MOODY'S
INVESTORS SERVICE

SECTOR IN-DEPTH
25 April 2019

Rate this Research

TABLE OF CONTENTS

Summary 1
Application of blockchain technology in securitisations is still at an early stage 2
Blockchain will improve the operational efficiency within securitisations 3
New risks will emerge, alongside existing challenges 10
Appendix — Blockchain fundamentals 15
Moody's related publications 21

Contacts

Frank Cerveny +49.69.70730.730
VP-Senior Research Analyst
frank.cerveny@moodys.com

Monica Curti Ph.D. +39.02.9148.1106
VP-Sr Credit Officer
monica.curti@moodys.com

Gaston Wieder +34.91.768.8247
VP-Senior Analyst
gaston.wieder@moodys.com

CLIENT SERVICES

Americas	1-212-553-1653
Asia Pacific	852-3551-3077
Japan	81-3-5408-4100
EMEA	44-20-7772-5454

Structured Finance — Global

Blockchain improves operational efficiency for securitisations, amid new risks

Summary

» **Application of blockchain technology in securitisations is still at an early stage.** Already, there have been a handful of transactions globally. Securitisation is likely to follow other market segments in their application of blockchain technology.

» **Blockchain will improve the operational efficiency within securitisations.** Amid the new technology, stakeholders could have easy access to all details of a securitisation transaction. Data placed on the blockchain becomes immutable and time-stamped, creating a reliable audit trail. It reduces the risk of fraudulent activities and lessens the need for redundant reconciliation efforts. Blockchain will simplify and accelerate security issuance and settlement by requiring the participation of fewer parties, ultimately reducing transaction fees.

» Implementation of blockchain technology in securitisation will most likely be gradual and partial (limited to certain elements of the securitisation process, like note settlement). Applications, in the near-term, will remain experimental, limited to pilot phases with a small number of participants and/or parallel processing with conventional technologies.

» **New risks will emerge, alongside existing challenges.** Concentration risk is highly relevant, particularly in private, permissioned blockchains, likely to be used in securitisation, with increased dependence on central administration via a gatekeeper.

» As blockchain technology and its application evolves with high pace, the risk of cyber attacks will increase as well. The situation also adds additional complexity and new challenges to risk management and analysis of future blockchain based deals.

» There is some degree of legal uncertainty on how to replicate a securitisation transaction's contractual framework within a blockchain environment. The extent to which the latter can be adopted in structured finance and increase transactions' operational efficiencies will ultimately be determined by technological feasibility and legal/regulatory recognition.

Blockchain sometimes erroneously is confused with digital currencies (cryptocurrencies) or Initial Coin Offerings (ICOs). Our report exclusively focuses on the technological infrastructure of blockchain and the effects it could have on securitisation.

Application of blockchain technology in securitisations is still at an early stage

The use of blockchain technology starts trickling into the securitisation world, namely most recently via an ABCP[1], and a synthetic corporate loan securitisation for BBVA, with support from the EIB group[2].

Securitisation is more likely to follow other market segments in applying blockchain technology to their operations[3], such as bank lending (including trade finance), payment services[4] and securities trading.[5] Adoption of blockchain technology is a strategic decision and we assume banks will focus first on high impact areas within their overall business model, with potential to increase efficiency, reduce cost and attract clients.

However, blockchain is still very much in its infancy, given broad based technology substitution or implementation has yet to materialise. However implementation has either been focused on parts of the process chain, and/or limited to just a few transaction parties, under experimental conditions and/or in parallel processing with traditional technology, a trend set to continue.

Securitisation transactions making use of blockchain technology will have to cope with challenges such as legacy IT systems, interoperability issues between different blockchain platforms and (groups of) transaction parties, of which some are expected adapting slower than others.

Blockchain adoption in the securitisation market will also have to cater for scalability issues, with the challenge of achieving sufficient critical mass and necessary participation. At least over a transition period, there may be market fragmentation, with only larger originators and investors willing and able to make necessary technological infrastructure investments. Lingering legal and regulatory uncertainty could also hamper the adoption of blockchain.

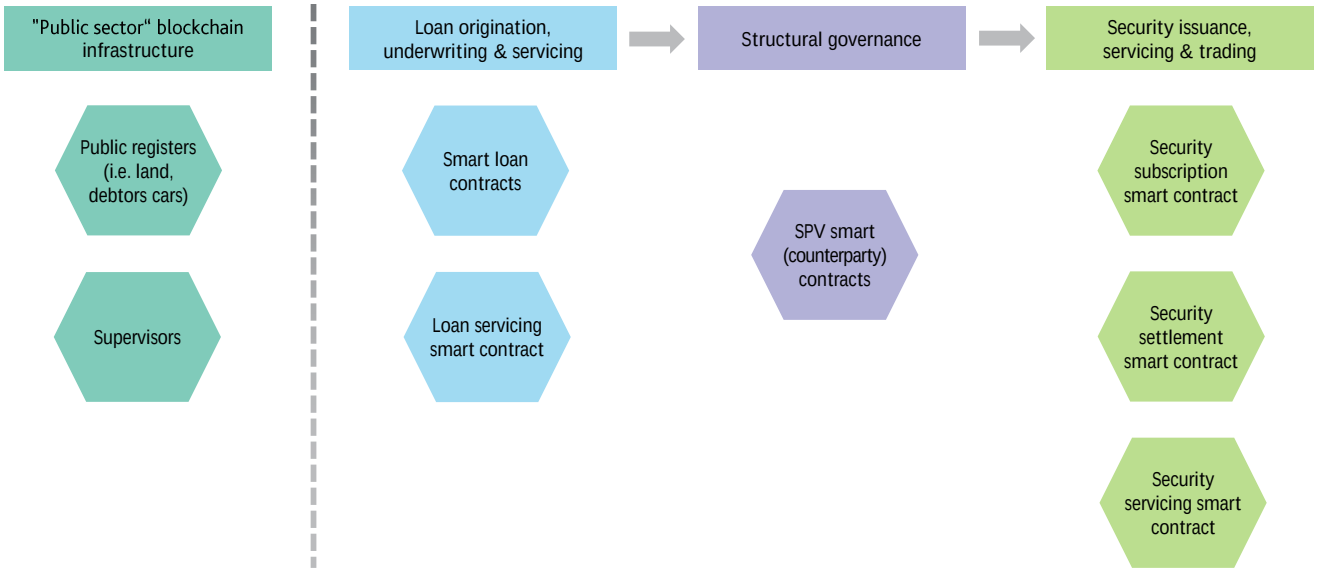
Blockchain will improve the operational efficiency within securitisations

Blockchain, technology for sharing and synchronising, digital databases, has the potential to increase operational efficiencies for securitised transactions. It affects the whole securitisation process chain, including more peripheral procedures, such as administration of public registers and supervision (see Exhibit 1)[6].

Amid the new technology, stakeholders (e.g. transaction parties, primary and secondary market participants) could have easy access to all details of a securitisation transaction, from loan origination to investment and trading. Direct access to information could also facilitate and potentially reduce reporting requirements for both, investors and regulators.

Exhibit 1

Potential securitisation process in a blockchain world



Source: Structured Finance Industry Group (SFIG), Chamber of Digital Commerce, Deloitte

Operational efficiency gains could ultimately materialise in terms of time and cost reductions, for instance via quicker and better data availability, increasing transparency, elimination of transaction parties and automation. It also reduces the need for lengthy and redundant reconciliation processes across transaction parties, replacing sequential actions with parallel execution.

However, such efficiencies are only achievable with initial upfront investment in both technology and personnel. In addition, sound control and governance mechanisms will have to be put in place, specifying roles, rights and accountabilities to safely operate blockchain technology in a securitisation environment.

Public sector blockchain infrastructure sets the framework for efficiency gains

Public, blockchain based registers (for example, land, cars, debtors) could facilitate and/or allow for information gathering, reporting and transfer of title with regards to securitisation collateral. For instance, transfer of title for a real estate property typically requires an entry into a land register. As proof of ownership, a lender will ask any borrower for either a land register deed or authorisation to access an electronic land register.

Existence of blockchain based land registers would create a connection between the public and private sectors. It could lead to a free exchange of information between the bank, land register and securitisation blockchains, subject to compliance with data protection provisions.

A few European countries have started to work on a blockchain based land register, to varying degrees (e.g. Sweden[7],UK[8],Russia[9]and Georgia)[10].Without blockchain based land registers, efficiency gains on the asset side of a mortgage backed securitisation transaction will remain limited.

A similar issue exists with regards to auto loans, as far as a pledge of the car is required by the lender. A blockchain based car registration register, could help to avoid physical transfer of registration documents from seller to purchaser and from purchaser to lender, as well as additional digitisation for securitisation purposes.

Issuance and trading of securitised notes does not require a public register, neither for the acquisition in the primary and transfer of ownership in the secondary market, nor a written contract. However, they do require legal recognition of blockchain based dematerialised notes. Such notes are issued in digitised, uncertificated form only, and a token is stored on the blockchain, representing the security, as much as a paper security would do. Certain European countries have recently established commensurate legislation, for example, Luxembourg[11],Liechtenstein, [12]and France[13], while Switzerland[14] and Germany have only recently started to consider legislative steps, the latter still being in an early stage.[15]

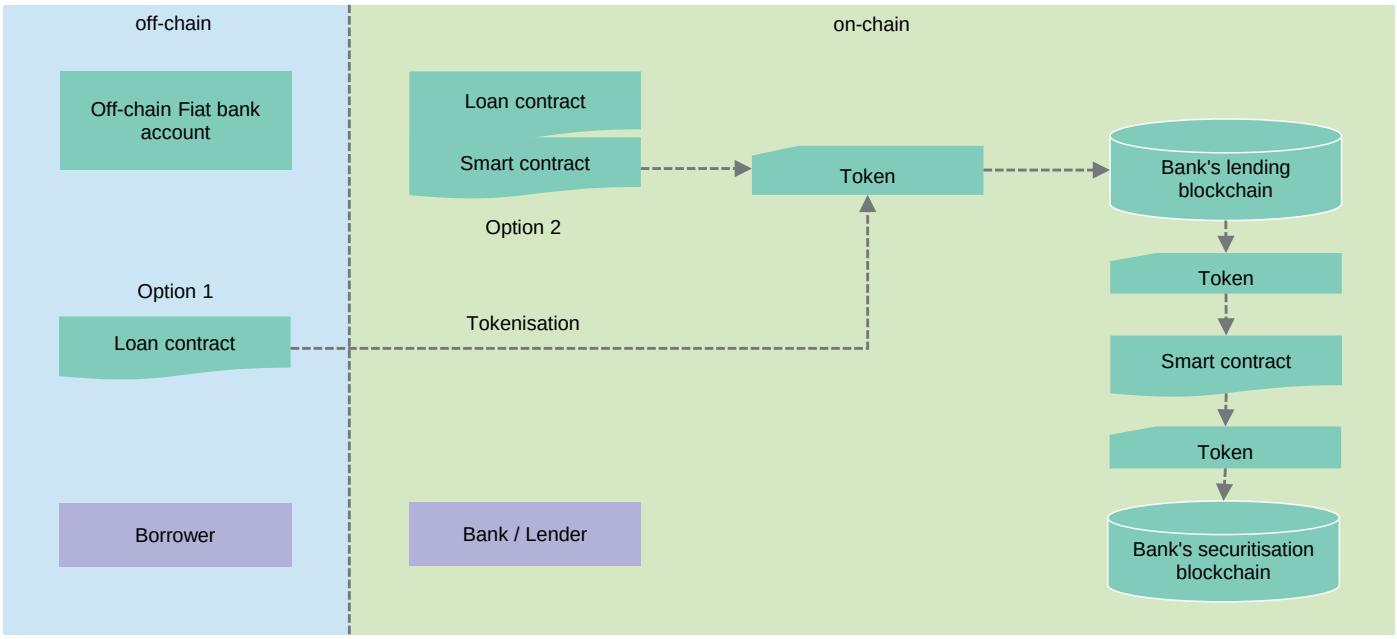
Loan origination and servicing could be streamlined

Blockchain technology and in particular the use of smart contracts would streamline the securitisation process with regards to portfolio selection and performance reporting. Native digital assets are created directly in a blockchain (on-chain), alongside their legal existence. For instance, a bank originator makes use of a blockchain for its lending business and also implements a blockchain for a related securitisation transaction. The securitisation blockchain can rely on data provided by the lending blockchain, subject to (automated) checks and controls. Non-native digital assets are typically bank loans with conventional origination and administration, kept in traditional IT systems, and additional representation through a so-called "token" on the blockchain.

If lender and borrower have digitally agreed upon the terms and conditions of a loan, all relevant information automatically feeds into a so-called "smart loan contract". The digitally originated loan, as well as any related collateral, will be represented via a token in the blockchain, set up for the originator's whole loan book. If the loan is originated in a traditional, non-digital or "off-chain" way, the loan as well as its related collateral will first need to be digitised or "tokenised," to become part of the blockchain. The latter requires additional process steps and, by default, reduces efficiency gains (see Exhibit 2).

Exhibit 2

Loan origination and tokenisation of off-chain loans



Source: Moody's Investors Service

Tokens denote different types of cryptoassets, beyond cryptocurrencies

At this stage, there is no single agreed definition or conceptualisation for cryptoassets and tokens. However, most recently the UK Financial Conduct Authority (FCA) suggested a categorisation[16] that refers to cryptoassets as a broad term, using "tokens" to denote different forms of cryptoassets, focusing on their functions. Generally, the FCA defines cryptoassets as "a cryptographically secured digital representation of value or contractual rights, powered by forms of distributed ledger technology (DLT) and can be stored, transferred or traded electronically."

The FCA further distinguishes between exchange tokens (means of exchange or tool for buying and selling goods and services without traditional intermediaries), security tokens (share or debt instruments) and utility tokens (granting access to a product or service).

While the FCA's objective is to identify potential financial instruments that fall into their supervisory perimeter, tokens can be thought of as "avatars of real world goods, services or rights"[17]. In the context of securitisation, tokens could represent specific assets (loans/receivables and related collateral) and payments.

A smart loan contract and the related token will contain all underwriting information relevant for a securitisation transaction (for example, representations and warranties, rating/scoring, borrower's financial status, balance sheet information, collateral value, loan-to-value (LTV)), in-line with today's regulatory and European Central Bank (ECB) loan level data requirements.[18] A token could even exceed such minimum requirements, as it is able to include whole loan files, including security agreements, documents attached to collateral, expert opinions and photos. However, the depth of available loan information depends on the relevant blockchain and design of the smart loan contract.

Loan smart contracts and tokens will be continuously updated and amended, reflecting information such as borrower payment behaviour, loan modifications, ongoing correspondence between lender and borrower, as well as other credit related information.

Compliance of characteristics at loan level with a securitisation transaction's eligibility criteria could be checked automatically, without recourse to an external auditor. It would be accomplished via a matching routine between the individual loan and a securitisation transaction smart contract, which checks portfolio eligibility criteria and/or guidelines.

Each individual loan with a profile that matches transaction eligibility criteria will be flagged accordingly as "eligible" and added to the transaction's portfolio. Loan information available from smart contracts and tokens will be used to update portfolio characteristics on a recurring basis.

Data can be accessible by loan, transaction or across deals in the same securitisation blockchain of an originator, facilitating overlap and concentration analysis, while minimising necessary interfaces.

All relevant information required for loan servicing feeds from the loan smart contract into a loan servicing smart contract. Payments collected on performing loans are verified and directed from the loan servicing smart contract via token to the securitisation blockchain.

After a borrower misses a payment and a loan becomes delinquent, the servicing smart contract automatically would send a reminder to the debtor. If delinquency persists, the smart contract could automatically transfer the loan to a third party special servicer with access to the blockchain. Loan file/asset token would be updated accordingly.

If a loan defaults, all relevant information about the workout, as well as related recovery proceeds would be entered into the blockchain. Payments would be directed between the smart contracts via tokens as previously outlined.

Soundness of structural governance may increase

Data placed on the blockchain becomes immutable and time-stamped, creating a reliable audit trail. It reduces the risk of fraudulent activities and lessens the need for redundant reconciliation efforts.

Typically, each transaction party maintains its own data records, relying on regular reporting and/or input from other participants (e.g. making/verifying payments). Dispersed data sets and sequential information flow can result in duplicative processes and inconsistencies between records of different transactions parties. The sequential sharing of information can lead to delays, with one transaction party waiting for another. A blockchain allows for simultaneous data access and processing, which could eliminate such problems.

Differentiated access rights could be granted to transaction parties, investors, supervisors and the broader market (e.g. potential secondary market investors and traders), according to their needs and regulatory or legal requirements, like data protection and privacy.

Smart contracts could be used to monitor new assets by tagging each loan transferred to the special purpose vehicle (SPV). Tagging of loans in the blockchain could help prevent fraudulent double-pledging of assets to more than one creditor, in a pure blockchain environment. Only one token per asset/loan can exist in the whole loan book/securitisation blockchain of an originator and that token can contain a flag to indicate a previous pledge. An automated check via a smart contract can help avoid the creation of an erroneous additional pledge.

Smart contracts to heighten efficiency via automation of processes/contractual elements

Smart contract code refers to computer programmable language that, when executed, uses conditional logic (if-then) to assess whether one or more pre-defined conditions are met and if so, automatically executes specific tasks. These tasks may but must not have legal relevance, for example to issue instructions for a loan payment, send a termination notice on a lease, or to transfer ownership of assets. By contrast, smart legal contracts are in part or in whole represented and/or performed by software. The contractual obligations of one party to the contract are discharged through the automated execution of the software code.

Smart contracts are not new but stand out because of their automatic execution, which cannot be stopped, unless specifically built in the code. Consequently, time and costs can be reduced with regard to a real-world contract's execution, enforcement and reconciliation process. Smart legal contracts may automate onerous administrative tasks among parties, like swap counterparties, with the calculation of nominal amounts, as well as transferring and confirming of payments.

In a securitisation context, the cash flow waterfall or priority of payments (see Exhibit 3), could become a prototype for a smart contract, while other transaction provisions, for instance with regard to representations and warranties or servicer replacement, appear more complex and difficult to replicate in smart contract code.

Exhibit 3

Conceptual smart contract based cash flow waterfall

Identify terms and conditions	Define external sources or systems	Code the contract and record it on the blockchain	Self-execution when the defined conditions are met
The different parties agree on the terms of transactions, conditions and desired outcome. Conditions may be derived from existing legal agreements or templates.	Some smart contracts require access to data sources outside of blockchain to function or to verfiy if the agreed upon conditions are met.	A computer program is written to produce a desired outcome when conditions are met. Code is placed on blockchain where it cannot be modified without agreement of the relevant parties.	The computer program self-executes when the agreed upon conditions are met. The outcome is recorded on the blockchain, which creates an immutable audit trail.
Example: securitisation waterfall	Example: Reference index on floating rate notes	Example: waterfall tie-out process between accountants and banks	Example: distribution of payments to investors based on waterfall rules

Source: Structured Finance Industry Group (SFIG), Chamber of Digital Commerce, Deloitte

Terms and conditions (T&C) of a transaction, such as collateral, tranches, payment distribution/cash flow waterfall, could also be modeled as smart contracts. All transaction parties would approve the T&C smart contract before it is recorded in the blockchain, creating a so-called "single version of truth," easily accessible at any point in time by all participants.

Blockchain technology may also help to decrease disruptive effects in case an exchange of transaction parties becomes necessary. It can also facilitate the transfer of roles and responsibilities to another entity, by simple transfer of access rights to the system.

Debt instrument issuance, settlement, servicing will quicken via blockchain

Blockchain could simplify and accelerate security issuance and settlement by requiring the participation of fewer parties, ultimately reducing transaction fees. The settlement process clearly benefits the most from a reduction in manual reconciliation across intermediaries' and counterparties' ledgers.[19]

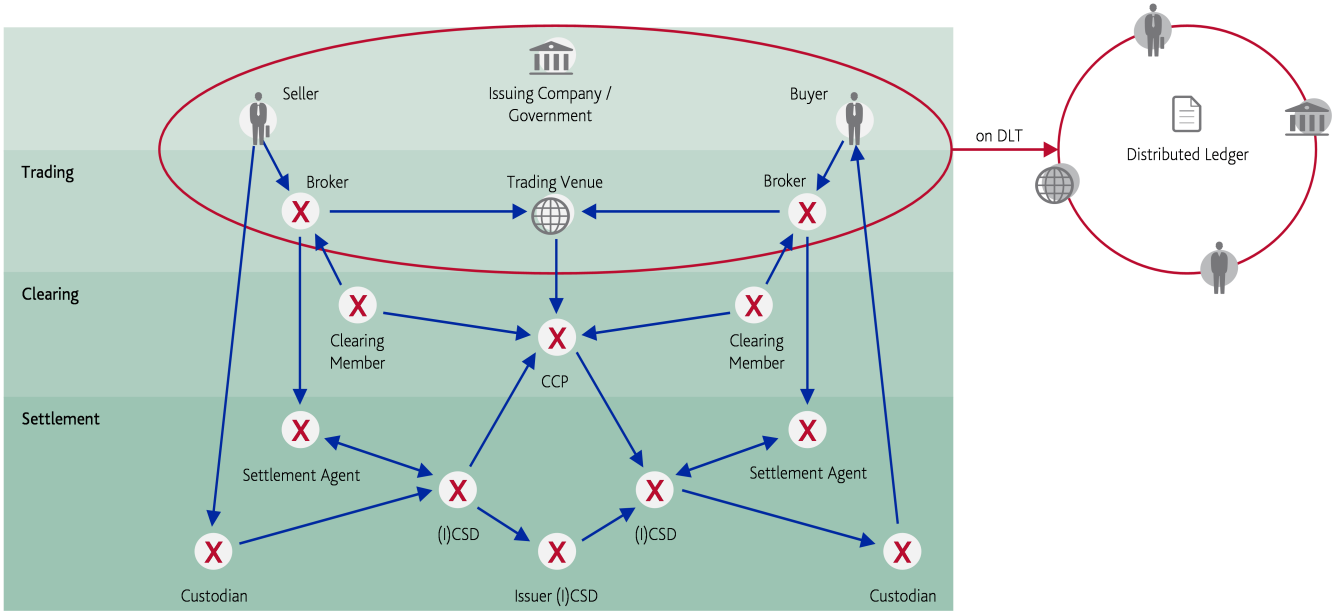
Today, in some cases, more than a dozen intermediaries are involved in the transfer of a security and cash between a seller and a buyer. Each of these parties maintains its own ledger with trade information that must be reconciled with the others.

While it currently can take days to transfer a security post-trade, the period between trade execution and trade settlement via blockchain can be shortened to a few minutes or even seconds.

Automated clearing and settlement processes could be executed directly in the blockchain ledger (see Exhibit 4)[20], subject to applicable national laws and their recognition with regard to issuance of dematerialised debt instruments.

Exhibit 4

Network of issuers and investors could supersede current post trade processes



Source: European Central Bank

For instance, in a securitisation transaction, collections would become 100% transparent to all blockchain participants, on any payment date, without requiring a payment report. A security servicing smart contract could automatically generate periodic payment reports.

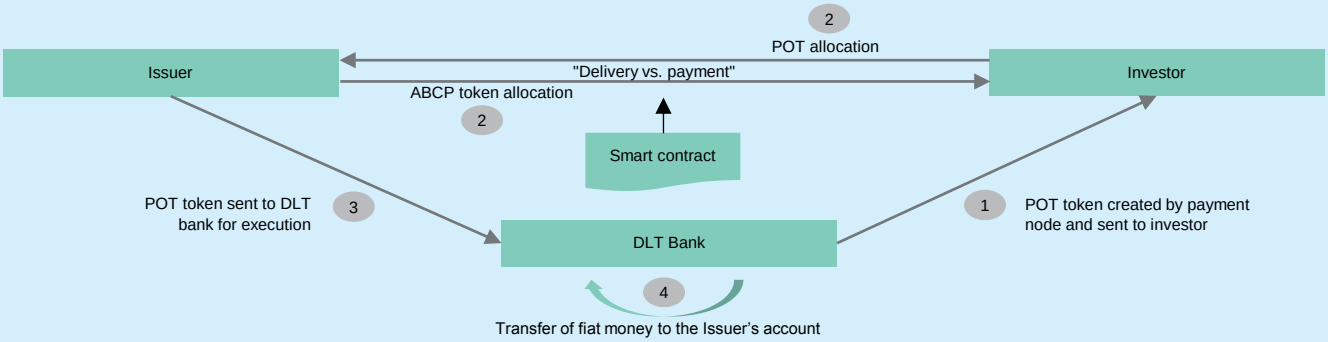
Securitised notes' servicing could be streamlined via servicing smart contracts, that collect and direct payments through a transaction, from the securitised loans to the noteholder. However, for the time being, it appears likely that ultimate payments to investors will be made via traditional payment systems and in fiat currencies. We understand that there is no strong desire on the investor side to execute securitisation transactions in crypto currencies. Therefore, it is crucial that a blockchain is able to communicate with traditional payment systems.

First ABCP issuance using blockchain technology improves settlement process and reduces operational risk[21]

On 14 February, Weinberg Capital DAC ("Weinberg Capital") issued and settled asset-backed commercial paper (ABCP) notes for the first time using distributed ledger technology (DLT). The inaugural €1 million note, part of a pilot phase, had a five-day maturity and was issued to MEAG Cash Management GmbH (MEAG, not rated) as sole investor. The use of DLT technology allows for reductions in ABCP settlement times, improvements in operational efficiency, as well as increasing transparency and security.

The transaction starts once the investor accepts an offer to buy a DLT ABCP note. The payment node, operated by LBBW, checks and then blocks the funds for the purchase amount in the investor's account. Afterwards, two tokens are created: (1) an ABCP token, an electronic register within the DLT platform recording title to the note (and its issue terms) and (2) a payment order token (POT), an electronic register within the DLT platform of a bank payment order. Note delivery occurs only against payment, through operation of a smart contract which will: (1) allocate the ABCP token from the issuer to the investor and (2) allocate the POT from the investor to the issuer, whereby both token allocations are simultaneous and one cannot occur without the other. In a next step, the POT is sent from the issuer to the payment node (Exhibit 5).

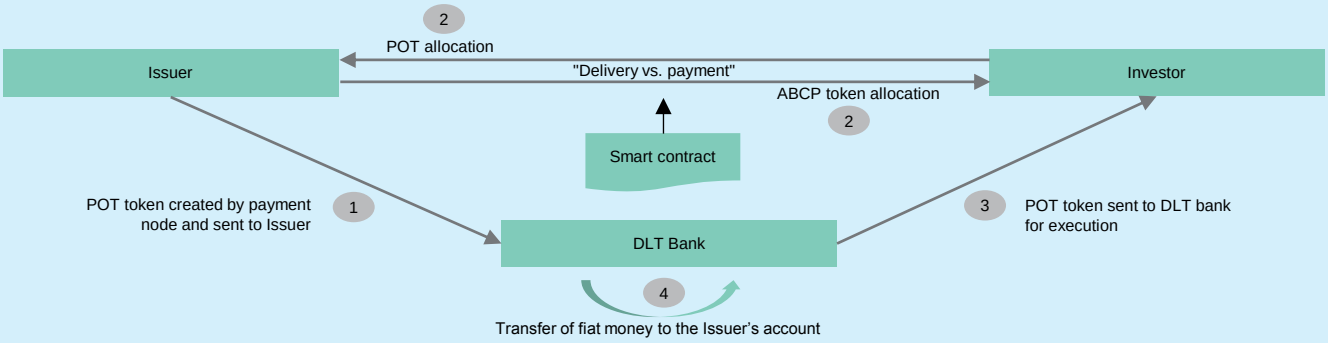
Exhibit 5
DLT ABCP issuance process



Source: Moody's Investors Service

Conversely, on the maturity date, the exchange of tokens is reversed. Again, delivery occurs only against payment through the operation of the smart contract, which will: (1) allocate the ABCP token from the investor back to the issuer and (2) allocate the POT from the issuer to investor, whereby both token allocations are simultaneous and one cannot occur without the other. In a next step, the POT is sent from the investor to the payment node (Exhibit 6).

Exhibit 6
DLT ABCP redemption process



Source: Moody's Investors Service

New risks will emerge, alongside existing challenges

New risks may emerge with the reinforcement of some already existing ones, like counterparty risk concentration, IT/operational risks, inappropriate blockchain governance and legal/regulatory issues.

Mixed credit effects on counterparty risk: elimination versus concentration[22]

Blockchain technology can modify the role of a securitisation transaction party, or, in fewer cases, even make certain transaction parties redundant. By way of example, a calculation agent could become redundant, because his task could be automated, and required data or information become easier accessible. Fewer transaction counterparties, would mean less counterparty risk within a securitisation transaction, but there are offsetting effects.

New key transaction parties will be introduced to the process, namely the entities that serve as developer, provider and operator of a blockchain. They may be either closely linked or identical with the originator, or independent third party service providers, which could lead to a certain degree of counterparty concentration risk.

Concentration risk is highly relevant, given that blockchains cannot operate autonomously, especially if structural changes to a transaction have to be implemented. For example, it may become necessary to substitute or amend transaction parties, or to deal with errors, like incorrect distribution of payments.

Within private blockchains, there is typically increased dependence on central administration via a kind of gatekeeper[23] Either a single administrator or a consortium (a limited subset of nodes in the blockchain) administers the system, vets participating parties and decides on criteria for validating and recording information on transactions. Outsiders are only able to make limited inquiries.[24] Private, permissioned blockchains, with differentiated access and information rights to match the needs of transaction parties, will most likely be the type of blockchain, typically applied to securitisation (see Appendix).

Concentration risk may also assume a systemic component, if multiple transactions and their parties rely on the same blockchain service provider.[25] In addition, some transaction parties may not disappear, with changes in their roles and responsibilities making them even more relevant in a blockchain environment. Smart loan contracts can make a pool audit, conducted by an external audit firm redundant, since compliance with eligibility criteria could be checked automatically. However, other types of audits with regards to processes, transaction parties and IT infrastructure may become more common.

Operational risks are likely to increase

Cyber risk assessment of securitisation is medium to low[26]

We recently assessed the cyber risk exposure inherent to securitisation and 34 other broad sectors, based on two factors: (1) vulnerability to a cyber event or attack and (2) the effects in terms of potential disruption of critical business processes, data disclosure and reputational effects

Allowing for some variation across sectors, the overall risk to structured finance transactions from cyberattacks is medium to low. Although some transaction parties may be in sectors that have a high exposure to cyber events (for example, a bank lender that sponsors a transaction), the legal separation between the deal and the assets' originator dilutes the risk of a cyberattack affecting the generation of cash flow from the originator's underlying assets.

A cyberattack that affects a sponsor's operational ability or credit quality can have some effects on a structured transaction's performance in some cases (for example, by continuing to service the accounts). However, the likelihood of such a disruption lasting long enough to have a significant negative credit effect on the transaction is low. The dependence of structured transactions on third-party entities adds to their vulnerability. They include servicers, trustees and other administrative entities, such as paying agents, calculation agents and custodians. However, mitigants such as minimum counterparty rating requirements, coupled with transfer provisions, add to the durability of transaction service providers. Servicers also often have backups to protect themselves against operational disruptions from catastrophic events, including cyberattacks, which also serves as a significant risk mitigant.

The growing adoption and complexity of new technologies like blockchain, in tandem with a talent gap for security and technology professionals in charge of their implementation and management also contribute to risks. As with any new technology, there is elevated human resource and key man risk. Blockchain related knowledge and skills are currently a scarce resource with its concentration among a small number of people.

As blockchain technology and its application in securitisation is evolving with high pace, the risk of cyber attacks will increase as well. The situation adds additional layers of complexity and new challenges to the risk management and analysis of future blockchain based securitisation transactions, in particular:

» Decentralisation of record keeping inevitably increases the number of gateways for any potential cyberattack. The risk profile of blockchains may differ across a broad spectrum, from private/centralised to public/decentralised structures. In case of the former, a centralised attack seems more likely, while for the latter, a cyberattack will often target the weakest link in the chain.

» There is a trade off between standardisation and automatisation of process steps, versus easier dissemination and more difficult reversal of errors, unless adequate checks and controls are implemented. Left unnoticed, a mistake in smart contract coding or reference data import may create damage over an extended period of time and affect a greater number of participants (namely investors).

» Private/centralised blockchains are more exposed to fraud risk because system design and administration remains concentrated with one or few parties. In addition, consensus mechanisms may not be in place or may be relatively weaker than in a public/decentralised network. Within private/centralised blockchains, a single administrator or a consortium typically administers the system, vets participating parties and decides on the criteria for validating and recording information and transactions.[27] While in theory, data and transactions on a private blockchain could be verifiable by different subsets of nodes, reaching from one to all participants, we expect verification by one or few transaction parties with requisite knowledge, as previously said.[28]

» Digitisation of off-chain assets creates redundancy, duplicates data storage, with the potential for data inconsistencies on-chain vs. off-chain. Non-native digital assets require strict safeguards to determine how a trustworthy backing of digital tokens by underlying real world assets can be technically and legally achieved.

» Securitisation typically relies on long-dated, multiyear arrangements, which could expose a transaction to risk of technological change (for example, advances in technology available to execute cyber attacks). Hence it seems appropriate to define a process as to how to stay abreast of technological developments and implement necessary changes, already at closing.

» In the short to mid-term, complexity is likely to increase and at least partially outweigh potential operational efficiency gains. Given the gradual deployment of the technology, parallel processing within current systems and establishing interfaces with legacy systems may still be required.

» The effects of blockchain technology on business continuity appears to be ambivalent. Risk will be mitigated by the decentralised ledger structures which facilitates data recovery, while preserving a complete audit trail. However, the number of gateways for attacks increases and blockchain application will frequently shorten process execution times (payments). While a robust business continuity plan should be present, it should also account for shorter recovery and execution times.[29]

Blockchain technology replaces trust in the "known other" (other humans, institutions, intermediaries) with trust in the "unknown other" (code, entities and dynamics that are hard to see and understand from the outside)[30]. Effective checks and balances as elements of a robust system of controls are therefore key.

Sound blockchain governance is key for risk management. In this context, governance refers to the processes, rules and procedures relied on to maintain the blockchain. A governance-free blockchain is exposed to failure, as software errors cannot be remedied and the blockchain can never be upgraded. Functional blockchain processes should allow the system to efficiently react to unexpected real-world events, for example the default of a transaction counter party, or system outages.

A blockchain governance structure should provide checks and balances between participating groups, like the parties capable of suggesting changes, deciding on upgrades and implementing these modifications. In private and permissioned systems, only a few entities (for example, originator/sponsor) play a key role.

A governance system can be designed more easily for permissioned (for example, the securitisation case) than for unpermissioned blockchains, as its software is controlled by a single party or a consortium that determines the system's rules of operation. Therefore, relatively clear accountability is given. As a disadvantage, a permissioned system can foster centralisation. When there is a single entity as gatekeeper authority (Exhibit 7), operational risk is concentrated in a single entity.

Exhibit 7

Gatekeepers in permissioned blockchains perform a wide range of tasks

Gatekeeper task	Description
Access control	Authenticating participants and granting them access to the network (enrollment process).
Permissions management	Issuing a set of keys to each participant depending on the permissions granted.
Terms & conditions	Defining the rules of the network including what transactions are considered valid, how the state of the ledger is updated.
Software maintenance and updates	Maintaining and periodically upgrading the codebase to introduce new features; fixing bugs and other issues.
Dispute resolution/arbitration	Intervening in the case of a dispute or disagreement by arbitrating between involved parties.
Setting terms for asset issuance/ tokenisation	Deciding on the T&C under which new assets can be issued and existing assets can be tokenised.
Other	Optional: regular reporting to regulators, data mining, setting additional T&C for using the network/application, assistance in case of key compromise, etc..

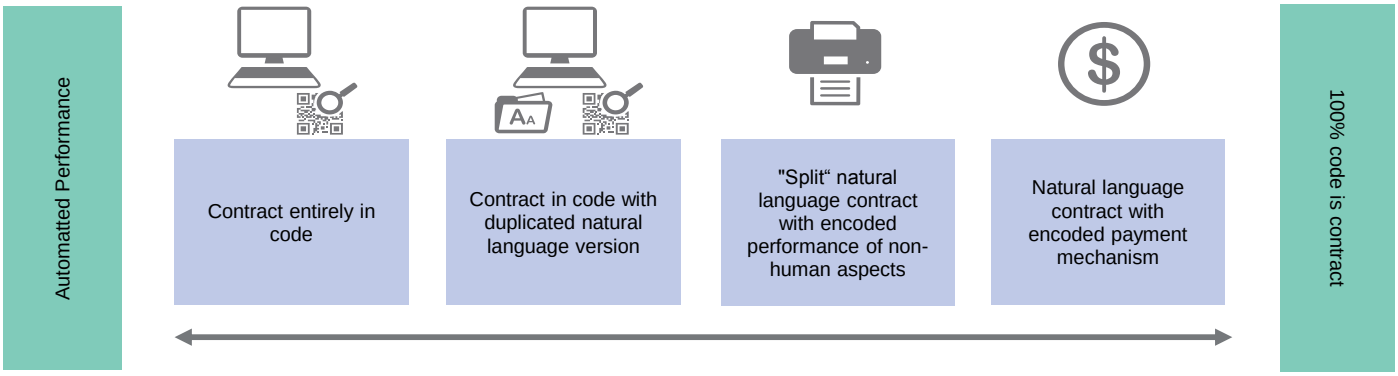
Source: Cambridge Center for Alternative Finance

Legal and regulatory risks — uncertainty prevails in an evolving landscape

There is some degree of legal uncertainty on how to replicate a securitisation transaction's contractual framework within a blockchain environment. The extent to which the latter can be adopted in securitisation and enfold its potential to increase transactions' operational efficiencies will ultimately be determined by two factors, namely technological feasibility and legal/regulatory recognition. They are particularly relevant when it comes to a contract that is replicable in a blockchain via a smart contract. However, there is a broad spectrum of possibilities how and to what extent real world contracts translate into smart contracts, as Exhibit 8 shows.[31]

Exhibit 8

Spectrum of smart contracts from a legal perspective is broad



Source: R3, Norton Rose Fulbright

In essence, there are two extreme formats of "smart contracting." Under the first extreme, code would constitute the entire terms of a contract, assuming they are 100% expressed in code, which would completely replace natural language agreements. On the other extreme end of the spectrum, a smart contract would simply be the digitised performance of business operations (for example, payments). In other words, digitisation would be limited to certain limited, programmable parts of a natural language contract. In between these scenarios, there is a range of intermediate or split solutions, that typically mix natural language contractual and code elements. However, it remains to be seen, if and to what extent a complex contract can be coded, that includes numerous legal expressions open to interpretation and legal analysis (for example, material adverse change or reasonable endeavours).

In a recent white paper, the Chamber of Digital Commerce concluded that in certain jurisdictions (for example, Spain) and under certain circumstances, smart contracts may be considered legally binding. Nevertheless, according to the authors, it would be wrong to generalise from conclusions for one jurisdiction versus others. Also, a full replacement of natural language contracts by computer code is unlikely, because of a lack of flexibility with regards to the scripting language. Furthermore, parties to a smart contract should consider governance and control mechanisms to ensure that modifications to the original contract can be made at a later stage without greater difficulties.[32]

"At present, it is not viable for smart contracts and blockchain based registers to act autonomously. Instead, a high level of hybridisation is necessary to surmount a disjuncture, most notably, between technological aspirations and legal (property, contractual) norms and cultures. This means smart contracts, working in tandem with on- and offline and on- and off-chain, transactional modalities. Further, it means blockchain-based registers acting like, rather than superseding, traditional databases or similar electronic archives. As a consequence, significant new laws and regulations tailored to smart contracts and blockchain-based registers are yet to emerge."[33]

From today's perspective, it seems ambitious to fully digitise the contractual framework around a securitisation transaction within a blockchain environment, in the medium term. Realistically, the focus should be on the previously mentioned split solutions. For instance, while it seems realistic to code a transaction's cash flow waterfall within a smart contract, representations and warranties or transaction party replacement provisions are likely to remain in natural language format.

We believe that replication of a securitisation transaction's asset side (in other words, securitised loans) in a blockchain, via smart contract and/or token, in a legally binding way, would significantly improve operational efficiencies, far beyond what can be achieved

by focusing on a transactions' liability side. However, we understand that legal uncertainties around transfer of ownership and enforceability (in case of default) in a blockchain context are still unsolved.

In Europe, at both European Union and member state level, there is lingering legal uncertainty over blockchains because of an overall lack of jurisprudence (in other words, case laws, legislation, regulation, directives), with few exceptions.

However, in a recently adopted resolution on DLTs and blockchain[34], the European Parliament is encouraging both the European Commission and national competent authorities to swiftly build up technical expertise and regulatory capacity, allowing for rapid legislative/regulatory action if and when appropriate. Parliament also underlines, that the EU should not regulate DLT per se but should try to remove existing barriers to implementing blockchains. More specifically, lawmakers are calling for the Commission to promote the development of technical standards with regard to smart contracts and to conduct an in-depth analysis of the existing legal framework in relation to the enforceability of smart contracts. Ultimately, the goal is to provide guidance on how General Data Protection Regulation (GDPR) applies to DLT, to develop a European legal framework to solve any jurisdictional problems that may arise.

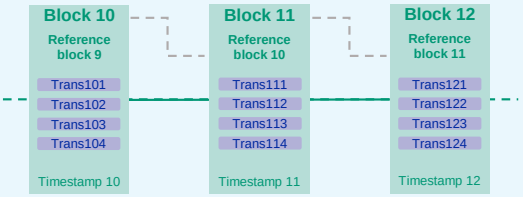
While there is no legislative activity yet at EU level, some member states became active at country level but typically with limited focus, either on cryptocurrencies or securities issuance (that is dematerialised notes). Few European legislation are more advanced and recognise (Italy) or are about to recognise (Guernsey) smart contracts as legally valid and enforceable.

In addition, data protection requirements may constitute a challenge for securitisation transactions in a blockchain environment. Data protection issues related to public, permissionless blockchains are more problematic, than for private, permissioned blockchains because data access is easier to control in case of the latter. Again, the question of whether a blockchain solution is compliant with GDPR, must be examined on a case-by-case basis, in absence of conclusive regulatory/supervisory guidance. [35]

Appendix — Blockchain fundamentals

Blockchain 101[36]

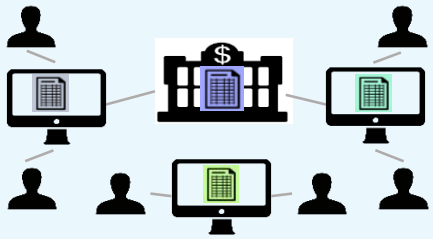
1. What is a Blockchain?



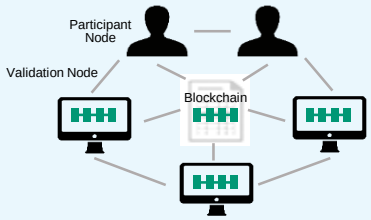
- A blockchain is a continuously growing list of data records that is organised into a series of blocks, each containing a batch of records or transactions.
- Each block also has a timestamp and a reference to the previous block, allowing all blocks to be linked together to form a 'chain' that includes a history of all transactions executed in the network, thereby increasing the transparency and auditability of transactions.
- A transaction includes information on the asset transfer, including the identity of the sender/seller and the receiver/buyer, the transaction asset/value, the transaction time, and/or potential contractual clauses.
- A blockchain can be used to transfer any assets that can be presented in digital form, such as financial instruments, contracts, ownership rights, corporate records or personal records.

2. Separate centralised v. single distributed ledgers

Centralised Ledgers

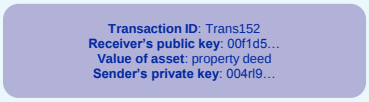


Distributed Ledgers



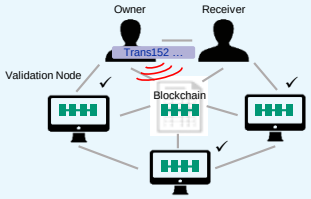
- Historically, databases or 'ledgers' have been held centrally, with all transactions sent to and maintained by a central 'owner' or authority and several layers of intermediaries. Some issues with this approach include:
  - Each institution maintains its own ledger, creating risk of a 'central-point-of-failure'.
  - Transaction completion takes time as it has to go through several ledgers for reconciliation, creating risk of error and duplication of effort.
- Under a distributed framework, such as that used in the blockchain, databases or ledgers are spread across all participants or 'nodes', of the peer-to-peer network. Depending on the blockchain framework, these participants can be the same as in current centralised processes or new participants that might replace some of the existing participants. Nodes can create and/or validate new data. Each node's copy of the ledger is synchronised with all others to ensure that each member has real-time access to the most current data.
  - One ledger shared among a network is robust against a failure of a node (that is, no central-point-of-failure), increasing resilience to outages or attacks.
  - Time for transaction completion is shorter as no reconciliation is required, which reduces infrastructure costs by streamlining back-office and administrative processes. Additionally, accuracy of data ledgers will improve as the risk of human error is reduced.

3. How is a blockchain transaction originated?



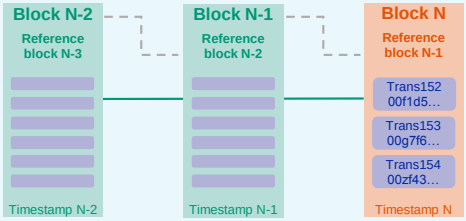
- The 'sender' of a transaction transmits a message to the network indicating a transaction ID; the address, or 'public key', of the receiver; the transaction value; a timestamp and the sender's digital signature or 'private key'. Blockchain increases data security using cryptography (see item 7 below).
- For example, two network members have agreed to an exchange of a property deed:
  - The property owner sets up a transaction including the network address of the receiver to clarify to whom the property deed should be sent.
  - The sender approves the transaction by signing it off with his private key.

4. How is the authenticity of a transaction ensured?



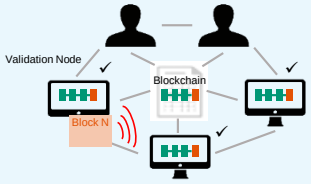
- Once the property owner has sent the transaction to the network, all network nodes receive the transaction message. They then verify the authenticity of the transaction with the network rules by decrypting the transaction using the sender's public key.
- Once the transaction is verified it is added to a queue of pending transactions.

5. How are transactions grouped into blocks?



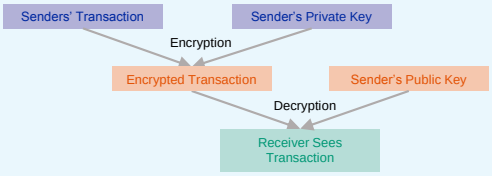
- All validation nodes group recent verified transactions of property deeds into a new block that they try to add to the blockchain (see item 6 below). Blocks with corrupt transactions will not be accepted by the network (see item 8 below).
- A new block also includes a header with the name of the new block, a timestamp to indicate when the new block was created and a reference to the previous block of property deed transactions to ensure that the blocks are linked to each other and form a chain with the entire history of property deed transactions.

6. How is a block added to the blockchain?



- Before the new block with the property deed transfer can be added to the chain, it is validated through an iterative process that requires consensus from a majority of the members (validation nodes). They will verify the work of the node that added the new block, for example, by ensuring that the network rules were followed and checking the accuracy of the property deed's ownership history. The members will approve valid blocks and decline fraudulent blocks.
  - Note: Distributed consensus can be realised through different methods (for example, 'proof of work', 'proof of stake' and a probabilistic iterative process).
  - Depending on the blockchain type, validation nodes could be, for example, real estate agents, financing banks and the land registry authority.
- Once the block is validated it is added to the blockchain and the updated state of the blockchain is broadcast to the network. As the blockchain maintains the history of all transactions, it grows with the number of transactions.

7. How does the blockchain increase security?



» Transactions completed via a blockchain are secured through public-key cryptography, which includes a public and private key pair that are related to each other through an algorithm (this ensures that the public key can be determined from the private key, while it is almost impossible to determine the private key from the public key).

» The private key is only known by the sender / owner of assets and is used to sign a transaction. The signature is based on the combination of the transaction content and the private key.

» The public key is the sender's public address or account number, which is visible to the entire network. The public key allows anyone on the network to verify that the transaction was sent by the asset owner.

8. How is the blockchain protected from fraud?

» While it is relatively easy to add a new block of transactions to the blockchain, it is hard to add an incorrect block with conflicting transactions since the other network nodes would not accept it. Rather than attach a new block to the incorrect block (in red) they would go back and attach it to the latest correct block (in green). In effect, a corrupted block would hit a dead end.

» Blockchain could provide an 'immutable repository of truth', increase data integrity and reduce fraud in ledgers. Manipulating data in earlier blocks is close to impossible, as it would require an update of all subsequent blocks and, accordingly, agreement from a majority of members to change all those blocks.

Blockchain typology — closed, permissioned structure most likely case for securitisation

Blockchains can be segmented by distinguishing between different types of permission models.[37] The permission model refers to the different types of authorisations that are granted to participants in a blockchain network. There are three major types of permission that can be set when configuring a blockchain network: (1) read — accessibility to the ledger and ability to view transactions), (2) write — for those who can generate transactions and send them to the network and (3) commit — for those who can update the state of the ledger. In this context, 'public/private' refers to the 'Read' capability, whereas 'permissionless/permissioned' refers to the 'write/commit' capability.

Key differences between open and closed blockchains relate to their security and threat model. Public, permissionless blockchains operate in a hostile environment with unknown actors, requiring specific mechanisms to incentivise participants to behave honestly.[38] In contrast, private permissioned blockchains operate in an environment where participants are already known and vetted, removing the need to incentivise good behaviour. Participants will be held liable through off-chain legal contracts and agreements, with the incentive o behave honestly via the threat of legal prosecution in the event of any misconduct.

Exhibit 9

Blockchain typology segmented by permission model; "private, permissioned" is the most likely model for securitisation purposes

Blockchain type		Read	Write	Commit	Examples
Open	Public permissionless	Open to anyone	Anyone	Anyone	Bitcoin, Etherum
	Public permissioned	Open to anyone	Authorised participants	All or a subset of authorised participants	Sovrin
Closed	Private permissioned ("consortium")	Restricted to an authorised set of participants	Authorised participants	All or subset of authorised participants	Securitisation; multiple banks operating a shared ledger
	Private permissioned ("enterprise")	Fully private or restricted to a limited set of authorised nodes	Network operator only	Network operator only	Internal bank ledger shared between parent company and subsidiaries

Source: Cambridge Center for Alternative Finance

Examples and typology of cyber attacks targeting blockchain use cases

Exhibit 10

Blockchain cyberrisk materialises on a regular basis via hacker attacks, causing significant monetary damages

Year	Target	Estimated damage	Source/Reference
2014	Mt. Gox	US$473 million	cointelegraph blog post, 9 March 2018
2016	TheDAO	US$50 million	New York Times, 17 June 2016
2016	Bitfinex	US$72 million	Reuters news, 3 August 2016
2017	Veritaseum	US$8 million	coindesk blog post, 26 July 2017
2017	CoinDash	US$7 million	coindesk blog post, 17 July 2017
2017	Enigma	US$500 thousand	cointelegraph blog post, 22 August 2017
2017	Parity	n/a; failed hack; customer accounts frozen	businessinsider blog post, 13 November 2017
2017	Tether	US$30 million	Coindesk blog post, 21 November 2017
2017	Nice Hash	US$62 million	Coindesk blog post, 6 December 2017
2017	Bitfinex	n/a; multiple DoS attacks	Bloomberg news, 12 December 2017
2018	Bitcoin Gold	US$18 million	Coinswitch blog post, 24 May 2018
2018	Electroneum	US$40 million	BitcoinExchangeGuide blog post, 4 April 2018
2018	Monacoin	US$90 thousand	ccn blog post, 22 May 2018
2018	Verge	US$2 million	thenextweb blog post, 21 May 2018
2018	ZenCash	US$550 thousand	etherumworldnews blog post, 4 June 2018
2018	Conrail	US$40 million	GBHackers blog post, 11 June 2018
2018	Coincheck	US$500 million	MarketWatch blog post, 20 September 2018
2018	ZAIF	US$60 million	Coindesk blog post, 20 September 2018

Source: Diverse IT related web blogs, as indicated in the right column of the table

As illustrated by the examples above, blockchains, as well as more traditional entities active in the financial sector (in other words, banks, exchanges), are targets of a broad array of cyber attacks, the most common ones described in the following table[39]:

Exhibit 11

Types of cyberattacks that threaten both, traditional financial institutions and blockchains

Type of cyber attack	Description
Malware	Malicious software that comprises either an institution's data or information systems. Malware can be introduced in a variety of ways, for instance via pishing, where hackers induce a person to click on a link to a malicious URL or attachment that installs malware on the person's IT system. Such campaigns can be used to obtain customer log-in credentials and other sensitive information.
Web application attacks	Data gleaned from a web application attack can form part of an advanced brute force attack that leverages stolen usernames and passwords to gain access to customer accounts. In this type of attack – known as "credential stuffing" – stolen login credentials are systematically and repeatedly input into the login fields of a website using automated scripts or modified software in order to gain access. Once the hacker successfully accesses an account using a stolen username and password, the hacker has access to the account funds and financial data.
Distributed Denial of Service (DDoS) attacks	Using botnets or other compromised systems, a DDoS attack sends a stream of traffic and data to a targeted website to overload the system and temporarily or permanently disrupt system operations. In a blockchain network, the cybersecurity controls established at each node provide an additional layer of security that contributes perimeter defense and defense in depth for the network.
Man-in-the-Middle (MITM) attack	A MITM attack involves an unauthorised actor positioning its system or access tool in transmissions between a user and a trusted party in order to capture or intercept data. There are two types of MITM attacks. A standard attack involves an unauthorised actor within physical proximity of the target who can gain access to an unsecured network, such as a Wi-Fi router. A second type is commonly referred to as a "Man-in-the-Browser" attack and involves the use of malware, which is injected into an unsuspecting user's system and, without the knowledge of the user, records the data that is being sent to a trusted third party website, such as a bank.
Ransomware attacks	Ransomware attacks threaten to block an institution's access to its own data unless the institution makes a payment to the hackers. They are especially pernicious in the financial services industry given the importance of customer data and the broader risks if it is compromised. Such attacks pose reputational risk for targeted financial institutions because depositors may withdraw funds en masse based on concerns that their funds are not secure. Ransomware attacks are popular because they can be carried out anonymously.
Theft of keys	The majority of attacks related to blockchains have been designed to steal cryptographic keys, not necessarily attack the blockchain itself. The experience underscores the importance of enterprise key management to reduce the risk of stolen or compromised keys.
Attacks on process	Blockchain also introduces different attack vectors that malicious actors may seek to exploit. For example, advanced attackers will look to influence decision-making processes around the blockchain in order to add new parts to the chain, change rules or policies, or manipulate a managing entity in such a way that is not transparent or is fraudulent. Attackers will also seek to create new fraud through mechanisms that will need to be created to adjudicate and remediate fraud. Ultimately, an integrity control system will be needed to ensure that those in control of decision-making in relation to the chain are acting as fiduciaries, rather than as self-interested owners of the chain.

Source: Microsoft / Chamber of Digital Commerce

Moody's related publications

- Weinberg Capital Designated Activity Company / Weinberg Capital LLC: First ABCP issuance using blockchain technology improves settlement process and reduces operational risk, 12 March 2019
- Cross-Sector — Global: Credit implications of cyber risk will hinge on business disruptions, reputational effects, 28 February 2019
- Credit Strategy — Blockchain Technology: Robust, cost-effective applications key to unlocking bockchain's potential credit benefits, 21 July 2016
- Trade finance: Blockchain efficiencies could streamline transactions but reduce banks' fee income, 16 April 2018
- SFG US: Housing-related industries lay foundation for 21st century technology
- Securities Trading: Blockchain Has potential to transform many elements of securities trading

To access any of these reports, click on the entry above. Note that these references are current as of the date of publication of this report and that more recent reports may be available. All research may not be available to all clients.

Endnotes

1 See Weinberg Capital Designated Activity Company / Weinberg Capital LLC: First ABCP issuance using blockchain technology improves settlement process and reduces operational risk, 12 March 2019.

2 See European Commission: Investment plan for Europe — EIB Group and BBVA will provide €360 million to finance SMEs and midcaps investment projects, 20 December 2018.

3 See Credit Strategy — Blockchain Technology: Robust, cost-effective applications key to unlocking blockchain's potential credit benefits, 21 July 2016.

4 See Banking — Global: Blockchain efficiencies could streamline transactions but reduce banks' fee income, 16 April 2018.

5 See Credit Strategy — Blockchain Technology: Blockchain has potential to transform many elements of securities trading, 12 April 2017.

6 See Structured Finance Industry Group, Chamber of Digital Commerce, Deloitte: Applying blockchain in securitization: opportunities for reinvention, 27 February 2017.

7 See coindesk: Sweden's land registry demos live transaction on a blockchain, 15 June 2018.

8 See HM Land Registry (press release): HM Land Registry to explore the benefits of blockchain, 1 October 2018.

9 See coindesk: Russia's government to test blockchain land registry system, 20 October 2017.

10 See The Bitfury Group (press release): The Bitfury Group and Government of Republic of Georgia expand historic blockchain land-titling project, 7 February 2016 and Government of Georgia (press release): Plots registered under land registration reform make over 300,000 hectares, 12 February 2019.

11 See Chambre des députés du Grand-Duché de Luxembourg: Circulation des titres via la blockchain, 14 February 2019 and Chambre des députés du Grand-Duché de Luxembourg:Role des affaires, 21 February 2019.

12 See Government Principality of Liechtenstein (press release): Consultation launched on Blockchain Act, 29 August 2018.

13 See Legifrance: Décret n° 2018-1226 du 24 décembre 2018 relatif à l'utilisation d'un dispositif d'enregistrement éléctronique partagé pour la représentation et la transmission de titres financiers et pour l'émission et la cession de minibonds, 28 December 2018.

14 See Schweizerische Eidgenossenschaft — Federal Department of Finance (press release): Federal Council wants to further improve framework conditions for blockchain/DLT, 14 December 2018.

15 See German Ministry of Justice: Eckpunkte für die regulatorische Behandlung von elektronischen Wertpapieren und Krypto-Token, 1 March 2019.

16 See FCA: CP 19/3 — Guidance on cryptoassets, 23 January 2019.

17 See Michèle Finck: Blockchain regulation and governance in Europe, December 2018.

18 According to a recent ECB press release, the Bank has decided that its own loan-level data reporting requirements will converge towards European standards, see ECB: Transparency requirements of EU securitisation regulation to be incorporated into Eurosystem collateral framework, 22 March 2019.

19 See Credit Strategy — Blockchain Technology: Blockchain has potential to transform many elements of securities trading, 12 April 2017.

20 See European Central Bank: Distributed ledger technologies in securities post trading — revolution or evolution?, April 2016.

21 See Weinberg Capital Designated Activity Company / Weinberg Capital LLC: First ABCP issuance using blockchain technology improves settlement process and reduces operational risk, 12 March 2019.

22 See Cross sector methodology: Moody's approach of assessing counterparty risk in structured finance, 29 January 2019.

23 See for example BaFin — Federal Financial Supervisory Authority — Blockchain technology, updated on 9 June 2017.

24 See Structured Finance Industry Group, Chamber of Digital Commerce, Deloitte: Applying blockchain in securitization: opportunities for reinvention, 27 February 2017.

25 See European Banking Authority (EBA): Report on the prudential risks and opportunities arising for institutions from fintech, 3 July 2018.

26 See Cross-Sector — Global: Credit implications of cyber risk will hinge on business disruptions, reputational effects, 28 February 2019.

27 See Structured Finance Industry Group, Chamber of Digital Commerce, Deloitte: Applying blockchain in securitization: opportunities for reinvention, 27 February 2017.

28 See Clifford Chance: The new spring for securitisation, 23 May 2018.

29 See Deloitte: Blockchain risk management — Risk functions need to play an active role in shaping blockchain strategy, 27 September 2017.

30 See Michèle Finck: Blockchain regulation and governance in Europe, December 2018.

31 See R3 / Norton Rose Fulbright: Can smart contracts be legally binding contracts? An R3 and Norton Rose Fulbright White Paper, 2018.

32 See Chamber of Digital Commerce: Smart contracts: Is the law ready?, 27 September 2018.

33 See Robert Herian: Legal recognition of blockchain registries and smart contracts, 8 December 2018.

34 See European Parliament: Distributed ledger technologies and blockchains: building trust with disintermediation, 3 October 2018.

35 See CMS: The tension between GDPR and the rise of blockchain technologies, January 2019.

36 See Credit Strategy: Blockchain technology — Robust, cost-effective applications key to unlocking blockchains' potential credit benefits, 21 July 2016.

37 See Cambridge Centre for Alternative Finance — Global Blockchain Benchmarking Study 2017, 27 September 2017.

38 Mechanisms are typically based upon the use of 'crypto-economics' — a combination of game theory and economic incentive design applied to cryptographic systems (for example by rewarding miners with tokens native to the system, such as bitcoins).

39 See Microsoft / Chamber of Digital Commerce — White paper — Advancing blockchain cybersecurity. Technical and policy considerations for the financial services industry, March 2018.

REPORT NUMBER 1138725

CLIENT SERVICES

Americas	1-212-553-1653
Asia Pacific	852-3551-3077
Japan	81-3-5408-4100
EMEA	44-20-7772-5454

MOODY'S
INVESTORS SERVICE