Bird & Bird & Private Blockchains

Introduction

This briefing note summarises the basic principles relating to private blockchains: what are they, how do they work, why are they different to central databases and the legal issues to consider.

This note is high-level. For more in-depth content on a variety of blockchain topics, please visit our Blockchain in Focus webpage or download our 'Blockchains uncut' report.

What is a private blockchain?

In another briefing note (found on our Blockchain in Focus webpage) we summarised the basic principles relating to public blockchains. There are however a number of reasons why public blockchains may not be suitable for enterprises. For example, for privacy reasons it may not suit an enterprise for every participant on a blockchain to have access to its entire contents. Alternatively, participants may want more accountability on the running and operation of the blockchain, which is not possible with public blockchains where there is no entity in charge. Enterprises may therefore wish to set up a private blockchain.

Private blockchains are often referred to as 'permissioned' blockchains. Unlike public blockchains, where anyone can download the software, form a node, view the ledger and interact with the blockchain, private blockchains are often run and operated by an entity (the "**trusted intermediary**").

As the trusted intermediary is in charge of the running of the blockchain it will control who can access the private blockchain and may also control the type of access rights each participant has. For example, some participants may be restricted to viewing (some or all of) the data on the ledger , whereas others may also have permission to submit new transactions for recording on the blockchain.

How do private blockchains work?

Generally speaking, here's how it can work:

- Access to a private blockchain is controlled by a trusted intermediary.
- The trusted intermediary might be a joint venture entity or a company limited by guarantee, in each case, set up with the purpose of trying to solve a particular problem using blockchain technology. It will therefore comprise a number of interested parties who are shareholders/members in the joint venture entity/company limited by guarantee.
- The trusted intermediary will build the blockchain software (that will underpin the private blockchain) itself or will license it from a third party (e.g. Corda or ConsenSys). This software is used to set up nodes that form the private blockchain network and need to be accessed in order to participate.
- The trusted intermediary will run the core collection nodes itself or delegate the running of the nodes to subcontractors. This will help ensure continued availability of the blockchain.
- The nodes run by (or on behalf of) the trusted intermediary will be in charge of validating the transactions prior to them being recorded on the ledger (the "**Validator Nodes**").
- The trusted intermediary will build a software application ("**app**") that interfaces with the Validator Nodes via an API. The app will be accessed by participants and will enable them to send transactions for recording on the blockchain.
- Participants can access the private blockchain either by accessing the app on a software-as-a-service basis. In some cases, they may also be permitted to set up their own node (this node will not be able to perform the same tasks as the Validator Nodes, e.g. it will not be able to validate transactions).

Bird & Bird & Private Blockchains

Expanding on this summary, there are two main ways to set up a private blockchain:

1. **Distributed ledger model:** the trusted intermediary runs the Validator Nodes and participants interact with the private blockchain either by accessing: (1) the Validator Nodes via the app (access by participant X in the diagram below); or (2) their own operated node via the app (access by participant Y in the diagram below (where they are accessing part of the ledger covering data relevant to them only).
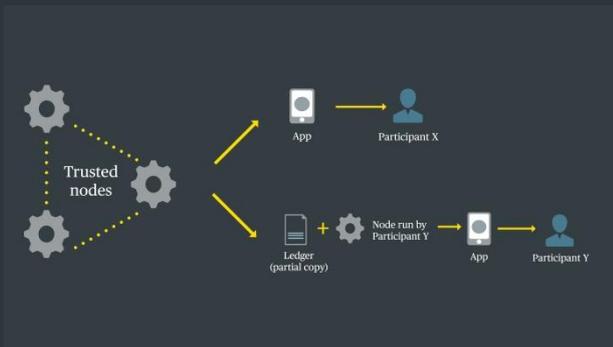
Distributed ledger model

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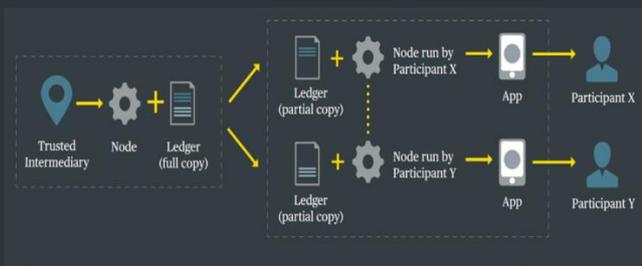
Shared ledger model

Private blockchain or centralised database?

As you can see from the two examples above, both private blockchain models require the presence of a trusted intermediary, this raises the question as to how a private blockchain is different from a traditional database controlled by a central authority (such as the Her Majesty's Land Registry which controls the records of property ownership in the UK). Aren't we just swapping one central authority for another? This is not an unfair comparison on the face of things, however it ignores some of the intrinsic features of blockchain technology that make private blockchains preferable to centralised databases in certain circumstances.

For example:

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

- **Digital signatures:** the use of digital signatures makes it easier for parties that don't know or trust each other to approve and send transaction data for recording on to the blockchain without third party involvement. This makes it easier to coordinate input from disparate parties.

Bird & Bird & Private Blockchains

Private blockchain use cases

Below are just a few examples of how private blockchain technology can be deployed. For a more detailed breakdown, please see our 'Blockchain: Use Case' briefing note, found on our [Blockchain in Focus webpage.](#)

- **Business-to-business communication:** the deployment of private blockchains as a method of storing and viewing information both within and between organisations offers a more secure way of information transmission. Due to the immutability and cryptographic security of blockchain technology, counterparties to a transaction could use a private blockchain as a method of sending confidential information that ensures its integrity, as an alternative to courier or email.

- **'Track and trace' in a supply chain:** private blockchains can be set up to track each stage of delivery of goods relating to a supply chain. For example, a supermarket may act as the trusted intermediary and establish a private blockchain. Farmers will act as participants and send transactions for recording on this blockchain (e.g. produce delivered to the supermarket's warehouse). The private blockchain will contain the data entries from each stage of the supply chain, allowing the supermarket to more easily track and verify a pallet of goods from pick-up of the goods from the farm to their delivery to the supermarket shelves.

Legal issues associated with blockchain:

There are two key areas to consider. The commercial contract workstream and the corporate workstream.

Under the commercial contract workstream, there are a variety of contracts for the trusted intermediary to consider:

- **Blockchain services agreement:** if it is licensing the blockchain software from a third party, the trusted intermediary will need to have in place an appropriate blockchain licence and services agreement governing the rights to use the software and provision of ancillary services.
- **Subcontracts:** the trusted intermediary will need to have in place contracts with the subcontractors it uses to operate the Validator Nodes. These will include a variety of responsibilities on the subcontractors to help ensure availability of the blockchain.
- **Cloud services agreement:** there will need to be a simple access agreement governing each participant's access to the private blockchain.

Under the corporate workstream, there are a variety of issues to consider. For example:

- **Constitutional documentation:** the trusted intermediary's articles of association and shareholders agreement will need to carefully consider the rules governing how the blockchain will be run. This may also include the rules governing how the private blockchain will be run, although this will often be a separate document signed by all shareholders.

- **IP ownership:** if the blockchain software or the app is being developed in-house, based on feedback from the shareholders, then they should be asked to sign up to a separate IP agreement making it clear that the shareholders will assign any IPRs created as part of their collaboration to the trusted intermediary.

Bird & Bird & Private Blockchains

For more information or a free initial meeting, please contact:

Key contacts

Jonathan Emmanuel
Partner

Tel: +442074156052
jonathan.emmanuel@twobirds.com

Gavin Punia
Senior Associate

Tel: +442030176884
gavin.punia@twobirds.com

Ash Shah
Associate

Tel: +442074156606
ash.shah@twobirds.com

Thomas Hepplewhite
Associate

Tel: +442074156777
tom.hepplewhite@twobirds.com

Charles Hill
Trainee Solicitor

Tel: +442074156745
charles.hill@twobirds.com

The firm is at the forefront of some of the most cutting-edge mandates in the area, advising on innovative matters in payments, crowdfunding, open banking and blockchain.

Chambers FinTech UK, 2020

twobirds.com

Abu Dhabi & Amsterdam & Beijing & Bratislava & Brussels & Budapest & Copenhagen & Dubai & Dusseldorf & Frankfurt & The Hague & Hamburg & Helsinki & Hong Kong & London & Luxembourg & Lyon & Madrid & Milan & Munich & Paris & Prague & Rome & San Francisco & Shanghai & Singapore & Stockholm & Sydney & Warsaw