Bird & Bird & Public Blockchains

Introduction

This note first explains the basics of blockchain technology and then, more specifically, public blockchain technology. It also summarises some of public blockchain technology's advantages and related legal issues.

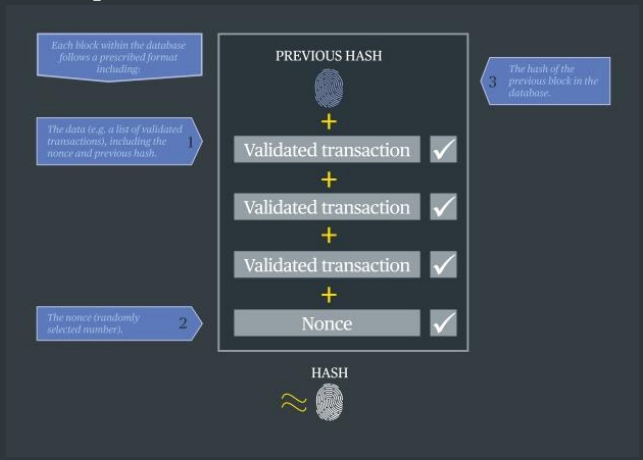
This note is high-level. For more in-depth content on a variety of blockchain topics, please visit our Blockchain in Focus webpage or download our 'Blockchains uncut' report.

Blockchain technology

What is a blockchain?

There is no one "the" blockchain, just as there is no one "the" internet or "the" database. There are different blockchain varieties, suitable for different use cases. At one end of the spectrum are public blockchains (e.g. the public Bitcoin blockchain), and at the other end are private blockchains (e.g. R3's Corda Enterprise). Despite these variances, blockchains often share some common features. For example:

- a blockchain is a ledger that comprises a list of the transactions that have been validated by a peer-to-peer network;
- the list of transactions is recorded in blocks of data that are time-stamped and are structured in a prescribed format; and
- each block is linked to the next forming an uninterrupted chain of record (hence the phrase, "blockchain").



Public blockchain technology

What is a public blockchain?

In this note we use the example of the public Bitcoin blockchain ("**Bitcoin Blockchain**"), as this is the most well-known example of a public blockchain.

The Bitcoin Blockchain is fully decentralised, meaning that access and control over the ledger and its contents isn't restricted to a single, always available, central authority that manages it (e.g. Her Majesty's Land Registry which controls the ledger of property records in the United Kingdom). In fact, there is no one in charge of the running and operation of this blockchain.

As no one is in charge, there is no need for a person to get permission to access the Bitcoin Blockchain to participate. Instead, any person ("**the participant**") is able to interact with this blockchain either by setting up his own node (a computer that has downloaded the relevant Bitcoin Blockchain software, including the latest copy of the ledger) or by interacting with the Bitcoin Blockchain via a third party operated node.

Once a node has been set up it connects with other nodes over the internet. The collection of these connected nodes comprises the Bitcoin Blockchain. As no one is in charge of the Bitcoin Blockchain each node in this blockchain is called a "peer" treated as equal in status to any other node. If one node is corrupted then the other nodes continue to operate and provide access to the ledger.

Once a participant has set up a node or has access to a third party operated node he can access a copy of the ledger and submit new transactions for recording on the blockchain. For the Bitcoin Blockchain the ledger is the record of every validated Bitcoin payment instruction.

Bird & Bird & Public Blockchains

How does it work?

Each participant in the Bitcoin Blockchain uses an **account** to connect to a node in order to interact with the blockchain. Think of it like a bank account that's used to send/receive money. Accounts are stored in software applications called **wallets**. An account comprises a pair of **cryptographic keys**, one **public** (which is shared with the blockchain) and one **private** (which should not be shared). These keys comprise a string of numbers that are mathematically related and generated as a pair. The public key is used to create a **Bitcoin address**. This address operates like a bank account number so participants know where Bitcoins can be sent to. The private key is like a password used to access the account to interact with the blockchain.

We've summarised below the key steps involved in sending a transaction for recording on the Bitcoin Blockchain (e.g. X participant sends Bitcoin to Y participant):

1. X logs-in to his wallet and accesses one of his accounts, which stores some Bitcoin.
2. X accesses his account and creates a transaction. The transaction includes information on the amount of Bitcoin being sent and X's and Y's Bitcoin addresses so it's clear where the Bitcoin is being sent from/to.
3. The transaction is then approved by X by being digitally signed by X using his private key (creating a digital signature).
4. The transaction is then broadcast over the internet with the digital signature from X's wallet to nearby nodes.
5. A node that receives the transaction and digital signature needs to check it is valid. First, it needs to check it has been approved by X. It applies the public key for X's account against the digital signature. (The node knows which public key to apply as the transaction provides information on X's Bitcoin address which is derived from his public key, which has been shared with the network.) This decrypts the digital signature to reveal the transaction data. If this revealed transaction data matches the transaction sent with the digital signature, then the node can be confident that X approved it. A node will also perform other checks in accordance with the blockchain protocol to check the transaction is valid (e.g. checking X owns the Bitcoins it is attempting to spend).
6. If the node considers the transaction is valid, it shares the transaction with other nearby nodes. The other nodes follow the same process, ensuring eventual propagation of the validated transaction to all nodes.
7. Mining nodes (nodes that have downloaded special "mining" software) will come across the validated transaction and compete with other mining nodes to pack it with other validated transactions in a block and be the first to create a valid block. The rules governing how the network agrees on what data gets recorded in a valid block on the blockchain is called the consensus protocol. There are different consensus protocols available for different blockchains. The consensus protocol for the Bitcoin Blockchain is called "proof of work". Once this phase is complete, the transaction is added to the blockchain as a new block.

For more details on the validation and mining process, please see our 'Blockchains uncut' report.

Bird & Bird & Public Blockchains

What are the advantages of blockchain?

Here are some of the advantages of a public blockchain network over a traditional centralised database:

- Immutable: it is very hard to interfere with data in existing valid blocks without the change being obvious to all parties and therefore rejected. This means participants can be confident they can trust the data recorded in the blockchain, rather than have to trust a central authority to properly manage data entries.
- Decentralised and trustless: participants do not need to rely on a trusted central authority to set up accounts. Instead, they rely on cryptographic keys, that they can generate themselves, to participate. Participants also do not need to rely on a central authority to maintain the ledger as anyone can set up a node and download the same ledger and create and send transactions and the blockchain's protocol determines when transactions are recorded onto the ledger. The absence of a central authority cuts costs and increases efficiencies.
- Security: public/private key cryptography (used to set up an account) is very secure.
- Peer-to-peer: because the 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 server where the network could go down if the server is unavailable.

Legal issues associated with blockchain:

Here are examples of some of the legal issues enterprises commonly encounter with the deployment of public blockchain technology:

- Data Protection: the General Data Protection Regulation (GDPR), which sets out the European legal framework for processing personal data, was not drafted with blockchain technologies in mind and so there are some conflicts between some GDPR principles and the features of some blockchains. For example, the GDPR requires companies operating in the EU to be able to delete or update personal data. Individuals also have the right to be forgotten. However, if personal data is recorded on a blockchain, it is not clear how these requirements can be complied with given the immutable nature of blockchains. Some proposals have been issued (e.g. by the French Data Protection Authority), however, they do not necessarily solve the conflict but merely mitigate its impact. For now (and until further guidance on this point is published by regulators), the law and technology are in conflict.
- Intellectual Property: IP is of particular importance in relation to the software underpinning a blockchain network. Most public blockchains are built on open source software. Enterprises may try to customise this software to create their own private blockchain or build user facing apps on top of the software. In both circumstances, careful analysis of the underlying open source software licence terms should be undertaken so organisations are not placed in difficult situations where they are forced to license their customisations or apps to the public in circumstances where they thought they owned the IP and were free to commercialise it on licence terms of their choosing.

Bird & Bird & Public Blockchains

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

Key contacts

Jonathan Emmanuel
Partner

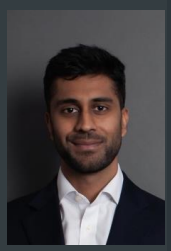
Tel: +442074156052
jonathan.emmanuel@twobirds.com

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