What is Blockchain?

How is it used in finance?

Michelle Byun 15 February 2022
Michelle is a graduate analyst with Antares Equities. She joined Antares in 2021 having successfully completed a Bachelor of Commerce (Finance) and Laws

Introduction
“Crypto has one feature that has never existed before - trust” – Ben Horowitz, cofounder and general partner at Andreessen Horowitz, a venture capital firm in Silicon Valley that backs technology focused start-ups and businesses. Cryptocurrency and blockchain are gaining wide traction from investors globally due to its innovative concept. In particular, investors are wanting to understand blockchain which is a technology that enables cryptocurrencies as well as other blockchain-based projects including Non-Fungible Tokens (NFTs) and Decentralised Finance (DeFi). This paper aims to explain how blockchain operates and the attributes which makes the technology secure. Furthermore, the paper includes an example of how blockchain can be utilised other than for cryptocurrencies and its use case in the Australian landscape.

How blockchain works
Blockchain is a peer-to-peer (P2P) network that uses a distributed ledger system. There are four broad types of blockchain networks – public, private, consortium and hybrid – that vary in terms of decentralisation and permission status. This paper focuses on public blockchain which underpins networks such as Bitcoin (BTC) and Ethereum (ETH) and is primarily used for decentralised finance applications. A glossary of terms is included at the end of this paper.

Public blockchain is decentralised, meaning the decision-making power and control is distributed equally amongst the participants, or **nodes**, in the network. As such, blockchain provides transparency and efficiencies that come from disintermediation.

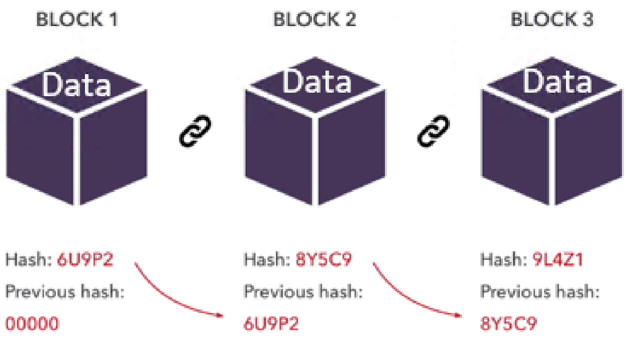
Nodes refer to any computer that runs a blockchain network implementation and keeps the record of the entire blockchain database. Essentially, nodes are the participants of the network. The P2P protocol of blockchain allows nodes to communicate to each other regarding information about transactions and new blocks.

Security is one of the defining attributes of blockchain networks. Providing security are several features:

(1) Cryptography
Each ‘block’ contains three elements – data, hash and hash of a previous block. Hash is a unique identifier, like a fingerprint of the block – when the data changes, the hash changes as well. Data can record any information such as the amount transacted, the sender and receiver.

Blocks are arranged in a sequence and chained together by the hash of the previous block.

Figure 1: Components of a blockchain



Source: https://www.ig.com/en/trading-strategies/what-is-blockchain-technology--200710

Remember that hash changes when the data changes. This means that when someone tries to alter the data in block 1, the chain that connects it to the subsequent blocks will be broken. This is because the hash of block 1 will change along with the data and it will no longer match the original hash of block 1 that is contained in block 2. Hence, the cryptographic property of the hash function and the way the blocks are chained together makes blockchain immutable, meaning it cannot be manipulated or reversed.

(2) Distributed & Decentralised

Blockchain is a distributed ledger system and all nodes get an identical, updated copy of the blockchain database. Additionally, decentralisation ensures that the governing authority is shared equally across all the nodes in the network. Through this feature, each node maintains its sovereignty and independence when deciding which block goes on the blockchain ledger – this process is described in the next paragraph. Given the decision-making power and control is decentralised, it prevents a single point of authority from validating a block solely by themselves. Hence, in the above scenario when the chain is broken, not only will this be visible to all the nodes (distribution) but it will allow the nodes to come together and invalidate the changes in the block (decentralisation).

(3) Consensus Algorithm

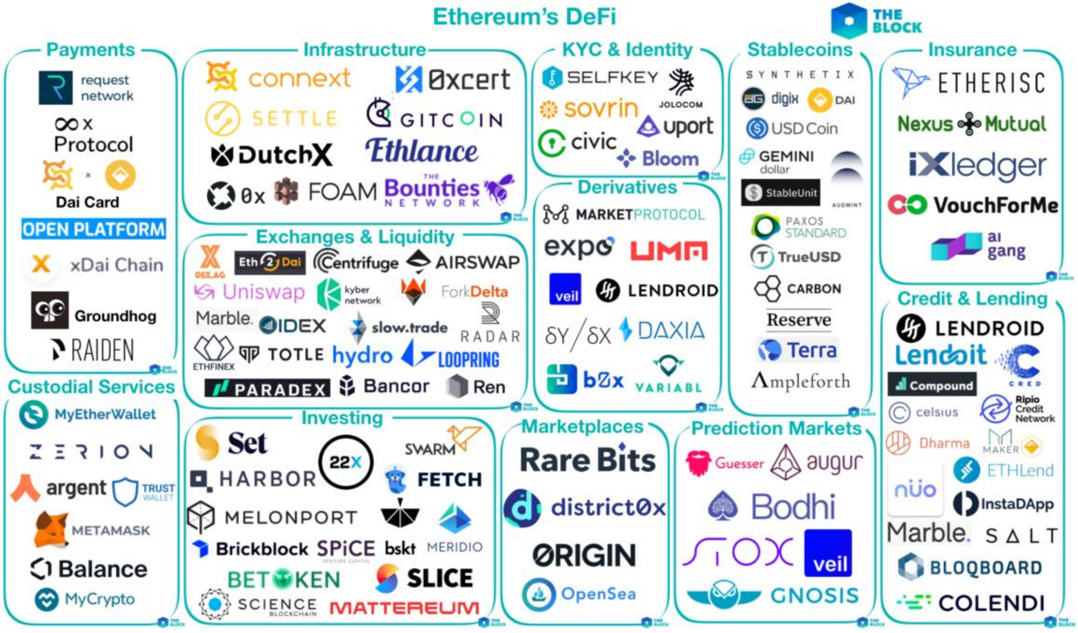
Once a new transaction is entered, the information is sent to all the nodes in the blockchain network and the majority of the nodes must validate the transaction before it goes through onto the blockchain. So how do the nodes decide on which block goes on the blockchain ledger? This is where consensus mechanisms come in – they are methodologies used to achieve agreement, trust and security. Essentially, it ensures that a new block added to the blockchain is the single source of truth, agreed upon by the majority of the nodes. The most common consensus mechanisms include Proof-of-Work (PoW) and Proof-of-Stake (PoS). Once the majority of the nodes agree that a transaction is valid, it is added to the ledger.

Blockchain in Finance

How can blockchain be used? So far, cryptocurrencies are the most famous users of blockchain, with Bitcoin recently recording US$65,000 per unit. Another industry where blockchain can be used is financial services.

Decentralised Finance refers to financial products and services that are based on blockchain technology. DeFi has grown significantly over the past few years, and in 2021, the total value locked (TVL) in DeFi Applications (DApps) had reached US$247b. Some examples of DApps include lending platforms, exchanges, asset management, payments and insurance. Currently, the majority of DApps are based on the Ethereum network. Figure 2 is an illustration of some DApps of different categories in finance that are based on the Ethereum network.

Figure 2: Ethereum's DeFi



Source: The Block; accessed on 08 November 2021

Contrary to the traditional financial systems where a central authority oversees the entire system, the biggest difference with DeFi comes from decentralisation. Smart contracts replace the function of intermediaries in the traditional financial system model. As such, DeFi can solve the inefficiencies that stem from the involvement of intermediaries including:

- Lack of transparency
- Cost
- Transaction time
- Accessibility

What are Smart Contracts?
A Smart Contract is a self-executing, digital contract which includes codes that execute the terms of an agreement. As this process is automated, there is no need for an intermediary to facilitate its execution.

Lending: an example of DeFi:
Lending is one of the fastest growing areas of DeFi. The TVL in five leading lending protocols has exceeded $45 billion as of December 2021. Conceptually, DeFi loans work in a similar way to traditional loans. Borrowers provide collateral in form of crypto assets such as ETH or BTC and obtain a loan often in form of stablecoins. A major difference to conventional lending is that DeFi loans operate as peer-to-peer lending – lenders are individuals who directly enlist their tokens on a platform to earn interest, without the help of a bank.

What is a stablecoin?
Stablecoin is a cryptocurrency that is pegged to a "stable" asset such as the USD or gold. The aim of stablecoins is to reduce the price volatility relative to unpegged cryptocurrencies like BTC and ETH. Hence, stablecoins are ideal for trading on crypto exchanges. One example of a stablecoin is DAI which is linked to the USD.

So, what benefits does DeFi lending provide over conventional banks? Most importantly, it operates without a central authority, enabling an open-source and transparent environment. As such, the process can be more straightforward and users can avoid preferential treatment based on their credit history.

Instead of intermediaries like banks, smart contracts play an integral role in facilitating DeFi loans. Smart contracts determine and distribute interest to lenders and enforce loan terms on both parties. Furthermore, DeFi lending offers a significantly higher yield to lenders compared to the interest rates on savings accounts. For example, US-based crypto exchange, Bitfinex offers an 8.50% yield on stablecoin DAI, whereas the average interest rate on a savings account was 0.06% according to Bankrate's weekly survey of institutions on January 5, 2022.

As users are not required to provide their credit history, counterparty risk is a major concern. To address this problem, most of the loans are over-collateralised, meaning that borrowers need to supply collateral that is worth more than the actual loan. For example, MakerDAO, a DeFi lending protocol, requires 150% minimum collateralisation ratio. This means that borrowers must deposit a minimum of $150 in ETH to borrow $100 worth of DAIs, a stablecoin token generated by MakerDAO.

Another question may arise: why would someone want to obtain a loan when they can simply sell their assets to generate the amount? A possible explanation is that they may want additional liquidity but do not wish to sell their crypto assets in case they increase in value. As mentioned earlier, often people borrow stablecoins such as DAI or Tether which are exposed to less price volatility, hence making it an effective medium of exchange, similar to cash. On the other hand, crypto assets like BTC and ETH are more volatile and have significant upside (and downside) price risk, making it an attractive store of value, akin to gold. Hence, investors who bet that the price of their crypto assets will rise in the future will not want to sell them immediately, but would rather borrow stablecoins to cover their expenses in the meantime.

However, there are liquidation risks associated with collateralisation. If the value of the collateral falls under the minimum collateralisation ratio, the lending protocol will liquidate the collateral. A key event took place on March 12, 2020 when there were 3994 liquidations, worth over $10m of collateral on MakerDAO. This was triggered as a result of the uncertainty around COVID-19 which sent the value of cryptocurrencies such as ETH down by 50%. Given the highly volatile nature of crypto assets, borrowers are encouraged to maintain their collateral above the threshold.

DeFi lending is one of various examples where DeFi replaces the role of a conventional bank. There are inherent risks in DeFi lending, including counterparty risk associated with the peer-to-peer structure and liquidation risks stemming from price volatility of crypto assets. Despite these uncertainties, people are attracted to DeFi loans for their advantages over traditional loans – for lenders it is the high interest rates, and for borrowers it is the straightforward and transparent lending process without the preferential treatment of banks. Hence, DeFi loans offer new opportunities as well as risks for both borrowers and lenders.

Be aware

While blockchain has many advantages, there are some key issues that potential users should be aware of before deciding to transact on DeFi platforms:

- **Irreversible transactions** – Unlike a centralised network, such as credit card systems which can reverse a transaction in form of chargebacks, blockchain transactions are irreversible. This goes back to the earlier point of what makes blockchain a secure network. As more blocks are added after your transaction's block, it becomes extremely difficult to modify the transaction as you would have to decrypt all the blocks preceding your transaction block.

- **Scalability** – In essence, scalability becomes an issue where a large amount of transaction data can't be processed in a practical amount of time due to a lack of capacity in the blockchain network. Blockchain requires every single transaction to be registered on the distributed ledger system for all participants to access. Although this ensures transparency and security, it can also cause congestion in the network during times of high transaction volumes, leading to longer transaction times and higher transaction fees. Layer 2 solutions have emerged in an attempt to resolve this issue. They are networks that operate over the native blockchain to improve certain aspects of the underlying network.

- **Security** – Despite the security measures underpinning blockchain technology, it is not completely immune to hacks. According to a report by Elliptic, DeFi protocols lost a total of US$10.5b to theft and fraud in 2021. While the amount may seem significant at face value, the total amount lost represents around 4% of the TVL in DeFi protocols. The most common reasons cited for the vulnerability include developer incompetence, coding mistakes and misuse of third-party protocols.

Blockchain is quickly being adopted in the finance industry with its potential to address the gaps in traditional settings. DApps are made to solve problems associated with dealing with intermediaries including lack of transparency, high costs, inefficiency and limited access. DeFi and blockchain technology in general is still very new and there are some aspects that can be improved with further developer experience and stronger regulations. Nonetheless, blockchain technology has exhibited great potential for its use across diverse industries, including finance.

Blockchain in the Australian landscape

Australia is no exception to the rest of the world when it comes to adopting blockchain technology. Recently Rio Tinto (RIO) launched START, a sustainability label which uses blockchain to trace aluminium's carbon footprint and thereby enabling its customers to understand their contribution to a sustainable future.

In November 2021, Commonwealth Bank (CBA) announced that they will be the first Australian bank to allow customers to directly trade crypto assets through the CommBank app. DigitalX (DCC) is another example of an ASX-listed company that delivers digital asset funds management services for institutional investors. It is clear that Australian corporates are already realising the array of benefits the innovative technology could provide.

One of the most notable use cases of blockchain technology is by Australian Securities Exchange (ASX). In 2016, ASX announced that it will be replacing its current post-trade settlements program, CHESS, with a blockchain technology which will be delivered in partnership with Digital Assets, a NY-based blockchain start-up company and VMWare, a cloud computing software company.

To be more specific, blockchain technology in this case of ASX, refers to the distributed ledger technology (DLT) and there are some distinctions to the public blockchain as explained earlier in this article. Unlike the public blockchain which is decentralised and where the nodes have the power to approve transactions, ASX will employ a private or a permissioned blockchain, meaning that ASX retains the central database and the sole authority to approve new blocks of data. Despite the limited authority, the users of the network will still be able to reap the benefits of DLT by having the access to the synchronised ledger which they can use to match their own records to those of the ASX in real-time.

Benefits

Accordingly, the DLT is expected to offer considerable benefits including greater market efficiencies through better record keeping, reduced reconciliation, more timely transactions and better quality data. Perhaps one of the biggest benefits can be realised from the regulatory aspect. Transactions will be mathematically tamper-detectable through the cryptographic attribute of blockchain data and the distributed ledger system, as explained earlier. Cliff Richards, ASX executive general manager emphasised that the DLT will boast a powerful audit quality which will be useful for dispute resolution.

Another area of innovation is that the users and third-party developers will be able to build new applications such as fintechs on top of the ASX blockchain. The applications will be built using DAML which is a smart contract programming language created by Digital Assets. The potential for smart contracts in finance has been widely recognised (please refer to the DeFi discussion for context) and Digital Assets has previously partnered with several prominent companies. For example, BNP Paribas chose DAML to build applications for its' new DLT-based trading platform and to automate and digitise processing workflows. As such, the potential for ASX's new DLT network reaches far beyond the proposed purpose.

Criticisms

However, the change is also met by criticisms from the relevant stakeholders. Share registries such as Computershare (ASX:CPU) record changes in share ownership, issue shareholding statements and manage dividend payments for listed companies. Following ASX's announcement, there have been concerns that the new technology will replace the role of share registries. This is because one of the main features of DLT is that it delivers irrefutable, real-time record-keeping which overlaps with some share registries' services. Furthermore, the fact that DLT is versatile and allows for additional functions to be built on top the network is fuelling concerns that ASX will be able to extend its dominant market position in the future.
distributed ledger technology for the real-time access. Recently, ASX also launched Synfini, which is a platform that offers "DLT-as-a-service".

ASX's adoption of DLT is expected to have significant implications for investors especially from the regulatory perspective. While other stock exchanges in different countries are also testing out blockchain-based technologies, ASX will be one of the first exchanges in the world to fully implement the technology. CHESS replacement will be rolled out in two phases and will be made available in 2023.

Glossary:

Blocks in blockchain - Contains 3 elements: data, hash and hash of a previous block.

Data - Data can record any information such as the amount transacted, the sender and receiver.

DApps - DeFi Applications

Decentralised Finance (DeFi) - DeFi refers to financial products and services that are based on blockchain technology.

Distributed Ledger - Database that is synchronised and updated in real-time when new blocks are added to the blockchain network.

Hash - Hash is a unique identifier, like a fingerprint of the block – when the data changes, the hash changes as well.

Layer 2 solutions – set of technologies that run on top of a blockchain network to improve and resolve underlying problems in the blockchain.

Nodes - Any computer that runs a blockchain network implementation and keeps a record of the entire blockchain database. Essentially, nodes are the participants of the network. Blockchain allows nodes to communicate with each other regarding information about transactions and new blocks.

Proof of Work (PoW) - One example of consensus algorithm. It is a mathematical puzzle that needs to be solved with computational effort in order for a transaction to be verified and added onto the blockchain network.

Proof of Stake (PoS) - One example of consensus algorithm. Transactions can be validated by someone who already holds the blockchain token as they stake their coins to guarantee that the transaction is safe and legitimate.

Smart Contracts - A Smart Contract is a self-executing, digital contract which includes codes that execute the terms of an agreement. As this process is automated, there is no need for an intermediary to facilitate its execution.

Stablecoin – cryptocurrency that is pegged to an external reference such as USD or gold. It offers less exposure to price volatility in comparison to unpegged cryptocurrencies such as BTC or ETH.

TVL - total value locked; refers to how much money is in DeFi across all the existing DApps

Important information

Antares Capital Partners Ltd ABN 85 066 081 114, AFSL 234483 (‘ACP’), is the Responsible Entity of, and the issuer of units in, the Antares Australian Equities Fund ARSN: 090 827 802, Antares Dividend Builder ARSN: 115 694 794, Antares Elite Opportunities Fund ARSN: 102 675 641, Antares Ex-20 Australian Equities Fund ARSN: 635 799 530, Antares High Growth Shares Fund.

This report has been prepared in good faith, where applicable, using information from sources believed to be reliable and accurate as at the time of preparation. However, no representation or warranty (express or implied) is given as to its accuracy, reliability or completeness (which may change without notice). This communication contains general information and may constitute general advice. This report does not take account of an investor’s particular objectives, financial situation or needs. Investors should therefore, before acting on information in this report, consider its appropriateness, having regard to the investor’s particular own objectives, financial situation or needs.

An investor should consider the current Product Disclosure Statement and Product Guide for the Fund (‘PDS’) in deciding whether to acquire, or continue to hold, units in the Fund and consider whether units in the Fund is an appropriate investment for the investor and the risks of any investment.

We recommend investors obtain financial advice specific to their situation. Past performance is not a reliable indicator of future performance. Returns are not guaranteed and actual returns may vary from any target returns described in this document. Any projection or other forward-looking statement (‘Projection’) in this report is provided for information purposes only. No representation is made as to the accuracy or reasonableness of any such Projection or that it will be met. Actual events may vary materially.

ACP is part of the IOOF group of companies (comprising IOOF Holdings Ltd ABN 49 100 103 722 and its related bodies corporate) (‘IOOF Group’). The capital value, payment of income and performance of any financial product offered by any member of the IOOF Group including but not limited to Antares, are not guaranteed. An investment in any product offered by any member of the IOOF Group including but not limited to Antares, is subject to investment risk, including possible delays in repayment of capital and loss of income and principal invested.

Any opinions expressed by ACP constitute ACP’s judgement at the time of writing and may change without notice. In some cases the information is provided to us by third parties, while it is believed that the information is accurate and reliable, the accuracy of that information is not guaranteed in any way. None of ACP, any other member or the IOOF Group, or the employees or directors of the IOOF Group are liable for any loss arising from any person relying on information provided by third parties. This information is directed to and prepared for Australian residents only. ACP disclaims all responsibility and liability for any loss, claim or damage which any person may have and/or suffer as a result of any persons reliance on any information, predictions, performance data and the like contained within this document, whether the loss or damage is caused by, or as a result of any fault or negligence of ACP, it’s officers, employees, agents and/or its related bodies corporate.