

"FASTER" PAYMENTS

The race for the fastest payment



Introduction

Cryptocurrencies and related technologies continue to attract interest in the payments sector but regulators and central banks are no longer in the dark about Bitcoin and its offshoots. This article looks at the current situation, how regulation is catching up with the technology, and how to ensure that participants can continue to develop in a regulated environment.

The use of blockchain technologies and distributed ledger technologies has developed, particularly in the cross border payments space (in this article, references to **DLT** include both blockchain and distributed ledger technology). In the last year, FinTechs, banks, central banks (including the "old person" of Threadneedle Street), card networks and SWIFT have confirmed their interest in DLT, with various proof-of-concepts being tested.

In this article, we look at the commercial developments in this area and related regulatory and contractual issues which are increasingly being discussed as DLT propositions are brought to market:

1. DLT

2. What's disruptive?

- ▶ Innovations in DLT
- ▶ Using DLT to innovate in other markets
- ▶ In payments

3. Points of interest

- ▶ Financial services regulation
- ▶ Consumer protection
- ▶ Anti-money laundering
- ▶ Smart contracts
- ▶ Data protection

1. DLT

DLT enables data storage structure with no central authority. The data is maintained and replicated across a decentralised network of data storage sites (known as "nodes").

Each node has a full copy of the relevant data and is constantly updating the data such that each node will have a verified and complete copy of the data at all times, ensuring maximum integrity and resilience of the data.

In the case of blockchain, the data is stored in encrypted blocks. New data is added to the blocks using a complex (and cryptographically secure) maths equation. No block can be changed until all the nodes agree that there is a complete and verified "chain" of data in each block that is verified by solving the complex maths equation proving the transaction (aka mining) – so "blockchain".

Any participant can see the data and the transaction history in relation to such data at any time. The integrity of the data is underwritten by the maths and therefore does not require the participants to "trust" each other. DLT is therefore frequently referred to as "trustless".

Because transaction integrity is mathematical rather than based around trusted participants, costs are reduced and the settlement cycles, potential speed of transfer, efficiencies and removal of intermediation are much shorter. However, each time a transaction is added to a block, the maths gets more complicated and this can slow a transaction down.

The UK regulators have taken a technology neutral approach to regulation, meaning that DLT is not currently regulated as a methodology. Having said that, there is increased focus on the use of the methodology in regulated markets to ensure that DLT and crypto produce regulatory compliant outcomes for participants.

2. What's disruptive?

Many of the early innovators in payments aimed to disrupt these markets through increasing speed of transaction and settlement (such as Ripple); but disruptors have moved on to other areas of banking, such as asset management, securities and trade finance, but the last year has seen a new focus on consumer facing applications and payments.

The players in this space can roughly be divided into two categories: (1) those innovating to improve DLT for its current purposes (i.e. transactions using crypto-assets); and (2) those exploring the idea that DLT can improve the security, speed and costs in other markets, such as currency transfers and cross-border payments.

Innovations in DLT

The crypto-market is crystallising around the BitCoin and Ethereum platforms, but there are challenges, including in connecting these to legacy financial and banking systems and processing lag time for a transaction. As a result, a number of firms have focused on smoothing out these difficulties, with a view to increasing saleability for enterprise rather than just individuals.

For example:

- ▶ Havven has developed a dual token to **reduce price volatility**, the fees from transactions within the system are used to collateralise the network and establish an asset-backed, more stable, token;
- ▶ BlockEx is in the FCA's latest Sandbox cohort, and developing a proposition for blockchain based assets. It aims to **manage each stage of the asset's lifecycle** from the marketing of initial coin offerings to clearing and settlement using APIs; and
- ▶ 20|30, also in the Sandbox, have a number of propositions on the route to market, including CryptX index which aims to be an industry leading benchmark for all crypto-currencies and so create a **uniform pricing standard**.

The regulators are interested in the development of solutions to the particular challenges faced by existing DLT participants and which could act as disincentives to other players. Key focuses include improving liquidity, platform functionality and exchange both between crypto-assets and as against external goods and services or fiat currencies. The FCA is supporting these initiatives in the Sandbox.

Using DLT to innovate in other markets

There are a number of firms using DLT to solve problems which exist in other markets. These applications include using DLT to harmonise governance rules for decentralised platforms, improve efficiency in business processes and reduce transaction costs, automate intermediary roles and improve financial inclusion.

For example:

- ▶ Natwest is developing a platform which uses **smart contracts to codify a common set of governance rules** for participants to run decentralised technologies on;
 - ▶ Community First Credit Union is developing a DLT token to support customers who lack traditional forms of identification to **help them access bank account services** in the UK; and
- Etherisc is developing a service using smart contracts on the blockchain to provide completely **automated and decentralised insurance** products.

In payments

More than 75 of the largest banks (including Société Générale, Santander, JPMorgan, Royal Bank of Canada and ANZ) have joined the Interbank Information Network (**IIN**) to see if DLT can speed up problematic payments. IIN utilises a mutually accessible ledger to permit banks to carry on compliance checks and resolve issues around missing data in real time allowing for quicker issue resolution.

Other examples:

- ▶ **MasterCard** launched a business-to-business blockchain network for cross-border payments. The service aims to enable clearing of credit card transactions, eliminate administration tasks using smart contract rules and increase the speed of transaction settlement;
- ▶ **Visa** applied blockchain technology to its Visa B2B Connect payment platform; and
- ▶ **American Express** has also used DLT and filed a patent in the US related to the use of blockchain in payment transactions. The filing describes a solution to receive requests for payment, which would then be approved or rejected based on a risk analysis. If approved, the platform would automate processing and adjust accounts on both ends of the transaction.

3. Points of interest

Financial services regulation

The expansion of technology and other non-financial services companies into the regulated payments sector has resulted in increasing engagement from regulators. Financial services legislation and regulatory standards pre-date the rapid advances in DLT, but the FCA and other European regulators have publicly announced their support and launched initiatives to encourage innovation in this area. This is in contrast to a more cautious approach to crypto-assets.

DLT and crypto-assets are not specifically regulated (yet) in the UK (though a recent Treasury Committee report means we have moved a step closer to regulation of crypto-assets). However, the existing regulatory regime can be applicable, for example, to initial coin offerings (**ICOs**).

Many ICOs are outside of the regulatory regime. However, the answer to the question of whether a particular ICO is regulated depends on how the tokens are structured and some tokens may be regulated investments (meaning that issuing, selling or marketing them may involve regulated activities). Examples include transferable securities, collective investment schemes, crowdfunding, e-money or payment services. Certain characteristics might make a token more or less likely to be regulated. For example, where the token is not transferable and has no inherent value then, on a spectrum of risk, it is less likely to be a regulated investment.

Even if a token is not regulated at the point of issuance, tokens could become regulated investments at a later stage because they become regulated or there is a change in law or interpretation.

Consumer protection

As the practical application of DLT develops, firms are moving closer and closer to direct provision of their services to consumers (as some, such as wallet providers, already do). The recent Treasury Committee report calls for enhanced protection for consumers but it should be noted that the Consumer Rights Act 2015 (**CRA**) already applies to digital content provided to consumers.

The amendments to EU consumer rights legislation which have been consulted on at a high level and are now being discussed by European Parliament could extend more fulsome protections to free digital content (which currently only apply to digital content that has been paid for).

This would mean that:

- ▶ contracts with consumers will be subject to implied terms about the satisfactory quality of the digital content and that it will match the suppliers description of what it is and what it can do; and
- ▶ the consumer would have access to various remedies if the digital content does not confirm to the contract (including the implied terms) such as a right to the repair or replacement of the digital content (this is in addition to any other remedies outside of the CRA e.g. claiming damages etc.).

Currently if any free or paid for digital content causes damage to a device or other digital content belonging to the consumer and is of a kind that would not have occurred if the supplier had exercised reasonable care and skill then the consumer can require the supplier to repair the damage or provide compensation.

Anti-money laundering

The fifth anti-money laundering directive (Directive 2018/843) (**AMLD5**), extends EU anti-money laundering requirements to:

- ▶ providers engaged in exchange services between virtual currencies and fiat currencies (**VX Providers**); and
- ▶ entities providing services for the safeguarding of private cryptographic keys on behalf of customers, to hold, store and transfer virtual currencies (**custodian wallet providers** or **CWPs**).

This perhaps represents the start of a regulatory creep into cryptocurrencies and associated services. In explaining the rationale for the introduction of AMLD5, there are some interesting comments made on the issues the amendments aim to solve and virtual currencies more generally. In particular, as users of virtual currencies can also transact without the use of VX Providers and CWPs there is a suggestion that the risk resulting from this functionality should be "combatted" by ensuring that national bodies can obtain information allowing them to associate virtual currency addresses to the identity of the owner of the virtual currency.

Smart contracts

Innovations which use DLT feature a smart contract. A smart contract is a computerised process which automates the execution of a contract using DLT to record and execute the transaction. There is a spectrum of smart contract models which range from coding the entirety of a natural language contract (the "code is the contract" approach) to coding to perform a specific process (whether or not that is linked to a natural language contract). Some firms propose a split contract model under which a natural language contract is connected to code which will automatically execute certain elements of it such as payment.

The automated nature of smart contracts bring with it benefits including increased efficiency, reduction in transaction costs and increased transparency but there are also legal issues to consider. These include:

- ▶ **enforceability** – as smart contracts run automatically without user intervention, thought should be given as to how the basic requirements for a contract to exist of offer, acceptance, consideration and intention to create legal relations to are met. One example of an area where issues may arise is "follow-on" contracts. These are further, separate contracts which the parties are entered into automatically by the code in certain conditions and therefore the analysis of how the criteria for a legally binding contract to exist will need consider the lack of human intervention.
- ▶ **unilateral nature** - smart contracts are designed to behave in a particular way in particular circumstances which means they are likely to be unilateral in nature. A unilateral nature means that the terms are likely to not be negotiable and if the contract is with a consumer, care needs to be taken to ensure that the code behaves in a way which complies with the CRA;
- ▶ **dispute resolution** - smart contracts need to ensure they have adequate processes to effectively resolve disputes, whether arising as a result of disagreement over the intent of the parties, bugs in the code or external factors. This is particularly relevant where the smart contract has no central authority to administer it or if it is impossible to unwind a transaction without agreement of all of the participants even if the direct parties wish for this;
- ▶ **electronic execution** – the current law around electronic execution of contracts primarily deals with contracts which are available in an electronic format but smart contract technology goes further than this because it is a purely electronic process. The English courts have generally been accommodating in relation to the use of electronic signatures and this approach may be carried over to smart contracts but the enforceability of smart contracts has not yet been determined. Contracting by electronic means can also be an issue in other jurisdictions;
- ▶ **unintended consequences** - the lack of flexibility and practical difficulties of implementing new code into a smart contract can give rise to problems if circumstances change and a different outcome is desired compared to when the smart contract was entered into; and
- ▶ **immutability** – writing code with no flaws is difficult and, in the context of smart contracts, flaws in the code can cause significant issues. A notable example of this is the Decentralized Autonomous Organisation (**DAO**) case – the DAO was a smart contract for decentralised investments which lost more than half its value in two days in June 2016 because its code was exploited and Ether (the cryptocurrency the DAO held to invest) fell in value as a result.

Data protection

The General Data Protection Regulation (Regulation 2016/679) (**GDPR**) is now in force (and supported in the UK by the Data Protection Act 2018 (**DPA 2018**)). The issues which arise in the context of DLT under the GDPR and DPA 2018 include:

- ▶ **cross-border transfers of personal data** – the decentralised nature of DLT means that the data held on it exists in many places at the same time. To the extent personal data within the EEA is transferred outside of the EEA, that transfer will need to comply with the rules on transfers of data to third countries;
- ▶ **rights of data subjects** – the GDPR provides a number of rights to data subjects which include a right to have a data controller rectify inaccurate personal data and a right to have personal data erased (provided certain conditions are met). The data controller also has an obligation to keep only up to date, accurate and proportionate information pertaining to the data subject. The immutable nature of DLT can cause conflict with these rules; and
- ▶ **allocation of responsibilities** – DLT is decentralised and this may cause tension about how responsibilities and the costs of compliance with data protection legislation are allocated across the nodes.

Conclusion

This article tries to highlight some of the recent DLT initiatives and some of the legal issues arising from them. This area is unexplored and constantly changing. The benefits these initiatives can bring both in terms of addressing issues with cryptocurrencies and using DLT to solve problems in other markets are attractive and it is expected that innovation using DLT will continue. However, as is often the case with new innovations, there are a number of issues which businesses (and particularly those in regulated sectors) will need to consider before adopting them.

If you have any questions please contact:



WILL JAMES
Partner, Head of Payments
020 7880 5771
07831652807
william.james@addleshawgoddard.com



JACK HOUSELANDER
Associate
0207 788 5147
07864248047
jack.houselander@addleshawgoddard.com



JENNIFER CUTTING
Associate
0207 788 5111
07802 338650
jennifer.cutting@addleshawgoddard.com

addleshawgoddard.com

Aberdeen, Doha, Dubai, Edinburgh, Glasgow, Hong Kong, Leeds, London, Manchester, Muscat, Singapore and Tokyo*

*a formal alliance with Hashidate Law Office

© 2018 Addleshaw Goddard LLP. All rights reserved. Extracts may be copied with prior permission and provided their source is acknowledged. This document is for general information only. It is not legal advice and should not be acted or relied on as being so, accordingly Addleshaw Goddard disclaims any responsibility. It does not create a solicitor-client relationship between Addleshaw Goddard and any other person. Legal advice should be taken before applying any information in this document to any facts and circumstances. Addleshaw Goddard is an international legal practice carried on by Addleshaw Goddard LLP (a limited liability partnership registered in England & Wales and authorised and regulated by the Solicitors Regulation Authority and the Law Society of Scotland) and its affiliated undertakings. Addleshaw Goddard operates in the Dubai International Financial Centre through Addleshaw Goddard (Middle East) LLP (registered with and regulated by the DFSA), in the Qatar Financial Centre through Addleshaw Goddard (GCC) LLP (licensed by the QFCA), in Oman through Addleshaw Goddard (Middle East) LLP in association with Nasser Al Habsi & Saif Al Mamari Law Firm (licensed by the Oman Ministry of Justice) and in Hong Kong through Addleshaw Goddard (Hong Kong) LLP, a Hong Kong limited liability partnership pursuant to the Legal Practitioners Ordinance and regulated by the Law Society of Hong Kong. In Tokyo, legal services are offered through Addleshaw Goddard's formal alliance with Hashidate Law Office. A list of members/principals for each firm will be provided upon request. The term partner refers to any individual who is a member of any Addleshaw Goddard entity or association or an employee or consultant with equivalent standing and qualifications. If you prefer not to receive promotional material from us, please email us at unsubscribe@addleshawgoddard.com. For further information please consult our website www.addleshawgoddard.com or www.aglaw.com.