Part 1: Developing Technologies

Section 2

Commercial Application

Section 2: Commercial Application

Jonathan Emmanuel, Bird & Bird LLP

Introduction

Since the publication of the first edition of this guidance the media hype surrounding blockchain technologies has continued with ideas such as “metaverse”, “DeFi” and “NFTs” attracting considerable attention. Yet increasingly the evidence is that business is catching up; the ecosystem has changed. Venture capital backers are growing more comfortable with investment in the technology, as evidenced by the huge cryptocurrency-focused fund created by Andreessen Horowitz’s venture capital firm ($2.2 billion), blockchain-focused software companies like ConsenSys have rapidly expanded to scale-up and beyond, and real-life use cases are now being deployed by clients in a variety of sectors. All this shows that the technology is more than just a fad.

This section analyses a live use case in the financial services sector. The most successful use cases still tend to relate to taking advantage of blockchain technology to allow for the better sharing and recording of data (sometimes with the assistance of smart contracts) between disparate parties. When we refer to blockchain in this section, we are referring to the network of nodes comprising a blockchain, which could be a private or public blockchain depending on the context. First, therefore, it is important to understand why enterprises are choosing private blockchains over public blockchains or centralised databases. **Public vs private?**

Bitcoin and Ether are examples of cryptoassets underpinned by **public blockchains** (the public Bitcoin blockchain and the public Ethereum blockchain, respectively). Generally speaking, these blockchains share some common features:

- **Fully decentralised:** anyone can download the blockchain software on their computer to set up a node that connects with other nodes in the network over the internet. Each node in the network is a “peer” meaning there is no one node or entity in charge of running the network. The network is run by the blockchain software or protocol.

- **Broadcast-based blockchain:** once connected, these nodes can download a copy of the blockchain, send transactions for recording on the blockchain and view all entries in the blockchain.

- **No contracts:** there are no (or very limited) formal contracts in place governing the rights and responsibilities of the participants. For example, there are no (or very limited) rules governing stakeholder participation in the blockchain.

- **Consensus mechanism:** the blockchain will have a consensus mechanism built into the blockchain software that determines when a new transaction can be recorded on the blockchain.

There are many benefits associated with these features. As the blockchain is decentralised, participants do not have to trust an always-available central authority to manage it, and the blockchain’s broadcast-based nature means that there is full transparency on the data held on the blockchain.

However, there are also drawbacks. The lack of formal contracts in place makes it harder for participants to easily understand their rights and responsibilities and bring claims against entities they think have caused them to suffer loss. For example, if the blockchain goes down because of a bug in the software operating on all the nodes, what recourse do affected participants have? Moreover, the consensus mechanism (“proof of work” for the Bitcoin public blockchain) is time-consuming and costly to run.

For these reasons, and in our experience, enterprises are more interested in private blockchains. Again, these blockchains share some common features:

- **Trusted intermediary:** there is one entity in charge of running the nodes that make up the private blockchain network. Depending on the use case, this could be a regulator, joint venture entity or a company limited by guarantee.

- **Control:** the trusted intermediary decides what data participants can send for recording on the blockchain and what data they can view.

- **Contracts:** there are formal contracts in place governing the development of the blockchain and participation in it, which provide stakeholders with more certainty over their rights if things go wrong.

The preference for private blockchains is not absolute though. For example, one use case for blockchain technologies, discussed in Section 5, is non-fungible tokens **(NFTs)**. When it comes to selling NFTs for example, it is very common for the relevant entity to use public blockchain networks such as Ethereum to enable the creation of the NFTs, which are then made available for sale by customers via interoperable marketplaces like OpenSea.

Private vs central database?

One question to ask is why should enterprises implement private blockchains given that the existence of a trusted intermediary reintroduces the concept of a central authority, resulting in little difference between a private blockchain and a centralised database?

Whilst there is some truth to this, there are in fact many benefits specific to blockchain technologies (compared with centralised databases) which mean that private blockchains can be useful in the right circumstances. For example:

- **Immutability:** once data has been recorded on a blockchain, it is very difficult to change it without it becoming immediately obvious to all participants and rejected by them (as necessary).

- **Digital signatures:** the use of digital signatures makes it easier for disparate parties to approve and send data for recording on a blockchain without the need to rely on a third party. This makes it easier to coordinate input from disparate parties.

- **Peer-to-peer:** as the blockchain network is peer-to-peer, it can continue to function even if some of the nodes in the network become unavailable. This makes the network more robust than networks reliant on a central database as there is no single point of failure which could result in the database being unavailable if the server hosting it is unavailable.

Setting up a private blockchain

The process of setting up a private blockchain is, generally, as follows:

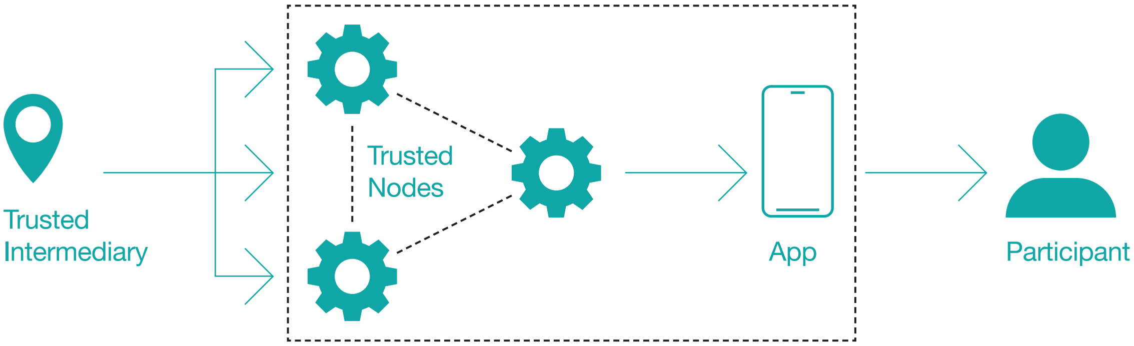
- **Trusted intermediary:** the trusted intermediary downloads the blockchain software and sets up the nodes that comprise the network. It is not necessary to have only one trusted intermediary, although this is common; the process may in fact involve multiple trusted intermediaries with authority over the blockchain software, who may then subcontract out this authority to other entities. A trusted intermediary, or each of the trusted intermediaries where more than one is used, is in charge of the blockchain because it runs and operates the nodes that comprise the network, either by itself or by delegating the running of the nodes (and therefore the validation of transactions on the blockchain) to its subcontractors.

- **User-facing application (app):** the trusted intermediary builds an app (for example, a mobile app) that interfaces with the nodes and through which participants can access the nodes.

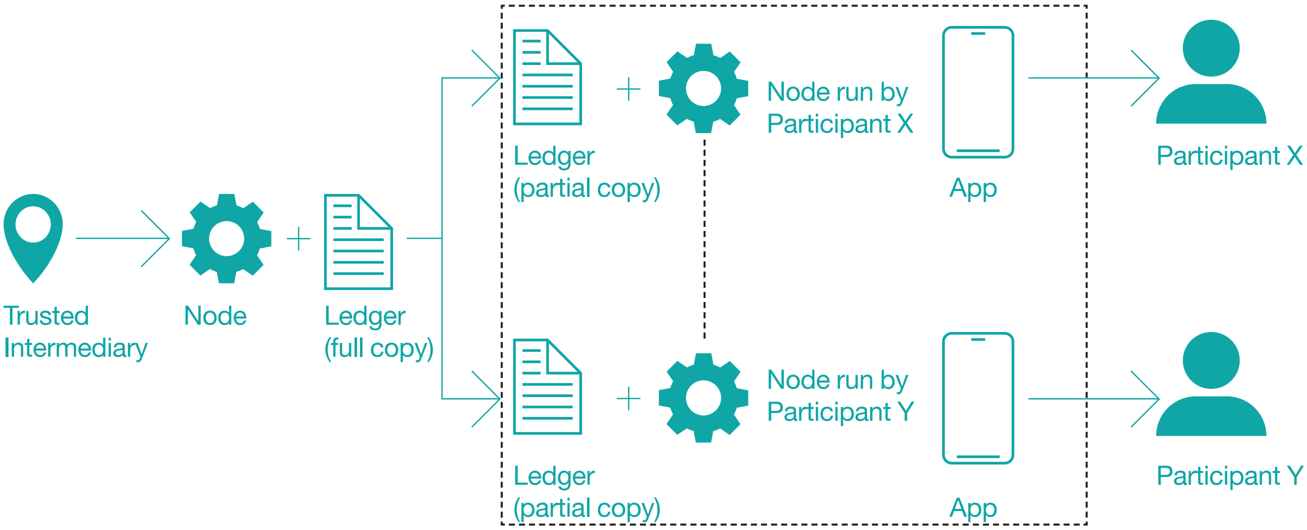
- **Participants:** the participants access the trusted intermediary's nodes via the app. Using the app, participants can send data to be recorded on the private blockchain and view the data recorded on the private blockchain.

There are two models that are most commonly used when setting up a private blockchain:

- **Distributed ledger model:** the trusted intermediary runs all the nodes and participants access the nodes on a software-as-a-service basis.



- **Shared ledger model:** the trusted intermediary runs a node that hosts a full copy of the database. Participants can also run their own nodes that download a partial copy of the database (this copy only includes data to which the relevant participant is a counterparty).



Use case

One of the most common use cases relates to the better sharing and recording of data in the context of trade finance projects through the use of blockchain technologies and smart contracts. Trade finance often operates in cross-border sale of goods arrangements. In these arrangements, there are normally four key stakeholders involved: the seller, the buyer, the seller's bank and the buyer's bank. These arrangements raise some concerns for the seller and the buyer. The seller wants to sell the goods to the buyer but is concerned that the buyer takes receipt of the goods but then never pays for them, so incurring considerable costs trying to enforce a claim for payment against the buyer. The buyer is concerned that if he pays for the goods before they are delivered then the seller may never deliver them. In order to mitigate against these concerns, the seller will require a buyer to pre-pay for the goods it has shipped and the buyer will pre-pay for them subject to obtaining proof that the goods have been shipped, so are in transit, such as a bill of lading.

It works as follows:

- The seller and the buyer sign the sale of goods contract.

- The buyer's bank issues a letter of credit guaranteeing payment of the goods to the seller's bank subject to certain conditions being met such as the bill of lading being provided by a certain date.

- The goods are then shipped, and the seller sends the buyer the bill of lading and then the buyer sends this to its bank who makes the payment subject to the terms of the letter of credit.

The challenge with this arrangement is that there are a number of different documents (e.g. the sale of goods contract, the bill of lading, the letter of credit) being shared in a number of different formats (e.g. by post, fax or electronic mail) by disparate parties who do not necessarily trust each other. Documents can be lost or arrive late (in which case the buyer's bank may refuse to make payment pursuant to the letter of credit) or be easily forged (e.g. forging a bill of lading to give the impression the goods have been shipped).

As a result, these stakeholders often expend a lot of time and money dealing with managing the documentation and disputes. As an alternative, these stakeholders are now looking at technologies like blockchain to streamline the process, taking advantage of the benefits of the technology: once data is recorded to the blockchain it can't easily be changed and smart contracts (deployed to the blockchain) can help automate certain steps in order to make the process more efficient.

It might work as follows:

- The trusted intermediary sets up a private blockchain (based on the distributed ledger model described above).

- The buyer, the seller and their banks access the private blockchain by accessing the app built by the trusted intermediary.

- The buyer sends the letter of credit for recording to the blockchain. The letter of credit refers to a smart contract which the parties to the letter of credit agree will implement certain obligations relating to letter of credit, in accordance with its terms.

- The smart contract is created and (once approved by the parties to the letter of credit) is deployed to the blockchain. The smart contract works on a simple if/then conditional: if the seller sends and records a bill of lading to the blockchain on or before the agreed date specified in the letter of credit and this is approved by the relevant consensus protocol on or before such agreed date, then the smart contract issues an instruction to the buyer's bank to send payment for the relevant goods to the seller's bank.

- The seller sends the bill of lading for recording to the blockchain (and if it is recorded on time then the buyer's bank is automatically instructed by the smart contract to pay the seller's bank).

Contracting for private blockchains

As mentioned above, enterprises are likely to be attracted to private blockchains over public blockchains for a number of reasons, including because there is greater certainty of the rules governing how these blockchain networks operate. These rules will be set out in contracts.

Generally, there are two main contracts:

- **Blockchain services contract:** this is the bilateral contract between the blockchain developer and the trusted intermediary. Under this contract, the blockchain developer will licence its blockchain software and provide support services to the trusted intermediary to help it set up the network and operate it.

- **Participation contracts:** these are the contracts that govern access to the blockchain network and are made between the trusted intermediary and each participant. Often, they comprise a bilateral technology agreement and a multilateral rulebook. The technology agreement governs the use of the blockchain technologies in order to enable the participant to send data for recording on the blockchain. It will deal with the usual types of issues you would expect to face when drafting or negotiating cloud services agreements: licence conditions, implementation, liabilities and indemnities (including in relation to loss or corruption of data), security, service levels, suspension and termination rights, access to data on termination or expiry and IP (see more on this in Section 10). The rule book is the set of terms between the trusted intermediary and each participant and between each participant. It will sit alongside the technology agreement and focuses on principles such as membership and eligibility criteria, the process for implementing changes to the rule book terms, general representations and warranties (e.g. not to use the blockchain network for any "prohibited purpose") and the process for how transactions are agreed to be validated and recorded to the blockchain.

It is important that any commitments made by the trusted intermediary (for example, availability service levels) under the technology agreement are appropriately backed off under the terms of the blockchain services contract.

Who owns IP in the blockchain?

At a basic level, the blockchain network will constitute the back-end blockchain software and the user-facing app.

The blockchain software determines how data is recorded on the distributed database. The user-facing app is what each participant accesses to send transactions for recording onto the blockchain and will interoperate with the blockchain software via application programming interfaces **(APIs)**.

The blockchain software will often be pre-existing software that is used by the blockchain developer to service multiple clients. The user-facing app will often be bespoke software developed by the blockchain developer for the trusted intermediary to solve its particular use case.

One of the key IP battlegrounds between the blockchain developer and trusted intermediary is who owns the IP in the user-facing app. Analogous to traditional software development agreements, there are commercial considerations for parties around various aspects of the IP in both the blockchain software and the user-facing app. Establishing the ownership and licence limitations of pre-existing IP and IP generated in the development of the blockchain network is fundamental and will likely be influenced to a greater or lesser degree by the level of customisation and bespoke design necessary to the creation of the app, in addition to any proposals to "white-label" the app. Further considerations around use of, and liability for, the incorporation of both third party and open source software into the development of the app should be addressed early in the development process. One potential middle-ground position is for the IP in the app to vest with the blockchain developer, but for the trusted intermediary to have a wide licence (for example, exclusive for a certain period of time) to use the IP in the app in order to use the blockchain network and also to modify the app for use with other blockchain networks (i.e. with another blockchain developer's software). For this to work, it is important that the app is developed in such a way to avoid "lock-in" with a particular blockchain developer's solution.

Conclusion

Critics of blockchains have described them as “a solution looking for a problem”. There is no doubt that blockchain is not the solution for every kind of problem. However, in some specific cases, a private blockchain may be useful because the technology makes it hard to edit data once it has been recorded on the blockchain; and, by virtue of the use of digital signatures, helps to bring together disparate parties for better coordination and sharing of data. In other cases, however, having a trusted central authority as the golden source of data is no bad thing, and can often be the best option. For example, people trust a government department such as HM Land Registry in the UK to run a central database for recording land and property ownership because they trust the UK government, and they trust the UK government to compensate anyone who suffers loss because of any error or omission in the central database. Sometimes centralised is better than decentralised.