MAYER·BROWN

Blockchain for Business

By Authors Rohith P. George, Brad L. Peterson, Oliver Yaros, David L. Beam, Julian M. Dibbell, and Riley C. Moore[1]

Introduction

Interest in blockchain has grown dramatically, with a rapid increase in investment and engagement. Over the course of 2017, numerous companies in financial, automotive, healthcare, insurance, real estate, retail, and other sectors have developed sophisticated proof-of-concepts and some are on the path to significant production deployments.

Despite the increasing attention to blockchain, the topic remains novel for many business lawyers. As companies begin to explore blockchain, however, it is increasingly important for lawyers to be able to spot the right issues and ask the right questions. In light of this, our goal is to introduce blockchain in simple terms, provide example use cases, and highlight some of the most pressing legal issues.

What Is Blockchain?

Blockchain technology was first implemented in 2009 as the underlying platform designed to solve the "double-spending" problem for Bitcoin (that is, how to transfer digital value without relying on a trusted third party). However, the attributes that make blockchain technology essential for Bitcoin can be used to solve a variety of other problems. A blockchain is:

A digital ledger representing a history of transactions,

That is distributed on computers (also called "nodes") operated by different participants,

That allows participants to introduce records with cryptographic protection that are validated and immutable.

The records in a blockchain are immutable because information in the digital ledger is stored in blocks of data that are represented by a unique cryptographic identifier (or "hash"). Each subsequent block of data includes the hash of the prior block to create a chain that links all the way back to the first block of data (hence "blockchain"). If data in any block in the chain is later illicitly altered in any node's version of the ledger, the hash for that and every subsequent block must change, making such altered ledger readily identifiable as an illicit version. That illicit version is then rejected by consensus among the nodes.

A feature of some blockchains is the capability to create "smart contracts." For example, the Ethereum and Hyperledger blockchain platforms permit the recording of software programs within a block on the blockchain itself. This software automatically performs certain actions on the blockchain when a prescribed condition is met. As an example, a supplier who today ships goods to a customer, sends an invoice, and waits 30, 45, or 90 days for payment would prefer to have the order in a "smart contract" that pays automatically when

the customer acknowledges receipt of goods on the blockchain. Alternatively, the software can trigger payment based on data from an outside source, referred to as an "oracle." For example, "parametric" travel insurance could pay automatically if an airline cancels a flight, with the airline's flight records being the "oracle."

Where Can Blockchain Be Useful?

Because of the shared and immutable nature of information stored on a blockchain, blockchains can be expected to drive the most value for businesses by solving problems in maintaining consistency of records between multiple entities, maintaining auditable information trails, efficiently settling and tracking exchanges of value, and authenticating user identity.

At this point, commercial blockchain is largely in the pilot or proof-of-concept stage across a wide range of use cases. Payments and supply chain are two of the most promising use cases.

Payments

With the rise in global business and trade, financial institutions are focused on optimizing cross-border payment inefficiencies. Current protocols require correspondent banking relationships and include intermediaries, resulting in high fees and inordinate delays. Using a blockchain to handle such payments can permit a bilateral, immutable transfer of value while reducing the fees charged and delays caused by existing processes. A number of financial institutions have announced pilots testing such blockchain solutions. In addition, the R3 and Hyperledger consortia are each working towards creating blockchain standards for payment and other financial sector use cases.

Supply Chain

- Current supply chain processes rely on non-standardized paper and digital records held among various parties, often resulting in minimal or delayed ability to pinpoint where problems arise in the supply chain.
- Diamond companies are testing an industry-wide blockchain that allows suppliers to record each movement of a diamond, tracking its conflict status.
- Retail and e-commerce companies are developing in-house blockchains to similarly track authenticity of goods they sell and combat counterfeiting.
- Transport and logistics companies have tested using blockchain to track freight, reduce delays, and replace related paper processes with on-chain records.[2]
- A number of food giants have partnered with IBM to use blockchain to track foodstuffs from farm to store.

Possible Legal Issues

We set out possible legal issues below, including (i) issues that can be partially or wholly addressed by the way that the blockchain is designed, (ii) issues that can be partially or wholly addressed by a separate off-chain agreement among participants, and (iii) other issues to be weighed in determining whether to implement a blockchain solution.

Legal Issues to Address in On-Chain Programming

Confidentiality Requirements. In a "permissionless" blockchain, data can be viewed by anyone on the Internet. For some applications, such as an online database to prove auto insurance coverage, that may be preferred. If there are obligations of confidentiality, however, the blockchain may be "permissioned" (so that participation is limited by either having an administrator determine ability to participate or having objective requirements that must be met to participate) and can limit viewing of the full record only to specific participants.

Accountability Requirements. Many public blockchains allow people to become participants

and engage in transactions by revealing only their public key (as is the case with Bitcoin). However, if the use case requires that a known person be accountable for what is placed on the blockchain, the blockchain or its governing body can require proof of identify before a participant is provided access. The blockchain might then require that the participant's identity be visible to transactional counterparties, to trusted nodes, or to all participants, as applicable.

Data Privacy. Blockchains have key challenges in relation to data privacy laws. For example, a node in a non-EU country recording a block in the chain that includes personal data of an EU resident may be considered a cross-border transfer of personal data. As another example, recording personal data in an "immutable" ledger may violate a right for data subjects to require that their data be removed (the "right to be forgotten"). The blockchain could be designed to encrypt the personal data with an encryption key that can be forgotten or to store the personal data off-chain in a database permitting deletion with only links to such data stored on-chain.

Legal Issues to Address in Off-Chain Agreements

Design, Build, and Run. A blockchain must be designed and financed by a team with deep understanding of the use and may be implemented using software developers on a licensed or subscription platform—a large effort involving numerous contracts.

Amendments and Modifications. A blockchain may need to adapt to survive and maintain its usefulness. For permissionless blockchains, success may depend on whether the participants can make the right modifications through consensus. For permissioned blockchains, however, the founders can formalize the governance process off-chain via a separate, manually signed, natural-language agreement. In that off-chain agreement, the consortium or founding participants can set rules and principles for how to come to agreement (or designate trust in an administrator) to modify the blockchain's programming.

Allocation of Liability. A participant may be damaged, for example, by a vulnerability in the underlying technology, an issue with one of the nodes, a participant's failure to protect their private keys, or an issue involving the way an external system integrates or operates with the blockchain. The law is at best unclear on whether the damaged participant would have a claim against other participants, the programmers, the technology providers or others. Blockchain consortia can address this problem by requiring participants to enter into a legally binding off-chain agreement that allocates responsibility and liability.

Jurisdiction, Governing Law, and Dispute Resolution. Blockchains, by definition, involve numerous nodes keeping simultaneous copies of the digital ledger in their own hosting locations, which may be in separate countries. Each node may participate in the process of creating consensus and recording information to the blockchain. Thus, it is not clear which country(ies) have jurisdiction or what law(s) govern. Again, a consortium or founding group can stipulate the governing law, jurisdiction and the agreed dispute resolution process (such as arbitration) for all participants in the off-chain agreement.

Smart Contracts. A "smart contract" is made up entirely of code. While one might argue that the digital interaction between "smart contract" software and a participant (or a participant's software) constitutes offer and acceptance and a legally binding contract, this would be a legally novel interpretation of traditional contract formalities. Until regulators decide how to approach this technological advancement (as they have had to do in the case of e-signatures, electronic contracts, clickwrap agreements, and other deviations from traditional contract formalities), a "smart contract" could be

supported by appropriate off-chain natural language contracts. At that point, it will be critical to verify that the "smart contract" code actually carries forward the legal effect of the traditional contract.

Oracles. There is a risk that the oracle is incorrect, inaccurate, or ambiguous. In such scenarios, companies may document how such inaccuracies are to be handled and how risk and liability is allocated in such events in the off-chain agreement.

Other Issues

Distributed Autonomous Organizations. Some view a blockchain operating independently of a consortium as a distributed autonomous organization (DAO) consisting of code running on distributed servers. A key question in participating in a DAO is whether participants have any recourse against anyone for the actions of the DAO.

Functionality Limitations. Blockchain is an emerging technology with potential functionality limitations. For example, currently many blockchains have limited capability to perform advanced searches or otherwise retrieve information stored on-chain. Companies should weigh these limitations against the advantages gained, at least until the limitations are addressed.

Integration. Commercial blockchain will require the communication of data to and from each blockchain. Currently interoperability between blockchains is limited and few interfaces have been built to ERP systems and systems of record. Solving this problem will require participants to agree on technical standards and software providers to build interfaces.

Antitrust. Consortia created for the purposes of arriving at common technical standards and frameworks for industry blockchains might be viewed as improper collusion between the participants or as resulting in anti-competitive effects. For example, in a permissioned network, industry competitors who are not included may be disadvantaged. Antitrust and competition law advice are thus essential.

Endnotes

[1] Rohith George is a partner in the Technology Transactions practice in Mayer Brown's Palo Alto office. Brad Peterson is a partner in Mayer Brown's Chicago office. He leads the Technology Transactions practice. Oliver Yaros is a partner in the Intellectual Property & IT Group of the London office, having joined Mayer Brown as a trainee in 2004 and admitted to practice in 2006. David Beam is a partner in Mayer Brown's Washington, DC office. He is a member of the firm's Financial Services Regulatory & Enforcement group. Julian Dibbell is an associate in Mayer Brown's Chicago office and a member of the Technology Transactions practice. Riley Moore is an associate in Mayer Brown's Technology Transactions and Corporate & Securities practice.

[2] https://techcrunch.com/2018/03/02/blockchain-will-work-in-trucking-but-onlyif-these-three-things-happen/