Blackaby Blockchain Executive Summary

- Types of Blockchain

There is no ONE type of blockchain. It is not a static "thing". It is a tool, and we need to be careful to talk about it in terms of its application, rather than blockchain as a static entity. Blockchains can utilize both centralized and decentralized ledgers, be public or private, permissioned or open, using various methods of deriving consensus. They may have integrated smart contracts, call outs to oracles or other third party information or arbitral sources. They can do many things. We should refrain from concentrating on what they are, and look more at what they can do, and what we are and will be doing with them.

To say that fitting blockchain into law is like fitting a square peg into a round hole is more than a bit disingenuous. It's more like trying to coat an electrified barbed wire fence with melted marshmallows. Messy, incomplete, sometimes painful, and to a lawyer, doesn't often smell right. Just how the fence-makers designed it. But don't think of blockchain as illegal. Think of it as A-legal. As in built without respect to the legal context. And the legal context is going to have to adjust.

Why do I say this? Let's start with one of the foundational descriptive aspects of law, one of the first concepts we teach about how to do legal research – JURISDICTION- the who, what, where, and how of the law—in other words, which law applies. Again I would point to the use that it's being put to as your first clue.

In terms of blockchain, who is the who? Who owns a blockchain? – The what of it- especially in the case of a decentralized ledger- makes this difficult. It is designed to live everywhere and nowhere, so imputing ownership is almost impossible. It's not cloud storage in the traditional sense where Google or Facebook have made click through innumerable pages saying that you own nothing and they own everything. It sits on no one computer or server, but several, all at once, all reaffirming with every transaction. When we normally look at international issues like this, we can fall back on physical jurisdiction. Where is the server? So where exactly is it? All of the answers to those types of questions are increasingly circumstantial, and not really widely applicable.

- Autonomy

Then there's the issue of AUTONOMY and smart contracts. What do I mean by autonomy in this case? Who is autonomous? First, I have to understand that to a lawyer, the term smart contracts is somewhat…incomplete The idea of smart contracts is that by coding a transaction process into a blockchain, you can transfer the legal process into an automated self-functioning event – one that even references outside oracles or third parties –much akin to the contract you make with a vending machine when it finally takes your rumpled up dollar bills—that implied contract that it's supposed to give you a Coke. For every contract there are multiple parties and multiple actions. In a smart contract, some people would see these as ceding agency to the vending machine. But can you get rid of liability and responsibility so easily? And how do you transfer these concepts into code and into the blockchain? You might see this referred to as "recourse mechanism". If the blockchain is immutable, how do I take things back? The APPEND rather than DELETE nature of blockchain makes this difficult.

Thing is, there's a lot of things that go into a contract that blockchain just isn't equipped to handle YET, given that a contract is more than just a tool. Think of the contract that most people have – their lease. You and your landlord both have certain rights under a lease, but the lease itself, and you as the lessor or lessee have flexibility. Your landlord can give you a break on the rent if you're having a hard week. You can do some DIY in case you don't feel like calling the landlord to fix your sink. The bank can choose not to foreclose on your delinquent mortgage. The more you automate these processes, the more difficult it is to implement these flexibilities at the margins. I'm not saying blockchain won't be able to do this – both the law and computer coding are flexible enough to do it. I'm saying that we're not there YET.

- Finance

The third legal concern I have on this slide is BANKS. Banks have begun to use blockchain. The Australian Securities Exchange is using it for post-trade clearing and settlement (basically after the dust settles on a trade, making sure all the money owed gets to the right parties and from the right accounts), and others have started using it for payment systems, trade finance, identity verification, and for syndicated loans (imaging your mortgage or packaged into a fork of a blockchain.) Financial options are complicated, as our financial crisis of 2008 demonstrated, and blockchain, especially its nature of appending data rather than overwriting it, lends itself to being an auditable trail of activity and trades. Financial derivatives such as put options can be integrated into via a smart contract – essentially locking in one's financial decisions – but currently such things are not transparent. I currently have to read the market to determine someone's position on a stock. With an open blockchain record of transactions – that changes the playing field.

Blockchain can also function, as we've seen with Bitcoin, as a payment and remittance system, one that currently has no geographic limitations or boundaries. Several banks both in the US and elsewhere are experimenting with payment systems such as those designed by Ripple Labs.

The question with the application to banks is does blockchain meet current banking standards and laws, standards and laws which have multiple layers (and lawyers) involved – there are local, state, international and transnational banking laws and regulations – so either the banking laws are going to have adjust to the blockchain or the use of blockchain is going to have to fit into the regulations. This has been done before – Remember the era before debit cards? Changes in tech are not new.

What might be most challenging for banks is blockchain's use as currency – such as Bitcoin, Zcash, Monero, or any other kind of store of value—how do you value it. If you've paid any attention to the price of Bitcoin over the last year, you'll note that it's not known for its stability. So how do cryptocurrencies or value stored in a blockchain feature on a balance sheet? As the result of our last financial crisis, investment banks such as Goldman Sachs or JP Morgan Chase have to have meet certain capitalization requirements – so just as they had trouble valuing the credit default swaps on their books in 2008, they are going to have to determine how to evaluate blockchain based holdings.

- GDPR

And then there's the GDPR – the European General Data Protection Regulation that kicked in just a few weeks ago, resulting in our inboxes being filled with notifications that privacy policies have changed, and made every website you visit tell you about cookies. The GDPR has very specific requirements of data providers in reference to data users – with a blockchain, it's not clear how that's going to shake out. How do you impose the "right to be forgotten" onto something that is ostensibly immutable? From the opposite end of the regulatory spectrum, there are AML – anti-money laundering laws – that mandate that data providers adhere to concepts called KYC and CDD – Know Your Client and Customer Due Diligence- that run counter to both the GDPR and the anonymizing nature of a decentralized ledger.

Blockchain can be both data storage and a store of value or traded as a security or record of transactions– so is it content or provider, given the decentralized ledger? Let's think of it akin to a copyright issue and digital rights management. When someone is thought to have violated someone's copyright, they are sent a takedown notice by the copyright holder – but think back to my first concern, JURISDICTION – who are we sending the notice to? The blockchain itself? Are we forcing a fork into the chain to deal with it? How do we assign responsibility for the contents of the blockchain? Some of you may have heard concerns about the discovery of pornographic image data in the Bitcoin blockchain – but don't worry, if you own Bitcoin, people aren't going to accuse you of having porn on your computer. Thing is, you kind of do. The law just doesn't know what to do with that. YET.

These are all issues that the law must and will deal with. The blockchain is a tool, and not a panacea, and it should not be as one author on the Verge website called it, a 'belief system'. As I said before, it may be messy and painful, and far from perfect. But the law will and can adjust. If you want a great overview of just where things stand and the issues people have identified, check out Primavera De Felippi and Aaron Wright's new book, Blockchain and the Law. I've only hinted at some of the issues, they take a deep dive.