benchtv
a benchmark production

Précis Paper

Blockchain and Cryptocurrency

An in-depth discussion of Blockchain technology and cryptocurrencies in a legal and technological sense.

Discussion Includes

- **What is Blockchain?**
- **What is the difference between a "public Blockchain" and a "private Blockchain"?**
- **How does a transaction flow through a Blockchain system?**
- **How do the blocks in a blockchain hold together?**
- **The difference between Blockchain technology and cryptocurrencies**
- **The elements of the blockchain ecosystem in greater detail**
- **Smart contracts – an overview**
- **Tokens**
- **Cases study: smart contracts and Blockchain deployments in the mortgage industry**
- **The legal validity of smart contracts**
- **Advice to lawyers looking to learn more about Blockchain**

Précis Paper

Blockchain and Cryptocurrency

1. **In this edition of BenchTV, Michael Bacina (Partner – Piper Alderman, Sydney) and Darren Younger (Non-Executive Director – Lakeba Group) provide an in-depth discussion of Blockchain technology and cryptocurrencies in a legal and technological sense.**

What is Blockchain?

2. **Essentially, Blockchain is akin to having data store in a cloud that cannot be changed. It is essentially a ledger that is distributed so it cannot be hacked into and altered, and if one wanted to make any changes to it, those changes would also need to be made to the many distributed nodes connected to it. An analogy may be drawn to taking an accounting ledger, splitting it up, and spreading it all around the world, and using cryptography to link all the pieces together.**

3. **A problem currently faced by Blockchain technology is the difficulty in defining it. Definitions of various parts of the technology have been approached in different ways. The Merriam-Webster Dictionary defines Blockchain as "a digital database containing information that can be simultaneously used and shared within a large, decentralised, publicly accessible network, and also the technology used to create such a database". From the perspective of those working inside the Blockchain industry, however, while the second part of this definition is very true, the first part of it is only true to a limited extent. This is because it describes what is known as a "public Blockchain".**

4. **Blockchain is the technology underpinning cryptocurrency and Bitcoin, and is poised to change much of the way in which lawyers practice.**

What is the difference between a "public Blockchain" and a "private Blockchain"?

5. **A "public Blockchain" is one that is open to the public. This means that it is visible and that anybody can query the ledger and its history, which is why all of the transactions that occur on the Blockchain of cryptocurrencies like Bitcoin and Etherium are visible. "Private Blockchains", on the other hand, are controlled by an organisation or a unit and are not accessible to the outside world, unless one has what is called a "private key".**

How does a transaction flow through a Blockchain system?

6. The flow of a transaction through the Blockchain system can best be understood through the analogy of an Excel spreadsheet. Let us say that within this Excel spreadsheet, which forms what is known as a "block", there is an amount of value, say $100, moving from A's wallet address to B's wallet address. Many other transactions could also fill up this same block or Excel spreadsheet. There are various computers, or nodes, which look at the transactions, keep copies of them, and verify them. In a public system, the nodes all take copies of this Excel spreadsheet, and ensure that the transactions inside the spreadsheet are true, meaning that, looking at the older blocks in the system and the entire database, it is evident that A has the value to transfer to B, and that A is not trying to spend $100 of value twice.

7. This 'double spend' problem is the reason why Blockchain, Bitcoin and other cryptocurrencies were invented. Earlier attempts at digital currency in the late 1990s and early 2000s failed, in part because the 'double spending' problem required a central party in the middle to authorise and check each transaction - in effect, playing the role of a bank. This meant that those central parties could be easily approached and shut down by governments, who saw them as creating a new money supply and taking control of money supply away from them. Therefore, an important aspect seen in the Bitcoin deployment of a blockchain is a system where the participants in the blockchain are effectively their own bank. As such, all of the nodes present can verify that the transactions taking place are real, and by checking in with each other, they can ensure that no one is trying to gain the system.

8. Another useful analogy for describing a blockchain is that of the childhood game of "telephone" or (albeit slightly politically incorrectly-named) "Chinese whispers", as it was then known, where a phrase being whispered around a room has been passed around so many people that someone is bound to utter it incorrectly, and once it reaches the end, the phrase is different to what was started with. When applying Blockchain and the process of verifying transactions to this game, each person involved, as the phrase is whispered to them, shouts it out to the entire room before whispering it on. If this is done, everybody is aware of what is happening at each step as the information is passed around. This is a very good way to think of how Blockchain technology verifies transactions in a crowd of people, without having to rely upon a central authority to decide what is true.

9. Assuming that the verification has taken place and the nodes have all approved that the transactions that have occurred are correct (that is, to use the example described above, A has the $100 in question to transfer to B), that block is then closed off and added to the previous blocks, forming a chain – hence the name 'Blockchain'. The process then starts all over again on the next block.

How do the blocks in a blockchain hold together?

10. **The blocks in a blockchain hold together through a process known as "hashing", which, in computer terms, is a very old cryptographic process where data can be put through a one-way algorithm which will always result in a fixed length of numbers and letters. The essence of hashing is that it makes it extraordinarily difficult, if not impossible, to take that string of numbers and letters and recreate the input that was put in at the start. What is called the "hash output" can be used to verify the input through the algorithm.**

11. **The blocks in a blockchain start with a hash at the top, which is the hash from the previous block, and when they are closed off by the network, a new hash is appended to the block, which is then used as a starting hash for the next block.**

12. **One of the most interesting features of hash functions is that if a single character in any of the input is changed, this change will be evident. To take a Word document as an example, if, in the normal course of things, a lawyer wished to make changes to the document, they would have to do Track Changes, give it to the lawyer or client on the other side of the transaction for them to make any comments and changes, and if it were returned with them saying they had made no changes, the initial lawyer, as a matter of good practice, would run Track Changes over the document to ensure that nothing had in fact been changed. However, if the hash function was to be applied to this document, it would be a fast-track way to not having to take this kind of step, as even a single-digit change in the document would be reflected.**

13. **Blockchains may be summarised as a collection of existing technologies which have always been in the IT space, but which are now being used in a really creative way. Bitcoin, which is now ten years' old, was the first practical deployment of a blockchain.**

The difference between Blockchain technology and cryptocurrencies

14. **Cryptocurrency is actually built on the fundamentals of Blockchain. Essentially, cryptocurrencies are a way of storing and transferring value. It is helpful to think of cryptocurrency as being the value that is being moved, and the blockchain as the data store or ledger that the information or value is being stored on.**

15. **The actual contracts that enable transfers of cryptocurrencies in a blockchain are called "smart contracts", which contain all the business logic that moves the value.**

There may be multiple parties that need value transferred in one transaction - it is the smart contract that enables this transfer to happen.

<u>The elements of the blockchain ecosystem in greater detail</u>

16. **There are three key elements in the blockchain ecosystem:**
    (i) the cryptocurrency - the value that is being moved;
    (ii) the blockchain - the data store or the ledger that the information is being stored on; and
    (iii) the smart contract - the action or rule set that makes it all happen.

17. **Blockchain technology is really in its infancy, much as the Internet was back in 1995. This creates excellent opportunities for those involved in the Blockchain space, both on the technical side and the legal side. Just like the Internet in 1995, no one could have predicted how widespread it would become and how it would grow and touch almost every facet of our lives, later accelerated by the rise of smartphones.**

18. **It is useful to think of cryptocurrencies as an application, the first application that has became popular using the blockchain technology, much as email was the first application that became popular using the Internet.**

19. **One of the key features of the Blockchain system is its decentralised nature (at least as far as a public blockchain is concerned), meaning that there is no central point of failure. This is a very powerful aspect of Blockchain technology. When it comes to smart contracts, the inability of anyone to stop a smart contract from executing is a particular problem in the legal world, and has not been the subject of considered reported cases and legislative intervention to date.**

20. **The censorship-resistant architecture of Blockchain makes it almost impossible to change records in certain public ledgers. In practical terms, it is impossible for someone to go back and erase a recorded transaction. Not only would it require a large amount of computing power, it would be obvious to everyone in the network that there had been some kind of tampering. The nature of open systems such as Blockchain makes tampering with them quite difficult; conversely, their open nature makes them a fantastic audit system. There has been legislative recognition of Blockchain storage of data as a source of truth – the US state of Arizona is leading the way with the progress of a Bill in the area, as are a number of other US states. This shows how far along the US is in recognising that the outputs from smart contracts and Blockchain records themselves are able to be recognised, through statutory intervention, as evidence in court proceedings. Most recently in Australia, there have been criminal prosecutions**

involving fraudsters who have been stealing cryptocurrencies, which indicates that there is recognition by the courts that cryptocurrencies are things of real value, and a form of asset.

Smart contracts – an overview

21. Smart contracts are simply a process or computer code that take a certain input, and with a required set of variables, should create an output. Vending machines are a classic example of a smart contract. If the correct buttons are pressed, and a certain amount of money is put into the vending machine, the machine should, reliably, always do the same thing, namely, deliver the selected item of food or drink to the purchaser. Another example of a smart contract is the terms of service for software such as Netflix or the App Store. When signing up to use such software, people usually give their credit card over to be charged on an automated basis; this use of the software is "smart", in one sense of the word. Smart contracts can also be seen in contracts which rely upon the parties working together to achieve some kind of output which is coming from computers in the financial services space. Many of these contracts are highly automated, but they are still centralised.

22. What is being seen now is the rise of smart legal contracts. In a strict legal sense, it can be argued that smart contracts are not really contracts, as they do not meet some of the requirements for a legally enforceable contract, which can be problematic. However, the rise of so-called smart legal contracts, where those parts of the contracts that can be automated, are, is an exciting space at the moment, and there are a number of projects involved with this. They are not trying to get away from the human readable contract, but rather are trying to harness those parts of the contract which can be automated. Good examples of smart legal contracts are: escrow; transactions involving multiple parties who would like to automate part of the process; and contracts concerning the transfer of value that is linked to an asset, particularly where there are multiple parties involved.

23. Another pertinent example of a smart legal contract can be found in the real estate sphere. Specifically, NSW Land Registry Services is looking to move land titles onto Blockchain, which gives rise to the question of how can a smart contract be created around this? The smart contract can not only transfer the property but also manage a number of things, such as making sure that the annual rates are up to date.

24. Smart contracts can also hold value and release that value over time. This is particularly useful in the Netflix example, where if someone pays for something that is a monthly,

ongoing service, a smart contract could potentially hold that value and then release it over time as the service is being delivered.

25. There is a lot of interest in smart contracts in areas such as construction, where a large value might be paid upfront, but there are multiple parties that need to be paid over time. Traditionally, this large upfront payment may get misused and projects do not reach final completion because they have not been allocated in the best possible way. A smart contract could help mitigate these types of issues.

26. In summary, although smart contracts do not necessarily need to be the fully legally binding contract as we know it, the business logic behind them can be very valuable. The vending machine is a prime example, because the product will not be released by the machine until the money has been paid and the button has been pressed, that is, until all of the necessary things have been achieved.

27. Further, the self-enforcing nature of a smart contract leaves little room for interference from lawyers with any kind of injunctive relief between parties. One of the touted benefits of smart contracts is that once they are released onto a public Blockchain (in the case where they are public smart contracts), they cannot be stopped, much as a transaction cannot be stopped if it is moved onto a public Blockchain, because there is no central party to stop it. Therefore, value placed in an escrow smart contract cannot be released, notwithstanding the desire of the parties, until the terms of the relevant code have been met.

28. The extreme position of smart contracts as they were originally envisaged by Nick Zarbos, considered the father of smart contracts, and certainly in the last couple of years with Blockchain, is the situation where smart contracts would be fully automated, allowing the parties to interact without any need for any kind of written agreement, where everything would be embodied in the code. From a legal perspective, this can create serious problems of offer and acceptance and notification of terms, as anyone who does not understand the code (most likely anyone who is not a qualified programmer in that particular code) will not have an understanding of the terms of the contract.

29. In summary, a disadvantage to smart contracts being unchangeable once they are out in the wild, so to speak, is that when things go wrong, they can go wrong quite badly.

<u>Tokens</u>

30. Tokens are another example of how value can be transferred. There are many different types of tokens, including: loyalty tokens, collectibles, pre-sale tokens, stable tokens, security tokens, asset-backed tokens, and utility tokens. The latter four of these will be described below.

31. The concept behind stable tokens is to have the token linked to something of stable value, such as the US dollar (an example of this is the token Tether, where one token is always equal to one US dollar), or a hard asset, such as gold, metals, etc. The rationale behind stable tokens is to create something that does not change in value and does not have the volatility associated with changing value. These tokens are then used as an exchange mechanism, enabling trade within the cryptocommunity.

32. Security tokens rely on backing from some kind of security, typically an equity, or some kind of physical store which will provide value back to the token holder. Much like a share in a company, security tokens are designed to provide value back to their owner.

33. In relation to asset-backed tokens, an interesting shift is taking place, especially in the area of real estate. Like the stable tokens being backed by the dollar or a hard asset, asset-backed tokens are backed by the ownership of real estate.

34. The tokens that have been seen to date in the Blockchain world have been heavily skewed towards what have been described as utility tokens. There has been a challenge surrounding defining utility tokens, and for the most part, attempts to define them have been made by reference to what they are not. For instance, parties issuing utility tokens state that these tokens are not financial products, nor shares, nor derivatives, but something else. These tokens can be put to a variety of uses and be programmed in almost infinite ways. Once you have "programmable money", which is how tokens, as well as smart contracts, have been referred to, one can do a multitude of things. An example of the use of programmable money is Canadian project Polymath, which is looking to implement the ST-20 Standard, where digital representations of security tokens cannot be traded other than between persons who are on a "white list", helping to address issues of anti-money laundering and counter-terrorism financing. In the security space, we are therefore likely to see an approach of "white listing" to give comfort to regulators in relation to the risk of the use of utility tokens in financial crime.

<u>Case study: smart contracts and Blockchain deployments in the mortgage industry</u>

35. A good example of the use of Blockchain for the benefit of all concerns the mortgage industry. One of the challenges currently faced by the banks and lending organisations in this sphere is the ability to verify a person's income. One of the applications recently deployed by Lakeba Group is entirely concerned with understanding the validity of payslips and payroll information. A very good use case of Blockchain is taking the information at its source, in this case, payrolls or payslips, and creating the hash, previously described, a piece of information that is irreversible, and storing it on the Blockchain. This process has the effect of securing the relevant payslip and by extension, the information on it.

36. If a consumer then takes this payslip into a financial institution to verify their income, the institution is able to check the validity of the payslip by putting it through the same process which, theoretically, would create the same hash as that which was originally created when the payslip was first stored on the Blockchain. If that hash is checked on the Blockchain and it is non-existent, this indicates that the payslip is incorrect or has been modified from the time it was generated to the present point in time. This is a very simple, albeit powerful, illustration of how Blockchain technology and cryptography can be used to bring about positive change to an industry.

<u>The legal validity of smart contracts</u>

37. There is the overarching issue that a smart contract on a public Blockchain cannot be stopped by a court. The only person who can be recognised as really having liability is the developer themselves. In this vein, some US academics have suggested that a new fiduciary obligation on developers ought to be recognised by the courts. This would be a very interesting development, but it would also be very chilling on Blockchain development, because there has been scant recognition of developers of software platforms being under a duty to act in the best interests of the users of the software. It is well-recognised that software represents that it will do a certain thing, and if it does not do that thing, the parties selling the software may become liable, and may have a claim against the developers of the software under a different contract, or perhaps in negligence further down the chain. It would be a novel step indeed to ascribe liability to a software developer, but Michael Bacina sees this as the only way for there to be liability as the developers are the only parties who are building these smart contracts that are being put on a public ledger with no central party.

38. As of January 2017, the amount of money stolen in scams and hacks was over US $1 billion. There is a significant amount of fraud and scams going on in the Blockchain world, which has made some business somewhat reticent to use Blockchain technology.

Advice to lawyers looking to learn more about Blockchain technology

39. **The following resources are suggested for lawyers who wish to learn more about Blockchain technology:**

(i) Legaler, one of Michael Bacina's clients, who originally built a slack-like platform and video chat for lawyers to interact with their clients, and have evolved to building a law-firm specific blockchain upon which smart contracts and so-called decentralised applications (such as the previously discussed examples of verification of documents and identification) are being built.

(ii) The Legal Technology Association;

(iii) The Open Law Movement, underpinned by Consensus, one of the leading development organisations in the world around Blockchain;

(iv) The Accord Project, which is looking to bring a simpler way of building smart legal contracts to the legal community, because unfortunately, at this stage, the legal community has a lesser level of skill in coding than specialist and expert developers like the Lakeba Group.

(v) The Australian National Blockchain, which is currently in pilot. A number of firms have become involved in this project to date.

(vi) Numerous Blockchain events - lawyers looking to learn more about Blockchain are advised to attend these as a lot of information is presented at these events.

BIOGRAPHY

Michael Bacina

Partner, Piper Alderman, Sydney

Michael is a Partner in Piper Alderman's national Dispute Resolution team based in Sydney. Michael has over 10 years' experience as a commercial litigator. He regularly appears before the Supreme Court and Federal Court in large dispute matters involving complex evidence, and has successfully prosecuted numerous urgent injunctions in matters involving shareholder oppression. Michael also provides an outsourced counsel service for businesses looking for the benefits of an in-house counsel while maintaining known legal spends.

Darren Younger

Non-Executive Director, Lakeba Group, City

Darren Younger is the Chief Growth Officer and Co-Founder of the Lakeba Group. He holds this title alongside his Head of Lakeba Future Hub role.
Recognised early in his career as an innovator and technology entrepreneur, Darren's role as Chief Growth Officer for Lakeba is to drive the vision and momentum of Lakeba's Future Hub, a forward looking division of Lakeba with a focus on emerging technologies including Blockchain, AI, Machine Learning and Quantum Computing.

BIBLIOGRAPHY

Legislation

Xyz

Other