3 Three examples

of blockchain smart contracts – Internet of Things, commercial paper and daos

For thousands of years, society has recorded information in ledgers, ranging from clay tablets, books through to cloud based computer systems. Despite the advance of technology, all of these ledgers have effectively been siloed with access (or "permission") to write and read information generally being restricted.

Blockchain is a new technology that flips the traditional model of a ledger upside down. Rather than have multiple separate silos, a blockchain (in its purest form) can act as a unified database that's accessible (on a read and write basis) by everyone (it is in effect "permissionless"). The ledger stored on a blockchain is shared amongst a distributed network of computers. The use of cryptography enables users to modify the master ledger without the need for a central authority.

It is the distributed nature of the ledger that is such a powerful idea and which causes some to think that the blockchain will be as revolutionary as the internet. As noted above, with a blockchain there is no need for a central trusted authority or for intermediaries. The disintermediation of intermediaries could redefine the value chain in a wide range of industries, from financial services to media, and puts the power and value of data back in the hands of the people creating that data. Blockchains can be public (such as the Bitcoin blockchain or the Ethereum blockchain) – these are effectively permissionless, or they can be private (where access is restricted to a selected group of users).

Other arguments in favour of the use of blockchains has been the argument that they are immutable (i.e. cannot be altered) and the distributed nature of the network means that it is practically impossible to hack. However, as we will see this is not necessarily the case.

One of the most exciting areas of development are smart contracts built using blockchain technology. A "smart contract" is computer code that self-executes the terms of a contract – this is not a new idea, indeed the phrase "smart contract" was first coined by Nick Szabo in the 1990s. However, the blockchain can now serve as the platform which can support countless smart contract transactions, that as we will see can be programmed to carry out certain tasks without the need for human input or intervention.

In this article we are going to touch on three areas which we believe will see significant growth for smart contract based solutions – there are countless others which are outside the scope of this article.

Internet of Things transactions

As noted above, smart contracts refer to self-executing tasks that can be programmed into the blockchain database. A vending machine is a good example: I insert a quarter, and the machine delivers a candy bar, with no human intervention. The blockchain permits this vending

machine model to be extended to millions of objects connected to the internet. A start-up called Slock.it has developed an application for renting apartments in which the apartment's door automatically unlocks itself if the prospective renter has paid his or her deposit, shows up at the right date, and produces proof of identity. The door checks these facts on the blockchain, and if they are verified, the door opens.

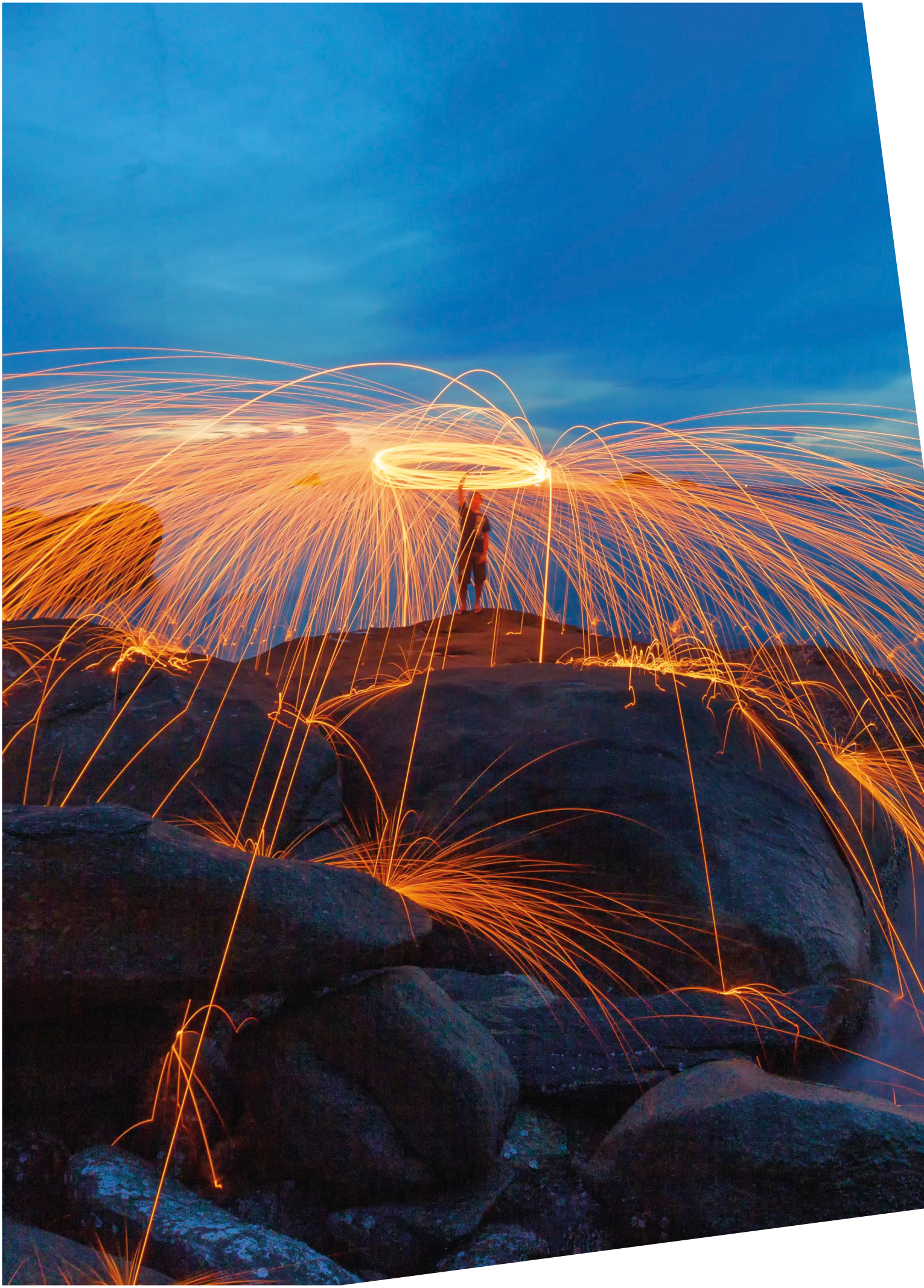
The smart door example can be extended to a multitude of Internet of Things transactions. For example, one application would permit electric vehicles, when stopped in traffic, to sell small amounts of electricity to each other depending on their battery needs. The contract would be executed in microseconds. The blockchain eliminates the need for a trusted intermediary or counterparty. The trust is in the code, so the cars do not need to have any pre-existing relationship with each other.

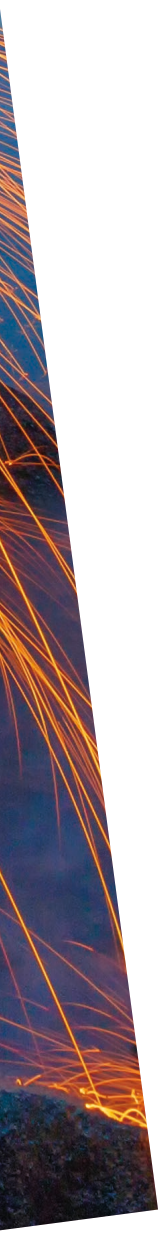
But can you enter into a contract with a door, or with a car? From a technical angle, the blockchain code certainly permits it. Contract law, by contrast, requires a person with legal capacity to contract and to be sued. Think of our example of the vending machine: If the vending machine does not deliver the chocolate bar, I will have a claim against the person or entity managing the vending machine, not against the vending machine itself. Machine contracts will always require a "human" contractual overlay. This may prove challenging when transactions are executed on the fly between millions of machines that do not have any pre-existing relationship. For example, imagine that my car purchases electricity from the car of a stranger located in another lane of traffic, and that for whatever reason, the electricity delivered did not conform to my expectations. Whom do I sue? The car's owner may claim that he or she did not even know that the car was trading electricity, so it may be difficult to argue that the car's owner was bound by contract. Perhaps the liability would be covered by insurance, and transactions could only occur if the blockchain shows valid insurance coverage for the relevant car. As this example shows, smart contracts cannot develop on their own without robust liability rules to back them up.

Commercial paper

Commercial paper consists of non-convertible unsecured short-term debt obligations. Issuers of commercial paper are generally financial institutions and investment grade-rated public corporations. A commercial paper note is, in its essence, a promise by its issuer to pay a predetermined amount on a predetermined date to the holder of the instrument.

As far as financial instruments go, commercial paper is particularly susceptible to the transition to a blockchain environment because holders of commercial paper notes do not benefit from a fiduciary or other party acting on their behalf. Once issued, it is up to each holder individually to collect and enforce amounts due. Also, because of the short-term nature of the instrument and the high credit quality of many issuers, defaults





in this space are rare. Given these factors and the relative simplicity of these instruments, blockchain technology and smart contract concepts may be able to create streamlined documentation and efficient execution of transactions in these instruments.

Traditionally, a financial intermediary acting as issuing and paying agent on behalf of the issuer facilitates the issuance of commercial paper under an issuing and paying agency agreement, with investors purchasing and, sometimes, trading these instruments through one or more investment banks acting as placement agents or dealers. The instruments are settled and cleared through the U.S. clearing system (DTC). The notes are held by the nominee of DTC (Cede & Co.) in "global" form where a single paper instrument represents the entire issue and interests in that global note are held only by direct participants in DTC. These intermediaries act for the benefit of the investors who are the beneficial owners of the notes. As a result, in a very real sense, investors in the traditional system never directly "own" their notes. In addition, in order to make payments on these instruments, the issuer typically provides funds to a paying agent which in turn distributes funds to be paid to the clearing system for eventual distribution to the beneficial owners of the instruments.

Smart contract technology could potentially bring increased efficiency to the issuance, settlement, clearance and payment of commercial paper notes. The issuance and ownership of a commercial paper note could be recorded directly on a blockchain with programming through a smart contract containing a trigger for repayment at the maturity of the instrument.

With the use of smart contracts, investors really would own their own notes (albeit in dematerialized form) and transfers of the notes could be recorded on the ledger so that the repayment of the instrument would be made to the owner without the need for intermediary brokers or an external clearing system. Repayment could be automatic, made directly to a designated account of the owner.

While a smart contract linked to the terms of the commercial paper note would provide a level of automation and efficiency, it is important to observe that until one or more so-called fiat currencies (such as U.S. dollars, pounds sterling or euros) are issued in digital form (with balances able to reside on a blockchain rather than in a bank account), the successful execution of payments in a fiat currency would be contingent on further action by the issuer of the note or a level of interoperability between the blockchain holding the instruction from the smart contract and the issuer's conventional banking services provider, in order to create a payment order.

1 L. Lessig, "Code is Law - On Liberty in Cyberspace", Harvard Magazine, Jan. 1, 2000.

2 J. Reidenberg, "Lex Informatica: The Formulation of Information Policy Rules through Technology", 76 Texas L. Rev. 553 (1998).

In addition, even with the availability of fiat currencies in digital form, a smart contract would not eliminate counterparty risk since upon the receipt of funds from the issuance of a financial instrument, the issuer would want to make use of such funds (rather than maintain such funds solely for purposes of payments under the financial instrument). Thus, holders of the right to receive payment under the instrument would be exposed to the risk that the funds necessary for any such payment would not be available at the time of payment.

Because the smart contract relating to the issuance would reference a conventional contract containing not only the commercial terms embedded in the smart contract code, but also other critical provisions such as the chosen governing law and a submission to the jurisdiction of designated courts, such an arrangement should fit fairly smoothly into our current legal system, although interesting questions might arise as to insuring that the occurrence of a bankruptcy filing by the issuer would be recorded onto the relevant blockchain to avoid a prohibited post-petition payment being made by the relevant smart contract code.

The DAO

The idea of smart-contracts has been extended into more complex ideas, including the concept of the "Decentralized Autonomous Corporation" ("DAC") or a "Decentralized Autonomous Organization" ("DAO") (for the purposes of this article we will refer to DAC when referring to this concept of a decentralised entity). A DAC aims to be exactly that – a digital equivalent of a traditional corporation, save that with a DAC records of every decision or financial transaction could be recorded onto a single blockchain ledger (ensuring absolute transparency). And this is not just a thought experiment – in May 2016 The DAO (a DAC that was set up as a crowd led investment platform) was launched on the Ethereum blockchain, raising in excess of the equivalent of US$150m (making it the most successful crowd funded investment to date). Rather than subscribe for shares in a company or units in an investment trust, investors in The DAO exchanged 'Ether' (the native cryptocurrency for the Ethereum blockchain) for tokens in The DAO. Holders of tokens in The DAO would in turn determine how those funds would be invested (with voting being linked to the number of tokens each participant held, thus favouring investors with more sizeable investments). The DAO would have contracts in place with specific individuals or organisations (known as Contractors) who would be in turn execute the wishes of The DAO in the real world. There was no central management or control other than the control framework enshrined in the software code.

However on 17 June 2016 a weakness in The DAO's code was exploited and it became compromised, resulting in more than US$50m of the Ether raised by The DAO being diverted into an account controlled by the hackers.

The Ethereum developer community subsequently recovered the stolen funds by implementing what is known as a "hard fork" (which resulted in them rewriting the transaction history of the blockchain to eliminate the theft). However, the fact The DAO code was compromised clearly spooked investors and some within the developer community as they saw the hard fork as an abuse of the very nature of a decentralised system. At the time of writing approximately 43% of the original funds

associated with The DAO had been withdrawn and the Ethereum developer community is now split into Core and Classic, with those supporting Core backing the hard fork and those running Classic being against.

The DAO has therefore been a very high profile test case for DACs and as well as obvious questions regarding the security and accuracy of the underlying code, it raises a number of questions regarding the legal status of The DAO and DACs more generally.

Legally it is uncertain as to what class of asset a token from The DAO represented. If tokens for The DAO are regarded as securities, then should the rules regarding the issuance of shares to the public apply – if so which set of rules should be applied to an entity that is effectively stateless?

On a more fundamental level is a DAC a corporation in the classic sense, with members having limited liability, or is it more akin to an unincorporated association or general partnership, with participants being held liable for the actions of the DAC on a personal basis?

If DACs such as The DAO are going to become mainstream, it seems as though legislators will need to decide whether this "digital entity" should be afforded legal personality – as noted above for the idea of smart contracts to truly fulfil its potential we will need to address how the real world rubs up against the digital one.

Conclusion

During the early days of the internet, scholars speculated that code could replace law, and that a transnational "lex informatica" might supplant national legal rules. Over 15 years later, we see that national laws continue to apply to internet transactions, sometimes with a new-found vigor. We expect the same to hold true for blockchain contracts. Self-executing contracts over the blockchain work beautifully… until they don't. And when they don't, the contracts will cease to be smart, and will become simple "contracts", requiring smart lawyers to sort them out.

Richard Diffenthal
Partner, London
T +44 20 7296 5868
richard.diffenthal@hoganlovells.com

Lewis Rinaudo Cohen
Partner, New York
T +1 212 918 3663
lewis.rinaudo Cohen@hoganlovells.com

Winston Maxwell
Partner, Paris
T +33 1 5367 4847
winston.maxwell@hoganlovells.com