Cross-Chain Governance

Florian Möslein, Michael Birkner

Abstract *The governance of blockchain-based decentralized autonomous organisations (DAOs) is shaped, in part, by the architecture of the underlying blockchain networks. This chapter examines the governance challenges posed by cross-chain blockchains – advanced technologies that enable interoperability between otherwise discrete blockchain ecosystems. Building on the normative and conceptual frameworks developed in earlier chapters on digital governance and trust in AI, we argue that effective cross-chain governance requires more than technical solutions. It must also address legal coordination, participant evaluative capacities, and the design of systems capable of fostering trust. Cross-chain technologies introduce novel complexities in managing decentralized interactions across heterogeneous networks, necessitating governance models that uphold standards of security, scalability, and decentralisation. Beyond these technical criteria, we argue that legitimate and trustworthy digital governance must also incorporate normative foundations such as agency, responsibility, and practical freedom.*

1. Introduction

As blockchain technology matures, governance models are increasingly shifting from isolated, single-chain systems to complex, cross-chain ecosystems. These ecosystems are often organized through decentralized autonomous organizations (DAOs), which enable collective decision-making through smart contracts and distributed infrastructure. While DAOs promise radical decentralization, they also depend on complex forms of coordination and trust – especially when operating across multiple blockchain networks.

1.1. Challenges regarding Cross-Chain Governance

Cross-chain governance presents new challenges: synchronizing decisions across technical boundaries, maintaining security across different architectures, and ensuring compliance with legal frameworks not designed for decentralized systems. These complexities require more than technical solutions – they require a

rethinking of governance itself. This chapter addresses these challenges by situating cross-chain DAO governance within the broader conceptual framework of digital governance developed in previous chapters. We draw on two complementary perspectives: the enabling capacities approach, which emphasizes the conditions under which individuals and organizations can meaningfully evaluate and engage with digital systems; and a virtue-based account of trust in technology, which shifts the focus from mere system reliability to the normative qualities embedded in the design and operation of technical infrastructures.

1.2. Conditions for Effective Governance

Applying these perspectives to the governance of cross-chain DAOs, we argue that effective governance must do more than ensure interoperability and legal compliance. It must also support participants' ability to understand, evaluate and shape governance processes – and foster trust by embedding norms of responsibility, transparency, and fairness in technical design. Our analysis thus frames cross-chain governance as a case study in applied digital governance. We explore how autonomy, legal accountability, and technological integration can be balanced in a way that preserves practical freedom and allows for normative evaluation. To this end, we examine both the technical mechanisms that underpin cross-chain interoperability and the legal challenges these systems face, drawing in particular on analogies to corporate group law within the German legal tradition (*Konzernrecht*). By integrating technical, legal, and ethical perspectives, this chapter contributes to a more holistic understanding of how decentralized systems can be governed across blockchain boundaries.

2. The Governance Model in DAOs

The governance model in DAOs is a system that allows participants to collectively make decisions about the organization's operations, direction, and policies without centralized leadership (Wright 2021). The decision-making process is not an isolated on-chain-phenomenon; rather, it must be integrated into the existing off-chain legal framework. In this regard, it falls upon the law to consider the actual intentions of the parties in question as far as is feasible within context of legal categorization.

2.1. Legal Qualification of DAOs

As opposed to traditional organizations and companies, however, the legal status of DAOs remains a complex and evolving issue, largely dependent on the jurisdiction in which they operate (for a broad comparative overview, see the contributions in Pere-

strelo de Oliveira and Rolo 2021). DAOs are digital organizations governed primarily by smart contracts and decentralized decision-making processes, making their legal recognition challenging under traditional legal frameworks. In most jurisdictions, DAOs acquire legal personality by default as partnerships, even without formal registration. This classification grants DAOs the ability to enter into contracts and own assets but also exposes their members to potential legal liabilities (Mienert 2022: 116 et seqs.). The absence of limited liability is a significant drawback, as participants in non-wrapped DAOs – those that do not register under a specific legal framework – may face unlimited personal liability for the organization's obligations (Möslein and Ostrovski 2024: 109 et seq.).

2.1.1. "Wrapped" DAOs and Personal Liability

To mitigate this risk, many DAOs choose to be "wrapped" by incorporating as a legal entity, such as a Limited Liability Company (LLC) or a foundation, in jurisdictions that provide a suitable regulatory framework. Some US federal states, particularly Wyoming and Vermont, have introduced specialized DAO LLC structures that provide limited liability while maintaining the decentralized governance principles of DAOs (Guntermann 2024: 480). Similarly, jurisdictions like Switzerland and the Cayman Islands offer foundation structures that can serve as legal wrappers for DAOs.

Recent legal cases highlight the risks DAO participants face due to the lack of clear legal structures. For instance, U.S. courts ruled that token holders participating in governance decisions could be held personally liable (Samuels v. Lido DAO, 3:23-cv-06492, (N.D. Cal.), see also Commodity Futures Trading Commission v. Ooki DAO, 3:22-cv-05416, (N.D. Cal.)), reinforcing the argument that DAOs need clearer legal frameworks to ensure regulatory compliance and limit liability exposure.

2.1.2. DAOs in Decentralized Finance

Beyond their role as a nexus for contracts, DAOs are increasingly relevant as a nexus for regulation (Möslein and Ostrovski 2024: 97 et seq.), particularly in the context of Decentralized Finance (DeFi). In financial markets, obtaining a license to operate legally often requires a recognized legal entity with accountable representatives. Since many jurisdictions do not allow partnerships to obtain financial service licenses, DAOs face significant regulatory hurdles. Furthermore, financial supervision laws typically assume centralized management structures, creating additional challenges for DAOs that operate through decentralized governance.

2.2. Decision-making and Governance in a Decentralized Environment

As a consequence, decision-making and governance in DAOs are fundamentally different from traditional corporate structures. DAOs operate through blockchain-

based smart contracts that automate governance processes and ensure decentralization (Möslein 2020: 898 et seq.). Unlike conventional organizations, which rely on hierarchical management, DAOs distribute voting- power among their members, typically through governance tokens.

2.2.1. Token-based Voting Mechanism

DAO governance is based on a voting mechanism where members, holding governance tokens, vote on proposals related to the organization's operations. These tokens function similarly to shares in traditional companies, providing voting rights and sometimes financial benefits (Bauer 2025: 42 et seqs.). Governance token holders can vote on key issues such as protocol upgrades, resource allocation, and strategic directions.

Voting power in DAOs is often proportional to the number of governance tokens held by a participant. While this ensures that those with a larger stake have more influence, it can also lead to power centralization among wealthy participants, a challenge sometimes referred to as "whale dominance". Some DAOs attempt to mitigate this issue by introducing quadratic voting, delegation systems, or token-weighted participation thresholds (Axelsen, Jensen and Ross 2025: 77).

2.2.2. Dual-layer or Direct Token-based Voting Mechanism

The governance structure of DAOs varies widely. Some DAOs, like MakerDAO, implement a dual-layer governance system that includes both off-chain discussions (via forums and social media) and on-chain voting mechanisms. In this model, informal proposals are debated before being formally put to a vote through smart contracts. Other DAOs, such as Compound and Uniswap, use direct token-based voting where governance proposals are immediately subjected to on-chain voting (Bauer 2025: 3 et seq.).

2.3. Governance of Cross-Chain DAOs

DAOs and cross-chain governance interact by enabling decentralized decision-making across multiple blockchain networks, allowing DAOs to operate beyond a single blockchain ecosystem. As many DAOs manage assets and protocols on different blockchains, cross-chain governance mechanisms ensure that decisions made by token holders can be executed across various networks. Technologies such as cross-chain bridges, interoperability protocols (e.g., Polkadot, Cosmos), and multi-signature wallets facilitate secure communication and execution of governance actions across chains (see for instance, McCarthy 2022: 18). Smart contracts on different blockchains can synchronize DAO votes and proposals, ensuring seamless coordination. However, cross-chain governance also introduces challenges such as security risks, synchronization delays, and fragmentation of voting power, necessitating in-

novative solutions like oracle-based verification and decentralized interoperability frameworks.

3. Technological Background Behind Cross-Chain Interoperability

As the number of blockchains in use continues to grow, the necessity for interoperability between these disparate systems also increases. A blockchain system by its very nature operates in isolation, resulting in the so-called "blockchain-islands" phenomenon (Zhu, Zhang and Tao 2024: 1; Ou et al. 2022: 1; Li and Zhao 2024: 12007). Differences in architecture, data structure, security mechanism, or contract execution hinder the circulation of information among systems (Fu et al. 2024: 71). The creation of a unified, user-friendly ecosystem in which various blockchain platforms are interconnected, enabling the seamless performance of transactions and access to services across multiple networks without friction, represents a significant challenge for system developers. Cross-chain technology has been developed with the objective of facilitating efficient communication mechanisms between blockchains. Besides the exchange of digital assets or data between blockchains, cross-chain interoperability improves the scalability of blockchain systems.

From a technical perspective, four core strategies for cross-chain interoperability have been established: (1.) notary schemes, (2.) sidechain/relay, (3.) hash-locking and (4.) distributed private key control (Ou et al. 2022: 4). All technologies have in common that they solve the island phenomenon to a certain degree taking into account the respective limitation of each approach.

3.1. Notary Schemes

Notary schemes introduce one or more trusted third-parties to verify information between cross-chain transactions (Li, Wu and Cui 2023: 150; Ou et al. 2022: 4; similar to the role of notaries in cross-chain transactions see the role of connectors in interledger payments in: Thomas and Schwartz 2015: 2). The notary acts as an intermediary on both chains to monitor events or information and if necessary, responds on the respective blockchain (Li, Wu and Cui 2023: 150).

3.1.1. Overview: Simplified Transaction Procedure in Notary Schemes

Depending on the implemented scheme, the mechanism requires one single notary or a group of notaries (Ou et al. 2022: 4). When a transaction is conducted, a node, a group of nodes, or another entity acting as notary collects the data, verifies and confirms the transaction in the network (Ou et al. 2022: 4; on the basis of the Interledger project see Xiong et al. 2022: 1060). A node is one of the network participants that collectively run the blockchain's software. It enables the blockchain to val-

idate transactions and keep the network secure ensuring the decentralization of the network. By using the notary scheme, the network significantly relies on the honesty and trustworthiness of each notary. The number of notaries required, the selection mechanism and consensus mechanism to be employed prior to the execution of a transaction can be individually determined by the participants in the network. Three main notary schemes have been established which differ in terms of the used signature method.

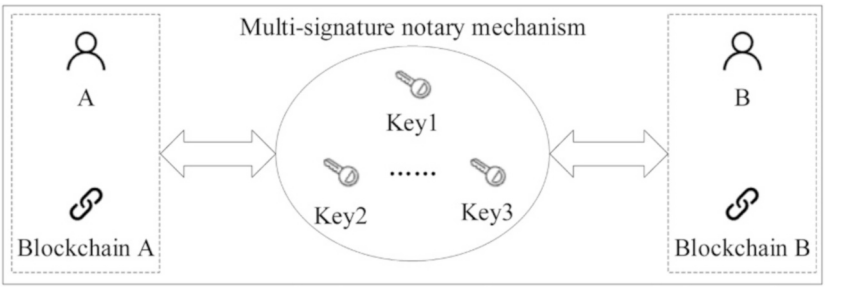
3.1.2. Single-Signature Notary Schemes

The single-signature notary scheme (also: centralized notary scheme) is the simplest of methods and delegates all notarial tasks to one single node or entity (Li, Wu and Cui 2023: 150; Ou et al. 2022: 4). In the absence of complex proof mechanisms relying on one notary may accelerate transaction times depending on the responsiveness of the single notary (Ou et al 2022: 4; Xiong et al. 2022: 1060). By entrusting solely one notary, the network significantly changes the way trust is established on blockchains. A system based purely on the distinctive characteristics of blockchain technology ("technological trust") is then supplemented by trust in the individual notary ("personal trust") in the case of cross-chain transactions. The simplicity of the single signature scheme is accompanied by the hazards of a single point of failure and a conflict with the concept of decentralization which in fact is inherent to the blockchain (Xiong et al. 2022: 1060; Mao et al. 2023: 45532).

3.1.3. Multi-Signature Notary Schemes

Multi-signature notary schemes avoid the risks of the single-signature scheme by delegating the notarial tasks to a randomly selected number of notaries out of a notary group. By giving each notary of the group a key to collusively confirm any cross-chain transaction, a higher degree of security and decentralization is achieved (Wu et al. 2023: 3; Ou et al. 2022: 4). In case of a malicious attack on some nodes or entities, the operation of the remaining system is not necessarily affected. The confirmation of the transaction depends on a certain percentage of notaries jointly signing and reaching consensus (Ou et al. 2022: 4).

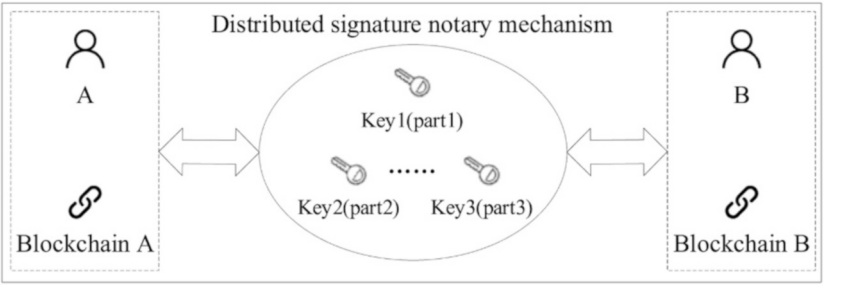
Figure 1: Multi-signature Notary Mechanism (Ou et al. 2022: 4).



3.1.4. Distributed Signature Notary Schemes

The distributed signature notary scheme intensifies the level of security and reliability compared to the multi-signature scheme. Also avoiding centralization through the utilization of notary groups it adds a layer of security by adopting a multi-party computation (MPC) mechanism (Li, Wu and Cui 2023: 150; Ou et al. 2022: 4). The MPC is a cryptographic technique that allows multiple parties to jointly calculate an output from their private inputs while ensuring the privacy of the participants and used data (Evans, Kolesnikov and Rosulek 2020: 7 et seq.). In context of the distributed signature notary scheme, MPC is used to securitize the notary key needed to verify data and transactions. The signature key is split into multiple fragments and distributed between notaries (Ou et al. 2022: 4). The signature is only considered complete if a specific threshold of key fragments is achieved.

Figure 2: Distributed Signature Notary Mechanism (Ou et al. 2022: 5).



3.2. Sidechain/Relay

Sidechain and relay are two distinct cross-chain mechanisms which although often used together differ in their characterizing purpose.

3.2.1. Communication Between Blockchains via Sidechain

The sidechain is an independent blockchain linked to another blockchain. The two blockchains may be either two existing standalone blockchains, in which case they are to be treated as equals, or one blockchain may derive directly from the other (Gaži, Kiayias and Zindros 2019: 139) The term sidechain is ambiguous. A subordination relationship between both chains is not mandatory. Sidechains allow multiple blockchains to communicate with each other and react to events in the other (ibid.: 139). By use of a two-way pegging mechanism (Ou et al. 2022: 5) they allow for transfer of assets between side- and mainchain (Ou et al. 2022: 5). In principle, assets can be temporarily locked on the mainchain with subsequent release on the sidechain and vice-versa (Ou et al. 2022: 5). The assets on either chain are released once a certain number of nodes verify the locking of asset on the other blockchain. Through sidechain developers may increase the functionalities of existing and unalterable blockchain protocols by outsourcing or expanding certain functions to another blockchain (Xiong et al. 2022: 1060).

3.2.2. Relay as a Translation Tool between Blockchains

A relay facilitates cross-chain communication by providing a unified language to isolated blockchains. The purpose is limited to observation, collection, and verification of data on blockchains (Fu et al. 2024: 71). Relay builds an additional operational layer in a blockchain effectively by using smart contracts who are able to take on and verify information from other blockchains (With a relay example for Bitcoin or Ethereum see Frauenthaler et al. 2020: 2). In contrast to sidechain relays are implemented directly on the blockchain (Mao et al. 2023: 45533).

3.3. Hash-locking

3.3.1. Functionality of Hash-locks

The principle of hash-locking is based on the cryptograph technique of hash-locks in combination with a time-lock mechanism. The use of hash-locking enables the locking of assets on a blockchain via smart contracts. The lock is connected to the hash which can only be accessed by providing the correct key (Li and Zhao 2024: 12011). Time-lock mechanisms ensure that in the event of one party failing to claim their asset via key within the specified time frame, the assets of both parties in question are returned to their sender (Ou et al. 2022: 4; Li and Zhao 2024: 12011; Li, Wu and Cui 2023: 151). In this context cross chain transactions are called “atomic-swaps” meaning that the transaction is either successfully executed between both parties or no exchange of assets takes place at all.

3.3.2. The Hash – a Digital Fingerprint of Data

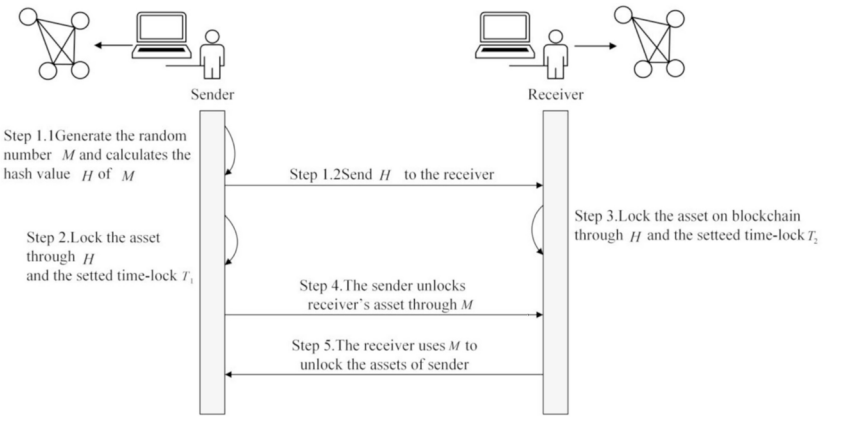
The hash (H) is a unique sequence of numbers and letters that represent the result of applying a cryptographic hash function to an arbitrary amount of data (Kaulartz 2016: 475). The uniqueness of the hash follows from its determinism. This means that the input of the same amount of data will always generate the same hash (Schlatt et al. 2016: 8). The amount of data (M) used in the calculation of the aforementioned hash-value represent the key to unlock the hash-lock. By sharing M, the sender enables the receiver to access the data or asset locked by H on the other blockchain.

3.3.3. Example: Cross-Chain Transaction Using Hash-locks

Example of cross-chain transaction: The sender with an asset on Blockchain A wants to exchange assets with receiver who holds an asset on Blockchain B. Typically, an exchange of assets between Blockchain A and Blockchain B via hash-locking requires 5 steps:

1) Sender generates, based on amount of data (M), a hash (H) and sends H to receiver.
2) Sender locks asset on Blockchain A through the use of H and a time-lock.
3) Receiver locks asset on Blockchain A through the use of H and a time-lock.
4) Sender can use M to unlock asset of receiver on Blockchain B.
5) By unlocking asset of receiver with M, receiver obtains M through the system and can in turn unlock asset of sender on Blockchain A.

Figure 3: Flowchart of Cross-chain Transaction Using Hash-locking (Li and Zhao 2024: 12012).



In the event that either the sender or the receiver is unable to unlock the asset on either Blockchain within the specified time frame, the cross-chain transaction collapses in on itself. In order to gain actual access to the asset, it is not sufficient to open the lock with M. Access is granted simultaneously when both parties have successfully completed the unlocking process for the asset.

3.3.4. Advantages and Disadvantages

In comparison to the notary scheme no intermediaries are required for security reasons. Due to the "all or nothing"-approach of the cross-chain transaction no trust is required between parties. Hash-locking has the advantage of low transaction costs but is limited to a specific use-case (Li and Zhao 2024: 12012; Li, Wu and Cui 2023: 151). The transaction is limited to an exchange of assets, a transfer of assets between blockchains is not possible. The total number of assets on the respective blockchain remains identical throughout the entire transaction process.

3.4 Distributed Private Key Control

Distributed private key control refers to a validation mechanism for transactions between different blockchains. Validation is required for the purpose of asset locking on the source blockchain, the creation of an equivalent asset on the target blockchain or reverse transfers of both. The validation method operates similar to the distributed signature notary scheme (see Fig. 2) by splitting the private key into fragments and distributing them across the network. By using distributed secret key generators involving the entire network of nodes a higher degree of decentralization is achieved compared to a mechanism selecting a predefined number of nodes/notaries (Ou et al. 2022: 6). During the validation process no trust between the transaction parties or any intermediary facilitating the transaction is required. Each node only saves parts of the private key and does not transmit or assemble any fragments of the whole private key. Thereby any central authority is precluded from acquiring full control over the assets (Yu and Zhang 2023: 638).

A transaction has to be confirmed on both blockchains by a number of nodes. The required validation quorum of key fragments can be defined by the protocol developer in advance (Mao et al. 2023: 45533). No single entity has full control over the asset (Yu and Zhang 2023: 638; Ou et al. 2022: 6). Ownership of the asset and the right of use fall apart (Yu and Zhang 2023: 638; Ou et al. 2022: 6). A transfer of assets or any other process may always require the authority of more than the original owner.

4. Interconnection of Blockchains

Through the interconnection of different blockchains, the user has access to several systems with different practical applications. The use of different blockchains raises the question of whether users can now expect a duplication of the governance structure, or whether interoperability as a connecting element between the chains will lead to the establishment of a single governance structure adapted to the new area of application.

4.1. Governance in Multi-Layer Systems

Cross-chain governance in DAOs does not necessarily lead to a direct duplication of their governance structure, but it often results in a more complex, multi-layered system. Since DAOs operate across multiple blockchain networks, they must establish mechanisms to coordinate decision-making and execute governance actions on different chains. This can lead to parallel governance frameworks, where each chain has its own governance process, yet remains interconnected with the broader DAO ecosystem. Some DAOs address this by using interoperability protocols, multi-chain governance tokens, or cross-chain bridges to ensure that decisions made on one blockchain are recognized and enforced on others. While these solutions promote consistency, they can also introduce inefficiencies, such as latency in governance execution and potential discrepancies in decision enforcement across chains.

4.1.1. Unification of Governance Structures

Despite these challenges, many DAOs strive to maintain a unified governance structure by implementing interoperability solutions that allow for seamless communication between different blockchain environments. Instead of fully duplicating governance processes, DAOs may adopt a federated or hierarchical model, where a primary governance layer oversees cross-chain operations while individual chains handle localized decisions. This approach minimizes redundancy while maintaining decentralized decision-making. However, achieving full coordination remains a technical and organizational challenge, requiring innovative smart contract designs, oracle-based verification systems, and standardized cross-chain protocols to ensure governance integrity and efficiency across multiple blockchain networks.

4.1.2. Legal Challenges

Cross-chain governance in DAOs also raises significant legal challenges, particularly regarding jurisdiction, regulatory compliance, and liability. Since DAOs operate across multiple blockchain networks, determining which legal framework applies to their governance decisions becomes complex. Different jurisdictions may have conflicting regulations on smart contracts, securities laws, and financial oversight,

creating uncertainty for DAO participants. Additionally, enforcing governance decisions across chains can be legally ambiguous, as smart contract execution may not always align with traditional legal enforcement mechanisms. Liability is another key concern – if governance decisions lead to financial losses or regulatory breaches, it remains unclear whether responsibility falls on individual token holders, developers, or the DAO itself. As DAOs expand their cross-chain presence, legal clarity will be essential to ensure regulatory compliance while preserving decentralization and interoperability.

4.2. The Company Statute ("*Gesellschaftsstatut*") in the Cross Chain Context

In case the cross-chain model not only involves bridging the gap between different blockchains but also involves various jurisdictions it raises the question which national law system applies to the relevant legal issue (e.g. incorporation rules, liability regime, registration obligations). The applicable law in each case crucially determines the governance structure. According to German law, specifically Art. 3 EGBGB resolves this conflict of jurisdictions by applying particular rules for international private law conflicts. Sources of these rules are international treaties, the law of the European Union and German conflict of law principles which themselves are based on customary law (Mienert 2022: 83 et seq.). The international treaties and EU law prevail over national legal principles. The overriding objective of all the rules is to choose the jurisdiction with the closest connection to the subject matter.

4.2.1. Real Seat Theory ("*Sitztheorie*") or Incorporation Theory ("*Gründungstheorie*")

Due to the digital structure of cross-chain models, with the difficulty of accurate geographical allocation of users, hardware, or area of business it seems appropriate to look for a general point of contact to determine the statue of the company (for DAOs see Mienert 2022: 86). From a European perspective the real seat theory ("*Sitztheorie*") and incorporation theory ("*Gründungstheorie*") is often discussed in this context.

The idea of real seat theory connects the actual corporate seat (e.g. head offices) to the applicable company law. According to the theory, a conflict of jurisdictions is usually to be settled within the framework where the main administration is located. That sounds reasonable as it can be expected that the majority of stakeholders will also be located in this jurisdiction.

The incorporation theory determines the applicable law by reference to the jurisdiction where the company was incorporated and registered. This approach enhances legal certainty because the determination of where a company was established can usually objectively be established.

4.2.2. Application to Cross-Chain Models

Considering both theories under the organization structure of cross-chain models, significant difficulties arise in the context of applicability. Due to the decentralized nature of the chosen structure, there is no universally applicable headquarter with regard to the real seat theory.

The incorporation theory does also not help in this matter. With regard to this theory the applicable law is determined by the place of incorporation, the place of the registered office under the articles of association, the place of registration, the place chosen by the company founders (*freie Rechtswahl*) or the place under whose law the company is organized (Mienert 2022: 91). Cross-chain structures are typically built within a complete digital infrastructure without formal documentation (with the White Paper as an exception to this general rule) relying solely on its source code without references to any jurisdiction or applicable law. To determine a link between these factual levels and the legal requirements seems not useful.

4.2.3. Conflict of Chain Rules

As noted above, it is difficult to link traditional conflict of law theories to the determination of the company statue because of the special factual structures of cross-chain models. One solution could be for future cross-chain models to provide more guidance on the applicable law in the White Paper. Another option is to extend the range of connecting factors regarding jurisdiction. In addition to the country of incorporation or head office, it may be possible to resolve jurisdictional issues by focusing on the location of the main assets or servers of the cross-chain network. Even simpler, the location that is disclosed in the imprint or legal notice on the homepage of the respective project could also be considered as a reasonable linking point (Mienert 2022: 95 et seqs.).

4.3. Balancing Hierarchy and Autonomy: Parallels to Group Law ("*Konzernrecht*")

The legal challenges arising from the cross-chain governance of DAOs are primarily related to the tension between hierarchy and autonomy: On the one hand, the aim is to achieve hierarchical control across individual networks, but without giving up the advantages of decentralized autonomy. The connection and interoperability established between the different blockchains raises the question of how to manage the actual and legal relationships between them. The coming together of two previously autonomous structures leads to an area of friction that is particularly evident in the management of the structures. It is at the parties' discretion to establish a union of equals or a relationship of superiority and subordination. In the latter case effective measures have to be taken to ensure sufficient protection of minority rights. In this respect, cross-chain governance of DAOs shares notable parallels with the gov-

ernance of corporate groups (*Konzernrecht*) in traditional company law, particularly under German law (for an overview: see Scheuch 2016).

4.3.1. Corporate Groups – Legally Independent but Economically Connected

In a corporate group (*Konzern*), multiple legally independent entities operate under a unified economic structure, often controlled by a parent company. Similarly, DAOs with cross-chain governance manage decentralized operations across multiple blockchain networks, where different chains function as interconnected yet technically distinct environments. In both cases, governance mechanisms must balance central oversight with local autonomy, ensuring coherence while respecting the distinct legal and operational contexts of each entity or blockchain. Just as corporate group law (*Konzernrecht)* addresses decision-making within a corporate group to prevent conflicts of interest and protect minority shareholders, cross-chain DAOs must navigate decentralized governance challenges, including voting synchronization, execution consistency, and accountability.

4.3.2. German *Konzernrecht* – Key Principles

From a legal perspective, German *Konzernrecht* imposes specific duties on the parent company in a corporate group to protect subsidiary companies and minority shareholders, particularly under the German Stock Corporation Act (AktG). A key principle is the so-called *Gleichordnungskonzern* (coordinated group), where legally independent entities operate under a common governance framework, akin to how DAOs coordinate decision-making across chains. If a DAO's governance structure resembles a so-called *Unterordnungskonzern* (hierarchical group), where a dominant chain or governance body exerts significant control over sub-chains, fiduciary duties and liability risks arise. In traditional corporate law, a parent company can be held liable if it exerts excessive influence leading to financial harm for subsidiaries (§ 311 AktG). Applying this to DAOs, if a primary governance layer enforces decisions across chains that negatively impact participants, questions of legal liability, fiduciary obligations, and regulatory compliance emerge. While DAOs generally lack formal legal personhood under German law, their growing complexity and resemblance to corporate structures may prompt future regulatory frameworks addressing governance accountability in cross-chain environments.

4.4. Liability Considerations in Multi Layer Systems

4.4.1. Personal Liability in Single Layer Systems

In the majority of jurisdictions, DAOs qualify as legal partnerships. The liability consequences for each token holder are significantly detrimental. Under the German legal framework each token holder is liable without limitation, jointly and severally for any kind of obligation of the DAO (Florstedt 2023: 843; Guntermann 2024: 480).

This applies for any obligation established before and during the membership as well as for a certain period of time after leaving the DAO. The individual token holder's liability therefore derives from the company's liability to third parties. The legal possibility of taking recourse against the company or another token holder is limited by practical concerns about anonymity and the lack of centralized management or responsibility structures (Guntermann 2024: 480). In order to avoid unfair outcomes and in view of the factual structure of the DAO, some authors suggest an institutional limitation (*institutionelle Haftungsbeschränkung*) of liability (Korch 2023: 2024). This case law established for specific subgroups of partnerships has not yet found its way into DAO case law.

The outlined liability system refers to a single-layer system. This means that a single DAO entity operates under cooperation with its token holders with third parties. This is different from the case of cross-chain models, which involve a multi-layered system based on a variety of blockchains that are linked together by the technological connection tool of their choice. In this case, different autonomous DAOs may choose to cooperate by linking their networks together to form a coherent multi-layer network. This creates a de facto merger between at least two independently functioning eco-systems to one cohesive system.

4.4.2. No Change in Liability due to the De-facto Merger of Systems

This de facto merger raises questions about the application of liability principles in multi-layer networks. In principle all token holders are liable for any obligations owed by their own network. This principle is followed by the question whether after the de facto merger in the multi-layer-system the token holders of network A are now responsible for network B's obligations and vice versa (transfer of liability). A transfer of liability may be possible by contractual assumption of obligations or by legal merger between both networks. Assuming such transfer of liability, the already existing liability risks for token holders will only be exacerbated. A contractual assumption of obligations appears implausible. Token holders typically seek for ways to limit, not expand, their liability exposure.

The aim of a legal merger is that two formerly independent legal entities (e.g. two networks) will not only be merged de facto but also de jure into one single legal entity. The assets of the legal entity being acquired and its liabilities will devolve to the acquiring legal entity. Under the German Transformation Act (UmwG) partnerships can only be merged if they are registered with the company register (*Gesellschaftsregister*). DAOs typically operating without formal registrations on a multinational basis will not be qualified for a merger under the UmwG. Another option is for one DAO to dissolve and all token holders to join the other DAO. Alternatively, both DAOs could dissolve and form a new joint DAO. Both alternatives do not constitute a merger within the meaning of the UmwG but practically lead to a combination of all token holders within one entity. However, any dissolution

of partnerships requires a subsequent entity liquidation process or similar. All obligations of the DAO must be met by either the DAO or its token holders. Only after this liquidation process has been completed, the dissolvement of the entity can be realized. It is therefore not possible for any liabilities to be transferred to another entity.

4.4.3. Sole Responsibility and its Limits

As there is no possibility of transfer, the stated principle remains that each network and its token holders are solely responsible for their own liabilities. This is certainly the case when two existing DAOs decide to implement a cross-chain solution at a later stage. It may be different if a cross-chain solution is implemented from the beginning by will of all token holders. In this case, similar to single-layer solutions, a legally binding objective intent (*Rechtsbindungswille*) to form a single partnership using multiple layers is required (Fleischer 2024: 1508).

5. Enabling-Capacities Approach in Cross-Chain Governance

The Enabling-Capacities approach focuses on a shift in perspective from a purely objective focus on system characteristics to a combination with a subjective, individually driven approach. This addition recognizes that individuals cannot rely on system characteristics alone but need to acquire capacities that enable them to evaluate the system they are using on the basis of a subjective evaluation matrix. Exemplary, this matrix can be used with regard to the evaluation of the used technology within the network. The prerequisite for the Enabling-Capacity approach is that the token holders are provided with sufficient basic information.

In a rapidly growing blockchain ecosystem, an evaluation process from the token holder's perspective appears to be significantly cumbersome and depending on the investment volume not economical. This applies all the more when, in context of cross-chain solutions, a de facto merger can lead to a duplication of structures that need to be examined. The large number of presented technological cross-chain solutions are an exemplary for the complexity of the technology. We therefore propose that the flow of information must be centralized from the single network itself to each token holder by White Paper or prior to each individual decision by an individual letter of information. The latter may be incorporated within a smart contract by means of an if-then formula. If a network collectively decides to opt for a cross-chain solution, then all token holders have to be thoroughly informed about the possible technological solutions as well as their advantages and disadvantages. From a legal perspective, this results in a mandatory preventive fulfilment of the information rights (§ 717 BGB) of token holders. Preventative fulfilment is central for the Enabling-Capacities approach due to the lack of a central authority in the DAO

meaning that legal enforcement of information rights by its token holders involve considerable practical difficulties (Guntermann 2024: 481).

6. Conclusion

Cross-chain governance represents a critical evolution in the decentralized ecosystem, enabling DAOs to operate beyond the limitations of single-blockchain frameworks. However, this expansion introduces significant challenges related to governance coordination, security risks, and legal uncertainties. Technological solutions such as cross-chain bridges, interoperability protocols, and oracle-based verification systems offer pathways to more effective governance, yet their implementation remains complex. From a legal perspective, the parallels between cross-chain DAOs and corporate group law highlight the need for regulatory clarity, particularly in ensuring accountability and protecting stakeholder interests.

6.1. Harmonization and Legal Certainty

As DAOs continue to scale across multiple blockchains, future regulatory and technological developments will be crucial in shaping a governance model that balances decentralization, efficiency, and legal compliance. Legislators across the world face a constantly changing digital ecosystem and may find it challenging to adapt their regulatory approach to an evolving system which does not wait on approval, frameworks, or jurisdictions. The accelerating interconnection of blockchains is driving the internationalization of ecosystems and increase the need for overarching, harmonizing regulations. Exemplary, in the context of public limited liability companies (*Aktiengesellschaften*), the EU legislator has ensured minimum equivalent protection for shareholders and creditors by the use of a harmonizing directive (Directive EU 2017/1132).

In addition to preventive general legislation, the judiciary can facilitate legal certainty with regard to these new governance structures by applying already existing laws through case law. However, the responsibility falls upon the private sector to initiate legal proceedings in such cases.

6.2. Sandboxes as Education Tools

Regulators, supervising authorities and private cross-chain innovators may engage in a regulatory dialogue in a safe, confidential and controlled environment. Sandboxes can help to identify barriers from a legal, regulatory and private perspective involving all relevant stakeholders. Cross-chain governance models can be tested for a limited period of time before being integrated into existing market structures.

Overall, this can help remove barriers and strike a balance between innovation and regulatory oversight, thereby improving legal certainty.

The idea of controlled testing environments at EU-level is not new and has already been established with regard to the European Blockchain Regulatory Sandbox or within the EU Artificial Intelligence Act. It seems reasonable to build on existing structures with a particular focus on cross-chain models. The integration into the European Blockchain Regulatory Sandbox with the expansion of supported projects is advisable.

References

Axelsen, Henrik, Jensen, Johannes R. and Ross, Omri (2024): "When is a DAO Decentralized?", in: Perestrelo de Oliveira and Rolo, Decentralised Autonomous Organisation (DAO) Regulation. Principles and Perspectives for the Future, pp. 59–91.

Bauer, Philipp (2025): Governance-Token. Ein dezentralisiertes und tokenisiertes Mitgliedschaftspapier?, Mohr Siebeck.

Directive (EU) 2017/1132 of the European Parliament and the Council Directive (EU) of 14 June 2017 relating to certain aspects of company law.

Evans, David, Kolesnikov, Vladimir and Rosulek, Mike (2020): A Pragmatic Introduction to Secure Multi-Party Computation, Boston, MA: Now Publishers.

Fleischer, Holger (2024): "Plötzlich Personengesellschafter. Eine kleine Phänomenologie unbeabsichtigter Personengesellschaften", in: ZIP: Zeitschrift für Wirtschaftsrecht 45(27), pp. 1501–1512.

Florstedt, Tim (2023): "Tokengesellschaftsrecht – Zur Organisations- und Vermögensverfassung digitaler Gesellschaften (Decentralized Autonomous Organizations)", in: Zeitschrift für Unternehmens- und Gesellschaftsrecht 52(6), pp. 816–848.

Frauenthaler, Philipp et al. (2020): "Leveraging Blockchain Relays for Cross-Chain Token Transfers", in: White Paper, TU Wien, pp. 1–5.

Fu, Wanshu et al. (2024): "A Blockchain Cross-Chain Solution Based on Relays", in: International Journal of Knowledge and Innovation Studies 2(2), pp.70–80.

Gaži, Peter, Kiayias, Aggelos and Zindros, Dionysis (2019): "Proof-of-Stake Sidechains", in: 2019 IEEE Symposium on Security and Privacy 1, pp. 139–156.

Guntermann, Lisa (2024): "Wyoming DUNA – ein neuer 'legal wrapper' für DAOs", in: RDi 2024, pp. 476–486.

Kaulartz, Markus (2016): "Hintergründe zur Distributed Ledger Technology und zu Blockchains", in: Computer und Recht 32(7), pp. 474–480.

Korch, Stefan (2023): "Haftung und Haftungsprivilegien in Decentralized Autonomous Organizations", in: ZIP: Zeitschrift für Wirtschaftsrecht 44(39), pp. 2017–2025.

Li, Jiao and Zhao, Wanting (2024): "Blockchain Cross-chain Protocol Based on Improved Hashed Time-locked Contract, in: Cluster Computing 27, pp. 12007–12027.

Li, Li, Wu, Jiahao and Cui, Wei (2023): "A Review of Blockchain Cross-chain Technology", in: IET Blockchain 3(3), pp. 149–158.

Mao, Hanyu et al. (2023): "A Survey on Cross-chain Technology. Challenges, Development, and Prospect, in: Ieee Access 11, pp. 45527–45546.

McCarthy, Sam (2022): Stewards and Gatekeepers. Human and Technological Agency in the Governance of DeFi Protocols, SSRN, August 18, 2022, https://ssrn.com/abstract=4326903.

Mienert, Biyan (2022): Dezentrale autonome Organisationen (DAOs) und Gesellschaftsrecht. Zum Spannungsverhältnis Blockchain-basierter und juristischer Regeln, Mohr Siebeck 2022

Möslein, Florian (2020): "A Nexus of Smart Contracts? Gesellschaftsrechtspraxis und -theorie im Spiegel der Blockchain", in: Bachmann, Gregor and Grundmann, Stefan et al. (eds.), Festschrift für Christine Windbichler zum 70. Geburtstag, de Gruyter (2020), pp. 889–904.

Möslein, Florian and Ostrovski, Daniel (2024): "Legal Personality of Decentralized Autonomous Organisations (DAOs). Privilege or Necessity?", in: Perestrelo de Oliveira and Rolo, Decentralised Autonomous Organisation (DAO) Regulation. Principles and Perspectives for the Future, pp. 93–112.

Ou, Wei et al. (2022): An overview on cross-chain: Mechanism, platforms, challenges and advances, in: Computer Networks 218(109378), pp. 1–21.

Perestrelo de Oliveira, Madalena and Rolo, António G. (eds.) (2024): Decentralised Autonomous Organisation (DAO) Regulation. Principles and Perspectives for the Future, Mohr Siebeck.

Perestrelo de Oliveira, Madalena and Rolo, António G. (eds.) (2023): Decentralised Autonomous Organisations (DAOs) in Various Jurisdictions. From Old Rules to Innovative Approaches, https://www.cidp.pt/publication/decentralised-autonomous-organisations-daos-in-various-jurisdictions-from-old-rules-to-innovative-approaches/292, last access: April 5, 2025.

Scheuch, Alexander (2016): "Konzernrecht. An Overview of the German Regulation of Corporate Groups and Resulting Liability Issues", in: European Company Law 13, pp. 191–198.

Schlatt, Vincent et al. (2016): "Blockchain. Grundlagen, Anwendungen und Potenziale", Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT, https://www.fim-rc.de/Paperbibliothek/Veroeffentlicht/642/wi-642.pdf, last access: March 3, 2025.

Thomas, Stefan and Schwartz, Evan (2015): "A Protocol for Interledger Payments", https://interledger.org/developers/documents/interledger.pdf, last access: March 3, 2025.

Wright, Aaron (2021): "The Rise of Decentralized Autonomous Organizations. Opportunities and Challenges", in: Stanford Journal of Blockchain Law & Policy, pp. 152–176.

Wu, Xiaohua et al. (2023): "A Distributed Cross-chain Mechanism Based on Notary Schemes and Group Signatures", in: Journal of King Saud University – Computer and Information Sciences 35(101862), pp. 1–14.

Xiong, Anping et al. (2022): "A Review of Blockchain Cross-chain Technology, in: Digital Communications and Networks 8, pp. 1059–1067.

Yu, Yue and Zhang, Shibin (2023): "A Cross-Chain Identify Authentication Scheme Based on Block Chain", in: 2022 3rd International Conference on E-commerce and Internet Technology, Atlantis Press, pp. 635–643.

Zhu, Zeshuo, Zhang, Rui and Tao, Yang (2024): "Atomic Cross-chain Swap Based on Private Key Exchange", in: Cybersecurity 7(12), pp.1–22.