Towards Governance and Dispute Resolution for DLT and Smart Contracts

Jörn Erbguth
Institute of Information Service Science - CUI
Geneva School of Social Sciences,
University of Geneva
Route de Drize 7, 1227 Carouge, Switzerland
jorn.erbguth@unige.ch

Jean-Henry Morin
Institute of Information Service Science - CUI
Geneva School of Social Sciences,
University of Geneva
Route de Drize 7, 1227 Carouge, Switzerland
jean-henry.morin@unige.ch

Abstract— **Illegal content on a blockchain cannot be removed and the originator might not be identifiable. At the same time, node operators that have no control over the content stored on their nodes might be held legally responsible. As a decentralized system, Digital Ledger Technology (DLT) needs decentralized governance and smart contract dispute resolution. Existing DLT governance and dispute resolution is only aimed at balancing the interests of DLT and smart contract participants. It fails to address the interests of third parties and society. The failure to do so could trigger government and court intervention within DLT systems. Although the decentralized nature of a DLT system will offer some protection against this intervention, participants might be identifiable and subject to legal prosecution. We present a design also addressing the interests of society and third parties that will have to be accompanied by an international legal framework.**

Keywords-component; Blockchain; DLT; Dispute Resolution; Governance; Arbitration

I. INTRODUCTION

Society is increasingly reliant on digitally stored and managed data. Distributed Ledger Technology (DLT) ensures a high level of immutability and protection against unauthorized manipulation of data. A single participant, a single institution or even a single country cannot tamper with, or stop, such distributed ledgers.

But who has control over the content of a blockchain? The software needs maintenance updates to resist attacks. Bugs are inherent to software. No public blockchain can exist with static code for a long time. The software will decide over future content and whether to accept changes to existing content. Who decides if a software update is accepted? Finally, who is legally responsible for illegal content that is stored and not removed from a decentralized system? How can we balance decentralized systems, decentralized governance and legal responsibility?

In order to start addressing such questions and the corresponding complexity, this paper attempts to document the problem from a legal and technical perspective and proposes a possible design to serve as a basis for discussion and experimentation. The paper is structured as follows: section 2 describes the background and states the problem. Section 3 covers the state of the art along the different aspects of the problem. Section 4 describes the requirements towards a tentative design proposed in section 5. Finally, the paper concludes with a discussion and an outlook for future work.

II. BACKGROUND AND PROBLEM STATEMENT

Cryptography and decentralization are the means for DLT to ensure the immutability of records stored on the ledger. However, absolute immutability seems not to be desirable. Software needs to be updated, bugs need to be fixed. But how are these updates and patches decided upon?

A. DLT Governance

The physical layer is the basic layer of DLT governance. Whoever controls the hardware has the power to install whatever software version on a node. If participants want to, they can always install different software and thereby overturn any other governance decisions [5]. Whenever participants disagree on that level and install incompatible software, it results in a hard fork splitting the DLT system. To avoid a split of the system, governance on the second level is coordinated through

institutions or software. Collecting votes off-chain helps to predict the behavior of participants and reduces surprises regarding the adoption of updated versions of the software of the DLT system. Bitcoin [22] and Ethereum [7] have their proper proposal voting mechanism. Other DLT systems, like TEZOS [18] or EOS [9], integrate the voting and adoption of the vote into the DLT software.

B. *Dispute Resolution*

When there are disputes over smart contracts, it might not seem reasonable to involve the whole blockchain and even risk a hard fork. There should rather be an integrated dispute resolution mechanism allowing the parties to reach an agreement.

Smart contracts on blockchains can securely automate contracts. However, there are still many possible reasons why a smart contract should not be executed as coded. Integrating dispute resolution into the contract would ensure continuity even when smart contracts don't work out. How should such dispute resolution be designed to be flexible enough and, at the same time, provide the required trust for immutability?

C. *Justification, Legal Recognition of Governance, Node Operator Privilege and Liability*

Low voting participation, conflicts of interest, risk of centralization and dependence on experts are prevalent issues in the discussion of blockchain governance. The discussion in the blockchain community often focuses on game theory and finding a model where centralization of power is prevented and voting in favor of good decisions for a blockchain are in the individual commercial interest of everyone participating in the vote [5], [28]. However, if we want lawmakers and courts to respect autonomous decisions of DLT systems, we must address further issues:

1) Justification. Why should someone have the right to decide on issues that affect others? Why should someone have such power over others? We know models ranging from democracy (one person, one vote) to shareholders (vote dependent on the economic share somebody has in an activity) to stakeholders (votes depending on who is affected by a decision).

2) Recognition of decisions. Will a decision be recognized by the courts? A court that will not recognize a governance decision might force node operators and other actors to violate the rules of the DLT system. Although the distributed nature of a public blockchain renders it very difficult to completely enforce a decision, court cases overruling blockchain governance decisions can have a severe impact on the trust and value of tokens on a blockchain, and on local ventures using that blockchain.

3) Liability. Currently node operators – although without influence on the content of a blockchain – might be legally liable for illegal content stored on the blockchain. Possible issues range from data protection [11], [41], antitrust violations [26] to child pornography allegedly stored on blockchains [27]. Single node operators have no influence on the content stored in their node. They only have the choice to run a node or to shut it down. Should we have a blockchain node operator liability privilege that is comparable to the communication provider privilege we already know?

4) Liability for decisions. Node operators should not be liable because they have no choice regarding the content they store. However, with DLT governance, participants in that governance have a choice. Unlike the single node operator, participants have a choice to vote aligned with the law. German law limits the civil liability of judges to cases where their decisions are considered criminal acts (§ 839 Abs. 2 S. 1 BGB [16]). The German Bundesgerichtshof has also applied this privilege to private judges in arbitration courts [4]. On the other hand, supervisory board members of stock corporations are liable for illegal decisions they take [37]. Do participants in DLT governance equally need assurance that a decision they take in good faith will not lead to legal prosecution or should we impose a liability for negligent governance decisions?

D. *Problem Statement*

Blockchain governance and smart-contract-based arbitration currently only resolve disputes among their participants. They avoid addressing the issue of the accountability of their decisions to outside parties and society. Data stored on DLT might infringe on the rights of other people, like copyright or trademark owners. The execution of some smart contracts might contravene criminal law. The failure to address these interests will generate increasing court and government intervention with blockchains. Node operators, miners and other participants might be prosecuted for the mere fact of participating in a DLT system. Therefore, a technical framework of DLT governance and dispute resolution needs to be

established; one that goes beyond resolving disputes between DLT participants but also ensures the respect of third party rights and criminal law. A legal framework needs to set the rules for such a technical framework and should ensure the acceptance of decentralized decisions against the intervention of local courts or local government agencies.

III. STATE OF THE ART

A. *Distributed Ledger Technology*

Blockchain technology, although having some roots before, originated with the publication of the Bitcoin-paper [30]. It was published under the name of Satoshi Nakamoto, which still remains an unresolved pseudonym. Nakamoto created a cryptocurrency called "Bitcoin". Bitcoin is based on a decentralized autonomous blockchain. It is "trustless", which means that it does not require trust in a single authority organizing or controlling the cryptocurrency. Instead, trust is provided by its technology and the distribution of copies to many nodes. In 2015, blockchain technology started to attract general attention. The Economist ran a cover story [40]. The author, Jon Berkley, used the metaphor "The trust machine" to describe the very essence of blockchain technology that goes far beyond cryptocurrencies. The basis for blockchain technology existed long before Bitcoin. Blockchain technology is based on hash-functions, Merkle trees, public key cryptography and consensus algorithms. DLT is the more general concept of Blockchain technology. It is often used synonymously but also includes distributed ledgers that are not organized in linear blocks like hashgraphs [38].

IV. SMART CONTRACTS

The rules for transactions are hard coded on the Bitcoin blockchain: Rules, for example, limit the transfer of Bitcoins in a transaction to the number of coins the source accounts hold and a transaction must be signed by the private key of all source accounts. To build a system that supports different types of transactions with different rules, different blockchains are required. To avoid having to build specific blockchains for each transaction type and rule set, Buterin introduced Ethereum, with programmable rules that are called Smart Contracts [6]. Smart Contracts in this sense are small programs that implement the rules of a specific set of transactions on a blockchain. Smart contracts receive messages and perform transactions as a result. The Smart Contracts in Ethereum are Turing complete. Those Smart Contracts can store data and Ethereum's crypto coins ("Ether"). Depending on the rules in the Smart Contract and the messages sent, the Smart Contract will alter its internal data and/or will perform a crypto currency transaction on the blockchain.

The term Smart Contract was coined before by Nick Szabo, independently of the concept of a blockchain. His idea was to embed contractual clauses into automated systems. Today, smart contracts consist out of three possible aspects:

- the definition of contractual duties in the form of a computer program or algorithm,
- the execution of a legal contract by a machine and
- the transparent and secure combination of both aspects usually by means of DLT.

Traditionally, when people bought property, they were free to use, dissemble, transform, sell or transfer it. Today, many property purchases are transformed into services. Service contracts grant fewer rights than property: For example, the use of a service might be restricted to a certain territory or person and the resale might be forbidden. When consumers exceed those limits, for example by driving a car to certain countries or default on payment, the service provider reserves the right to block further use of their services. This denial of service is often enforced by technological means. The consumer, however, has no possibility to verify whether this blocking mechanism is only involved when the legal conditions are met. While a purchase of a property requires the seller to take legal action if contractual conditions are not met, in a service based economy, the consumer must sue the service provider if the contractually agreed upon full service is not provided. A Smart Contract can ensure that the rules for permitted service denial cannot be manipulated. In such cases, the smart contract acts like an automated trustee.

A. *Legal Nature of Smart Contracts*

A legal contract is an abstract legal instrument. Its main requirement is – as set forth in Article 1 of

the Swiss Code of Obligations – the mutual expression of intent by the parties. The expression of intent does not usually need a specific form and may be expressed or implied [15]. Therefore, a legal contract can be expressed in code and agreed upon through messages sent to a smart contract code on a blockchain [21], [29].

However, there can be numerous reasons why a smart contract code might not be recognized as a legal contract. For example, there might be conflicting consumer protection rules, transparency or specific form requirements. These risks, however, are not specific to smart contracts but exist for paper contracts too. Smart contracts bear the additional risk of legal uncertainty. The application of the law to DLT is not settled yet. A parallel paper contract might be a good means to counter this risk.

The law knows the principle *pactas sunt servanda* – agreements must be kept. But what is the agreement? It is not necessarily what is documented on paper or stored on a blockchain. Art. 18 of the Swiss Code of Obligations states that: "When assessing the form and terms of a contract, the true and common intention of the parties must be ascertained without dwelling on any inexact expressions or designations they may have used either in error or by way of disguising the true nature of the agreement" [15]. This legal principle is known as *falsa demonstratio non nocet* and exists in most jurisdictions.

There are exceptions to sticking to the intent of the parties. Changing circumstances might lead to an extraordinary right to terminate a contract: *clausula rebus sic stantibus* [29]. Conflicting mandatory law is another potential reason to deviate from the original intent of the parties.

As a result, code can be law [24]. But in numerous situations, the law will be different from what is written in the code. Therefore, code can be law, except when it isn't [33].

B. *Existing DLT Governance*

In open computer systems, the computer operator has the power to decide on any manipulation of the data stored on it. Closed computer systems, like iOS or Android, limit this power to a certain extent in favor of a trusted service provider. Neither model is desired for a DLT system. Only the holder of the relevant private key(s) shall have the power to conduct a transaction and no single entity should be able to undo a transaction. Since there is no physical control over the computer systems of the nodes, a consensus algorithm ensures that all nodes that deviate from the consensus will be excluded from the network.

1) Permissioned and Permissionless DLT Systems. In a *public* or *permissionless* system, anyone can take over any role. When forming a consensus, a sibyl attack must be prevented. In a sibyl attack, the attacker creates many virtual participants that outnumber the votes of the other participants. Common consensus mechanisms countering this attack are proof of work or proof of stake. The idea behind these algorithms is that no single potentially malicious entity will be able to have more computing power or more tokens than the others combined. In a *permissioned* DLT system, the participation in the system is limited to known participants. This ensures that no malicious outside participant can break the system. It also makes sure that accepted participants do not perform sibyl attacks. However, a lot of power is shifted to the process of participant acceptance. To ensure the distribution of power, the acceptance of participants needs to be distributed. Independent legal entities like corporations, associations or foundations are confronted with similar problems: For example, to increase the capital of a limited liability company (GmbH) in Germany, ¾ of existing votes need to be in favor of increasing capital and voting rights (§§ 3 Abs. 1 Nr. 3, 55, 53 Abs. 2 S. 1, 2 GmbHG [25]). Similar rules also exist in many other jurisdictions. Associations, as another example, regulate in their statutes who makes decisions about accepting new members and how this decision-process is being conducted. After being accepted, the new members themselves will have voting rights. Foundations, as a third example, regulate in their statutes as to how supervisory board members are selected.

2) On-Chain-Governance and Off-Chain-Governance. The basic layer of on-chain governance is the physical layer and is enforced by the consensus algorithm [5]. This is an integral part of blockchain software and makes sure that a non-compliant minority will be excluded from participating in the DLT system. This enables a basic form of governance through hard forks. Any other governance can be broken by a hard fork. Therefore, this basic level will always serve as a last resort control mechanism.

Supervisory boards like the NEO council [31] offer special rights to the founders and developers of a DLT system. However, their existence runs counter to the idea of decentralization and equal rights. Bitcoin [22] and Ethereum [7] both know voting mechanisms where the results are not automatically enforced. This off-chain-governance has the advantage that governance decisions will always be double-checked by humans. Governance must always be able to cope with the unexpected. The scope of on-chain-governance is always limited to certain foreseeable scenarios and decisions [34]. For these rare cases, however, on-chain-governance can always be complemented by off-chain-governance and hard forks.

Most recent DLT systems know some on-chain-governance. In *TEZOS* [18], only active coin holders have the right to vote. The voting process is a process staged in 4 parts and is held every 3 months. TEZOS knows a flexible quorum and a minimal vote for acceptance of 80%. *EOS* [9] has indirect voting. 21 block producers are selected by coin holders. EOS has a constitution. The constitution is voted upon and every participant must accept it. EOS is currently debating a proposal whether a two third majority of block producers can vote to freeze smart contracts where a party asserts that the code does not run as intended [2].

Lisk [19] knows 101 delegates who are elected by coin holders. To be elected, delegates share some of the block fees with their voters. This "cashback" is regarded as a bribe that fosters wrong decisions. Most delegates are from one of two consortiums. Voters will only receive their share of the block fees if they vote for the consortium with all their votes. Since delegates who are not voted for will not be able to receive votes, there is a strong tendency to preserve and concentrate power.

Unless it concerns legal systems where courts can be called to intervene, DLT governance aims to be designed in a way that neither offers nor requires a means to intervene in on-chain-governance decisions.

C. *Dispute Resolution For and With Smart Contracts*

The judicial system is the traditional system to resolve conflicts in our society. Justice is provided by ensuring a fair procedure and enforcing fundamental legal values. In common law countries like the U.S. and the U.K., emphasis is placed on executing a fair procedure, whereas in civil law countries like continental Europe the emphasis is on the fundamental legal values.

The legal system has many problems. A pertinent one is the limited access to justice. Trials are expensive and take a long time, so only a small percentage of conflicts are solved through the legal system. Another problem is the adversarial nature of the legal procedure. Conflicts are escalated and damage is maximized before a decision can be found. This tendency is especially criticized in family law where innocent children suffer the most from an escalated separation process.

People are increasingly hesitant to go to trial and the number of trials is decreasing.

1) Online Dispute Resolution (ODR). Conventional litigation in courts by sending paper documents and pleading in the physical court room is slow and expensive. Access to justice is often limited to people who can afford to pay a lawyer. Legal tech and eJustice promises to automate services, and render them more accessible and cheaper. Secure online communication between courts and lawyers, like the besondere elektronische Anwaltspostfach (beA) in Germany, is a late first step to replace paper letters by sending PDFs or scanned messages. Almost 3 years late, this project is finally working. Much further advanced is Denmark. Proceedings are managed via an integrated digital platform [8]. Clients have direct access to the system, which also manages the documents, deadlines and progress of the case.

2) Alternative Dispute Resolution (ADR). Alternative Dispute Resolution resolves disputes out of court. There is arbitration, which appoints one or several private arbitrators who form a private court to decide on a case in an adversarial procedure. Other forms of ADR use different approaches, like mediation. Mediation is a voluntary procedure where the participants aim to find a win-win solution by themselves, supported by a mediator [36]. Mediation fosters the constructive solution of conflicts, whereas litigation often takes longer and unnecessarily escalates problems leading to a lose-lose scenario. Especially in child custody cases, mediation produces better long-term results for all participants [10]. The EU has built a common online system for consumers to access different ADR providers [12], [14]. An arbitration procedure has been ported to smart contracts [20].

3) Platform-based Arbitration. Some platforms like *ebay* and *Paypal* offer a limited form of integrated dispute resolution mechanism [32]. These mechanisms are faster and cheaper than the court system. Courts in Germany have decided, however, that the use of these systems does not preempt court proceedings [3]. This means that a party that is not satisfied with the dispute resolution can still go to court in order to obtain a different decision.

4) Smart Contract API. Smart contracts will not replace lawyers and courts but smart contracts can implement procedures and simplify enforcement [17]. Dispute resolution can be implemented as a smart contract that is called by other smart contracts in the case of a dispute. Startups, like *Kleros* [23], announced to offer arbitration procedures that can be integrated into Ethereum smart contracts.

D. International convention

Most DLT systems are global. Legal rules, however, are specific to nation states. Legal rules in different countries are inconsistent and often contradictory. Compliance with all laws in all countries is not only a heavy burden but also, in many cases, impossible. In general, the law addresses these problems with three approaches:

1) Choice of law and choice of legal forum. Parties of a contract can choose a specific jurisdiction and a legal forum to govern their relations. However, countries reserve the right to apply their proper laws, when the outcome of a dispute runs against their basic principles of laws ('*ordre public*') or national interests.

2) International private law. Countries set laws that determine which court has jurisdiction over a dispute and which law governs a legal dispute involving actors from, or in, different jurisdictions. These rules are also called *conflict of laws*. For example the Swiss *Code on Private International Law* (CPIL) [44] regulates which law governs a marriage or a divorce, and on which conditions a foreign marriage or divorce is recognized. Some criminal laws claim universal jurisdiction. They apply to crimes comitted anywhere by anyone. Other laws are limited to crimes that have a connection to the country that has enacted the criminal law. Some investor protection laws apply to worldwide investments by nationals or residents. Initial Coin Offering (ICOs) therefore increasingly exclude some countries' nationals or residents from participating because full compliance with the laws of those countries is not ensured.

3) International conventions. To avoid conflicts and to remove the possibility to select a favorable legal forum (*forum shopping*), international conventions define uniform legal rules. Whereas most international conventions only oblige member states to implement the rules of an international convention in their laws, some international conventions are directly binding laws. Some conventions, like the European Convention on Human Rights [13], even establish an international court where individuals can directly commence legal proceedings when they feel their rights of the convention are being infringed upon. Member states are bound by the decisions of the European Court of Human Rights. A binding international convention combined with an international court is necessary for the uniform enforcement of human rights. At the same time, international courts are being criticized for limiting the sovereignty of a nation state [43].

4) Evaluation. A DLT system cannot comply with conflicting laws in different countries. Asking that a DLT system complies with all laws in all countries will lead to an unresolvable conflict. Restricting DLT systems to specific jurisdictions does not seem to be practicable regarding the global nature of DLT systems. Offering the possibility to choose a jurisdiction and a legal forum will let many DLT systems select the jurisdiction with the least amount of regulations and missing enforcement of third parties' rights. The need for a uniform body of law for DLT systems has been identified [45]. Starting with a model law, this uniform regulation can later be implemented by means of an international convention and an international court [39].

V. REQUIREMENTS

A. General Requirements

Governance and dispute resolution must work efficiently, bring reliable and consistent results, minimize conflicts of interest, and provide an incentive to participate in good faith.

B. Technical Requirements

DLT governance needs to avoid centralized oversight. However, without centralized oversight there is an increased risk of abuse of the system. There are two approaches to this problem: nominate a group of known and trusted supervisors or create a robust system for anonymous public participation. In case of the second alternative, game theory approaches can impede the monopolization of control of a system. Governance and dispute resolution should be an integral part of a DLT

system. On-chain-governance will not break the system when encountering a conflict. On-chain-governance, however, will not be able to solve every conflict. When there are issues or bugs connected to the governance procedure itself, a hard fork might still be necessary. However, on-chain-governance ensures that manual hard forks are the very exception of the rule.

C. *Legal Requirements*

Existing laws are not fully compatible with the principle of DLT systems. Even comparatively new regulation such as the GDPR in Europe does not take into account the decentralized nature of blockchains. This results in a lack of legal certainty. Some countries are starting to switch from explaining how to apply existing regulation to blockchain to designing appropriate legislation for DLT systems. Liechtenstein has proposed a law to regulate the token economy as *sui generis* [35], rather than trying to explain why the same type of token needs to be treated differently depending on the values and expectations connected to it. The design process for DLT governance and dispute resolution needs to create legal certainty and include a legal design based on established principles of the law.

1) Remedy Against Illegal Content. The legal system usually requires a) holding somebody responsible for illegal content and b) to foresee a possibility to take that illegal content down. Public blockchains usually grant neither remedy. This might be the toughest issue between the legal and the crypto community. Granting only one of both possible remedies might be a solution that society can accept. Take, for example, the freedom of the press. This grants the right to keep illegal content in already printed and sold publications e.g. in public libraries, but will hold the publisher responsible for publishing it in the first place. On the other hand, internet service providers are not responsible for illegal content, as long as they take it down upon notice.

2) Due Process and Right to a Fair Trial. The principle of due process can be found in most constitutions, human rights conventions, and in the New York Convention. Although often focused on criminal proceedings, it also applies to civil actions. Violation of due process is the most frequent ground on which arbitration awards are challenged. Due process means that legal proceedings are conducted according to the rules and principles established beforehand. Smart contracts are usually well-suited to enforce formal requirements. However, the right to a fair trial in Article 6 of the European Convention of Human Rights is more difficult to validate: it states that the right to access to court is practical and effective.

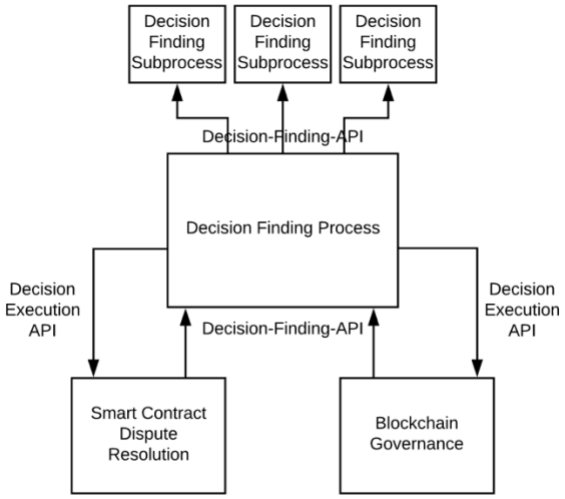

Figure 1: Architecture for decision-finding process

To preempt parallel court proceedings, the right to access a regular court must be waived by the participants of a blockchain. The arbitration must become mandatory. Persons may waive their right to access a regular court in favor of arbitration, provided that such waiver is permissible and is stated freely, in writing and unequivocally. The waiver must be attended by minimum safeguards commensurate to its importance.

3) Recognition of Smart-contract-based Arbitration. Similar to the New York Convention [42], arbitration awards that are not self-enforcing have to be recognized by the law. Courts must not allow a parallel court proceeding when DLT-based dispute resolution or governance is chosen.

VI. TENTATIVE DESIGN OF A COMBINED LEGAL AND TECHNICAL FRAMEWORK

The design of a DLT and Smart Contract governance framework should be a combination of a model law with technical architecture. The model law can be further developed towards an international convention and the technical architecture towards a technical standard.

A. *Model Law*

1) In line with the distribution of control in DLT systems. The model law needs to be in line with the distribution of control in DLT systems. Actors who are free to decide, should be fully responsible. Arbitrators who are bound by the rules of the system should only be liable if they act in gross negligence or purpose against the rules. Node operators or verifiers should only be responsible for performing the tasks in question but not the content it concerns.

How can we establish liability for a participant signing illegal content with his private key and sending it to a blockchain? Do we need to require identification? Does an anonymous participant need to bring some assets that will serve as compensation in case of illegal content?

2) Duty to Breaking a Blockchain. Modifications to existing content on blockchains should be avoided. However, there might be situations where modifications need to be made for technical reasons (bugs, attacks) or for severe legal reasons. This needs to remain the very exception. However, it is not possible to fully exclude this option. The model law should integrate a safeguard that makes sure that modifications are only demanded when the unmodified blockchain would induce a very high damage and there is an international agreement that this damage needs to be avoided at a high cost.

Safeguards can have an international body of judges decide on this issue and which must uniformly agree that a modification is necessary. Another safeguard can be to request a high service fee for those demanding a modification. Third, existing law should be complemented in a way that DLT stored data is exempted from rectification and deletion requirements in most cases.

B. *Technical Architecture*

Governance as well as dispute resolution consist out of two parts: the decision-finding module and the decision-enforcing module:

1) Decision-finding Module. The decision-finding module is connected via a decision API to the system where the dispute occurred. It needs to access the relevant data of the dispute in question. The decision can be taken by:

- rules in the decision-finding module itself,
- external rules, e.g. in a deep learning system,
- another decision-finding module connected via the decision API,
- a manual process that is supervised by the smart contract in the decision-finding module.

When a smart contract is used as a decision-finding module, all relevant data that the smart contract processes is publicly visible. There are different approaches to resolve this issue:

- Sidechains and private nodes: some systems provide a way to hide data and show it only to the participants of the dispute. *Hyperledger Fabric* [1] or side chains can be used for this.
- Acceptance of public pseudonyms: parties can have pseudonyms. Conventional court proceedings are also public and judgments are published under pseudonyms as well. The situation therefore is not worse than before.

2) Decision Execution Module. Decisions can be enforced either by the module where the conflict has originated in or by additional modules that can transfer assets for compensation. When the transaction has not been completed before the decision-finding process has been invoked, the transaction can still be modified to reflect the result of the decision-finding process. If the transaction is already completed, a reversal or a compensation transaction might be needed to enforce the decision. To implement a compensation transaction, the execution module may require a deposit of crypto assets of the involved parties that can be transferred for compensation.

3) Dispute Resolution vs. Governance. Governance of a DLT system concerns some part or the entire DLT system. Governance of a smart contract concerns updates and modification of a single smart contract that might be used in different contexts by different people. Dispute resolution resolves single disputes of a smart contract.

Both dispute resolution and governance can involve more than two parties. However, governance is established by the community behind a DLT system or a smart contract before other people possibly start using it. Dispute resolution, on the other hand, can be freely chosen when it is entered into a smart contract.

Smart contracts are well-suited to implement and keep records of a formal procedure. An API should be able to connect a DLT system or a smart contract

to the governance system. The system should account for different procedures depending on the issues. The smart contract for governance should itself be able to be governed through the same type of API by another smart-contract-based governance.

4) Interests of Third Parties and Governments. Anybody who feels that a DLT system infringes upon their rights should be able to start a dispute resolution procedure. Governments and courts should also have the ability to start a procedure when they observe criminal behavior.

5) Appeal. There needs to exist the possibility to ask for a review of decisions by governance and dispute resolution bodies. In order to avoid a recentralization of DLT systems, these reviews should be conducted in a decentralized way. Governments and courts could participate in this review, for example, by nominating jurors, thus increasing the likelihood of such decisions being accepted by society.

6) Other Contexts. DLT systems are not the only place where an effective global dispute resolution is needed. The approach can be used for non-DLT-related ADR and ODR disputes as well. Those offline disputes need to provide their data through a trusted data channel and can then run along the same lines.

VII. CONCLUSION AND FUTURE WORK

Liability and immutability are the two most demanding points of conflicts regarding DLT and the legal system. Creating a model law towards an international convention that provides for the recognition of DLT-based arbitration and governance will not be easy either. However, without addressing these issues, legal use of public blockchains will not be possible in the long run.

In order to achieve this goal, our next steps will focus on drafting an initial legal and technical framework. The legal part will consist of a proposal for a basic set of rules for the recognition of distributed governance and dispute resolution. The technical framework will define a proof of concept structure for the integration of governance and dispute resolution into distributed systems. It is planned to provide a definition of a model API, together with a reference implementation for the integration of governance and dispute resolution into smart contracts and to find actual cases for evaluation.

[1] E. Androulaki et al. “Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains,” Proceedings of the Thirteenth EuroSys Conference on Computer Systems - EuroSys ’18, pp. 1–15, 2018.

[2] block.one. “Block.one’s Proposal for EOS Constitution v2.0.” Jun. 28, 2018. [Online]. Available: https://block.one/news/block-ones-proposal-for-eos-constitution-v2-0/ [Nov. 12, 2018].

[3] Bundesgerichtshof (BGH), 22. Nov. 2017, ECLI:DE:BGH:2017:221117 UVIIIZR83.16.0. [Online]. Available : http://juris.bundesgerichtshof.de /cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=80382.

[4] Bundesgerichtshof (BGH), "Zur Haftung des Schiedsrichters", Oct. 6, 1954, II ZR 149/53. *Neue Juristische Wochenschrift NJW* 1954, pp. 1763–1764.

[5] V. Buterin. “Notes on Blockchain Governance.” *Vitalik.ca*, Dec. 17, 2017. [Online]. Available: https://vitalik.ca/general/2017/12/17/voting .html [Nov. 12, 2018].

[6] V. Buterin. “Ethereum White Paper A next-generation smart contract and decentralized application platform.” 2014. [Online]. Available: http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation _smart_contract_and_decentralized_application_platform-vitalik-buterin .pdf [Nov. 12, 2018].

[7] “CarbonVote”. [Online]. Available: http://carbonvote.com/ [Nov. 12, 2018].

[8] S. Cavaleri. “Digitalizing Dispute Resolution Processes: The Example of Denmark.” *Yearbook on International Arbitration and ADR* [Online]. Volume VI, Forthcoming. Available: https://papers.ssrn.com/sol3 /papers.cfm?abstract_id=3063982 [Sep. 9, 2018].

[9] block.one. “EOS.IO Technical White Paper v2.” Mar. 16, 2018. [Online]. Available: https://github.com/EOSIO/Documentation/blob /master/TechnicalWhitePaper.md [Nov. 12, 2018].

[10] R. Emery, L. Laumann-Billings, M. Waldron, D. Sbarra and P. Dillon. "Child custody mediation and litigation: Custody, contact, and coparenting 12 years after initial dispute resolution.", *Journal of Consulting and Clinical Psychology*, vol. 69, no. 2, pp. 323-332, 2001.

[11] J. Erbguth and J. G. Fasching. (2017, Dec.). “Wer ist Verantwortlicher einer Bitcoin-Transaktion?” *Zeitschrift für Datenschutz*. ZD, 2017, pp. 560–565. Available: https://erbguth.ch/ZD12-2017.pdf [Nov. 12, 2018].

[12] Online Dispute Resolution. *European Commission*. [Online]. Available: https://ec.europa.eu/consumers/odr/main/?event=main.home.show [Nov. 12, 2018].

[13] *European Convention on Human Rights*, 2010. [Online]. Available: https://www.echr.coe.int/Documents/Convention_ENG.pdf [Nov. 12, 2018].

[14] *Regulation (EU) No 524/2013 of the European Parliament and of the Council of 21 May 2013 on online dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Regulation on consumer ODR), vol. 165. 2013*, 2013. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT /PDF/?uri=CELEX:32013R0524&from=EN [Nov. 12, 2018].

[15] *Federal Act on the Amendment of the Swiss Civil Code - Part Five: Swiss Code of Obligations*. 1911/2017. [Online]. Available: https://www.admin.ch/opc/en/classified-compilation/19110009 /201704010000/220.pdf [Nov. 12, 2018].

[16] *German Civil Code, BGB*. 1896/2018. [Online]. Available: https://www.gesetze-im-internet.de/englisch_bgb/ [Nov. 12, 2018].

[17] D. Givari, M. Pravuljac, B. Susan and N. Sharma. "How Does Arbitration Intersect with the Blockchain Technology that underlies Cryptocurrencies?", *Kluwer Arbitration Blog*, 2018. [Online]. Available: http://arbitrationblog.kluwerarbitration.com/2018/05/05/scheduled-blockchain-arbitration-april-17-2018/ [Nov. 12, 2018].

[18] L. M. Goodman [A. Breitman]. “Tezos—a self-amending crypto-ledger White paper.” 2014. [Online]. Available: https://tezos.com/static /papers/white_paper.pdf [Nov. 12, 2018].

[19] S. Günther, “Lisk — the mafia blockchain.” Jun. 1, 2018. *Medium* [Online]. Available: https://medium.com/coinmonks/lisk-the-mafia-blockchain-47248915ae2f [Nov. 12, 2018].

[20] M. Kaulartz and J. Heckmann. “Erster Praxistest eines Schiedsverfahrens auf Blockchain-Basis mit CMS erfolgreich

abgeschlossen." Jul. 19, 2017. *CMS, Datarella, Press Release* [Online]. Available: https://cms.law/de/DEU/News-Information/Erster-Praxistest-eines-Schiedsverfahrens-auf-Blockchain-Basis-mit-CMS-erfolgreich-abgeschlossen [Nov. 12, 2018].

[21] M. Kaulartz and J. Heckmann. "Smart Contracts – Anwendungen der Blockchain-Technologie.". *Computer und Recht*, 2016, pp. 618-624.

[22] S. Khatwani. "What is a BIP (Bitcoin Improvement Proposal)? Why do you need to know about it?" Jul. 31, 2017. *CoinSutra - Bitcoin Community*. [Online]. Available: https://coinsutra.com/bip-bitcoin-improvement-proposa/ [Nov. 12, 2018].

[23] C. Lesaege and F. Ast, "Kleros Short paper v1.0.5." Jan. 2018. [Online]. Available: https://kleros.io/assets/whitepaper.pdf [Nov. 12, 2018].

[24] L. Lessig. "Code is Law: On Liberty in Cyberspace." *Harvard Magazine*, Jan.-Feb. 2000, 1-2. [Online]. Available: https://harvardmagazine.com/2000/01/code-is-law-html [Nov. 12, 2018].

[25] *Limited Liability Companies Act, GmbHG*. 1892/2017. [Online]. Available: https://www.gesetze-im-internet.de/englisch_gmbhg/ [Nov. 12, 2018].

[26] S. Louven and D. Saive. "Antitrust by Design – Das Verbot wettbewerbsbeschränkender Abstimmungen und der Konsens-mechanismus der Blockchain." *Neue Zeitschrift für Kartellrecht NZKart*, 2018, 348-354.

[27] R. Matzutt et al. 2018, "A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin," In Proceedings of*Financial Cryptography and Data Security* 2018: Twenty-Second International Conference FC'18, Curaçao, Netherlands, Feb. 26 – Mar. 2, 2018. [Online]. Available: https://fc18.ifca.ai/preproceedings/6.pdf [Nov. 12, 2018].

[28] R. C. Merkle, "DAOs, Democracy and Governance." May 2016. [Online]. Available: http://merkle.com/papers/DAOdemocracyDraft.pdf [Nov. 12, 2018]

[29] S. D. Meyer and B. Schuppli, "«Smart Contracts» und deren Einordnung in das schweizerische Vertragsrecht." *recht*, 2017, 204–224.

[30] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system." 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf [Nov. 12, 2018].

[31] NEO *White Paper*. [Online] Available: http://docs.neo.org/en-us/whitepaper.html [Nov. 12, 2018].

[32] PayPal. *Shop with peace of mind, we've got you covered*. [Online]. Available: https://www.paypal.com/lu/webapps/mpp/buyer-protection [Nov. 12, 2018].

[33] J. Peterson, "Code is law, except when it isn't." Jun. 30, 2016. *The Augur Report*. [Online wayback archive]. Available: https://web.archive.org/web/20170228200009/http://blog.augur.net/code-is-law/ [Nov. 12, 2018].

[34] Pool of Stake. "Revisiting the on-chain governance vs. off-chain governance discussion." May 22, 2018. *Medium*. [Online]. Available: https://medium.com/@poolofstake/revisiting-the-on-chain-governance-vs-off-chain-governance-discussion-f68d8c5c606 [Nov. 12, 2018].

[35] *Vernehmlassungsbericht der Regierung betreffend die Schaffung eines Gesetzes über auf vertrauenswürdigen Technologien (VT) beruhende Transaktionssysteme (Blockchain-Gesetz; VT-Gesetz; VTG) und die Abänderung weiterer Gesetze*. Sep. 2018. [Online]. Available: https://www.llv.li/files/srk/vnb-blockchain-gesetz.pdf [Nov. 12, 2018].

[36] C. D. Schäfer. *Einführung in die Mediation*. Wiesbaden, Germany: Springer Fachmedien 2017.

[37] S. Siepelt and L. Pütz, "Die Compliance-Verantwortung des Aufsichtsrats." 2018. *Corporate Compliance CCZ*, 2018, 78–84.

[38] S. Stein, "Hashgraph wants to give you the benefits of blockchain without the limitations." Mar. 2018. *TechCrunch*. [Online]. Available: https://techcrunch.com/2018/03/13/hashgraph-wants-to-give-you-the-benefits-of-blockchain-without-the-limitations/ [Nov. 12, 2018].

[39] A. Tabarrok, "Towards An International Court of Smart Contract Arbitration." Jun. 14, 2018. *Marginal Revolution*. [Online]. Available: https://marginalrevolution.com/marginalrevolution/2018/06/towards-international-court-smart-contract-arbitration.html [Nov. 12, 2018]

[40] The promise of the blockchain - The trust machine - The technology behind bitcoin could transform how the economy works. *The Economist*. Oct. 31, 2015. [Online]. Available: https://www.economist.com/leaders/2015/10/31/the-trust-machine [Nov. 12, 2018].

[41] Blockchain and the GDPR. *The European Union Blockchain Observatory and Forum.* Oct. 16, 2018. Available: https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf [Nov. 12, 2018].

[42] *The New York Convention*. 1958. Available: http://www.newyorkconvention.org/11165/web/files/original/1/5/15432.pdf [Nov. 12, 2018].

[43] S. Thurnheer, "Die EMRK und die Selbstbestimmungsinitiative." *Neue Zürcher Zeitung NZZ*. Jul. 17, 2018. Available: https://www.nzz.ch/meinung/die-emrk-und-die-selbstbestimmungsinitiative-ld.1392214?reduced=true [Nov. 12, 2018].

[44] Umbricht Attorneys. *Switzerland's Federal Code on Private International Law, CPIL*. 1987/2017. [Online]. Available: https://www.umbricht.ch/en/swiss-private-international-law-cpil/ [Nov. 12, 2018].

[45] A. Wright and P. De Filippi, "Decentralized Blockchain Technology and the Rise of Lex Cryptographia." 2015. *SSRN Electronic Journal*. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664 [Nov. 12, 2018].