Bird & Bird

Blockchain 2.0, smart contracts and challenges

Martin von Haller Grønbæk, Partner, Bird & Bird Copenhagen

This article is featured in Computers & Law, The SCL Magazine, June/July 2016 and an adapted version of it is printed here with their permission.

Introduction

Blockchain is a database of all transactions across a peer-to-peer network. This is seen as the main technical innovation of Bitcoin and other cryptocurrencies, with the potential to disrupt numerous business processes.

Bitcoin is by far the most famous application of blockchain technology. The cryptocurrency stores transactions in so-called Bitcoins, within a decentralised ledger of its blockchain. However, blockchain technology has many more applications, both existing and potential, as well as being used for cryptocurrency.

Among these applications are smart contracts. Entries into the ledger may consist of computer code that executes the terms and conditions of a contract between parties. Such parties will usually be parties to contracts, private individuals, corporate entities, public institutions or other entities. The more sophisticated the code, the more automated, self-executing, and "smarter" the contract. Ultimately, we may see autonomous parties in the form of computerised agents, such as Internet of Things (IoT) devices, connected online, entering into smart contracts without human interference.

This article explores the use of blockchain technology for applications other than cryptocurrency (*blockchain 2.0*), in particular the relationship between blockchain technology and smart contracts, and considers some of their potential business applications. *What are the properties of a smart contract and how will it benefit from the use of blockchain technology?* More interestingly from a regulatory point of view, *what are the legal challenges that developers of smart contracts face when bringing their applications to the market?* The article will only introduce some of the most fundamental and broadly applicable legal issues such as contract law, privacy and consumer protection. Accordingly, industry specific regulatory frameworks for the financial and other industry sectors will not be considered[1].

[1] Technological descriptions are based on entries from Wikipedia.

Blockchain technology

The blockchain is database technology that works on a network such as the Internet[2]. Users install the application locally and the "nodes" all hold a copy of the database. No central server holds control over the database. The database is structured as a ledger or a registry of entries into the blockchain. These entries are aggregated into data structure blocks. The blockchain consists of blocks that hold "time-stamped" batches of valid entries. Each block includes the "hash" of the prior block, linking the blocks together. The linked blocks form a chain, with each additional block re-inforcing those before it. From this process comes the name blockchain.

Entries - or transactions - are passed from user to user, or node to node, on a best-effort basis. The specific blockchain application defines a valid transaction. In cryptocurrency applications such as Bitcoin, a valid transaction must be digitally signed, spend one or more unspent outputs of previous transactions, and the sum of transaction outputs must not exceed the sum of inputs. Other applications may use a different method of validation, such as third party certification, or none at all.

Blocks record and confirm when, and in what sequence, transactions enter and are logged in the blockchain. Blocks are created by users, in Bitcoin known as "miners", who use specialised software or equipment designed specifically to create blocks. Block creation - or mining - is costly in terms of equipment and processing power (electricity). To create Bitcoin blocks, miners are incentivised to create blocks by two types of rewards: a pre-defined per-block award and fees offered within the transactions themselves, payable to any miner who successfully confirms the transaction. Other applications may incentivise block creators differently. If the blockchain application is run for internal use within a bank or a group of banks these may simply pay third parties or employees to perform this task.

Blockchain 2.0

The presumed inventor of the blockchain, Satoshi Nakamoto, never saw the use of blockchain technology limited to Bitcoin or other cryptocurrencies. In a communication from 2010[3] he envisioned that *"the [blockchain] design supports a tremendous variety of possible transaction types that I designed years ago. Escrow transactions, bonded contracts, third party arbitration, multiparty signatures, etc. If Bitcoin catches on in a big way, these are things that we'll want to explore in the future..."* This expansion of the use of blockchain technology in new applications is exactly what we are witnessing now.

The term blockchain 2.0 serves to distinguish between Bitcoin as an asset and the "blockchain as a programmable distributed trust infrastructure"[4] more generally, with additions of new scalable features of on-chain utility and extensibility. Instead of viewing the blockchain as part of the decentralisation of money and payments, blockchain 2.0 expands the scope of the technology to enable the decentralisation of markets more generally, and the transaction will involve other types of assets by providing registers for certificates and rights and obligations in real estate, IPR, cars, art works and so on.

As blockchain 2.0 is code the new application is said to be running on a new set of protocols ("blockchain 2.0 protocol"). A comparison with the protocols of the Internet and its layer of stacks illustrates the relation between blockchain 1.0 and blockchain 2.0. The former can be viewed as the TCP/IP transport layer whereas the latter can viewed as HTTP, SMTP and FTP. In this context blockchain 2.0 applications would be akin to browsers, social networks and file sharing services[5].

---

[2] The original definition was published by Satoshi Nakamoto, the presumed inventor of Bitcoin, in "Bitcoin: A Peer-to-Peer Electronic Cash System" (https://bitcoin.org/bitcoin.pdf) from 2008.
[3] Transactions and Scripts: DUP HASH160 ... EQUALVERIFY CHECKSIG, June 17, 2010 (https://bitcointalk.org/index.php?topic=195.msg1611#msg1611)
[4] Swanson, Tim (2014-04-08). "Blockchain 2.0 – Let a Thousand Chains Blossom" (https://letstalkbitcoin.com/blockchain-2-0-let-a-thousand-chains-blossom)
[5] Svan, Melanie. “Blockchain: Blueprint for a New Economy” Chapter 2, p. 10. O'Reilly Media, 2015.

Smart contracts

Smart contracts are computer protocols that embed the terms and conditions of a contract. The human readable terms (the source code) of a contract are compiled into executable computer code that can run on a network. Many kinds of contractual clauses may thus be made partially or fully self-executing, self-enforcing, or both. Smart contracts are not a new concept. The phrase "smart contracts" was coined by computer scientist Nick Szabo, probably around 1993, to emphasise the goal of bringing what he calls the "highly evolved" practices of contract law and related business practices to the design of electronic commerce protocols between strangers on the Internet[6]. An early adaptation of smart contracts is digital rights management schemes. These are smart contracts for copyright licences, as are financial cryptography schemes for financial contracts.

The blockchain technology enables smart contracts by building on its distributed ledger architecture. The code that makes up the smart contract can be added as part of an entry to the blockchain 2.0 application. Smart contracts among third parties unknown to each other can now be entered into due to the trust that is built into the blockchain as a database that cannot be forged or tampered with. In particular, contracts with many third parties can now be signed (*multisig contracts*) at low cost. Thus the definition of a blockchain-based smart contract: "a piece of code (the smart contract), deployed to the shared, replicated ledger, which can maintain its own state, control its own assets and which responds to the arrival of external information or the receipt of assets"[7].

Transparency and privacy

The original Bitcoin code has been released under an open source licence and all blockchain 2.0 applications have also been open source. To an outsider this may be revolutionary but, with the dominance of the open source models in all areas of computing innovation, it would actually be a paradigm shift if someone had opted for releasing a new platform such as the blockchain or a blockchain 2.0 application like Ethereum on a closed source licence. Nevertheless, the accessibility of the source code provides the blockchain with important transparency, which adds to the trust in the system and its ledger that comes with the consensus-driven distributed database structure. All users of the blockchain can verify if the underlying code has any security flaws or contains any back doors to allow tampering.

As a point of departure, information about all transactions on the blockchain is accessible to all users. This transparency allows all users to check their copy of the ledger for consistency with other users' copies. In addition, any well-connected node is able to determine, with reasonable certainty, whether a transaction does or does not exist in the data set. Any node that creates a transaction can, after a confirmation period, determine with a reasonable level of certainty whether the transaction is valid, able to take place and become final (i.e. that no conflicting transactions were confirmed into the blockchain elsewhere that would invalidate the transaction, such as the same cryptocurrency units "double-spent" somewhere else).

This transparency may be a challenge for the privacy of its user. The Bitcoin network strives to preserve the privacy of its users by allowing nodes to access the ledger under a pseudonym. As mentioned before, to transfer a Bitcoin the node does not have to reveal the physical identity of the person or organisation operating the node. All that is needed is that the node makes the transaction with a digital signature with a valid private cryptographic key. If the use of a blockchain 2.0 application demands a link to a user's identity, this personal information will be accessible for all who use the application. This creates challenges in respect of compliance with EU data protection regulation. Some of these challenges are similar to those faced by international e-commerce websites. Others may be new. If a blockchain database holds personal data in clear text, this information will be copied on all distributed copies of the ledger to all nodes. Who are these nodes? In an EU data protection context, who are data controllers and data processors?

---

[6] Szabo, Nick, "Formalizing and Securing Relationships on Public Networks". Vol. 2, no. 9. 1 September 1997. First Monday (http://firstmonday.org/ojs/index.php/fm/article/view/548)

[7] Brown, Richard Genda. "A simple model for smart contracts". 10 February 2015. (https://gendal.me/2015/02/10/a-simple-model-for-smart-contracts/)

Code is law

Lawrence Lessig famously said that *"code is law"*[8]. He pointed out that coders and software architects, by making a choice about the working and structure of IT networks and the applications that run on them, made important and often critical decisions about the rules under which the systems would be governed. In this capacity coders had replaced traditional legislators. This was and still is true with respect to the structure of many layers in the software stack. The coders working on the blockchain layer make such decisions. The same applies to the blockchain 2.0 applications such as the Ethereum scripting language.

Coders - or maybe more aptly their paymasters - formulate the content and scope of the smart contracts that coders will convert into computer executable code. This gives coders the serving right in deciding the framework and its limits for the contracts that can be used in their version of a blockchain 2.0 application. However, the reality is that this will become a customer-driven market. Parties to smart contracts will pay coders to tailor smart contracts to suit their specific needs. Coders will become akin to lawyers drafting "traditional" contracts, and coders will be assisted by lawyers specialised in the language and mechanics of smart contracts.

Just as it was quickly realised that cyberspace was not free from government interference, it must be understood that smart contracts are not only subjected to "code as law" but are governed by the law of the land. Even smart contracts with autonomous software agents as parties can trace their beginnings to human actions and will also impact human beings or other actors in the "real" world at some time. Just as there are many limits to freedom of contract in general, there will be many limits in contract law and regulation on the autonomy and self-enforcement of smart contracts. Smart contracts do not exist in a legal vacuum just as cyberspace is not cut off from the real world.

Adjudication and flexibility

Smart contracts can be - at least in theory - fully automated and self-enforcing. Once the terms and conditions are set in computer code the contract will run its course and the terms will be executed impartially by the computer on the basis of the code and the exogenous events. In many commercial relationships, in particular within financial services, these properties make smart contracts very attractive. Automation, combined with the lack of traditional trust-building costs associated with the blockchain's distributed nature, significantly decreases transaction costs, making such exchanges much more profitable.

But commercial (and private) exchanges are often very complex. As any contract lawyer would agree, drafting a contract that takes into account all possible contingencies and states all their responses is not possible.

A key function of courts is to adjudicate in matters where circumstances have changed in a way not foreseen by the parties at the time of entering into the contract. A smart contract may have allocated the risk in typical binary fashion of any deviation from the status quo and may have inserted some reference to an external arbiter of whether such deviation has occurred. Thus, the smart contract can be executed by the computer without any interference. However, the parties may be in a situation where they don't want the contract to be executed strictly. Both parties might *ex ante* agree that the contract's enforcement should be made contingent upon its fairness or conscionability. The party with particular interests in the smart contract being strictly enforced may, on second thoughts, want to apply a measure of fairness in order to ensure the continued commercial relationship with the other party.

Smart contracts can prove to be very inflexible, unable to adapt to changing circumstances and the parties' revised preferences. Increasingly, artificial intelligence (AI) can be applied to the drafting, managing and enforcement of smart contracts but AI cannot provide the necessary update of code based on embedded principles of fairness and economic efficiency. Probably, in the not too distant future, AI will be able to embrace these principles in both the initial drafting and the subsequent enforcement of smart contracts. However, for now, many smart contracts used to govern complex private and commercial relationships will have to remain open-ended and rely on the input from wetware lawyers and silk-robed judges.

[8] Lessig, Lawrence. “Code and Other Laws of Cyberspace”. Basic Books, 1999.

The link to the physical world

As we move toward blockchain 2.0 applications, the need for links to the physical becomes apparent. Setting up a blockchain-based land register on a server or coding a smart contract to be recorded as a transaction on a blockchain application may prove to be the easy part. Verifying that a person claiming that he has title to a piece of land, let alone verifying that the holder of a public key is who he claims to be, will often be an almost impossible task. And yet for the blockchain to be of value this valid link to the physical world must be established. In general, all rights and obligations (except for those in cryptocurrency) registered on blockchain 2.0 applications must rely on the validity under applicable law, and often on the certification by some government or third-party authority, that conditions under applicable regulation have been made. Establishing the physical links is often the most cumbersome and expensive part to be overcome, if exchanges have to be facilitated. While establishing a decentralised database structure based on blockchain will lower transaction cost significantly, that is often not enough.

The law of contracts

Fully automated and self-enforcing smart contracts may deal with commercial scenarios so complex and unpredictable that the code will fail to embed all possible answers to all possible questions. As mentioned above, in the foreseeable future smart contracts will often have to rely on courts and arbitration in matters of doubt. A component of contractual law regulates issues where the parties, as a matter of law, cannot deviate in their contracts from the mandatory provision laid down by contract law. Certain legal principles are so fundamental to the regulation of economic activity that courts will not enforce otherwise valid contracts if these principles are not complied with. There are also limits to the freedom of smart contracts.

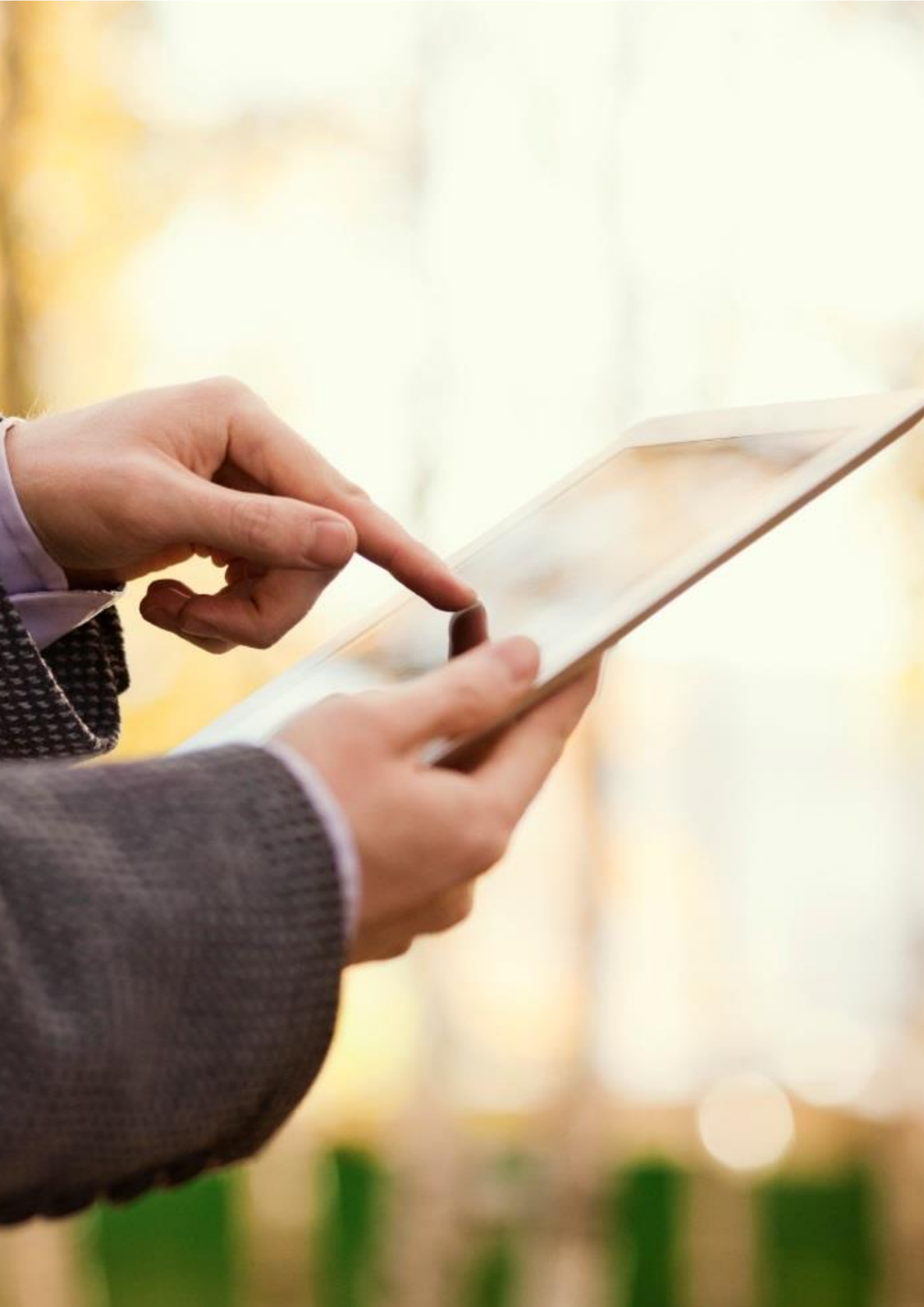
A court will provide remedies to the aggrieved parties to a smart contract that has been executed, if the contract would be deemed invalid by the court due to local versions of concepts such as fraud, duress, forgery, lack of legal capacity and unconscionability. These principles are so fundamental to regulation of exchanges that it would be counterproductive if these could be circumvented alone by subjecting to the *fait accompli* of a fully automated and self-enforcing smart contract. Invalidation of contracts with reference to principles of law remains an exception to the rule with respect to traditional contracts. There is no reason to believe that subjecting smart contracts to the same contractual law framework will prevent them from becoming widely adopted, in particular where the parties are businesses that are assumed to be more capable to protect themselves in contracts. On the contrary, parties to smart contracts must be assumed also to prefer such contractual law checks. It is likely that an innovative blockchain 2.0 start-up will come up with a semi-automated service that will lower the risk of contractual risk of fraud, and lack of legal capacity.

Consumer regulation

Smart contracts will organise exchange of economic value in a variety of sectors. Due to public interest considerations many of these sectors will be heavily regulated. Moving contracts onto a blockchain may lead to questions concerning the choice of law and jurisdiction but, like the majority of traditional international contracts, national courts and legislators will eventually develop a better level of understanding. As with international e-commerce, smart contracts will not (for long) operate outside of law and order. The challenge is not whether any national court will adjudicate a smart contract, rather it is that the queue of courts vying to become the legal forum and use its national body of law will probably be long.

Nowhere will this be more apparent than with respect to consumer regulation. Many smart contracts will have a consumer and a business as the parties. The business is likely to bear the cost of setting up and running the blockchain 2.0 application and to unilaterally draft the terms and conditions of the smart contracts. It should be obvious that smart contract terms with groups of users that are protected by legislation have to comply with minimum rights and prohibitions. The legal position of a consumer, a wage earner, a minor or a tenant cannot be worse under a smart contract than under traditional contracts. If this is the case, courts will invalidate a smart contract that fails to comply, regardless of automation and self-enforcement.

However, compliance with mandatory regulation is a challenge to smart contracts not a hindrance. It is merely a question of sophistication. The more challenging a legal framework, the more important it becomes to develop the code that embeds the rules of the framework into, for example, a smart consumer contract. Some mandatory provisions leave room for discretionary assessment by a third party for fairness, but consumer regulation is also highly apt for automation by coding terms regarding grace periods, formalistic notices and the like into a smart contract. Today e-commerce sites have incorporated almost all legal compliance into their e-commerce applications. These businesses already use smart contracts. Moving the e-commerce database to a blockchain will probably be the lesser task.



twobirds.com

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