers influence each other. Different tokens are linked to (and acquire meanings from) the logical layer they belong to, and the nature and meaning of data depend on the way in which the different layers inter-operate. As a result,

What has to be regulated are the logical layers and their interfaces, not the single elements of a network as stand-alone elements.

4.4. Muhammad Tanoli, Head of Blockchain R&D, Consumer Node

The focus is about blockchain and smart contract-based data governance to achieve the objective of GDPR. Decentralised model based on blockchain will enable data subjects to be part of governance at the collection, storage, aggregation and processing. Decentralisation will enable, accountability and user empowerment

Generally, the Blockchain technology is often confused with the use case such as bitcoin and Ethereum.

The regulation focus should be more at the use of technology for a specific use-case, and not the technology itself.

In a business to business data sharing, data governance on blockchain involve the data controller, data processor and data subject. The role and responsibilities are clearly defined in the business network. Whereas in public network use cases of blockchain technology, the controller definition and the data processor definition are often mixed up. Data governance in the business context is more between the business partner "collaborative environment".

Public network challenge GDPR data minimisation, data limitation, personal data protection, and cross border data processing. In Public network user of the network can be a controller as well as the processor. A node which sends and receive money is a controller and a node that process the blockchain is a processor.

The regulation adoption will be more at the use-case level, not technology level.

The centralised models are organisation centric and only benefit organisations. A centralised model often collects user data without including the data subject. Data broker collects data from a different source without our knowledge and often face fines and penalties. Smart apps collect our data, so do the third party's libraries which are part of the smart apps. The transparency is only on front end enabled by the privacy terms and conditions in the centralised models.

Decentralised data governance will be more transparent than centralised models.

The decentralised model can enable meaningful transparency by engaging the user into transaction-level processing.

Current centralised governance model has a lack of transparency. They exclude data subject from the process of data sharing, data processing

As a result of this, we can see fines in the EU and the UK due to lack of consent, lack of transparency, illegitimate processing data breach notification, security breaches. The most significant fine in the UK is BA and the Marriott as they could not address the security and privacy issues in the centralised model.

Distributed ledger technology and smart contract can be adopted for the decentralised governance which will protect both the business interest and the user concerns around who has access to my data, where it is stored and how it is used. GDPR will unlock innovation by enabling legitimate data sharing through rights over data approach. The right to data portability has been studied in the UK and across the world for the past two years. Smart data is one of initiative in the UK.

Blockchain and smart contract can be adopted for decentralised portability cross-sector, cross border, which can result in addressing the issue of loyalty penalty.

To enable meaningful transparency, accountability, and user empowerment distributed ledger technology can play an important role where the subject can be part of the governance of personal data under GDPR.

5. Contact details

APPG Blockchain Secretariat

Big Innovation Centre
62 Wilson Street
London EC2A 2BU
United Kingdom

info@biginnovationcentre.com
www.biginnovationcentre.com

www.biginnovationcentre.com