Blockchain will revolutionise financial services (and more)

A paper prepared by Trevor Matthews, MA, FIA, FIAA, FAICD, ASA
13 September 2018

“The consequences of this breakthrough are hard to overstate.” Marc Andreessen, Netscape Co-Founder

1. Introduction

On 24 August 2018 the Commonwealth Bank of Australia announced that it had helped the World Bank raise $110m through bond-i - the world’s first bond to be created, allocated, transferred and managed through its life cycle using distributed ledger technology (blockchain). The bond-i (Blockchain Offered New Debt Instrument) was developed at CBA’s Innovation Lab Blockchain Centre of Excellence in Sydney and named after a favourite tourist spot! The bond-i platform uses a private Ethereum blockchain and is designed to streamline substantially capital raising processes in the debt capital markets, which are currently made up of a complex web of interconnected agents and intermediaries.

This came shortly after CBA announced on 30 July 2018 that it had demonstrated a new blockchain platform underpinned by distributed ledger technology, smart contracts and the internet of things (IoT) to facilitate a trade experiment, - the tracking of a shipment of seventeen tonnes of almonds from packers in Sunraysia, Victoria to end delivery in Hamburg, Germany. Partners were able to view and track the location of the shipment as well as view the conditions, such as temperature and humidity inside the container, via four IoT devices. This level of data provided partners in the supply chain with a great level of transparency and efficiency regarding the location, condition and authentication of the goods being transported.

There is something going on here...

2. What is blockchain?

“Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. An asset can be tangible (a house, a car, cash, land) or intangible (intellectual property, patents, copyrights, branding). Virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved.”

3. Where did it come from?

Blockchain effectively made its public debut in 2008 when the mysterious Satoshi Nakamoto, whose true identity is still unknown, released a whitepaper, “Bitcoin: A Peer-to-Peer Electronic Cash System”. This paper describes a purely peer-to-peer version of electronic cash, which he christened

---

1 The author can be contacted at trevojohnmatthews@gmail.com
5 https://bitcoin.org/bitcoin.pdf
“Bitcoin”, and which effectively runs on a platform that has been given the name of blockchain. Nakamoto does not mention the term “blockchain” in his seminal paper however he does introduce “an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work.” Nakamoto observed that commerce on the internet at that time relied almost exclusively on financial institutions serving as trusted third parties to process electronic payments. The cost of mediation increases transaction costs and a certain percentage of fraud is accepted as unavoidable. He suggested an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party such as a bank. In this way he set out a protocol to solve the “double spending problem”, that is where in a digital cash system the same digital token or coin can be spent more than once. His solution envisaged using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. Blockchain can be thought of as an operating system, like Microsoft Windows or MacOS and bitcoin is just one of the many applications that can run on the operating system.

4. How does it work?

This diagram illustrates a blockchain transaction.⁶

Despite its apparent complexity a blockchain is just another type of database for recording transactions, one that is copied to all of the computers in a participating network. A blockchain can be referred to as a “distributed ledger”. As shown in the diagram above data in a blockchain is stored in fixed structures called “blocks”. The blockchain architecture gives participants the ability to share a ledger that is updated through peer-to-peer replication each time a transaction occurs. The following diagram from “Blockchain for dummies” referenced above contrasts the tracking of the ownership of a vehicle subject to lease without and with blockchain.

⁶ https://blockgeeks.com/guides/what-is-blockchain-technology/
Car leasing can be quite complicated. Each party within the network maintains its own ledger which can take days or weeks to synchronize. By using a shared ledger on a blockchain network every
authorised participant can access, monitor and analyse the state of the vehicle regardless of where it is within its lifecycle.

Blockchains store data in blocks linked together to form a chain. As the number of transactions grows so does the blockchain. Blocks record and confirm the time and sequence of transactions which are then logged into the blockchain within a discrete network governed by rules agreed by the network participants. The important parts of a block are its header and its content.

- The header includes a unique block reference number, the time the block was created and the link back to the previous block.
- The content usually includes a validated list of digital assets and instruction statements, such as transactions made, their amounts and the addresses of the parties to those transactions.

A feature of the header is the hash which is a digital fingerprint or unique identifier. In simple terms, hashing means taking an input string of any length and producing an output of a fixed length. In the context of cryptocurrencies like Bitcoin, the transactions are taken as an input and run through a hashing algorithm (Bitcoin uses SHA-256) which gives an output of a fixed length (256 bits). Here is an example of applying the SHA-256 algorithm to two pieces of data.

<table>
<thead>
<tr>
<th>INPUT</th>
<th>HASH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hi</td>
<td>636EFC0D08AB273B169E8E278C29A7DF02C03B1B1820E99FC95DCAA332658</td>
</tr>
<tr>
<td>Welcome</td>
<td>53A59FC9E2A09F080E60D849A701574CD9CF5F0FB498C41731881BCCD08A70C8</td>
</tr>
</tbody>
</table>

No matter how big or small the data is the result after hashing is always the same fixed length.

In summary blockchain is an open, decentralised ledger that records transactions between two parties in a permanent way without needing third-party authentication.

“Blockchain is to Bitcoin what the internet is to email. A big electronic system, on top of which you can build applications. Currency is just one.” Sally Davies, FT Technology reporter.

5. What is Ethereum?

One of the original contributors to the Bitcoin codebase, Vitalik Buterin became frustrated around 2013 with its programming limitations and agitated for a more malleable blockchain. In the face of resistance from the Bitcoin community he set out to build the second public blockchain which he called Ethereum and launched in 2015. The largest difference is that Ethereum can record other assets such as loans or contracts (or almonds), not just currencies. It can be used to build “smart contracts”, those that automatically process based on a set of criteria established in the Ethereum blockchain. Ethereum comes with its own cryptocurrency called “Ether”. Buterin picked the name “Ethereum” after browsing Wikipedia articles about elements and science fiction. When he found the name, he said, "I immediately realized that I liked it better than all of the other alternatives that I had seen; I suppose it was the fact that it sounded nice and it had the word ‘ether’, referring to the hypothetical invisible medium that permeates the universe and allows light to travel."

There are some other technical differences as well. The average time to validate and prove a new block is significantly less - something like twelve seconds compared to ten minutes. Ethereum has attracted a great deal of interest from institutions and developers. The CBA applications described in Section 1 are based on an Ethereum platform.
6. Who is developing blockchain solutions?

A recent Greenwich Associates Report estimates that the financial services industry is spending about US $ 1.7 billion per year on blockchain as banks and other firms move beyond the proof of concept stage and start rolling out commercial distributed ledger technology products.\(^7\) The study results show that blockchain budgets increased 67% last year, with one in ten of the banks and other companies now reporting blockchain budgets in excess of $10 million. The author of the report stated, “More than half the executives we interviewed told us that implementing DLT was harder than they expected...Nevertheless, more than three-quarters of projects currently under development are expected to be live within two years.”

In Australia, in addition to CBA, the ASX has announced that it is working with Digital Asset, a New York based fintech in which it holds a strategic stake, to replace the CHESS equity clearing and settlement system with a distributed ledger technology solution towards the end of 2020. Dominic Stevens the CEO says this could create hundreds of millions in savings in the system because it will remove the need for market participants to reconcile their databases with those held by the exchange, various custodians and brokers. He suggested in an analyst briefing that if the superannuation sector could save just 5% of its cost base with such a system the savings would be $1.15 billion.

Banks around the world are working in consortiums to investigate then possibly implement systems for

- Clearing and settlement,
- Payments
- Trade finance
- Identity checking, and
- Syndicated loans

Five major European insurance and reinsurance companies, Allianz, Aegon, Munich Re, Swiss Re and Zurich, are partnering to see if blockchain can help them deliver faster and more secure client services. They have dubbed this B3i following in the footsteps of initiatives like R3\(^8\), an enterprise blockchain software firm working with a broad ecosystem of more than 200 members and partners across multiple industries from both the private and public sectors to develop blockchain applications. A further example closer to home is Singapore based Galileo Platforms which aims to provide a blockchain platform to connect participants in the insurance industry efficiently and in real time.\(^9\)

The wrap platform company FNZ has formed a syndicate with asset managers in the UK representing 25% of total market assets under management to implement a blockchain based system designed to reduce costs and improve security.

There is an equally wide range of initiatives outside financial services. In Australia The CSIRO’s data science and innovation group Data61 has partnered with law firm Herbert Smith Freehill and IBM to

---

8 [https://www.r3.com](https://www.r3.com)
build a platform that will allow Australian firms to use digitised contracts, exchange data and confirm the authenticity and status of legal contracts using a blockchain platform. It is expected that smart contracts on the system will be able to record data from external sources such as IoT devices allowing clauses to self-execute when contact conditions are met.

There are even claims that blockchain could help solve privacy problems with digital advertising. A Sydney based start-up, the Tide Foundation proposes to use blockchain to allow individuals to own their own data and advertisers to find them and reward them without compromising privacy. An example they quote is a car manufacturer wanting to inform families who are expecting a baby about a new model SUV. They could request details of people who have recently purchased baby goods. The request is sent to the unidentifiable individuals who can opt in the SUV advertising campaign in exchange for tokens of some sort.

DHL is working with Accenture to establish a blockchain based track and trace serialisation system which will have application in the pharmaceuticals industry. Life science and healthcare companies create unique serial numbers for units of medication and pieces of equipment which are scanned, captured and verified at their point of origin. As each item moves through the supply chain additional verification information can be added using the blockchain functionality. This will result in an end to end system that is simpler and more secure than anything before, more private, more transparent, more efficient with less risk.

The World Economic Forum has said that simplifying paperwork and other trade impediments using blockchain technology - distributed ledgers - that sequentially and immutably record and store data whereby people have immediate access to the same information without having to pass through a central point could increase global trade by 15% and lift world GDP by 5%, a greater boost than trade would receive if tariffs were to be abolished. Some observers believe this innovation could be shipping’s biggest breakthrough since the first container ship sailed in 1956.

7. What are the risks?

The prizes described above will not come without risk. There will be privacy concerns, cyber security threats, concerns about excessive power demands and even possible capacity limits. KPMG have published details about two blockchain incidents. In the first, US $50 million was drained from a newly formed digital venture capital fund which employed smart contracts on the Ethereum blockchain. (The DAO Incident.) An attacker exploited a flaw in one of the smart contract functions that clearly in retrospect had not been tested exhaustively. In the second the Hong Kong based Bitfinex crypto currencies exchange suffered a security breach in which almost 120,000 Bitcoins were removed from customer accounts. The cause of this has not yet been confirmed but it appears there was a deficiency in one of the organisations using the blockchain and not the blockchain itself.

KPMG suggests that organisations that embark along the blockchain journey must at the same time develop a comprehensive security and risk framework to minimise the chance of catastrophic events.

8. What are the cryptocurrencies?

This paper has concentrated on blockchain platforms and not on the crypto currencies that reside on these platforms. Incredibly there are now over 1,600 cryptocurrencies! These could be the subject of

11 https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2017/05/securing-the-chain.pdf
future papers. The table below lists five of the most popular showing their market capitalisation and token or coin value as at July 2018.12

<table>
<thead>
<tr>
<th>Cryptocurrency</th>
<th>Market Capitalisation (US $)</th>
<th>Token or coin value (US $)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bitcoin</td>
<td>300 billion</td>
<td>8,000</td>
</tr>
<tr>
<td>Ethereum (Ether)</td>
<td>47.8 billion</td>
<td>474.66</td>
</tr>
<tr>
<td>Ripple</td>
<td>19.07 billion</td>
<td>0.486</td>
</tr>
<tr>
<td>Bitcoin cash</td>
<td>14.2 billion</td>
<td>827.15</td>
</tr>
<tr>
<td>Cardano</td>
<td>4.81 billion</td>
<td>0.186</td>
</tr>
</tbody>
</table>

9. **What are the investment implications?**

The blockchain revolution has the potential to have wide and profound implications for investment decision making. It is important for investors to understand what blockchain is, how it works, what is happening and what is possible, so they can consider the investment implications. Intermediaries in all sectors of the economy are likely to be affected to varying degrees as blockchain platforms expand into different areas. There are many start-ups, the nature of which means there will probably be some spectacular winners and almost certainly many losers. It is instructive that a large number of the major financial institutions are paying attention to this new development, clearly attracted by the opportunities for increased efficiencies but also no doubt concerned about the threats to their business models. It will become important for investors to monitor blockchain developments and gauge how well-established institutions adapt to the new world.

As well as impacting the obvious candidates such as banks, insurers, asset managers, stock exchanges and money transfer agencies blockchain will affect trading enterprises, legal firms, advertisers and other companies managing information and resources. Second order impacts may be felt by resource producers, graphic card makers and energy suppliers.

There certainly is something going on here.

*“We tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run.”* Roy Amara 1925–2007 American futurologist

---

12 [https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/](https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/)