Working Paper presented at the

Peer-to-Peer Financial Systems 2022 Workshop

2022

Stablecoins' Sense of Stability and Finality

Karsten Paetzmann

Karsten Paetzmann, Frankfurt School of Finance and Management

Powered by

P2P Financial Systems

Exponential Science

Challenges of Blockchain Technology in Financial Services: Use Cases, Smart Contracts and Governance

Abstract. Banks, asset managers, insurers and other financial services firms currently introduce distributed ledger technology and blockchain applications. Given the substantial usefulness in the area of verifying and transferring financial information and assets, this article explores potential challenges that come with the implementation of blockchain applications, especially with respect to smart contracts. We provide an overview of legal uncertainties due to a continued lack of common standards globally.

Keywords: Blockchain, financial services, FinTech, governance, smart contracts.

1 Introduction

The financial services industry is predicted to benefit the most from the development of distributed ledger technology (DLT) and, more specifically, from blockchain applications. In fact, there is a hype and significant investments are being made to explore the blockchain's usefulness in verifying and transferring financial information and assets (Zetzsche *et al.*, 2017; Carson *et al.*, 2018; EIOPA, 2021). Even more, proponents have projected that blockchain could account for as much as 10% of global gross domestic product (GDP) by 2025 (WEF, 2015).

At the same time, the implementation of blockchain in the financial services industry also presents substantial challenges which must not be ignored. Among such challenges are regulatory issues, of both domestic and cross-border nature, compliance risks as well as potential legal uncertainties due to a continued lack of common standards

(Baker & Werbach, 2019; Zetzsche *et al.*, 2020; Rühl, 2021). Such challenges need to be addressed, given the high degree of regulation and the global inter-connectedness of the financial services industry.

The aim of this paper is to explore these potential challenges, especially with respect to smart contracts, and to analyse regulatory issues, compliance risks and potential legal uncertainties, accompanied by an overview of potential solutions to the question of governing law for cross-border transactions.

This paper is structured as follows: The second section provides an overview on the basic principles of blockchain and on current use cases. Further, this section elaborates on legal issues when implementing blockchain in financial services. The third section discusses smart contracts and key legal challenges when implementing them. As a series of legal challenges results from blockchain applications, the fourth section describes how rights and obligations may be determined and how liability among blockchain participants can be allocated, especially in cross-border situations. A final section concludes this paper.

2 Blockchain technology in financial services

2.1 Common use cases in financial services

Blockchain solutions are one of the most well-known applications of DLT. A DLT is defined as a digital ledger that, in contrast to a traditional, centralised ledger has no central administrator and: (a) information is stored on a network of machines which allows changes to the ledger to be visible and applicable to all holders of the ledger, and (b) information contained in the ledger is authenticated based on a cryptographic

signature. Blockchain technology may automate complex, labour-intensive processes faster and cheaper than traditional infrastructure. They are especially suitable for situations where one or more of the following requirements are given: (i) data needs to be reconciled among multiple market participants, (ii) multiple records of the same data are maintained by multiple market participants, (iii) record-keeping and auditing of immutable data is required, and (iv) proof of identity of a counterparty and/or verification of the originator of a transaction is essential.

Main areas of application of blockchain technology in the financial services industry include trading, clearing and settlement, loan origination and securitisation, identification and customer due diligence, payments, trade finance, and insurance contracts.

1. Trading, clearing and settlement is expected to be the most active use case in the near term. The potential advantages of blockchain use in this area are related to quicker transaction times, a reduction in third-party costs and collateral obligations on participants as well as a decreased risk of information inconsistency between transaction parties which leads to a reduced need for reconciliation.
2. Another important use case for blockchain in financial services is loan origination and securitisation. Conventionally, originators, sponsors/issuers, servicers, rating agencies, trustees, investors, as well as regulators assess and track data and create databases resulting in significant duplication of work and data gaps that could create commercial and legal risks. Especially the avoidance of multiple manual data entries can prove to be beneficial to all parties involved. Potential advantages of blockchain not only include a reduced risk of errors and fraud but also lower costs and a higher degree of transparency. Based on so-called smart contracts, originators may engage

in more frequent granular and automated transactions, to meet their funding needs, instead of carrying out single large transactions. Furthermore, blockchain in the loan origination and securitisation area may also open up funding opportunities for new market entrants.

3. Another interesting use case in financial services is the identification and customer due diligence. Know your customer (KYC) requests may significantly delay banking transactions in both the retail and commercial segment. Further to time delays, conventional KYC processes require duplication of effort between banks and other third-party institutions and have significant cost implications. Based on blockchain, customers may provide relevant KYC information only once, entered in a format that is acceptable to a group of participating banks and provided on a ledger for KYC purposes available to all relevant banks that can rely on it. Potential advantages of blockchain involve enhanced customer experience, lower costs, higher degree of transparency and auditability for financial institutions. Further, blockchain in the area of identification and customer due diligence has the potential to increase security, reduce fraud risk and enhance compliance with regulatory KYC requirements.
4. A further active use case of blockchain in financial services relates to payments. The Bitcoin cryptocurrency system has already gained some prominence, while Bitcoin has lately been more used for investment than for payment purposes. The transfer of money has always been quite complicated and slow, particularly true for cross-border payments. Incumbent payment service platforms such as SWIFT or R3, the international bank consortium founded in 2015 that has transformed into an enterprise software firm with the largest blockchain ecosystem globally, are developing payment systems using blockchain. The aim of their projects is to support bank-to-bank,

business-to-bank and even business-to-business payments which are quicker and cheaper than conventional payments. The potential advantages of blockchain in the payment area are that they potentially provide quicker and cheaper payment transactions at lower costs and liquidity obligations on payment processors, at the same time enabling a higher degree of transparency and traceability of payments and a reduction in fraud risk.

5. Based on its ability to track real-world assets in real time and release payments automatically via smart contracts on delivery of goods, blockchain may also be an important use case in the area of trade finance. Conventional processes typically require the importer's bank to issue a letter of credit against shipped goods, sometimes resulting in delays in payment for the seller or exporter. The potential advantages of blockchain lies in the increased transparency of the transaction at every stage of the process, lower costs, a reduction in fraud, and fewer disputes over the terms of the transaction.
6. Finally, an another area of use cases relates to insurance contracts. EIOPA, the European Insurance and Occupational Pensions Authority, published a discussion paper on 'Blockchain and Smart Contracts in Insurance' in April 2021 that includes use cases throughout the entire insurance value chain, including client on-boarding, underwriting, the development of new products and services, and claims handling. Furthermore, according to EIOPA (2021) and a feedback statement on the responses received (EIOPA, 2022), blockchain can be used to combat fraud, to streamline information exchange and payments between insurers and reinsurers, and to facilitate accessing and sharing insurance-related personal and non-personal data (open insurance). B3i, the Blockchain Insurance Industry Initiative which was incorporated in

2018, serves as an example for an application in the reinsurance industry. As of 2021, more than 40 (re)insurance companies were involved in B3i as shareholders, customers, and community member, exploring the use of, *inter alia*, smart contracts for property XL catastrophe reinsurance.

2.2 Trend to permissioned blockchains

Blockchain technology applications in the financial services sector have been slightly moving away from the initial permissionless blockchain idea introduced by Nakamoto (2008). Recent developments, apart from cryptocurrencies and decentralised cryptoexchanges, are more at the centralised end of the spectrum with relatively few nodes appointed by the initiators. Even more, some applications have only one node that runs the validation network. For example, the R3 Corda platform is a permissioned blockchain platform, ensuring that data is shared only with parties who have a 'need to know'. Having specifically been designed to bring transparency and trust to interactions, while maintaining privacy and security, it serves as an example of financial services blockchains relying on a rather centralised than decentralised database structure.

The Corda example demonstrates that governance and privacy issues are too important for many financial services applications to use permissionless blockchains. Further, permissoned blockchains do not require much computational capacity to secure the network, and there is no incentivisation required for competing with hashing power for cryptocurrency rewards. It is simply in the interest of the participants to achieve that level of security, also meeting regulatory requirements. The need to reconcile multiple ledgers is eliminated by permissioned solutions, due to a single ledger architecture that

each participant has access to. Overall, there are many advantages to depart from the original decentralised idea of blockchain and to use permissioned blockchains in financial services.

However, there are also disadvantages of permissioned blockchains in financial services, a main one being the risk of collusion if validators change the ledger. Further, the identification of, for example, a legal consortium in charge of the network may be the object of an attack. The most prominent potential disadvantage of permissioned blockchains relates to the market power of the incumbent participants which may choose to 'close doors' and exclude other interested parties which is a threat to competition or to suppress innovation in order to maintain their relatively strong competitive position. Both issues are a complete deviation from Nakamoto's original ideas.

2.3 Legal issues when implementing blockchain in financial services

While the precise legal matters when implementing blockchain technology depend on the use case, sector and product, six general issues require consideration in the course of blockchain implementations (Jones Day, 2018): jurisdiction, liability, applicable law/regulation, cyber security and data privacy, intellectual property, and competition/antitrust.

1. Jurisdiction: An issue that requires attention is to determine the governing law of a blockchain transaction that is based on multiple verified nodes in more than one jurisdiction. For example, if the rules provide that the law where the asset is located constitutes the applicable law, it needs to be assessed what the place of performance of the transaction and what the nature of the asset being transferred is. In the EU, the

Rome I Regulation (EC) 593/2008 sets out which law has to be used for contracts with cross-border elements. Article 4(1) of the Regulation determines that, in the absence of choice of governing law, for example (a) a contract for the sale of goods will be governed by the law of the seller's habitual residence and (b) a contract for the provision of services will be governed by the service provider's habitual residence. The Rome I Regulation applies to all EU Member States (and continues to apply in cases involving the UK, as a matter of Parliamentary choice), except for the EU Member State Denmark which planned to reverse its initial opt-out (Recital 46 of the Rome I Regulation) to an opt-in based on a referendum in 2015, but failed to do so (Rühl, 2021).

2. Liability: Another important issue to consider when implementing blockchain technology relates to the responsibility for blockchain performance, the responsibility for the technology or design failure and how/if a transaction will be enforceable.
3. Applicable law/regulation: As part of the implementation, it needs to be ensured that the blockchain technology enforces existing laws and regulations (in various applicable jurisdiction) which may apply to an asset being transferred. In addition, participants should be limited to those who can legally transact.
4. Cybersecurity and data privacy: Further, it should be ensured that the blockchain technology complies with applicable cybersecurity and data privacy laws and regulations, also reflecting upon any data transfer issues across borders. This is a potentially complex area that needs to consider issues of data privacy, reporting as well as the risk of breach. There are possible issues around data that is shared anonymously due to the anonymous nature of the of the person sharing it and around the question how end users are made aware of their rights.

5. Intellectual property: Any blockchain implementation may, from a legal view, also include questions around patent acquisition and liability as well as open source usage, to ensure that no rights of any third parties are being breached.
6. Competition/antitrust: Finally, it should be considered if the inherent effect of permissioned blockchains excludes participants and therefore potential competitors. Contrasting, with regard to decentralised technology applications (nonpermissive blockchains), it may be not possible at all to identify a responsible person and to allocate liability and governance to any party.

3 Smart contracts

3.1 Smart contract models

The concept of 'smart contracts' was introduced by Szabo (1997), combining computer protocols with user interfaces to execute the terms of a contract (Nofer *et al.*, 2017). There are two common but clearly separable definitions of the term smart contract. One definition simply refers to a computer programme that, typically without any human intervention, executes terms of a legal contract. Another definition acknowledges that a smart contract actually constitutes a legally binding agreement itself which is partly or entirely performed by computer software. To mark the constituent feature of a smart contract, the Law Commission (2021) uses the term 'smart legal contract'. However, whether or not a smart contract will constitute a valid contract depends on various factors, including the respective jurisdiction and its requirements to legal agreements.

More generally, the term ‘smart contract’ refers to a transaction that follows a programmed ‘if this, then this’ logic, and the embedded transaction is therefore a conditional transaction. Being programmed in a computer code, smart contracts may be well suited for standardised transactions that are executed automatically. However, legal issues around, for example, a valid and binding contract raise questions that require attention.

Smart contracts appear to be efficient for financial services applications which involve highly standardised contract terms with clear conditions and repetitive terms. Importantly, the conditions (‘if this, then this’) need to be objectively determined and coded accordingly. In a simplified example, an insured automatically receives payments and benefits from the insurer when the ‘oracle’, a third party source incorporated by reference whose sole task is to supply objective real data from the outside into the ledger, determines the occurrence of a specified event such as rainfall, wind, injuries, death, or accidents (Chamber of Digital Commerce, 2016). For specific situations, the insurer and the insured would jointly enlist a trusted third party to monitor the processes of the blockchain and respond to an event such as a removal of an asset from the ledger, if necessary.

The Chamber of Digital Commerce (2016) presents a total of twelve use cases for smart contracts, reaching from digital identity and various financial services applications to clinical trials and cancer research. For example, the use case of clinical trials which appears interesting in the light of the Covid-19 pandemic suggests that such trials can benefit from smart contracts through improved data sharing between institutions while preserving privacy and tracking the consent for patient data. However, the data also describes considerations that require attention when using smart contracts in this

area, including identity, authentication and authorisation that remain open issues as well as questions around the evolution of a specific clinical trial data market which raises, for example, ethical, data privacy and cyber security questions.

There are also questions regarding the practicability of blockchain transactions based on smart contracts. As shown by Madir (2018), the assumptions on which a simple sale of a house on the blockchain are based, are critical. As part of such smart contract, the house needs to be tokenised, i.e. a token has been associated with the house which involves multiple legal and technical challenges itself. Furthermore, such transaction is, under real life conditions, much more complex than in a given example and includes encumbrances, pre-payments and additional contractual terms that cannot be easily coded by a simple 'if this, then this' logic but require natural language-based agreements.

In addition, many transactions require more than an 'if this, then this' logic in that they specifically refer to assessments of one party to be conducted 'to the satisfaction of', or actions taken 'in a commercially reasonable manner' which cannot be easily coded in a logic based on conditions that may be objectively determined but which typically require a subjective assessment. Such challenge may be, to a great extent, overcome by advanced technology as shown in the car manufacturing industry where quality control mechanisms that previously required human subjective assessment have, to a great extent, been forwarded to new technologies, even involving augmented reality. However, car production is highly repetitive and the quality criteria may be programmed and determined objectively.

In the end, the automatability of contractual clauses in smart contracts will most likely lie on a spectrum that reaches from a contract being entirely coded to a contract

that is drafted in natural language with a simple, encoded payment mechanism. In between these two extrema various permutations are likely to emerge in practice. For example, R3/Norton Rose Fulbright (2016) mentions a 'split smart contract' model under which natural language terms are connected to computer code using certain parameters that feed into computer systems for execution. In the end, the level of integration of a computer code will be based on multiple criteria, including the complexity and automatability of the contract and the requirement of subjective, human assessment (Barbosa, 2021).

3.2 Legal binding contractual effect of smart contracts

In common law, the four elements of a contract are offer and acceptance, consideration, intention to create legal relations, and certainty of terms. This includes contract law applied in the US, where a federal contract law, except for very limited cases, does not exist and where the Uniform Contract Code (UCC) represents a comprehensive, uniformely adopted state law.

- Offer and acceptance: Under English law and law in the US, a smart contract code likely constitutes an offer to the other participants on the ledger if they are permitted to execute on the code. English law today permits the use of email messages to constitute offer and acceptances. Accordingly, the messages sent over the internet to initiate a smart contract, typically secured based on public key infrastructure (PKI), will most likely be regarded a constitution of a legal offer. Under contract law in the US, the requirements that need to be met in order to constitute an offer will also be

met if a smart contract code is used on a distributed ledger. With regard to the acceptance under common law, an agreement of the counterparty to the substantive terms and an expressive acceptance of the counterparty within the time period and the procedure provided by the offer is sufficient to qualify as an acceptance. More precisely, according to English court decisions on similar cases, the parties of a smart contract can prescribe the particular content of a message that constitutes acceptance in relation to a given offer that has been previously messaged. Under other jurisdictions, including Australia, it also appears that the requirements in relation to the contract element 'offer and acceptance' can be met by smart contract codes used on a distributed ledger – at least in a B2B context.

- Consideration: According to English law, a consideration requires an exchange of value, or mutual benefit and burden, to qualify as an element of the contract. To a degree that a smart contract typically involves such consideration, English courts, as well as courts in the US and Australia, will agree that this element exists.
- Intention to create legal relations: Under English (also under law in the US and Australia) the intention to create legal relations is assessed by reference to objective criteria. Such criteria relate to the status of the communication of the parties involved, especially to what was communicated by words or conduct and if that leads objectively to a conclusion that the creation of legal relations was intended by both parties. However, a typical smart contract may be more complex than others, involving an initial, primary contract, which itself may enter the parties into an additional contract, the secondary contract. In fact, the initial primary contract binds the parties with the intention that the secondary contract makes coded decisions (the secondary

contract) which the parties have to accept. However, such coded secondary decisions, which are intentionally accepted by the parties involved in the primary contract, lead to the questions if the computer may be regarded an additional party of the contract. Is, in the end, the computer acting as an agent for one or more parties, the principal(s)? In Software Solutions Partners Ltd, R (on the application of) v HM Customs & Excise [2007] EWHC 971, the court considered a similar question in relation to Software Solutions Partners (SSP) which designs, supplies, installs and maintains computer software that enables insurance brokers to carry out certain transactions with those insurers with whom SSP has made previous arrangements. In this case, the court decided that such pre-arranged, automated system could not be regarded as an agent naming it an 'irrelevant question whether an automated system could be regarded as an 'agent', although on current authority the answer would appear in the negative, because only a person with a mind can be an agent of law' (paragraph 67).

- Certainty of terms: The question appears if smart contracts provide determinable commitments in so far as they are written in a programming language and published on a distributed ledger, only readable by computers. To avoid any disputes, it is recommended that, in addition to the code, any commitments by parties are described in natural language. However, the risk arises that the natural language and the code differ or the natural language leaves room for interpretation. In addition, any expression of a code in natural language should be admissible in any judicial and arbitration proceedings, to avoid potential expert evidence in conflict situations. A further concern relates to the impact of any variations of law which require potential modifications of the contract and therefore have an impact on the certainty of terms. Raskin

(2017) suggests that modifications which relate to the terms of a smart contract could be triggered by an application programming interface (API) that has access to a (newly created) publicly available database of the relevant jurisdiction. By use of such API, the smart contract would call those terms and update the relevant provisions of the contract.

Overall, reflecting upon the four elements that constitute a contract, it appears reasonable to assume that smart contracts can have a legally binding contractual effect under English law, depending on the type of contract, its provisions and the economic transaction covered.

3.3 Key legal challenges in relation to smart contracts

A challenge in relation to smart contracts arises if other unforeseen circumstances occur, such as impossibility of performance due to *force majeure*, which indicates reasons outside the parties' control. Such circumstances are most likely not foreseen by the software code. In such situation, due to impossibility of performance, the contract will not be performed and there will be most likely no damages.

However, if an event occurs once a contract has been concluded that makes the performance illegal or substantially different from what was inititally intended by the parties, this would ordinarily result in the frustration of the original contract. DLT, due to the immutability of the ledger, may make it difficult to put parties back into their original legal position. As a solution, a reversal of the economic transaction may be considered. In a DLT environment, such reversal may, however, prove to be not acceptable to one or both parties involved as a reversal is most likely no adequate substitute for a

contract being treated as void, as the public records on the digital ledger are not entirely expunged from the public records. In blockchain technology, such reversal will have the form of a 'hard fork', involving a return to an earlier version of the blockchain which does not include subsequent blocks. Such 'hard forks' represent a radical change to the protocols of a blockchain and are very seldom. They potentially expunge not only one transaction but affect various other, legitimate transactions as there is no way to distinguish between a malicous content and a legitimate string of transactions (Werbach & Cornell, 2017). The most prominent example of a 'hard fork' refers to 'The DAO' (Decentralised Autonomous Organisation), the Ethereum-based cooperative launched in 2016. After raising a total of $150 million worth of ether (ETH) through a token sale, The DAO was hacked due to vulnerabilities in its code base. Eventually, the Ethereum blockchain was 'hard forked' to restore the stolen funds, with however not all parties agreeing with this decision, which resulted in the network splitting into two distinct blockchains: Ethereum and Ethereum Classic. Although the holders of ether were compensated by tokens of Ethereum or Ethereum Classic and there was no financial loss, a 'hard fork' generally represents a fundamental obstruction of the whole system and undermines the whole point of the blockchain, which is the notion of immutable distributed trust.

A further challenge to smart contracts arises if the verification of the party's authority to sign on behalf of the company is to be automated. A publicly accessible company register that contains such information may serve as a starting point, but such registers do not include powers of attorney or board resolutions which are typically not publicly filed. A potential solution might be that the parties agree on private data sources that are being made available for the software. However, it appears questionable if such

software will be able to analyse a signature authorisation or a board resolution document correctly.

In order to determine whether a DLT-based smart contract can be considered to be 'in writing' under the applicable law, the respective law is to be analysed. It will typically prescribe the conditions that need to be met. In English law, subject to certain exceptions, there is however no law that contracts must be in writing. One requirement in most jurisdictions relates to the ability of the parties to access and save its contents in order to be able to inform themselves later about the contract's content. In relation to smart contracts which are legible only to computers, this is questionable. Further, it is doubtful to assume that even popular programming languages are enough understood by most contracting parties. To mitigate this problem and to ensure that the requirements of a contract being 'in writing' is met, the smart contract should be accompanied by a natural language 'translation'.

In case of a dispute, the claimant will have to prove the relevant facts which bears the risk that such facts cannot be properly proven. For such burden of proof in case of a dispute the specific circumstances of smart contracts may play a significant role in proving payments or non-payments as these are performed automatically. As also with usual contracts, a party bears the risk that the other party, after having received payment or before exercising a reversal payment, files for insolvency. Even more striking is the idea that a party tries to receive a reversal payment from a pseudonymous party.

Therefore, it is advisable to implement a dispute resolution mechanism to avoid the challenges of receiving a reversal payment as described above. Such dispute resolution mechanism should be based on a provision in the computer code that delegates to a chosen arbitrator. Today, such delegations to arbitrators are already effectively included

in smart contracts codes, in part delegating to so-called ‘libraries’ such as Codelegit of Munich-based Datarella. Further, the dispute resolution mechanism should also be provided in the natural language version of the smart contract.

Regarding the protection of personal information, it is important to note that the data included in smart contracts represents pseudonymised data, not anonymised data. Therefore, the data, if relating to a person, remains personal data for the purposes of the GDPR in the EU. Under the GDPR, which *inter alia* contains rights to correction of personal data, its deletion and the right to be forgotten, a differentiation between a data controller and a data processor applies. However, in a blockchain environment it is difficult to identify such roles, especially in a permissionless environment. To mitigate the personal data risk, personal information may not be directly entered into a ledger but a hyperlink to a file that stores personal information may be inserted. However, while such data treatment option makes it easier to amend or remove personal data, it does not diminish the fact the personal data is being processed which may well be regulated by the GDPR (Moerel, 2018). The personal data challenges in relation to the GDPR which may apply to certain parts of or a whole smart contract have been addressed by the Commission. As a starting point, a STOA Options Brief ‘Blockchain and GDPR’ (European Parliamentary Research Service, 2019) presented three policy options that could ensure that DLT develops in line with the objectives of the GDPR framework.

Further legal issues relevant to smart contracts include: (a) challenges with determining if a statutory signature requirement has been met by using a cryptographic key, (b) allocating liability for a glitch between the programming language and the executable computer code and for a code that acts not according to what was intended, (c)

burden of proof in case of a dispute, (d) difficulties with determining the applicable law and the applicable dispute resolution mechanism, and (e) challenges with regard to confidentiality on a distributed ledger.

4 Allocation of liability on distributed ledgers

4.1 Determining rights and obligations and allocating liability among blockchain participants

DLT involves five types of participants: (a) a core group setting up the code design and de facto governing the distributed ledger, (b) the owners of servers that run the code for validation purposes, *i.e.* nodes or network stakeholders authorised to validate transactions, (c) qualified users which *inter alia* include exchanges, lending institutions, miners, (d) simple users of the system such as investors in Bitcoin, and (e) third parties affected by the system such as clients of intermediaries that clear their financial assets via DLT. Note that in a Bitcoin network, the validation nodes (b) and qualified users (c) are identical. With regard to the participants, four areas of uncertainty appear that need to be clarified in order to understand a DLT:

- Uncertainty over contractual relationships: Due to its nature, being based on a decentralised network, relying on consensus, avoiding third-party interference, and representing a concept with multiple variations, the blockchain ecosystem challenges courts and other parties understanding the accountability and responsibilities of participants and the governance structure, if any. It needs to be determined how

the technological relationships translate into legal, contractual relationships, considering the relevant jurisdiction(s).

- Uncertainty as to tortious or delictual liability: Participants in blockchains may be pseudonymous with the exact identity only difficult or not determinable. It needs to be considered how and if such participants, under a common law perspective, owe one another any tortious or delictual duties. This could involve a duty of care from relationships or a liability for potentially misstating or omitting to disclose material facts, e.g. from securities law.
- Uncertainty over the correct defendant: As participants may act under a pseudonym, it may be difficult to determine the identity of a defendant, following, for example, a corrupted message or a defected code.
- Uncertainty regarding trust boundaries: A further area of uncertainty relates to trust boundaries in governance arrangements between the blockchain participants. In general, such trust boundary is defined as the place where a ledger integrates with anything that is not in the ledger, e.g. entitling an entity to issue an asset into the ledger and validating that the rights to a specific asset are owned by that entity. There is uncertainty, even despite rules of governance and dispute resolutions mechanisms being in place, regarding their application across trust boundaries.

In the light of these uncertainties, there are substantial concerns with regard to the allocation of liability. It remains unclear if, for example, such liability may fall to one or more parties in a distributed architecture or if a liability arises in relation to direct losses or extends also to indirect losses. The resolution of such disputes starts with the identification of the legal rights and obligations which may exist in a blockchain ecosystem.

Such rights and obligations vary between permissionless and permissioned blockchains.

As permissionless blockchains are typically not controlled by anyone but operate based on an informal consensus, it appears that no contractual rights or obligations among miners or end-uses arise. In fact, there is no established duty of care by miners or end-users owed to other blockchain miners or end-users. In Tulip Trading v Bitcoin Association [2022] EWHC 667 (Ch) the High Court rejected a claim that Bitcoin developers owed a duty of care or a fiduciary duty to an alleged owner of Bitcoin. The claimant, a Seychelles company, had suffered a hack and claimed a total of $4.5 billion from 16 developers alleging that they owed fiduciary and common law duties under English law. The Court determined that open source Bitcoin software developers, applying a code that is widely adopted to trade or store cryptocurrencies, do not owe fiduciary duties or a common law duty of care to parties who use that code to store or trade their crypto assets. However, the Court did not rule out duties being owed in other circumstances which leaves a degree of uncertainty for DLT developers, miners and end-users that a risk of unexpected liability may arise (Jones-Fenleigh & Sanitt, 2022). Furthermore, a group of participants acting fraudulently may be liable for conspiracy, deceit of fraudulent misrepresentation. Notably, it may be in particular difficult to identify participants of permissionless blockchains as these may act under a pseudonymous person. It has been therefore suggested that, in order to identify a pseudonymous participant, one has to be creative: for example, for assets held an order could be obtained to restrict the movement of usage by others which could provoke a reaction from the user, and such reaction would disclose the identity of the user.

In permissioned blockchains, by contrast, arrangements of ‘permitted’ participants, even in absence of a written contract, may represent a binding agreement. In addition, the typical administrator of permissioned blockchains does not only have specific powers but also assumes duties to the other participants, including minders and end-users. In contrast to permissionless blockchains, the identification of specific users will most likely be easy as such records are being held centrally.

Also relevant for liability allocation, blockchains differ from traditional networks such as a network of franchisor and franchisees in that all blockchain participants are linked together. In a traditional network, usually a hub-and-spokes model will be applied, with only the spokes (e.g. the franchisees) being connected to the hub (the franchisor). Therefore, only bilateral contracts apply, but not one multilateral contractual relationship. In a blockchain ecosystem, all nodes are directly linked together and communicate based on a consensus protocol. In contrast to traditional networks, no hierarchical hub-and-spoke model is implemented.

4.2 Types of disputes likely to arise in the blockchain system

Disputes likely to arise in blockchain ecosystems include, according to Norton Rose Fulbright (2016):

- Typical disputes in a permissioned blockchain: Permissioned blockchain rely on a stringent role of the administrators or super-users to only allow new participants onto the blockchain that meet entry requirements. If they fail to do so by permitting also other participants, this increases the counterparty risk and the risk of a breach of AML and KYC rules rises. Most likely, disputes will arise among participants. Other

similar disputes relate to miners not following the protocols when adding new blocks which results in payments or transfers of property not being properly recorded. Furthermore, the so-called 'forking', where two groups of participants accept a block differently and build on it in two different ways, potentially causes disputes among participants. Such disputes are very common as miners may not have received the relevant information about a new block, and they are solved as follows: In Bitcoin, the 'longest chain' of blocks is deemed to be the valid blockchain, with the phrase 'longest chain' usually referring to the chain with the greatest number of consecutive blocks, but actually making reference to the blockchain that has taken the most energy to build. Likewise, in Ethereum the fork choice is solved by means of a modified GHOST (Greediest Heaviest Observed Subtree) protocol which considers the mining power in creating blocks that have links to the main chain. Under this dispute resolution rule, the heaviest chain of blocks is deemed to be the valid blockchain (Narayanan *et al.*, 2016; Robinson, 2019).

- Technological dispute risk: Technological defects, errors and improperly formed messages may lead to unexpected outcome and may result in disputes. The consequences will, for example, depend on the nature of the software used. Insofar a software provided by a blockchain platform operator under a license agreement is used, such platform may be liable for any damage caused. This is most likely different if an open source software is applied where no contractual relationships exist. In such cases, a court would consider a duty of care of the developer towards the users of the software. Also related to technological defects is B2C2 Ltd v Quoine Pte Ltd [2019] SGHC(l) 3, where the Singapore International Commercial Court (SICC) ruled that virtual currencies can be considered as property and therefore capable of being held

on trust. In seven trades, the electronic market maker B2C2 had sold Ethereum in exchange for Bitcoin in 2017. The trades were automatically performed by Quoine's platform in response to orders from B2C2's custom algorithmic trading software. Due to a defect in Quoine's software, the trades were executed at a rate approximately 250 times the Ethereum and Bitcoin market exchange rate, in favour of B2C2's trades and B2C2's account was automatically credited with the proceeds of the sale. When Quoine realised a serious error had occurred, the trades were cancelled and the transactions were reversed. B2C2 brought proceedings against Quoine, claiming that Quoine's decision to reverse the trades was a breach of the contractual terms between the two parties. Quoine argued that it was right to reverse in accordance with the 'doctrine of mistake'. B2C2 was entitled to a claim in damages for both breach of contract and breach of trust, with damages to be assessed at a later hearing, if not agreed (Baker *et al.*, 2019). The Singapore Court of Appeal (SGCA) in Quoine Pte Ltd v B2C2 Ltd [2020] SGCA(I) 02 affirmed in part the SICC's ruling that Quoine breached its own contract but allowed the appeal on the breach of trust issue. The SICC had ruled that the practice of holding a customer's tokens in a segregated wallet was sufficient to create a trust in favour of the customer and that reversing the trades represented a breach of trust. This decision was reversed by the SGCA which ruled that there was no express trust over the digital tokens in B2C2's account as there existed no certainty of intention to create a trust. Further, the SGCA ruled that the mere fact that Quoine's assets were segregated from its customer's assets did not conclusively determine that a trust was created. Both the SICC ruling and the SGCA decision which in part reversed the first instance judgment provide guidance on how the doctrine of mistake (common mistake, mutual

mistake, unilateral mistake) can be applied to contracts that are automatically entered into through computer programming (Low & Mik, 2020).

- Oracle dispute risks and trust boundaries: A further set of potential disputes relates to oracles providing false data which could affect multi participants. Consequently, claims against oracles could arise. Further, end-user could start disputes among themselves, due to, for example, wrong payments, wrong demand for collaterals.

4.3 Regulation of decentralised autonomous organisations

Blockchain-based applications raise new legal questions concerning the regulation of decentralised autonomous organisations. Different from traditional online applications, the information is deployed on the blockchain and not stored on a server at a specified geographic location. Furthermore, blockchains are multinational and are not owned or controlled by any individual, agent or corporation. This raises the question who can be made responsible for any torts or wrongdoing (EIOPA, 2022). Wright and De Filippi (2015) make the following three proposals:

The first approach refers to the so-called ‘nearest person principle’ which also the consultation paper of the Maltese Parliamentary Secretariat (2018) proposed as a solution to assign a legal identity to autonomous entities that interact with humans. For example, if a self-driving autonomous car killed an individual by mistake, then, according to the nearest person principle, the car manufacturer would be held liable. If applied on a blockchain, the creators of a decentralised autonomous organisation would be held liable for damage. However, such approach neglects that the creators of such organisation will be most likely not identifiable.

The second approach proposed by Wright and De Filippi (2015) makes the users of the blockchain responsible and liable for any damage arising from the services they pay for, insofar they commercially benefit from the transactions. However, the problem stemming from the pseudonymous character of the participants arises.

As a third approach, the decentralised autonomous organisation itself could be held liable. It appears, however, impossible to recover any damages from rather virtual organisations without any legal, contractual relationships in place.

Decentralised autonomous organisations are a challenge to any regulator, and, if a complete shut down or a ban of certain online activity is to be avoided, the regulator needs to rely on the organisations' cooperative mode with the regulatory framework in which they operate. As a consequence, regulators could consider resorting to draconian measures with limited effect and, for example, filter internet service providers, blacklist malicious organisations and criminalise specific software developers.

4.4 Cross-border transactions: governing law and jurisdiction challenges

Questions regarding governing law and jurisdiction appear wherever cross-border transactions occur. Typically, a distributed ledger has nodes in multiple jurisdictions which gives rise to this matter. Furthermore, especially 'native' DLT assets, both tangible and intangible, where ownership records are held purely digitally, could be allocated to any jurisdiction globally.

Typically, courts will apply the law that all parties have expressively agreed to. If there is no express choice of governing law and jurisdiction by the parties involved, courts will generally consider existing conflicts of law rules to determine the relevant

law. For example, they will, *inter alia*, examine the applicability of the Rome I Regulation as discussed above (Rühl, 2021). As part of such considerations, courts may also evaluate if overriding provisions might apply, such as consumer protection law, data protection law, or laws with respect to general terms and conditions. If a dispute involves multiple contracts with multiple express choices, the determination of applicable law is more difficult (Law Commission, 2021).

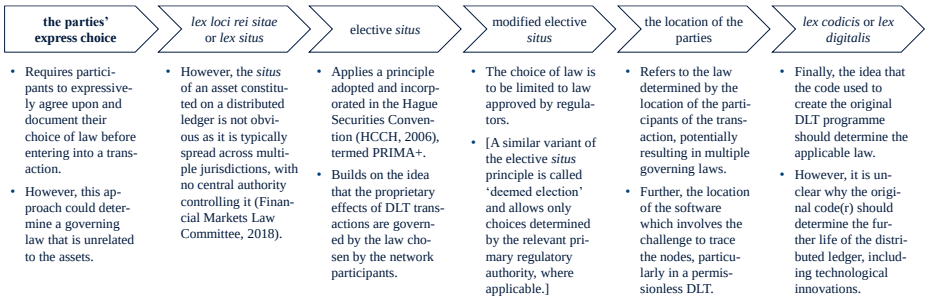

Fig. 1. Solutions to overcome the governing law and jurisdiction challenges of blockchains.

A series of possible solutions has been developed to overcome the governing law and jurisdiction challenges of blockchains, including the following six (Fig. 1):

1. Courts in most jurisdictions will uphold the parties' express choice of governing law and jurisdiction. Such approach requires participants to expressively agree upon and document their choice of law before entering into a transaction, most likely by entering this choice in a certain field in the code. However, this approach could determine a governing law that is potentially unrelated to the assets and that applies undue external or private influence.
2. One further possible solution may be the doctrine *lex loci rei sitae* ('law of the place where the property is situated'), also referred to as *lex situs* principle. However, the *situs* of an asset constituted on a distributed ledger is not obvious as it is typically

spread across multiple jurisdictions, with no central authority controlling it. More specifically, the Financial Markets Law Committee (2018) lists six questions that demonstrate the limitations of the *lex situs* principle in a DLT environment. However, the paper acknowledges that, wherever there is tangible (immovable) property involved, courts will most likely seek to apply the *lex situs* principle in relation to the underlying asset, as a result of its traditional conflict of laws analysis, irrespective of any new technology underpinning the transaction.

3. Another solution, referred to as elective *situs* approach (to preserve the analogy with the *lex situs* principle), applies a principle adopted and incorporated in the Hague Securities Convention (HCCH, 2006), termed PRIMA+, and builds on the idea that the proprietary effects of DLT transactions are governed by the law chosen (elected) by the network participants. Under such approach, the law governing ownership, transfer and use of assets is contractually chosen by the participants. The chosen law applies to the proprietary effects of all transactions on the system; it is transparent to all participants and can be reported for regulatory purposes. However, according to the Financial Markets Law Committee (2018), a significant challenge is that this approach may provoke the perceived regulatory risks in allowing an unfettered choice of law. In fact, the elective *situs* approach could determine a governing law for all participants that is potentially unrelated to the governed assets and that applies potentially undue external or private influence. However, assets could be, as a result, transferred to other jurisdictions which could represent some kind of 'regulatory arbitrage'. At the beginning of 2022, only three countries (Mauritius, Switzerland and

the US) had adopted the Hague Securities Convention, while, for example, the European Commission in 2009 withdrew a proposal for a Council decision that recommended that the Member States sign the convention.

4. The latter problem could be solved by applying a modified elective *situs* approach, under which the choice of law would be limited to law approved by regulators. A highly similar variant of the elective *situs* principle is called 'deemed election' and allows only choices determined by the relevant primary regulatory authority, where applicable. However, it is unclear how a DLT could come under the primary purview of a particular national regulatory authority.
5. Another solution refers to the law determined by the location of the participants of the transaction, potentially resulting in multiple laws governing various transactions comprising a block which appears unappealing. Further, such solution may refer to the location of the software which involves the challenge to trace the nodes, particularly in a permissionless DLT.
6. In connection with smart contracts, the idea has appeared that 'the code is the contract' and hence the code used to create the original DLT programme should determine the applicable law. Such *lex codicis* or *lex digitalis* will, however, most likely not be accepted in practice as it is unclear why the original code(r) should determine the further life of the distributed ledger, including potential various technological innovations that it will be adjusted to by the administrator (who is typically not identical to the original coder). In addition, and more fundamentally, courts and states will most likely not accept such approach which undermines basic principles of law.

As a practical advice, contracting parties should, as far as possible, enter into an 'umbrella dispute resolution agreement' that determines the governing law and the dispute resolution procedure. However, the implementation of such umbrella agreement will most likely be only possible in a permissioned, but not in a permissionless blockchain environment.

5 Conclusion

We study a series of uncertainties and potential challenges in relation to the implementation of distributed ledger technology and blockchain applications. Such challenges may be overcome but require common global standards in relation to, for example, the governing law and the allocation of liability. The decentralised, autonomous nature of DLTs, most likely implemented in a cross-border environment, creates complex problems. To benefit the most from blockchain and distributed ledger technology, financial services firms should ensure that they not only anticipate potential barriers, problems and disputes, but ensure that regulatory, compliance and legal risks are properly addressed and mitigated.

References

1. Baker, C., & Werbach, K.: 'Blockchain in financial services'. In Madir, J. (Ed.). FinTech: Law and Regulation, Cheltenham (2019).
2. Baker, S., Wackwitz, G., & Shields, E.: 'Cryptocurrencies: Property, Trust and Mistake' (2019). Available at https://www.whitecase.com/sites/whitecase/files/files/download/publications/cryptocurrencies-property-trust-and-mistake.pdf (accessed 1 April 2022).

3. Barbosa, L.P.: ‘Blockchain Smart Contracts: A Socio-Legal Approach’. European Business Law Review 32(2), pp. 251–294 (2021).
4. Carson, B., Romanelli, G., Walsh, P., & Zhumaev, A.: ‘Blockchain beyond the hype: What is the strategic business value?’, McKinsey & Company, 19 June (2018). Available at https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/blockchain-beyond-the-hypewhat-is-the-strategic-business-value (accessed 17 January 2022).
5. Chamber of Digital Commerce: ‘Smart contracts: 12 use cases for business & beyond’. December (2016). Available at http://digitalchamber.org/assets/smart-contracts-12-use-cases-for-business-and-beyond.pdf (accessed 17 January 2022).
6. EIOPA: ‘Discussion paper on blockchain and smart contracts in insurance’ (2021). Available at https://www.eiopa.europa.eu/sites/on-blockchain-29-04-2021.pdf (accessed 17 January 2022).
7. EIOPA: ‘Feedback statement – Discussion paper on blockchain and smart contracts in insurance’ (2022). Available at: https://www.eiopa.europa.eu/sites/default/files/feedback/feedback_statement_-_discussion_paper_on_blockchain_and_smart_contracts_in_insurance.pdf (accessed 8 May 2022).
8. European Parliamentary Research Services: ‘Blockchain and the General Data Protection Regulation’. STOA – Panel for the Future of Science and Technology (2019). Available at https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf (accessed 17 January 2022).
9. Financial Markets Law Committee: ‘Distributed Ledger Technology and Governing Law: Issues of Legal Uncertainty’ (2018). Available at http://fmlc.org/wp-content/uploads/2018/05/dlt_paper.pdf (accessed 17 January 2022).
10. HCCH: ‘36. Convention on the law applicable to certain rights in respect of securities with an intermediary’ (2006). Available at https://assets.hcch.net/docs/3afb8418-7eb7-4a0c-af85-c4f35995bb8a.pdf (accessed 17 January 2022).

11. Jones Day: ‘Blockchain for business’. White paper. September 2017, updated November 2018 (2018).
12. Jones-Fenleigh, H., & Sanitt, A.: ‘High Court rejects claim blockchain developers owe duties to users’ Insider Tech Law, 29 March (2022). Available at https://www.nortonrosefulbright.com/en/knowledge/publications/94fda209/high-court-rejects-claim-blockchain-developers-owe-duties-to-users (accessed 1 April 2022).
13. Law Commission: ‘Smart Legal Contracts: Advice to Government’, (2021). Available at https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/11/Smart-legal-contracts-accessible.pdf (accessed 1 April 2022).
14. Low, K.F.K., & Mik, E.: ‘Lost in Transmission: Unilateral Mistakes in Automated Contracts’. Law Quarterly Review 136(4), pp. 563–569 (2020).
15. Madir, J.: ‘Smart Contracts: (How) Do They Fit Under Existing Legal Frameworks?’ (2018). Available at https://ssrn.com/abstract=3301463 (accessed 17 January 2022).
16. Maltese Parliamentary Secretariat for Financial Services, Digital Economy and Innovation of the Office of the Prime Minister: ‘Malta, a leader in DLT regulation’ (2018). Available at https://meae.gov.mt/en/Public_Consultations/OPM/Documents/PS%20FSDEI%20%20DLT%20Regulation%20Document%20OUTPUT.PDF (accessed 17 January 2022).
17. Moerel, L.: ‘Blockchain & Data Protection … and Why They Are Not on a Collision Course’. European Review of Private Law 26(6), pp. 825—851 (2018).
18. Nakamoto, S.: ‘Bitcoin: A Peer-to-Peer Electronic Cash System’ (2008). Available at https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf (accessed 17 January 2022).
19. Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S.: ‘Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction’, Princeton (2016).
20. Nofer, M., Gomber, P., Hinz, O., & Schiereck, D.: ‘Blockchain’. Business & Information Systems Engineering 59(3), pp. 183–187 (2017).

21. Norton Rose Fulbright: ‘Unlocking the blockchain. A global legal and regulatory guide’ (2016). Available at https://www.nortonrosefulbright.com/en-de/knowledge/publications/238dab88/energy-technology-and-arbitration--the-latest-buzz (accessed 17 January 2022).
22. Pisa, M.: ‘Reassessing expectations for blockchain and development’. Essay paper. Center for Global Development (2018). Available at https://www.cgdev.org/sites/default/files/reassessing-expectations-blockchain-and-development-cost-complexity.pdf (accessed 17 January 2022).
23. Raskin, M.: ‘The law and legality of smart contracts’. Georgetown Law Technology Review 1(2), 305-341 (2017).
24. Robinson, P.: ‘The merits of using Ethereum MainNet as a Coordination Blockchain for Ethereum Private Sidechains’ (2019). Available at https://www.researchgate.net/publication/333716999_The_merits_of_using_Ethereum_MainNet_as_a_Coordination_Blockchain_for_Ethereum_Private_Sidechains (accessed 1 April 2022).
25. Rühl, G.: ‘Smart (legal) contracts, or: which (contract) law for smart contracts?’ In Cappiello, B., & Carullo, G. (Eds.). Blockchain, Law and Governance, Dordrecht/Heidelberg/New York/London (2021).
26. R2/Norton Rose Fulbright: ‘Can smart contracts be legally binding contracts? An R3 and Norton Rose Fulbright white paper’ (2016). Available at https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/imported/norton-rose-fulbright--r3-smart-contracts-white-paper-key-findings-nov-2016.pdf (accessed 17 January 2022).
27. Szabo, N.: ‘Smart contracts: formalizing and securing relationships on public networks’. First Monday 2(9) (1997). Available at https://firstmonday.org/ojs/index.php/fm/article/view/548/469 (accessed 17 January 2022).
28. Werbach, K. & Cornell, N.: ‘Contracts Ex Machina’, Duke Law Journal 67(2), 313-382 (2017).

29. World Economic Forum (WEF): ‘Deep Shift Technology Tipping Points and Societal Impact’, Survey Report, September 2015, Cologny/Geneva (2015).
30. Wright, A. & De Filippi, P.: ‘Decentralized blockchain technology and the rise of lex cryptographia’ (2015). Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664 (accessed 17 January 2022).
31. Zetzsche, D.A., Buckley, R.P., & Arner, D.W.: ‘The distributed liability of distribute ledgers: legal risks of blockchain’. EBI Working Paper Series, 2017 – No. 14 (2017). Available at https://www.researchgate.net/publication/319579191_The_Distributed_Liability_of_Distributed_Ledgers_Legal_Risks_of_Blockchain (accessed 17 January 2022).
32. Zetzsche, D.A., Arner, D.W., & Buckley, R.P.: ‘Decentralised Finance’. Journal of Financial Regulation 6(2), 172–203 (2020).