# Regulatory, Legal Trends In The Blockchain Space For 2020

By **Jonathan Emmanuel** (January 6, 2020)

The last couple of years have been awash with blockchain implementation projects. Many have not been successful because organizations have not focused on the problem that needs to be solved (i.e. the use case) and how blockchain (rather than other technologies, including those based on central databases) can help solve that problem.

The beauty of making mistakes is the lessons that can be learned. Following the completion of blockchain research and development programs and pilots (some unsuccessful), organizations have begun to understand the specific benefits of particular blockchain networks and the use cases they can be appropriately deployed towards. For many organizations, the future of blockchain is private or permissioned blockchain networks (where there is more control over who can join the network and read/write data to it), focusing on very specific uses cases: better data transparency and exchange, what some people have coined the "internet of record."
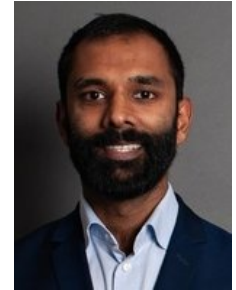
Jonathan Emmanuel

For example, Her Majesty's Land Registry, a department of the U.K. government, has trialled the use of blockchain technologies to help streamline the process of exchanging and recording data during the course of buying and selling a property. In this scenario there are several participants (the buyer, the seller, their lawyers, the lender, the surveyor, the estate agent, etc.) all sending data in different formats (email, fax, post) and at different times and storing the data in siloed databases.

As a result, it can be very difficult to quickly get transparency on what is happening at each stage of the property transaction process. HMLR partnered with blockchain software company R3 LLC to use its technology to help streamline the process.

A private blockchain network was established that acted as a work flow management engine which logged all the transactions recorded by participants (e.g., offer letter, acceptance of offer letter, lender's mortgage approval). It could be interrogated by the participants so everyone had visibility, in real time, of what stage of the property transaction they were in. This helped streamline the process which saved time and costs.

In the above example, there is always the debate over why the participants are using a decentralized rather than centralized database. Some reasons to use a decentralized database include:

- Trust: The participants prefer to trust the blockchain protocol to record transactions to the blockchain and ensure that once recorded the transactions cannot be changed over a centralized authority, where bad actors may be able to tamper with the data.

- No one wants to be the central authority: this is because it takes a lot of time and effort to manage the central database and ensure that transactions are validated and recorded.

- Cyberattacks: If the data is decentralized there is no one honey pot of data that can be hacked; instead, the data is decentralized amongst the nodes of the network: if one node loses its copy of the database then there are other nodes that can be ready to share their copy

We're Only Getting Started

More granular use cases will become more common, but we are only beginning to scratch the surface in terms of what blockchain technologies can achieve. It is great to have private blockchain networks spun up to solve particular problems, but they only allow for participants of that network to send transactions and view the blockchain. What if different private or public blockchain networks could communicate (e.g., share data) with each other to help solve more complex problems?

Blockchain software company Parity Technologies has been considering this challenge. Its aim, at a high level, is to create a software toolkit that makes it easier for users to build their own blockchain networks. The use of that toolkit — called Substrate — can ensure that blockchains built using it share common, underlying characteristics that make it easier for them to communicate with other public and private blockchain networks through the use of an interoperability protocol like the Web 3 Foundation's Polkadot, if desired.

During a Gold Rush, Sell Shovels

In 2020, we expect to see a greater increase in the number of organizations providing services to the blockchain ecosystem. These organizations may provide part of their services on-chain and part of their services off-chain. For example, organizations that help blockchain organizations complete know your customer/anti-money laundering checks on participants in their network. We expect this to be a high growth area in Europe in light of the fifth Anti-Money Laundering Directive, which comes into force in 2020 and requires crypto exchanges to perform customer due diligence on any customers they onboard.

Another example is organizations that provide applications that enable their clients to record hashes of input data on a blockchain. This service is useful because it provides third party proof that the input data existed at a point of time (i.e. when its hash was recorded on the blockchain). This might be helpful to provide proof of existence of time sensitive information like CCTV images or proof of attendance (e.g., audit visit).

Challenges Ahead

When considering the legal issues, it is important to differentiate between public and private blockchain networks. Public blockchain networks have no central authority in charge, and there are limited terms and conditions in place governing each participant's access and use of the network. For these reasons, most organizations will steer clear of them in favor of private blockchain networks.

Contracts

For private blockchain networks, it is important to understand the structure of the network and each stakeholder's role, otherwise stakeholders risk participating in projects without understanding their rights and obligations. To do this, stakeholders need to carefully consider the types of contracts they need to enter into and the terms that are appropriate to them. For example:

- Who has developed the blockchain software (e.g., has it been licensed from a third party like R3 (blockchain developer) or has it been developed in-house)?

- Who is in charge of launching and operating the network ("blockchain operator")? Is the blockchain operator one entity or a consortium?

- If the blockchain operator is relying on software and services provided by a blockchain developer, are there appropriate terms in place between the blockchain operator and blockchain developer?

- Is there a participation agreement in place between participants and the blockchain operator governing each participant's rights to access and use the blockchain network? If the blockchain operator is subcontracting certain services to the blockchain developer, has it backed off any commitments it gives to participants to the blockchain developer?

General Data Protection Regulation

There is a well-known tension between the European General Data Protection Regulation and blockchain technologies. The GDPR does not regulate technologies per se but regulates how actors use technologies in a context in which personal data is involved (e.g., where the blockchain records personal data).

The GDPR covers concepts such as the right to be forgotten and the requirement to delete data when it is no longer being used for the purposes for which it was initially collected. These requirements create tension with blockchain technologies because once personal data has been recorded on a blockchain it is not possible to unilaterally delete or remove such data from the blockchain.

This leads to a situation in which the law and technology are in conflict with no regulation in place to determine how that conflict might be resolved. In addition, where multiple participants are interacting with the blockchain, often in different jurisdictions, and where personal data is being processed, it will be important to establish the proper mechanism under the GDPR to allow for international data transfers (whether by standard contractual clauses or otherwise).

Regulation is starting to play catch up, but slowly. Currently, only one data protection authority (the French Data Protection Authority, CNIL) has issued guidance on blockchain technologies. In connection with the right to be forgotten conundrum, there is a recognition that it may not be possible to comply with this requirement, but it may be possible to mitigate its impact.

For example, participants could apply cryptographic hash functions to the personal data to make the underlying personal data practically inaccessible. However, participants should be aware that hashing operates on a spectrum and the use of more advanced hash functions to

ensure stronger privacy guarantees to make it harder to identify the encrypted personal data is recommended. For example, adding a random and secret bit of data to the personal data before applying the cryptographic hash function leads to a more secure hash which is more difficult to reverse engineer.

2020 and Beyond

Organizations are more aware of the pros and cons of blockchain technologies, and the expectation is that more granular and focused blockchain deployments will start to take place in 2020 and beyond. Regulation is still lagging behind technology, but it is starting to catch up. It is uncertain at this stage whether new regulation will help or hinder blockchain adoption.

Blockchain technologies have been compared to electricity. Electricity has many potential use cases (e.g., light up a room or boil a kettle) and provides the underlying infrastructure that is back-end and not customer-facing but is vital to many things we take for granted. In the future, many new organizations will be developing new applications to solve use cases that rely in whole or in part on the blockchain back-end, but we may not even know about it!

Jonathan Emmanuel is a partner at Bird & Bird LLP.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.