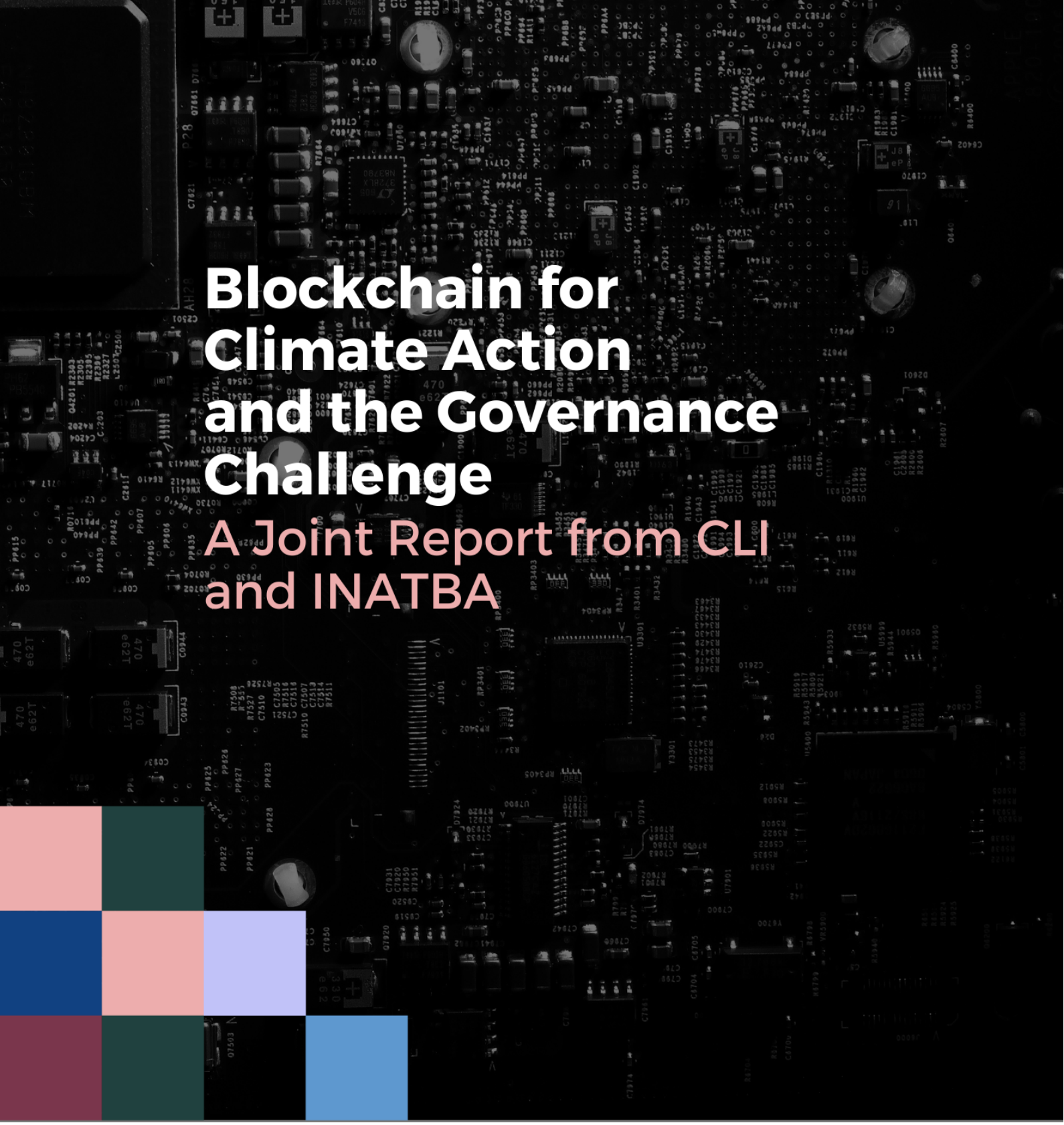


Blockchain for Climate Action and the Governance Challenge

A Joint Report from CLI and INATBA

International Association for Trusted Blockchain Applications

CLIMATE LEDGER INITIATIVE

Authors

Anik Kohli | Climate Ledger Initiative, INFRAS, Switzerland

Sven Braden | Climate Ledger Initiative, Peru

Jörn Erbguth | Geneva Macro Labs, University of Geneva, Switzerland

Marianna Belotti | Co-Chair INATBA Governance Working Group, Caisse des Dépôts Groupe, France

Contributors

Jan Stockhausen | Etherisc, the Netherlands

Susan David Carevic | World Bank, USA

Piet Kleffmann | KfW, Germany

Reviewers

Monique Bachner | Co-Chair INATBA Governance Working Group, ThinkBLOCKTank, Luxembourg

Michael Fabing | Co-Founder Wood Tracking Protocol, Peru

Jürg Füssler | Climate Ledger Initiative, INFRAS, Switzerland

Paolo Giudici | INATBA AAB Member, Professor of Statistics, Department of Economics and Management, University of Pavia, Italy

In Memoriam:

This report is dedicated in memory of Sven Braden who passed away shortly after this report's publication.

Sven was one of the report's authors and served as a Program Manager for Climate Ledger Initiative. Dedicated father, beloved colleague and climate action advocate, Sven will be dearly missed.

Table of Contents

Executive Summary **6**
Make sure that your blockchain project complies with international rules on climate change 6
Make sure governance on and off your blockchain is well defined 7
Make sure that your blockchain project for climate action complies with national laws 8

1. Introduction **10**

2. Governance at the international level: The Paris Agreement sets global rules for the application of blockchain for climate action **12**
2.1 The Paris Agreement's global climate action rules 12
2.2 Enhancing the digitisation and automation of measurement, reporting and verification (MRV) of climate data 13
2.3 Providing next-generation registries and tracking systems for decentralised market mechanisms 14
2.4 Enhancing climate finance flows as well as access to green technologies and clean energy 16
2.5 Non-party stakeholders have an important role in climate actions and implementing the Paris Agreement 18
Box 1: The Climate Chain Coalition 18
2.5.1 Role of non-party stakeholders in MRV, market mechanisms as well as climate finance and clean energy 19
2.5.2 Blockchain applications by non-party stakeholders to implement the Paris Agreement 20
Use case: World Bank Warehouse 21

3. Governance Challenges at the Blockchain Level: Defining the technical rules and management of climate action projects **24**
Box 2: Different types of blockchain 24
3.1 Is Blockchain the right solution? 25
3.2 Off-chain project governance and management 28
3.3 On-chain governance 29
3.3.1 Consensus mechanisms 29
3.3.2 Consensus performance and resource consumption 31
3.4 Technical interfaces and interoperability 33
3.4.1 Inherent limitations of capacity and data privacy of permissionless Blockchains 33
3.4.2 Off-chain data 33
3.4.3 Oracles and APIs - Interfaces to the outside world 33

3.4.5 Interoperability between blockchains 35
Use case: KfW's TruBudget Platform 38

4. Governance challenges at the national level: Regulatory framework for blockchain-based projects for climate action 41
4.1 National regulations 41
4.1.1 National blockchain and climate change laws 41
4.1.2 Experimentation via "sandboxes" 42
4.1.3 Legal coordination across borders 43
4.2 Legal challenges related to blockchains 43
4.2.1 Applicable laws in cases of conflicts 43
4.2.2 Blockchain-based entries as legal evidence 43
4.2.3 Validity of electronic signatures 44
4.2.4 Blockchain-based assets and registries 45
4.2.5 Smart contracts and their legal status 45
4.2.6 Ensuring data protection 47
Use case: Etherisc weather insurance in Kenya 50

Conclusions 53

Literature 57

Preface

This report was prepared by an international team of authors with a diverse set of experiences and insights. It is a knowledge product of the International Association for Trusted Blockchain Applications (INATBA) and the Climate Ledger Initiative (CLI). The report aims to highlight governance challenges that blockchain-based climate action is confronted with from a practical perspective. Issues related to governance are addressed at the international, national and blockchain levels, incorporating diverse perspectives from climate action, blockchain and legal communities.

The Climate Ledger Initiative (CLI):

The mission of the Climate Ledger Initiative is to accelerate climate action in line with the Paris Agreement and the Sustainable Development Goals (SDGs) through blockchain and other digital innovations applicable to climate change mitigation, adaptation and finance. The Climate Ledger Initiative was started in 2017 by Nick Beglinger of Cleantech21 and is jointly operated by INFRAS Consulting, Analysis and Research and the Gold Standard Foundation. The CLI is financially supported by the Government of Switzerland and the Government of Liechtenstein and maintains an ever-expanding platform of donors, partners and collaborators. The initiative sits at the nexus of one of the world's most pressing problems, climate change, and the world's most promising technological innovations, blockchain, and, more broadly, distributed ledger technology, the Internet of Things and artificial intelligence. CLI addresses policy and research questions and identifies specific innovation opportunities at the intersection of climate and digitisation. The work so far has greatly benefited from the contributions of participants in various workshops and events and from the support of partner use cases. The CLI is a member of CCC (Climate Change Coalition) which is a member of INATBA. For more information, visit climateledger.org

International Association for Trusted Blockchain Applications (INATBA):

INATBA is the leading convener in the global blockchain ecosystem, offering developers, companies, and users of blockchain/distributed ledger technology a forum to interact with regulators and policymakers and bring blockchain technology to its next stage. INATBA currently has 167+ active non-profit and enterprise members and is advised by more than 40 academic institutions and 23 governmental organisations and agencies from 15 countries across Europe, North America, Africa, and Asia. INATBA often issues research and commentary on blockchain regulation and policy from its 14 workgroups spanning finance, governance, education, healthcare, identity, climate action, and more. The mission of INATBA is to develop transparent and inclusive governance and cooperation models for blockchain applications, to inform policy and regulatory measures that may contribute to harnessing the many opportunities of blockchain through a close dialogue with policy-makers and regulators, and promote regulatory convergence that drives potential impacts for society and the economy from these technologies. To learn more, visit www.inatba.org

Executive Summary

The aim of the report is to provide an overview of the most relevant governance challenges facing blockchain-based climate action. This ranges from the appropriate technical design of such systems to compliance with legal regulation. The publication does not, however, attempt to exhaustively discuss governance issues.

While blockchain works without a central authority, this does not mean there is an absence of governance. Governance is defined as an allocation of power, risks and responsibilities and thus is also core to blockchain-based climate actions. Different governance challenges have to be carefully addressed in order to build trust and create confidence in the technology, particularly in using blockchain for climate action.

Governance challenges are structured along three different levels: international, national and blockchain. While the focus of the first two levels deals with compliance to existing national and international laws, the latter is about actively defining rules and designing systems to automatically enforce these rules. In the following, the main take-away messages for blockchain-based climate action projects on each level are presented.

Make sure that your blockchain project complies with international rules on climate change:

- **How does your project contribute to the Paris Agreement? (Section 2.1)**

Developers of blockchain projects on climate action should be aware of the international rules on climate change. The Paris Agreement on climate change is a global treaty that entered into force on 4 November 2016. 190 countries and the EU have ratified the treaty and are subject to the international rules it enacts. The UN Climate Change secretariat has recognised the potential of blockchain for climate action and the Paris Agreement.

- **Does your project fit in one of the following categories: measurement, reporting, verification (MRV), market mechanisms, climate finance flows, or clean energy? (Sections 2.2, 2.3, 2.4)**

This paper argues that some of the most promising applications of blockchain for climate action are (i) enhancing the digitisation and automation of measurement, reporting and verification of climate data, (ii) providing next-generation registries and tracking systems for decentralised market mechanisms, and (iii) enhancing climate finance flows as well as access to green technologies and clean energy.

- **What role can you have as a non-party stakeholder in the implementation of the Paris Agreement? (Section 2.5)**

Climate action by so called “non-party stakeholders” such as local governments, companies or NGOs has been formally recognised in the adoption of the Paris Agreement. The three use cases in this paper show examples of such climate action that utilise blockchain. The Climate Warehouse of the World Bank aims to support the implementation of market mechanisms under the Paris Agreement. It provides a blockchain-based shared data layer of information supplied by participating registry

operators about climate projects and their issuances, transfer and use. TruBudget, a tool created by the German development bank KfW, serves as a blockchain-based project management tool. It can complement the Paris Agreement by providing transparency on official development assistance (ODA), including ODA for climate action. Finally, Etherisc is providing its blockchain platform as a solution to automate an existing weather insurance product in Kenya. The solution has the potential to substantially reduce premiums and claim cycles and thus can help to increase adaptive capacities and access to financial sources as stipulated by the Paris Agreement.

Make sure governance on and off your blockchain is well defined:

- **Is Blockchain the right solution for your problem at hand? (Section 3.2)**

Identifying the appropriate technological solution is a key step in beginning a climate action project. Often, a traditional ledger base might be the most fitting solution. However, a project may benefit from blockchain's core features if there is a preference to entrust the public community or a group of selected actors with ledger maintenance and a need for the ledger to be publicly verifiable.

- **What is the right project governance and management? (Section 3.3)**

Similar to any other large-scale IT project, the role of governance and management processes must not be underestimated to ensure proper functioning of a blockchain project. For public, permissionless blockchains there is a significant debate as to whether to handle governance on-chain or off-chain, although a combination is often inevitable. Most blockchain consortia are governed off-chain through standard business practices and agreements. Issues to consider include, amongst others, how members can join and leave a consortium, who owns the intellectual property assets created by the consortium, and what competences IT staff should have.

- **What is the right consensus mechanism, particularly considering performance and resource consumption? (Section 3.4)**

A variety of consensus mechanisms exist, currently categorised into three main classes of algorithms: Proof-of-X consensus algorithm, Byzantine Fault Tolerant algorithm and hybrid consensus algorithms. When deciding on which consensus mechanism to employ, not only the participation mode of a blockchain matters but also performance and resource consumption in terms of energy use. For example, PoX consensus mechanisms perform as well as PoW algorithms in terms of node scalability and latency but the different nature of the consumed resources and work performed (i.e., virtual mining) make the system more performant in terms of throughput and eco-friendliness.

- **How does your blockchain interact with the outside world, including off-chain data and other blockchains? (Section 3.5)**

It is necessary to consider robust governance elements to ensure the integrity of data that comes from outside the blockchain, particularly if off-chain data automatically triggers a transaction on-chain. Many blockchain projects for climate action use oracles, i.e., interfaces from the real to the digital world. For example, Etherisc uses data from weather stations to trigger payouts via mobile phones, the Climate Warehouse of the World Bank is either directly or indirectly fed with information from registries of countries and other operators and TruBudget needs to be able to interact

with procurement and accounting systems of the various participants in a specific use case. Options to protect against manipulated data include, amongst others, the use of multiple data sources, decentralised oracle networks or the selection of high-quality data providers. A final issue to consider is that some blockchain-based climate action projects might interact with other blockchains, which can result in new governance challenges and conflicts if, for example, decisions on one blockchain affect operations on another blockchain.

Make sure that your blockchain project for climate action complies with national laws:

- **Is your case so disruptive that national laws are not well suited, yet? (Section 4.1)**

Projects using blockchain for climate action need to comply with national laws and regulations. Most countries apply a "technology-neutral" approach to laws and regulations and focus on ensuring they sufficiently deal with new possibilities offered by new technologies such as blockchain. Nevertheless, some national laws can still pose problems for blockchain-based climate action. It is particularly difficult for highly disruptive projects to fit into current legislative frameworks. Using blockchain to decentralise power generation and peer-to-peer electricity markets of "prosumers" is such an example. Allowing for regulatory sandboxes is a promising way to incentivise testing of blockchain projects.

- **What jurisdiction applies in case of conflicts and what national laws with global impacts do you have to consider? (Section 4.2.1)**

Many blockchain projects are operated across countries, which can make the identification of applicable national laws challenging. It can be helpful to include choice of law, arbitration/dispute resolution and choice of forum clauses in agreements. Nevertheless, some laws and regulations cannot be waived by contract. Of particular interest for blockchain-based climate action are e.g., criminal laws, the EU General Data Protection Regulation or the US financial regulation. Finally, "legal interoperability" across borders would be desirable due to the cross-border nature of blockchain infrastructure.

- **What legal status does an entry on your blockchain have? (Section 4.2.2)**

A blockchain can verify the time and source of an entry such as emission reductions, but can only provide limited guarantees regarding the accuracy of an entry. A blockchain can also protect against manipulation of data. Finally, a blockchain can provide protection against double spending of tokens or double reporting of emission reductions. The applicable jurisdiction decides whether an entry on a blockchain is recognised as evidence in front of a court.

- **Have you clarified the validity of electronic signatures, blockchain-based assets and registries and data protection in your project? (Sections 4.2.3, 4.2.4, 4.2.6)**

Developers of blockchain projects on climate action should be aware that the validity of electronic signatures is still limited to specific jurisdictions. In addition, some financial regulations have recently changed and clearly regulated the issuance and

trading of blockchain tokens as well as issuance and transfer of assets based on blockchains. Finally, an instrumental issue is that of data protection laws such as the GDPR that include the right to be forgotten or limit the transfer of personal data to "third countries".

- **What is the legal status of your smart contract? (Section 4.2.5)**

The term smart contract can describe different things. In some cases, it can describe the technology for a script for a programmable blockchain that (automatically) executes transactions. In other cases, it can describe the execution of a legal contract via blockchain. Finally, it can also describe the conclusion of a legal contract via blockchain. For the last option, it is advisable to have a basic legal contract in usual legal language as a master agreement that clearly defines the purpose and scope of the coded smart contract concluded on-chain.

The report demonstrates the importance of addressing governance issues on all three levels from the beginning of the project when using blockchain for climate action. This ensures that perspectives from the blockchain, climate change and legal communities are all included, allowing for the establishment of projects that build trust and create confidence in using blockchain for climate action.

In order to support expanded recognition of the topic of governance, knowledge exchange and mutual learning should be encouraged. In addition, it is important to support and study use cases to test the practical applicability of governance challenge solutions.

1. Introduction

Climate change is one of the most pressing existential threats to humanity. The dramatic transition to net-zero emissions by mid-century will require global action on an unprecedented scale. This tremendous global challenge coincides with the emergence of blockchain technology, or more generally Distributed Ledger Technology (DLT)[1], a new and innovative form of decentralised datastore that provides new means of securely exchanging and storing data and digital assets, primarily designed for peer-to-peer transaction platforms. The UN Climate Change Secretariat has acknowledged the potential of blockchain for climate action and the Paris Agreement.[2]

Blockchain technology allows large groups of people and organisations to reach consensus and permanently record information without a central authority.[3] However, not having a central authority does not necessarily mean there is an absence of governance. In this paper, governance is defined with the common explanations: "Governance is about organising power, risks and responsibilities,"[4] and "Governance determines who has power, who makes decisions, how other players make their voice heard and how account is rendered."[5] This allocation of power, risk and responsibility is also key to creating blockchain-based climate actions.

Projects using blockchain technology for climate action under the Paris Agreement tend to ask a similar set of questions related to governance, such as: Is blockchain the right technology to solve the problem at hand? Who can validate a transaction? Who decides how the blockchain will change over time? How do national laws apply to the project? How does the project fit into the international rulebook under the Paris Agreement?

Governance not only means different things in different contexts, but governance issues can also occur in various forms and on different levels. Indeed, the blockchain, climate change and legal communities emphasise different aspects of governance. In this paper, governance issues are structured along the following three levels: international, national and blockchain.

Governance at the international level: The Paris Agreement establishes numerous rules for climate action. It determines what climate-related information countries must provide, in which format and how often. It also determines how national inventories, Nationally Determined Contributions and international transfers of mitigation outcomes must be published. If blockchain technology is to accelerate the implementation of the Paris Agreement, developers need to ensure that projects comply with these internationally agreed rules.

Governance at the national level: Fundamental characteristics of blockchains such as decentralisation, anonymity, immutability and automation lead to difficult legal and regulatory questions. Issues to consider include data privacy, the right to be forgotten, digital identification of participants (humans and machines), "signatures" for smart

[1] In this report, we are using the more common term «blockchain» as a simplifying placeholder for the much broader concept that includes all blockchain technologies, even though blockchain is only one implementation of Distributed Ledger Technologies.
[2] UNFCCC 2018.
[3] EU Blockchain Observatory and Forum: FAQ.
[4] Interview with Monique Bachner, see CLI 2020.
[5] Institute on Governance: What is Governance?

legal contracts or enforcement of smart contracts. In the context of using blockchain for climate action, additional regulatory and legal issues arise. For example, many countries have energy laws that do not foresee peer-to-peer electricity markets of "prosumers".

Governance at the blockchain level: Protocol level governance issues are inherent to blockchain technology. The focus of the previous two governance levels is on compliance with existing laws and considering standards and best practices. Governance at the blockchain level, on the other hand, is about actively defining rules that will be automatically enforced. Core questions that need to be answered are: Who can use the network? Who can validate a transaction? What is the consensus mechanism? How are changes to the protocol implemented? How is interoperability with non-blockchain parts of the network ensured, such as a data warehouse, sensors or other data sources?

Blockchains involve decentralisation, not only of power, but also of trust.[6] Creating confidence in the technology is key,[7] especially as it is a technology which is distributed and highly automated. In order to build confidence and maintain trust in blockchain in general, and blockchain applications for climate action more specifically, it is crucial to carefully address the various governance issues at each of the three different levels outlined above.

This publication provides an overview of the most relevant governance challenges on these three levels. It aims to introduce practitioners from the climate policy and blockchain worlds to main governance issues. This will be further accomplished through exploration of three use cases which exemplify how some pertinent questions can be addressed. The publication does not, however, attempt to exhaustively discuss governance issues.

Chapter 2 provides an introduction to the Paris Agreement and outlines possibilities where blockchain and other digital innovations can foster its implementation and accelerate climate action. Chapter 3 discusses governance challenges at the blockchain level, i.e., defining the technical rules and management of climate action projects. Chapter 4 discusses governance challenges at the national level and compliance with existing laws. The publication concludes with final remarks on the governance challenges addressed throughout the publication.

[6] Interview with the co-chairs of INATBA's governance working group, see CLI 2020.
[7] Interview with the World Bank, see CLI 2020.

2. Governance at the international level: The Paris Agreement sets global rules for the application of blockchain for climate action

If blockchain technology is to accelerate the implementation of the Paris Agreement, it needs to be ensured that projects consider the relevant internationally agreed rules. These rules are established in the Paris Agreement, its accompanying international rulebook and in further decisions by the countries. Together, these rules constitute the ecosystem driving a crucial part of current international climate policies.

These rules determine what climate related information countries must provide, in which format and how often. Therefore, this chapter provides an overview of the relevant international rules for climate action. In addition, it elaborates on components of the international rules that possess particular potential for climate action blockchain applications. The UN Climate Change secretariat has acknowledged the potential of blockchain for climate action and the Paris Agreement.[8]

2.1 The Paris Agreement's global climate action rules

The Paris Agreement was adopted in 2015 at the 21st Conference of the Parties[9] to the United Nations Framework Convention on Climate Change (UNFCCC). The Paris Agreement is the successor to the Kyoto Protocol, whose second obligation period ended in December 2020. The Paris Agreement entered into force on 4 November 2016 and has been ratified by 190 countries and the EU,[10] representing more than 97% of global greenhouse gas emissions.[11] Thus, the Paris Agreement can be considered a global treaty and almost all countries worldwide are subject to the international rules it sets out.

The objective of the Paris Agreement is "to strengthen the global response to the threat of climate change [...] by holding the increase in the global average temperature to well below 2 °C above pre-industrial levels and pursuing efforts to limit the temperature increase to 1.5 °C above pre-industrial levels."[12]

Core to the Paris Agreements are the so-called nationally determined contributions (NDCs). Each country is required to submit an NDC that represents a national climate plan and efforts to reduce national emissions. It is a legal requirement to submit an NDC, but the targets in NDCs are not legally binding.[13] NDCs have to be renewed at least every five years and become steadily more ambitious over time.

These bottom-up initiatives are combined with top-down global guidelines on transparency and review. This is crucial as a solely bottom-up process is unlikely to be ambitious enough to achieve the global objective of the Paris Agreement. Every five years there is a global stocktake to assess progress made toward the global objective

[8] UNFCCC 2018.
[9] Currently, there are 197 Parties (196 States and 1 regional economic integration organisation) to the United Nations Framework Convention on Climate Change.
[10] United Nations 2021.
[11] WRI 2020.
[12] WRI 2020.
[13] See e.g., Kohli, Anik 2015.

and provide information for countries to renew their NDCs. In addition, there are extensive measurement and reporting obligations (national inventories of greenhouse gases and national reports on progress towards NDCs) and the information provided by parties is verified and reviewed.

This hybrid structure for the climate change regime is different from the top-down model embedded in the Kyoto Protocol which set out legally binding emission reduction targets for a limited number of countries listed in an annex.[14] The measurement and reporting requirements as well as the review process had also a bifurcated approach that differentiated between two groups of countries based on annexes.

The more decentralised structure of the Paris Agreement aligns with the decentralised nature of blockchain technologies. Possible applications are discussed in the following sections.

2.2 Enhancing the digitisation and automation of measurement, reporting and verification (MRV) of climate data

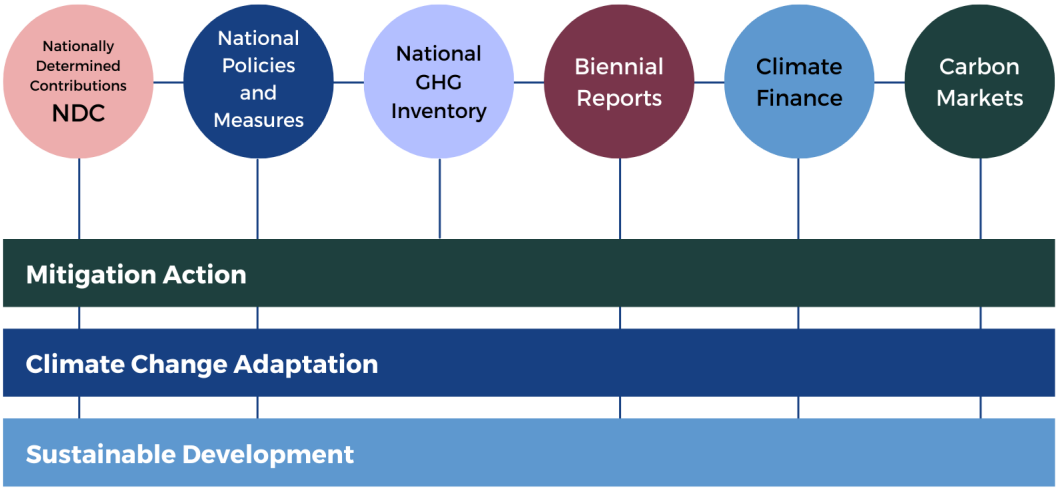
When communicating their NDCs, countries are required to provide "the information necessary for clarity, transparency and understanding".[15] Different types of NDCs require different information to understand the mitigation targets formulated. Developed country parties are requested to have quantified economy-wide emission reductions compared to 1990 as under the Kyoto Protocol. Other countries can also have targets such as sector-specific emission reduction targets, a target year for the peak of emissions, reduction of emissions per capita, or an increase in the share of renewable energy. This can make it difficult to understand the ambition of individual NDCs in comparison to others, complicating progress measurement and reporting.

The Paris Agreement establishes an "enhanced transparency framework for action and support".[16] This framework encompasses the reporting requirements by countries as well as the review of the information provided. Each Party must submit national inventories and other relevant information in order to track progress made in implementing their NDC.[17] While there is some flexibility foreseen for countries that need it,[18] the enhanced transparency framework and its reporting requirements are particularly challenging for developing country parties that did not face such extensive requirements under the Kyoto Protocol.

The information provided by parties undergoes a two-step verification process.[19] First, there is a technical expert review of the information provided that checks consistency of the information according to modalities, procedures and guidelines. Second, there is a multilateral consideration of progress.

[14] The Annex contained OECD countries of 1992 and economies in transition. Such an Annex did not allow to take into account changes in emissions and capacities of the Parties. As a consequence, countries such as Singapore, Mexico, Saudi Arabia, or South Korea did not have emission reduction obligations and did also have less extensive reporting obligations than, for example, Romania, Ukraine, or Italy.
[15] Paris Agreement, Article 4.8
[16] Paris Agreement, Article 13.1
[17] Paris Agreement, Article 13.7
[18] Paris Agreement, Article 13.2
[19] Paris Agreement, Article 13.11 and 13.12

Figure 1: Important Paris Agreement elements and related information flows



The main elements for the implementation of the Paris Agreement may also be seen as databases, sharing of data on actions, emissions, targets, transactions, payments, ownership and sustainable development benefits.

Source: Adapted from CLI 2018

The elements of the Paris Agreement create a considerable information flow for which the use of blockchain and other innovative technologies including remote sensors, Internet of Things (IoT), big data and artificial intelligence (AI) could be useful.[20]

- Data collection: Technology can reduce the time and cost of data collection as well as improve accuracy. The data could then be captured and properly secured on a blockchain.
- Impact quantification and reporting: Emission reductions are usually calculated based on a number of data parameters including usage rates, efficiency ratios, and "leakage". Blockchain-based smart contracts and cloud-based applications linked to IoT-derived data could enhance the impact quantification process.
- Verification: Smart contracts allow for encoding of methodologies and processes for verifying the data collected and assure its integrity and accuracy. AI can additionally be used to inform verification by comparing data with results obtained from other, similar activities to detect potential anomalies and irregularities.

2.3 Providing next-generation registries and tracking systems for decentralised market mechanisms

Under the Paris Agreement, parties can choose to engage in so-called "voluntary cooperation", i.e., market mechanisms, for the implementation of their NDCs. This

[20] See also CLI 2018.

means that an acquiring country can buy and use mitigation outcomes that are achieved through activities in a selling country.

Article 6 of the Paris Agreement foresees three mechanisms: cooperative approaches (Article 6.2), sustainable development mechanisms (Article 6.4), and non-market mechanisms (Article 6.8). Of particular interest for blockchain applications are the cooperative approaches that do not have a central governance.

Cooperative approaches involve the use of "internationally transferred mitigation outcomes" (ITMOs)[21] by two or more sovereign countries. While non-state actors such as private companies are often involved in the project implementation to achieve emission reductions, the transfer of ITMOs requires authorisation by the country. The cooperative approaches "shall apply robust accounting to ensure, inter alia, the avoidance of double counting".[22]

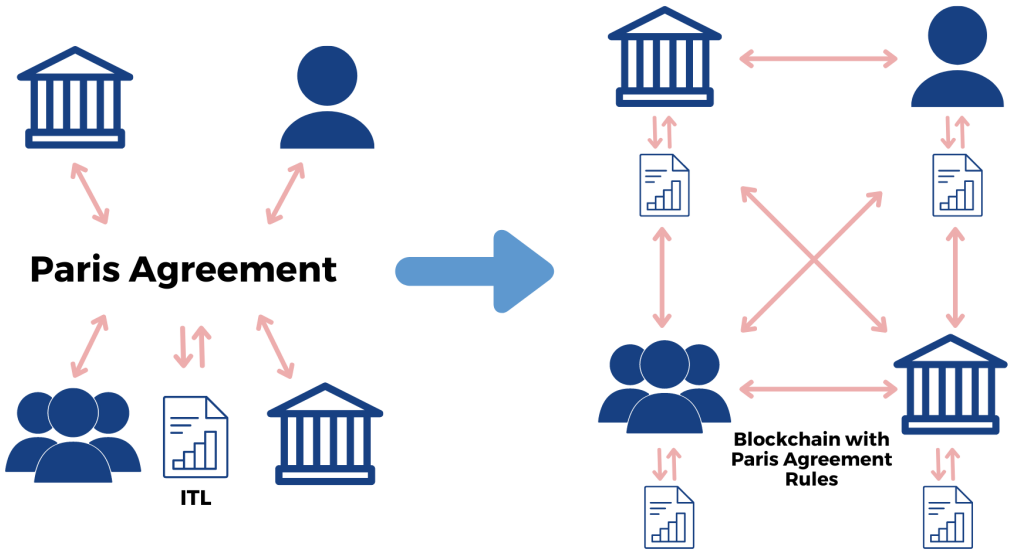
A major difference between the new market mechanisms under the Paris Agreement compared to the Kyoto Protocol is that all countries now have mitigation targets. Thus, it is imperative to avoid double counting of mitigation outcomes. Under the Kyoto Protocol, developed countries with mitigation targets could buy emission reductions from other countries that did not have any international targets to achieve themselves. Under the Paris Agreement, countries should apply "corresponding adjustments" (CAs) when reporting their emissions in case they used market mechanisms. Avoiding double counting is essential and requires robust accounting and tracking of units. The fact that the reporting cycles for parties is asynchronous adds an additional layer of complexity to this issue.

Another major difference between market mechanisms under the Paris Agreement and Kyoto Protocol is that countries may have different forms of mitigation targets (as outlined in Chapter 1.2). Different metrics of NDCs and ITMOs increase the challenges associated with accurately accounting for emission reductions.

It is important to mention that there are also national, sub-national and regional emissions trading systems (ETS) that contribute to the implementation of NDCs (see Chapter 2.1). The ETS of the EU is a regional example that sets caps and allocates emission allowances for more than 10,000 installations in 27 different countries. National ETS exist, for example, in the Republic of Korea, New Zealand and China. Sub-national actors such as California in the US or Quebec in Canada have also established ETS. These national, sub-national and regional ETS also require application of unified MRV rules in order to provide a level playing field for private sector participants within and across economies.

[21] Paris Agreement, Article 6.2
[22] Paris Agreement, Article 6.2

Figure 2: Centralised vs. decentralised technology



Source: Adapted from CLI 2018

The decentralised nature of the Paris Agreement and its governance structure requires new approaches to registries and tracking systems to handle heterogeneous rulesets for accounting and reporting as well as to allow for trusted, networked carbon markets. Thus, the functioning of the cooperative approaches align well with blockchain technology.[23] Blockchain technology accommodates the complexities of bottom-up governance with top-down rules on robust accounting. Blockchain provides a single point of access without the need for a centralised authority or database. The rules of the Paris Agreement can be encoded in smart contracts of a blockchain, and the hash function provides a secure and immutable way to validate content. National registries can then perform transactions bilaterally without a central system.

Smart contracts can also be used to ensure that ITMOs cannot be used unless a corresponding adjustment pair is available in the system. Additionally, smart contracts can be utilised to guarantee that the source of a unit is properly covered in the scope of the host country's NDC before use.

2.4 Enhancing climate finance flows as well as access to green technologies and clean energy

Climate finance flows and green technologies play an important role in the implementation of the Paris Agreement. Thus, one of the main objectives of the Paris Agreement is to make "finance flows consistent with a pathway towards low greenhouse gas emissions and climate-resilient development".[24] Not only monetary contributions from countries should be better aligned and contribute to climate mitigation and adaptation but also financial contributions from private sector sources should be utilised.

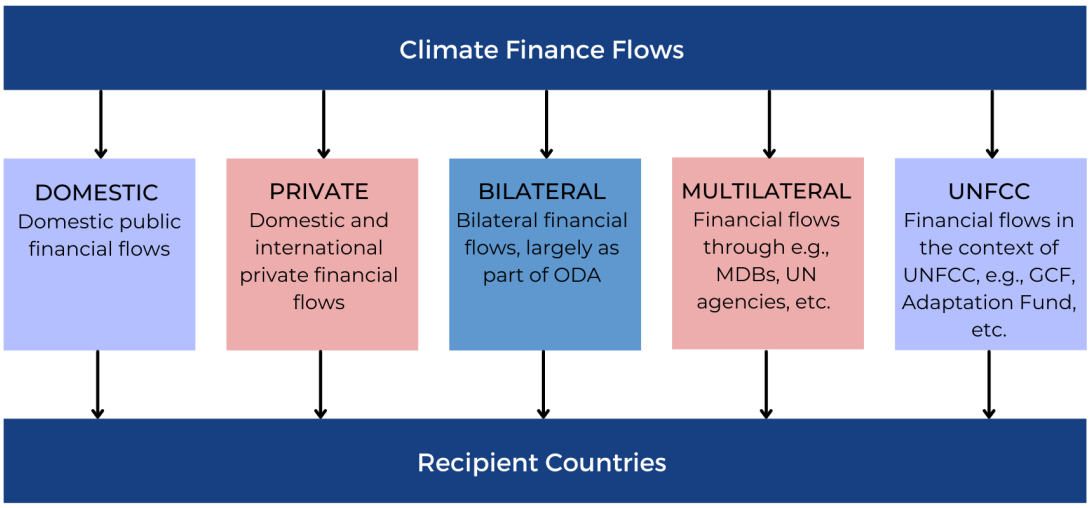
[23] see CLI 2018.
[24] Paris Agreement, Article 2.1(c)

The implementation of the Paris Agreement requires tremendous effort and particularly poorer countries need support in achieving their climate goals. To assist with this, developed country parties are required to provide financial resources to assist developing country parties in their climate efforts, and other parties are encouraged to do so as well.[25] The Agreement additionally emphasises that climate finance needs to come from "a wide variety of sources, instruments and channels".[26] Thus, financial flows from private actors are also important and part of a global goal to mobilise jointly USD 100 billion per year for the implementation of climate action.[27]

The Paris Agreement also notes the importance of technology development and transfer for the implementation of mitigation and adaptation actions, including, for example, clean energy technologies to lower emissions originating from energy production. Therefore, cooperative action on technology development and transfer shall be strengthened.[28]

Finally, the Paris Agreement's transparency framework requires developed country parties to provide information on financial, technology transfer and capacity-building support provided. In addition, developing country parties shall provide information on the support received.[29] The transparency framework can help to enhance the understanding of climate finance flows and how its mobilisation and distribution could be improved for increased effectiveness.

Figure 3: Climate finance flows



ODA = Official Development Assistance, MDBs = Multilateral Development Banks, UN = United Nations, UNFCCC = United Nations Framework Convention on Climate Change, GCF = Green Climate Fund

Source: Adapted from Schalatek 2017

[25] Paris Agreement, Article 9.1 and 9.2
[26] Paris Agreement, Article 9.3
[27] Decision 1/CP.21, para. 53
[28] Paris Agreement, Article 10
[29] Paris Agreement, Article 13.9 and 13.10

Blockchain could support the Paris Agreement's implementation with regard to climate finance and clean energy in various ways, including:[30]

- Prosumer of clean energy: Blockchain systems emerge as the backbone of new decentralised markets for clean energy where individual "prosumers" are empowered to produce and store their own renewable energy and trade with their neighbours.
- Access to climate finance: Blockchain technology combined with new fingerprint, iris or face recognition technology allows individuals who lack identity documents or bank accounts to access climate finance in the form of micro credits or micro insurances and subsidy schemes of payments for mitigation or adaptation actions.
- Result-based payment schemes: Using smart contracts for automated issuance, transfer and payment of climate outcomes can facilitate access to results-based finance schemes, particularly for the private sector in weaker regulatory frameworks.
- Transparency on financial flows: Blockchain and other innovative technologies could help with data collection and securely and transparently store information pertaining to financial flows. This could be of particular interest due to the various origins of financial flows, including those from private actors. It could also help to accurately track finance pledges at both domestic and international levels.

2.5 Non-party stakeholders have an important role in climate actions and implementing the Paris Agreement

When parties adopted the Paris Agreement, they also welcomed the efforts of "non-party stakeholders", such as local governments, companies or NGOs.[31] These stakeholders are invited to scale up their climate actions and demonstrate efforts via the "Non-State Actor Zone for Climate Action" (NAZCA)[32] platform. The platform provides an overview of individual actions and multi-stakeholder initiatives from several thousand actors. The actions and initiatives vary from "reducing city-wide emissions from transport by X% by year 20xx compared to a base year", to "removing commodity-driven deforestation from all supply chains by year 20xx", or to "amount of green bonds issued in a specific year".

Non-party stakeholders have a crucial role in the implementation of the Paris Agreement on the national level. National policies usually require and depend on actions by state and non-state actors, for example: businesses might develop new technologies that help to reduce emissions, community-based approaches can finance decarbonisation of economic sectors, NGOs can complement the government by educating people about climate change, or universities may contribute to gathering data necessary for national inventories. Therefore, parties are required to provide information on stakeholder engagement related to the implementation and achievement of NDCs in their biennial transparency report.[33]

[30] CLI 2018.
[31] Decision 1/CP.21
[32] https://climateaction.unfccc.int/
[33] Decision 18/CMA.1, Annex, para. 62

2.5.1 Role of non-party stakeholders in MRV, market mechanisms as well as climate finance and clean energy

There is also an important role for non-state actors across the three areas outlined in Sections 2.2, 2.3, 2.4.

In regard to reporting and reviewing relevant data, there is for example the GHG Protocol, a greenhouse gas accounting standard developed by the WRI and WBCSD.[34] The Corporate Accounting and Reporting Standard is widely used by companies around the world. More recently, the GHG Protocol has been used to develop standards, tools and trainings to help cities and countries to track progress toward their climate goals.

In the context of market mechanisms, existing standards include Verra[35] or the Gold Standard[36]. These verify that the emission reductions generated by projects are actually occurring. Certified emission reductions can then be traded in the market and used by companies as well as individuals to offset their own emissions.

The Task Force on Climate-related Financial Disclosures looks at climate finance flows.[37] The TCFD develops recommendations for more effective climate-related disclosures that could promote more informed investment, credit and insurance underwriting decisions. Improved information should allow companies to incorporate climate-related risks and opportunities into their risk management and strategic planning process. It should also direct private financial flows so that they support the transition to a low-carbon economy.

Decentralisation through the phenomenon of "prosumers", households or businesses that generate, consume and store electricity simultaneously using their own wind or photovoltaic systems is also increasing. These developments in the energy sector are supported by non-party activities such as RE100.[38] Under this initiative, led by the Climate Group and the Carbon Disclosure Project, almost 300 major businesses (e.g., 3M, Allianz, the BMW Group, Google, Johnson & Johnsen or Nestle) committed to using 100% renewable electricity for their operations before 2050, with an average target date of 2028.

Box 1: The Climate Chain Coalition

The UN Climate Change secretariat initiated and facilitated the creation of the Climate Chain Coalition (CCC) in 2017.[39] The CCC is an open global initiative to support collaboration among various stakeholders to advance blockchain and related digital solutions to help mobilise climate finance and (MRV) to scale climate actions for mitigation and adaptation. The network currently has more than 200 members.

[34] https://ghgprotocol.org/
[35] https://verra.org/
[36] https://www.goldstandard.org/
[37] https://www.fsb-tcfd.org/
[38] https://www.there100.org/
[39] https://www.climatechaincoalition.io/

2.5.2 Blockchain applications by non-party stakeholders to implement the Paris Agreement

There are already numerous examples of non-party stakeholders using blockchain for climate action. The supply chain sector has a number of ongoing projects where blockchains and other emerging technologies are used to solve traceability issues. Consumers increasingly desire to know the origin and impacts of the products they purchase. Blockchain can provide a solution because actors along a supply chain may not necessarily trust each other, but still need to share relevant data for traceability of goods. Additionally, blockchain in combination with IoT and AI can increase data quality and enable external third parties to check the accuracy of data.

The table below provides some examples of companies that offer climate-related products and services based on blockchain technology.

Table 1: Examples of climate related services on different blockchain networks

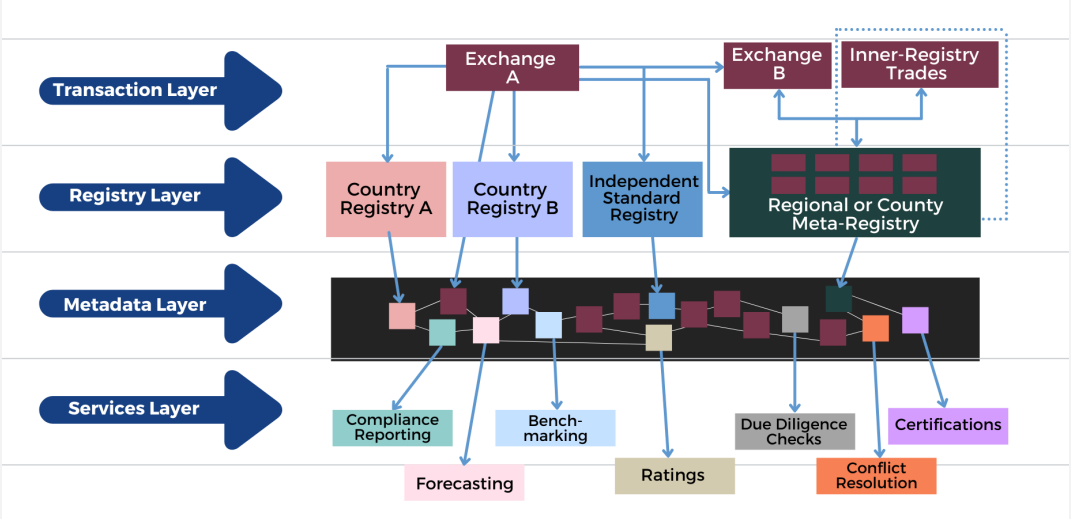
Companies	Climate Product/Service	Blockchain/DLT Network
Powerledger[40]	Trading of renewable energy	Ethereum (private network)[41]
ClimateTrade and Veridium Labs[42]	Carbon Offsetting	Stellar[43]
Yoma[44]	Self-sovereign ID platform supported by UNICEF which will be combined with incentives (tokens) to enable green services (Green Yoma), e.g., reforestation activities	Hyperledger[45]
Deposy[46]	Deposit return system that handles plastic waste	IOTA[47]
Trubudget[48]	Project Management Platform, used for example by Brazilian Development Bank BNDES to manage the Amazon Fund	Multichain[49]
BYD Electric Cars[50]	Drivers are rewarded based on their performance and carbon footprint.	VEchain[51]

Source: Own compilation by authors

[40] www.powerledger.io
[41] www.ethereum.org
[42] www.climatetrade.com and www.veridium.io
[43] www.stellar.org
[44] www.yoma.africa
[45] www.hyperledger.org
[46] www.deposy.org
[47] www.iota.org
[48] https://openkfw.github.io/trubudget-website/
[49] www.multichain.com
[50] www.byd.com
[51] www.vechain.org

Use case: World Bank Warehouse

Figure 4: The Climate Warehouse as publicly accessible meta-data layer within a carbon market ecosystem.



Source: World Bank.

To support the implementation of market mechanisms under the Paris Agreement, the World Bank has been working to develop a Climate Warehouse. It provides a blockchain-based, shared data layer of information supplied by participating registry operators about climate projects and their issuances, transfer and use. The aim is to provide transparency, traceability and auditability of information for the purpose of avoiding double counting and robust tracking of mitigation outcomes (MOs). Registry operators surface in near real-time agreed publicly available meta-data information to the Climate Warehouse blockchain through their node or a shared node. Thus, the information in connected registry systems is in sync with the data that is in the Climate Warehouse. By participating and providing data to the warehouse, governments will be able to increase the visibility of their projects, issuances, transfers and use of MOs across jurisdictions. Figure 1 depicts how an operational Climate Warehouse will integrate with participants within the Carbon Market ecosystem to provide an inclusive infrastructure to connect and share data.

Currently, the Climate Warehouse concept is being tested with partners through the use of a prototype developed by the World Bank to simulate the integration of registry functions.[52] Through the simulation, all partners are collectively learning how a future system can facilitate a simplified way to connect and integrate registry systems, what data will be needed and should be made publicly available, what processes should be supported and potential benefits and challenges associated with using blockchain.

Once a Climate Warehouse system is operational, it will provide an inclusive platform for countries to share information, increase the visibility of climate

[52] This is the second simulation that the World Bank is conducting with partners. For information on the first simulation and prototype completed in November 2019, see World Bank 2019.

projects in developing countries, and provide the data needed to facilitate buyers and sellers of carbon assets. Through participation in the Climate Warehouse, countries will have simplified access to data they need for their own analysis of double counting risks. By providing data to the Warehouse, participating countries and independent standards increase the transparency afforded to their projects. This will provide needed assurances to regulators, investors and other market participants that the issuances, transfers and usage of carbon assets have not been double counted.

Governance related to the international level

The Paris Agreement enables Parties to link decentralised climate markets (see section 1.3). The Agreement does not elaborate on how registry systems will be connected so that units issued from projects can be tracked. Going forward, international climate markets such as those under CORSIA[53] or Article 6, will likely require different registry systems to communicate with each other for transparency and compliance purposes. The World Bank is testing the concept of a Climate Warehouse that facilitates a peer-to-peer connection among decentralised registries by developing a common "language" and data architecture between registries.

The Climate Warehouse simulation is being used to create a data model in consultation with the participating partners that would be needed for a metadata layer to provide information about internationally transferrable mitigation outcomes (ITMOs) and that traces bilateral transactions between partnering countries. For participants, it could ease the necessary steps and efforts because the data needed for international reporting is captured in an immutable shared format that they can use to fulfil these requirements.

Governance related to the blockchain level

Blockchain is a good fit for the Climate Warehouse because its decentralised infrastructure enables transparency and ensures fair play between partners. The infrastructure presents a practical way to share information by providing partners the means to integrate directly with a node. Partners can build their own user interface and analytics on top of the data in their node.

The World Bank prototype of the Climate Warehouse was built to test its functions with partners and inform developers of the requirements needed for an operational system. Through simulation with partners and engaging them on the design and operational model, the participants will contribute their feedback into a future governance model of a Climate Warehouse, ensuring that an operational warehouse meets the needs and requirements of its primary stakeholders.

The Climate Warehouse prototype is managed by the World Bank and is built using a private blockchain as a service platform using a Proof of

[53] ICAO: CORSIA

Authority consensus mechanism. A private blockchain was chosen to provide prototype participants with a safe place to experiment and learn about the technology. Ease of use and removing barriers to participation were important requirements for the Warehouse. The prototype makes use of an auxiliary application that can function as a test-registry system for participants. The auxiliary application enables countries to participate utilising test data even if they do not have an operational registry system. Another advantage to this approach is the flexibility it offers to add and experiment with new features necessary to support Article 6 processes. Examples of other measures that could simplify the acceptance of the Warehouse of participating countries are:

- Registries are responsible for their own data and updates;
- Participants are not allowed to change data that does not belong to them;
- The Warehouse does not pull data from registry systems and registry administrators have full control over the data they share with the Climate Warehouse;
- Only agreed upon publicly available data is shared in the Warehouse and does not contain any personally identifiable information, and
- For the Warehouse concept to function, all partners need to agree that the data in the Warehouse is accurate and matches the data in their own registry systems, so that the data in the Warehouse can be relied upon for reporting and further services.

Governance related to the national level

It is not anticipated that there will be blockchain-specific legal challenges, partly due to the narrowly defined scope of the warehouse as a public good metadata layer of climate asset information. Because partners provide their own data into the system, participants will have the option of hosting and integrating with their own node or integrating with the warehouse through a partner node, such as a regional registry or a “meta-registry” system. Partners can choose the integration model that fits their regulatory environment or requirements.

Concluding remarks on Governance

Governance over decentralised infrastructure needs to strike a balance between the clarity and efficiency of a centralised governance model, and acceptance and shared responsibility of network participants. To build a truly inclusive system that will support and simplify participation in the Paris Agreement and create a cohesive carbon market ecosystem amongst stakeholders, governance design, functions and decisions need to reflect the visions of diverse participants.

3. Governance Challenges at the Blockchain Level: Defining the technical rules and management of climate action projects

Projects applying blockchain for climate action need to carefully consider the governance structure on the protocol level as well as on the management level. Rules about access, rights and duties have to be actively defined and how interoperability with non-blockchain parts of the system is ensured. This allows the smooth and efficient running of the project through automatically executed codes. In addition, rules need to be defined for specific cases e.g., how changes to the protocol can be implemented.

The following chapter will first discuss when to consider applying blockchain for climate action and the importance of off-chain project governance and management. It then elaborates on-chain governance issues as well as technical interfaces and interoperability issues.

Box 2: Different types of blockchain

In blockchain-based platforms, actors within the blockchain system hold a copy of the ledger of data, meaning that data is replicated for all entities participating in that blockchain (i.e., nodes or peers). Due to distributed data storage, it can be difficult to ensure that all nodes agree upon a common vision of the ledger – referred to as consensus among nodes. Consensus can be reached in different ways depending on the nodes' modes of operation.

Nodes can operate in a *permissionless* or *permissioned* mode with respect to accessing the blockchain network and maintaining the ledger. These different participation modes characterise the three main blockchain types presented in Table 2.

Table 2: Three main types of blockchains

Blockchain Type	Description
Permissionless Blockchain	Anyone can access the blockchain network and participation in the ledger maintenance is public, i.e., anybody can participate in the consensus process. This participation mode offers disintermediation, i.e., it cuts out any middleman.

Permissioned Blockchain	Participants have either restriction on writing (validation) rights only, or on both reading (access) and writing rights. Usually, this participation mode leads to less decentralised blockchains. Permissioned blockchain can be further classified as:
Open-permissioned Blockchain	The ledger is publicly readable, but any modification of the transaction ledger is entrusted to a selected set of nodes.
Full-permissioned Blockchain	Participants are selected in advance and all network activities are restricted to these actors only.

Source: Adapted from Belotti, Marianna et al. 2019.

Table 3: Further classification of permissioned blockchains

Permissioned Blockchains	Nature of the participants
Consortium	A consortium blockchain represents a joint effort of several entities sharing a common goal or business need that may involve actors of the same industry or cross-industry projects.
Private	A private blockchain involves actors in a company that operate in a disintermediated manner.

Source: author

With respect to the nature of participants, permissioned blockchains can be further classified in 'private' and 'consortium' systems according to the organisation of the participants or of consortia of different enterprises.

As specified in previous sections, blockchain technology could improve implementation of the Paris Agreement's requirements since it enables different (geographically distant) parties operating in the same ecosystem with different roles and authorities to cooperate in maintaining a ledger of climate relevant data. Hence, in the context of climate action, permissioned consortium implementations can enable cooperation among various stakeholders.

3.1 Is Blockchain the right solution?

During the past few years, research institutions along with industrial and governmental institutions have intensively worked on DLT and blockchain in

particular, trying to better understand the underlying features and the role of these technologies in today's society and economy. This resulted in many publications, experimentations (Proof of Concepts or PoCs), and standardisation activities well before the exploration of understanding when to use blockchain technologies or considering which projects may benefit from blockchain's core features. Blockchains are often part of a wider solution – usually combined with other technologies (IoT, AI, etc.) and digital platforms.

Blockchain technology offers cryptographic features (integrity, authenticity and non-repudiation) and immutability due to its usage of hash functions and digital signatures. Moreover, as it is a distributed technology, blockchain offers decentralisation and transparency at different levels depending on the chosen solution. Hence, there is a need to understand which blockchain features can benefit climate action projects and which types of on-chain governance structures could potentially be adopted.

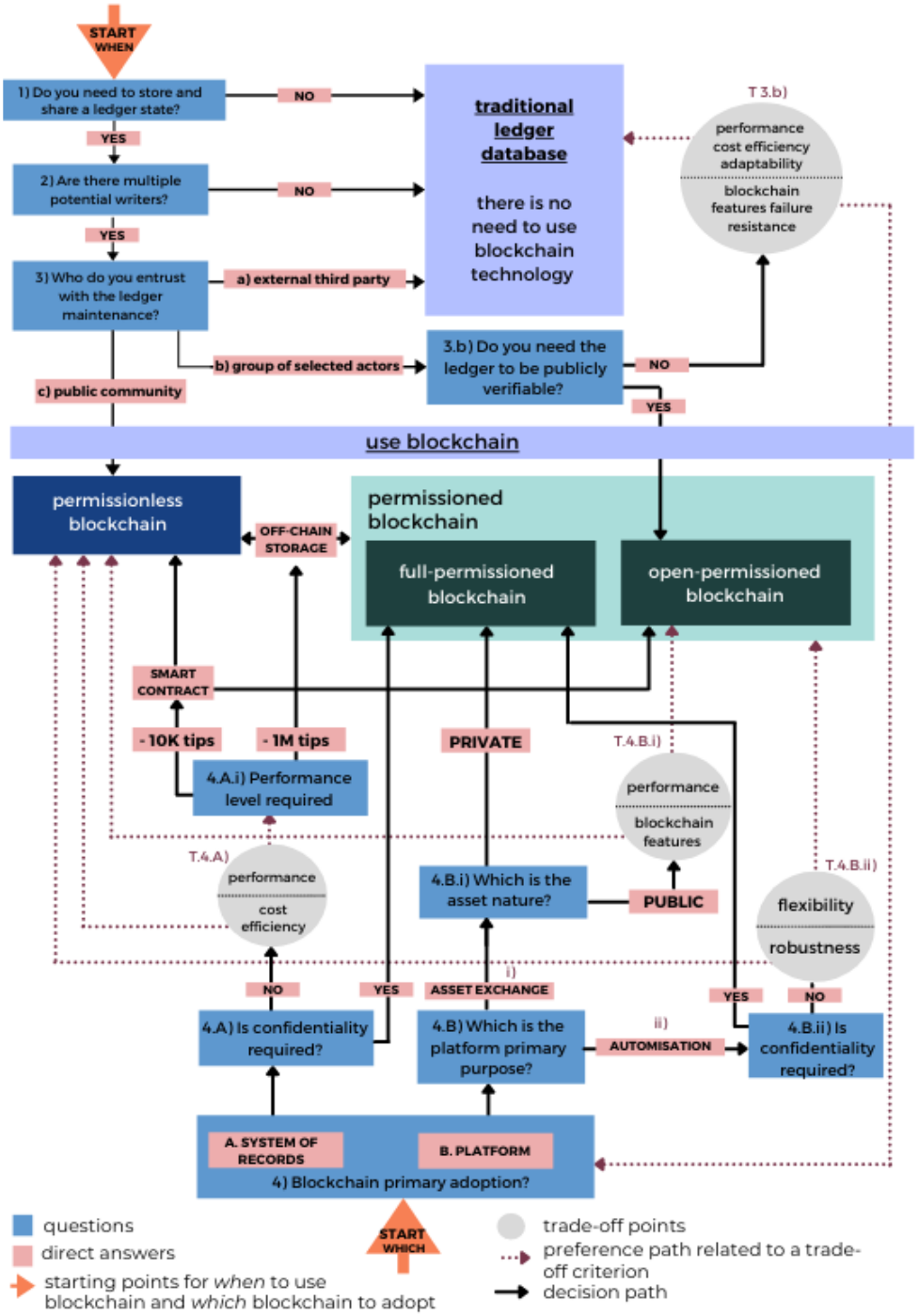
As specified in previous sections, blockchain could help in implementing the Paris Agreement's requirements since it enables different (geographically distant) parties to cooperate in maintaining a ledger (a register) of data updated by transactions instantiated by the different nodes of the system. The state (i.e., the version) of the ledger needs to be stored and shared across a community of different nodes to update the ledger state in a transparent fashion. The choice to use a blockchain technology and the nature of the adopted solution depends on the level of transparency (i.e., verifiability) of the system and is related to the level of trust in the actors characterising the project. Hence, it is the desired trust level in the different actors of the system that usually determines the choice of the technology.

Whenever a system requires public verifiability, i.e., it lets anyone in the public community observe the system's state and verify its correctness, writing rights may be kept restricted but at the same time everyone is free to observe the ledger state in open permissioned blockchains. On the other hand, for cases in which verification procedures must be kept private, the choice between a fully-permissioned blockchain and a centralised solution (e.g., central database) depends on the nature of the verifying nodes that may be centralised or distributed respectively. The adoption of a permissioned blockchain rather than a traditional database is a matter of trade-offs regarding mainly efficiency of the system (in terms of throughput) and the benefits offered by blockchain features.

The decision tree in Fig. 3.2 represents the steps to be taken when deciding whether or not to use the blockchain technology and choosing its participation mode. The first part of the chart, to be read from top to bottom, answers the fundamental question "when to use blockchain as a technology". When the decision has been made to adopt blockchain, the chart can be read from bottom to top to choose the participation mode by identifying the technology adoption for the specific business case between (i) a system of records (SOR) and a (ii) platform. The principal usage of a blockchain solution in climate action applications would likely be as a *system of records* (i.e., SOR) for storing data and the history of state changes (whether or not accessible to the public community). The level of data disclosure is the determining factor (in this case) in the choice between a permissioned (open or full) or permissionless blockchain implementation.

Figure 5: When to use blockchain, and which type, instead of adopting a traditional database system

Red circles represent trade-off points between crucial aspects for the different blockchain use-case. The red arrows indicate the consequence of giving priority to one aspect rather than the other, while black arrows report answers to all the questions – coming with an order – of anyone interested in the blockchain technology.



Source: Belotti, Marianna et al. 2019.

3.2 Off-chain project governance and management

Once there is clarity and agreement of the value a blockchain solution offers to a particular problem (see previous section), it is necessary to establish the project's governance and management. Similar to any other large-scale IT project, this step must not be underestimated to guarantee the well-functioning of a blockchain project. Governance choices should be led by the purpose and goal of a project.[54] Most blockchain consortia are governed off-chain and through standard business practices and agreements.[55] The steps to consider for consortium blockchains will be elaborated upon further below.

For public, permissionless blockchains, the approach to governance is less straightforward.[56] Most community-run blockchains use solutions similar to those of the open-source movement. For example, the Bitcoin Improvement Proposal process is copied from the Python Enhancement Proposal process.[57] There is a considerable debate as to whether to handle governance on-chain or off-chain, although a combination is often inevitable. In case of on-chain governance, the rules for changing the protocol are hard-coded into the protocol. In case of off-chain governance, decisions for changing the protocol are made in formal and informal processes off-chain among the community of stakeholders. The EU Blockchain Observatory and Forum suggests that a practical compromise could be useful where most rules are encoded on-chain, but in cases of severe disputes where human interpretation is necessary, more traditional commercial agreements and laws apply.[58]

Most blockchain consortia use standard business practices and agreements to set up a formal organisation for the project and to decide about the governance of the consortium. Consortium members can enter into a formal contractual arrangement or even form a legal entity. Other options include memorandums of understanding, associations, private entities, foundations or contracting with a private entity to build and run the project.[59] Selection of the organisation type and jurisdiction will be driven by many factors, including location of the founding and prospective members, tax issues, financing, regulatory requirements as well as blockchain related knowledge levels in a specific country.[60]

Some of the issues to consider for the governance of the consortium can be summarised as follows:[61]

- Purpose and goals: The purpose as well as short- and long-term goals of a project should be clarified and expressly stated so that they are clear to all members.
- Organisation and Board: The roles and responsibilities of the members should be clarified. Some members might be considerably larger companies than others, some might bring more financial or technical contributions, and some members are governmental or not-for-profit entities. Representation on a board as well as the voting rights, including procedures for critical issues, can be important considerations.

[54] Lyons, Tom et al. 2020.
[55] Radcliffe, Mark 2019; Lyons, Tom et al. 2020
[56] Lyons, Tom et al. 2020.
[57] Lyons, Tom et al. 2020.
[58] Lyons, Tom et al. 2020.
[59] Lyons, Tom et al. 2020.
[60] WEF 2020; Radcliffe, Mark 2019; CLI 2020.
[61] The summary is based on Lyons, Tom et al 2020; WEF 2020.

- On-boarding and off-boarding: Clarification on how members can join and leave a consortium is necessary. In case of enterprise consortia, it is advisable to also have an inclusive network based on objective criteria to join in order to avoid antitrust or competition law concerns.
- Intellectual property: Ownership of IP assets created by the consortium should be clarified early on.
- Competition and inclusivity: Policies and procedures should be put in place to ensure compliance with competition laws. In case of collaboration among competitors it can be particularly relevant to remain inclusive toward new consortium members.
- Liability and risk management: The members should have a clear understanding of how to manage risks and deal with liability issues.
- Financing and business strategy: Initial funding as well as long-term finance should be clarified. This includes discussions about investments, revenue models and distribution of profits.
- Changes and updates: The procedures for upgrades and changes needs to be determined. This includes who has control of the official codebase, who can request changes and who decides what changes are made. Due to the important role maintenance and upgrades play in blockchains, processes and procedures need to be in place from the beginning.
- Dispute resolution: The governing documents should clearly state what law will govern in case of disputes. In addition, a consortium might also consider an internal dispute resolution body.
- Technical decisions: Members of a consortium should also agree ahead of time how technical decisions are made and by whom. This includes clarification on who is managing the day-to-day project oversight, the competences of IT staff including for emergency operations like bug fixes or reaction to attacks, or who is executing specific project activities.

Balancing certainty with flexibility is a core aspect of defining governance structure. While the elements outlined above should be formalised through legal terms and conditions, blockchain is still a new technology with evolving legal, regulatory and interoperability frameworks, and common standards.

3.3 On-chain governance

3.3.1 Consensus mechanisms

Consensus in a general network refers to the process of achieving agreement among the network participants on specific state of the system, leading all network nodes to share the same data. Hence, consensus mechanisms or algorithms on blockchains:

(i) ensure that the data on the blockchains is the same for all network actors, and

(ii) prevent faulty nodes (acting both rationally or irrationally) from manipulating data.

The consensus mechanisms vary between different blockchain implementations according to the system nature (in particular permissionless/permissioned). A variety of consensus mechanisms exist, with currently three main classes of algorithm:

- *Proof-of-X* (PoX) consensus algorithms
- *Byzantine Fault Tolerant* (BFT) algorithms
- Hybrid consensus algorithms

More precisely, the first two classes characterise consensus in blockchains, since algorithms defined as 'hybrid' mix aspects of protocols from the first two classes. More complex consensus implementations are simply creative combinations of PoX and BFT protocols.

Consensus in distributed systems has been studied since the 1980s, long before the introduction of Bitcoin. Distributed systems need protocols that guarantee a common view of the shared data ledger.

- BFT algorithms (a class of State Machine Replication protocols) were adopted to deal with Byzantine nodes, i.e., rational nodes acting maliciously. These types of algorithms are based on voting procedures where network nodes are called to accept or reject a specific vision of the network's state.
- The advent of Bitcoin gave rise to a new technology based on a new innovative consensus system called *Proof-of-Work* (PoW). The idea driving development of a PoW consensus was to gain the right to validate the state of the ledger by proving to have worked from a computational point of view i.e., to have used a machine (e.g., a computer) to work for the system. This particular idea of gaining the right to propose and validate the agreement value proposed by the PoW consensus was really innovative for its time as it gave every node a chance to have an important governance role in the system. This gave rise to the larger category of *Proof-of-X* (PoX) consensus algorithms where *X* denotes the resource a network node is consuming/allocating to gain the right to propose and validate the agreement value. While in Bitcoin the *X* stands for "computational resources" for other consensus mechanisms it stands for a "stake" of the system (*Proof-of-Stake*), or for memory "capacity" (*Proof-of-Capacity*) or again wireless network "coverage" (*Proof-of-Coverage*).
- The advent of permissioned participation modes and the rise of permissioned blockchains and blockchains are making the industry reconsider traditional BFT. Here blockchains are no more *peer-to-peer* (P2P) systems where every node is given the chance to participate in the consensus of a blockchain but blockchains can be closed systems as the traditional distributed ones studied in the 20th century. This consensus phase is marked by protocol experimentation with BFT-based algorithms with the aim of preserving permissionless consensus while keeping the process efficient by reducing the number of participating nodes to the consensus. Hence, consensus is divided in two phases; the first one that determines the formation of a committee of voters elected through a PoX mechanism and the second one where nodes vote according to BFT consensus.

3.3.2 Consensus performance and resource consumption

Previous sections present the different types of existing consensus protocols and their evolution pattern with respect to the different types of blockchains. However, consensus evolution was not determined only by participation modes of blockchain, but two other factors played a crucial role in consensus evolution as well: (i) performance in terms of *throughput* and *latency* and (ii) resource consumption in terms of *energy impact*.

PoW consensus is based on the concept of making validation tasks difficult to perform but trivial to verify; whereas consensus participants (i.e., miners) are given a computational hard problem to solve to create rare and valuable goods i.e., new minted bitcoins. Over time, mining activities became more and more energy consuming and wasteful as the computational work needed to validate blocks grew exponentially. This resulted in more energy and machine waste due to hardware-based mining solutions deterioration. Moreover, PoW-based algorithms need to be highly scalable (i.e., to respond adequately to a growth in the number of nodes) because every node of the system that can potentially participate in the consensus need to be synchronised by receiving and transferring data from the ledger. This results in high latency levels caused by the transaction propagation mechanism. Therefore, there is a need for alternative schemes for permissionless implementation that (i) consume different resources and (ii) improve performance.

PoX consensus mechanisms perform as well as PoW algorithms in terms of node scalability and latency, but the different nature of the consumed reward and work performed (i.e., virtual mining) make the system more performant in terms of throughput and eco-friendliness. PoX algorithms enable reaching consensus both in permissioned and permissionless scenarios by saving considerable energy compared to the PoW consensus.

BFT algorithms, which only work for permissioned environments, have performance levels comparable to that of central databases because they do not have to scale. Data on the ledgers are transferred very efficiently, i.e., a significantly lower number of messages is sent to consensus nodes. This means transactions are processed in a fast manner and the energy cost to maintain the system is even lower than PoX mechanisms demand.

Hybrid BFT-based algorithms running for both permissioned and permissionless implementations allow for a combination of benefits from the previous mechanisms. They can perform as BFT algorithms in terms of throughput and energy impact while also representing a trade-off solution in terms of latency and node scalability.

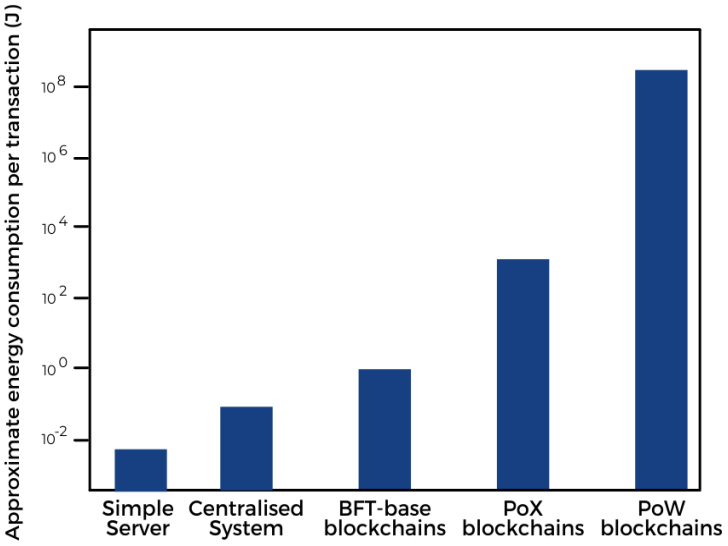
Table 4 summarises the performance while Figure 6 reports the consumption level of the four consensus categories and shows the tendency to implement performant blockchain-based systems with low energy impact and low latency.

Table 4: Summary about consensus performance

Property	PoW	PoX	BFT-based	Hybrid BFT-based
Node identity management	Permissionless	Both cases	Permissioned	Both cases
Nodes scalability	> 1000	> 1000	< 100	100-1000
Throughput (tx/s)	7-30	100-4000	Up to 110k	Up to 10k
Latency (s)	Up to 600	Up to 600	Less than 1	Up to 20

Source: Belotti, Marianna et al. 2019.

Figure 6: Consumption level of consensus categories



Source: Adapted from Sedlmeir, J. et al. 2020.

The Wood Tracking Protocol (WTP)[62] provides an example of the practical relevance an efficient consensus mechanism offers for climate action blockchain projects. The WTP provides a smart phone application for wood loggers to help document their work in the Peruvian Amazon. Part of the data generated is directly transferred to a blockchain in order to achieve immutability and, as a result, accountability of logging relevant data sets. WTP foresaw the interaction with the public Ethereum Blockchain. However, due to current scalability limitations (storing big data on Ethereum in March 2021 is prohibitively expensive) and the energy intensive use of Ethereum's Proof of Work consensus mechanism, WTP executes transactions on a private blockchain.

[62] www.wtp-project.com

3.4 Technical interfaces and interoperability

An interface is often referred to as the place at which independent and often unrelated systems meet and act on or communicate with each other. Blockchains need interfaces to enable data operations within their ledgers.

3.4.1 Inherent limitations of capacity and data privacy of permissionless Blockchains

Many projects that run on permissionless blockchains face the question of how to ensure transparent and swift data management while providing a certain level of data privacy. A blockchain is a shared state database that records transaction outputs. Permissionless or public ledgers like Ethereum require all nodes in the network to hold all the chain data to be able to validate transactions. That is why the data capacity of public blockchains is limited. Moreover, many blockchains are also magnitudes slower than today's traditional databases. Most blockchains favor transparency over privacy by design. Except for specialised blockchains like privacy coins, all transaction data, including sender account number, receiver account number and amounts transferred are completely open and copied to every node in the network. Everyone has access to this information around the clock by accessing a node or using a corresponding block explorer service. This inherent limitation of privacy and capacity, especially on permissionless blockchains, increases the relevance of the role technical interfaces and interoperability play.

3.4.2 Off-chain data

Limited data management capacities and privacy concerns are core drivers for project developers to store or interact with data outside the network of blockchains. Moving data off-chain can alleviate some of the concerns mentioned. For example, with off-chain storage, data no longer needs to be hosted by all nodes but only by the nodes that are performing the computation.[63] The cryptographic features of blockchain networks ensure the integrity of each individual ledger entry and the accuracy of the ledger as a whole. In fact, on-chain cryptography is often used with the sole purpose to validate data off-chain.

Any attempt to alter the data ex-post would be rejected by the consensus rule, and the attempt itself would become visible to all participating parties.[64] That means that independent of whether data is stored off chain or not, it needs to be ensured that the data, which is provided through a predetermined interface, is accurate and credible. It is therefore necessary to consider robust governance elements to ensure the integrity of data that comes from outside the network. The latter becomes even more relevant if off-chain data automatically triggers a transaction on-chain, for example through smart contracts (see Chapter 4.2.5).

3.4.3 Oracles and APIs - Interfaces to the outside world

Blockchains as such do not interact with the outer world or provide connections to, or interoperability with, traditional systems. A piece of infrastructure called an "oracle" must be adopted to connect the blockchain via the internet to external resources.[65] Oracles are interfaces from the real to the digital world. The range of what people regard as an oracle is broad. It can be the sensor of an IoT device, but also a web

[63] Mota, Miguel 2019.
[64] Maupin, Julie et al. 2019.
[65] Nazarov, Sergey et al. 2020.

service or a smartphone application. Application Programming Interfaces (APIs) serve as adapters for oracle applications and allow oracles to communicate with other applications. APIs can also be described like messengers that take requests, translate, and return responses.

How outside data provided by oracles becomes part of the network's state:

A participant in a blockchain network might write data about a financial transaction based on the current value of a carbon reduction unit traded at an energy exchange. Though the participant himself is not a trusted authority on the energy exchange, an existing non-blockchain-based trusted web service can provide a signed data value asserting the value of a carbon reduction unit at a given time (with a timestamp). The participant then publishes the transaction along with the signed value. The participant functions as an "oracle" because they published trusted data from an outside source to the blockchain. If a smart contract needs the price of a carbon reduction unit to execute (e.g., to release a corresponding payment), all nodes can agree on the same information, as it is already stored on the blockchain. Hence, it is possible to find an identical state of information and create a new block.

Oracles are crucial for widespread adoption of blockchain technologies not only in the climate space. Many of the anticipated projects for smart contracts and decentralised apps depend on data that is not existent on the blockchain a priori, e.g., the weather report for crop insurance or the amount of gigawatt produced by a solar panel for an automated sale of electricity. While these examples describe a situation where the oracle interacts only once to determine a specific situation (amount of renewable energy generated/a flooding event took place), it is also possible to have a specific oracle interacting with a blockchain on a continuous basis.

The future application of smart contracts under Article 6 of the Paris Agreement may serve as an example. This framework allows country A to finance/realise GHG reductions in country B and use these reductions for its own account. The Paris Agreement requires country B to execute a corresponding adjustment in its GHG inventory if GHG reductions are achieved on its territory and sold/transferred to another country. In that case, the database that manages the GHG inventory of the host country would act as oracle at least twice with a blockchain. The first time, the oracle would immutably determine the GHG inventory amount before the reduction of GHG takes place, and the second time they would confirm the adjusted GHG inventory amount after the reduction of GHG.

Two types of oracles can be distinguished: machines and human users. Machine oracles are sensors (e.g., Internet of Things, IoT) that generate and send digital information in a smart-contract-readable format. User oracles are people reporting on certain events using digital means of communication (e.g., smart phones). However, while blockchains can guarantee the origin and non-tampering of data, they do not protect against false declarations. In order to manipulate the outcome of a smart contract, oracles can be attacked by third parties or their provider could deliberately provide false data (e.g., to make a profit from the incorrect execution of the contract). Several approaches exist to ensure the secure and credible application of oracles; see the table below for full information.

Table 5: Approaches to ensure credible application of oracles

Approach	Description
Use of cryptography	Information shared by oracles is digitally signed using cryptographic values and is considered non-repudiable (assurance that the signature cannot be denied by the party who signed it). Signatures increase the accountability of data sources (machine or human).
Multiple data sources	Multiple data sources can decrease the likeliness of false data reporting. In that case, there are only two ways to receive erroneous data: most data sources were compromised, or the oracle itself is compromised (leaving a single point-of-failure).
Decentralised oracle networks	Many oracles can be combined to make up a decentralised oracle network, which can aggregate the responses of each node to ensure there is no single point of failure in the delivery of data while improving data integrity) and data manipulation protection.
Data platform with credential management systems	The use of high-quality data providers and enterprise systems such as web APIs, internet of things (IoT) networks, CRM/ERP systems and various other legacy systems that require authorised logins can improve the overall data quality.[66]
Reputation systems	The performance data of the oracle node on the blockchain is recorded and can be fed directly into a reputation system. This allows future customers to determine the quality of an oracle node operator and enables existing smart contracts to potentially remove nodes from data requests that were recently reported to have been malicious or unreliable.[67]

Source: own overview by author

3.4.5 Interoperability between blockchains

Interoperability between blockchains will be crucial for the success of blockchain-related digital climate applications.[68] Climate relevant areas, where interoperability between blockchains will become increasingly relevant, include the management of supply chains, climate finance flows, transportation and industrial production processes. Moreover, the ability to ensure smooth information sharing across blockchains enables the possibility of developing partnerships and sharing solutions.

Practical examples include the integration of payment options into climate risk insurance executed by smart contracts (Blockchain A) based on weather indices (Blockchain B), or tracking renewable energy production (Blockchain A) and converting the outcome into a carbon reduction (Blockchain B).

Most blockchains today represent stand-alone, disconnected networks with different ecosystems, data structures, algorithms, consensus models and communities.

[66] Nazarov, Sergey et al. 2020.
[67] Nazarov, Sergey et al. 2020.
[68] For a general overview of interoperability requirements related to climate-relevant applications, see Chapter 2 in CLI 2020.

Technically, blockchains may connect to each other if they would use consistent APIs. APIs do not require a governance structure which makes them flexible and expedient for certain projects. However, APIs are often inappropriate for organising blockchain interoperability because all blockchain networks run their own governance and regulatory controls. Moreover, interoperability solely based on APIs would lead to certain centralisation toward the provider of the API.

Blockchains can also be linked using cross-chain technology. Cross-chain technology enables interoperability by offering a protocol-based gateway that allows various blockchains to interact with another. The cross-chain gateway works like a chain on its own. However, while cross-chain technology allows blockchains to interact with each other and enables the transfer of values without the help of intermediaries, it does not, per se, address potential areas of conflicts that may arise from the interoperability. For a non-exhaustive overview of these challenges, see Table 6 below.

Table 6: Interoperability between blockchains and governance challenges

Areas of potential conflicts	Background	Challenges to be addressed
Dispute resolution	Blockchains may provide their own on-chain dispute resolution mechanisms or they may have explicitly moved dispute resolution off-chain, for example to arbitration or courts.	Which resolution mechanism prevails in case of disputes that occur at the intersection of two blockchains?
Auditing	One Blockchain may store transaction data visible to all participants while the other Blockchain only reveals a minimum of such data. Such a situation may occur in cases where private interoperate with public blockchains	Is a full auditing of transactions across chains possible?
Compliance	Blockchain-based application systems can be used to follow state and federal regulations, such as data privacy laws or KYC/AML provisions.	How is compliance ensured across blockchains?
Decision rights	Decision rights cover management rights that allow to create proposals (for example to improve network operations); they also cover the right to execute decisions.	What happens in cases where the executed decision on one blockchain affects operations on another blockchain?

Source: own overview by author

Governance challenges appear in various forms. Different conflicts call for different response mechanisms.[69] On-chain (see Chapter 3.3) and off-chain instruments (see Chapter 3.4.3) provide a broad spectrum of options to address conflicts and disputes that may occur during the interaction of different blockchains. Since it is almost impossible to anticipate all possible areas of conflicts and disputes, it is important to set up a dedicated governance framework that manages the processes by which disputes among parties are properly settled.

[69] An overview of dispute resolution mechanisms provides Alhabib, Abdulhakim et al. 2020.

Use case: KfW's TruBudget Platform

TruBudget is an open-source tool developed by the German development bank KfW that records the steps of a workflow in a permissioned blockchain (Multichain). The tool improves transparency of information between donors, fund managers and project implementers, using a "logbook" approach. For example, a government ministry can define the budget and the specific executing body can define the workflow, but there can also be built-in checks where donors have the right to approve certain steps before they can be enacted. To summarise, TruBudget serves as a project management platform that allows public investments to be carried out in a transparent and secure manner. But how do governance aspects relate to activities under Trubudget?

Governance related to the national level

With TruBudget, users can enhance compliance with domestic regulation relevant to their field of activities by leveraging the recording of information and related workflows. These activities differ by use case. In Brazil, for example, TruBudget is used by the Brazilian Development Bank BNDES to manage the Amazon Fund.[70] In Burkina Faso, the software assists the Ministry of Finance in improving data quality concerning donor funding which leads to a more effective budgeting.

A common challenge relevant to all use cases is the role of national regulations on data privacy.[71] TruBudget reflects these requirements by applying corresponding data principles. For example, instead of personal names, the software asks users to provide specific usernames which can be stored immutably on the blockchain. Documents relevant for the implementation of projects are stored off-chain while only the corresponding hash value of that document is stored on-chain.

The TruBudget blockchain is generally used to record basic information and underlying workflows. This information may differ depending on the administrative type of project. While a tender process would record procedures and events on-chain, a construction project would record data on finance transferred, corresponding confirmations and other related transactions.

Governance related to the international level

TruBudget serves as a tool to manage the collaboration of different stakeholders during the implementation of all kinds of projects. It is not

[70]For a description of how the Brazilian Development Bank (BNDES) is using TruBudget, see Ondera, Marcio 2019.
[71] For example, the EU's General Data Protection Regulation, GDPR which applies in all 27 member states establishes in its Art. 17 the right to be forgotten (e.g., in social media accounts).

intended to be a tool for implementing international agreements; it rather complements them.

TruBudget can lower transaction costs that arise from cumbersome project coordination and control efforts. As a result, official development assistance (ODA) becomes more targeted and measures are taken more effectively. This, in return, is in line with the goals of the Paris Declaration on Aid Effectiveness. In addition, ODA is important in supporting countries that need it to implement the obligations under the Paris Agreement on climate change (Article 9). Therefore, even if TruBudget is not guided by binding international provisions, it does contribute to the goals of international objectives as laid out by the Paris Declaration on Aid Effectiveness. This can help to convince governments to use transparency tools such as TruBudget.

Governance related to the blockchain level

On-chain Governance:

The TruBudget platform helps users to establish private blockchains to organise financial transactions. Since TruBudget is based on an open-source architecture, everyone can use it.[72] Once TruBudget is used to manage a concrete collaboration, it operates as a permissioned blockchain that is only accessible to trusted partners of such collaboration. The rights to participate are managed by a governing body of the collaboration, primarily the government of the country where the collaborative project is implemented. Validation of transactions happens through pre-selected nodes in the network. The consensus mechanism operates on the Round Robin algorithm wherein multiple nodes validate and vote for transactions. A block is added to the chain when a two-thirds majority of validators have signed and broadcasted confirmations for that block. The algorithm operates with high speed and immediate finality. Its setup reflects the joint business interests of the network participants.

Protocol changes are currently executed through the open-source channels of TruBudget, more precisely, Multichain. Because TruBudget has not been hard forked, it is still part of the open-source community of Multichain. This situation comes with pros and cons. As long as TruBudget remains part of the open-source community,[73] it will enjoy the high security standards as well as a continuous improvement of network features. However, the influence of TruBudget users on protocol changes is limited.

Decisions of users within a closed TruBudget collaboration to ignore a protocol update could lead to a hard fork of the network. This would mean that the collaboration group would leave the (block)chain originally managed by the Multichain community. From this point on, the group can design its own features and services. However, this “freedom” comes with a

[72] TruBudget is therefore not “owned” by KfW. The German Development Bank only owns the name and provides corresponding training and capacity building.
[73] The community status is maintained by integrating protocol updates provided by the community of developers.

price: the group would have to bear the workload of maintaining the chain's security and developing its features further.

It is possible that participants of a sector specific TruBudget application may decide to hard fork from the underlying Multichain blockchain, for example to implement national or international governance requirements. This has not yet happened, but such developments could occur in the future. If this occurs, it could make sense to think about a TruBudget Community that would support the new chain. So far, TruBudget has not had the resources necessary to build such a community, however such a community could be supported by a foundation operating with a broader scope that is more based on certain principles and remaining technology neutral. Concrete direction will depend on the political will and financial capabilities of the parties involved at the time this becomes relevant.

Technical interfaces and interoperability of TruBudget:

TruBudget interacts with various actors, such as governmental institutions, implementing agencies, construction companies and local banks. All these participants have their own procurement and accounting systems. To ensure efficient and secure data interoperability with non-blockchain parts of the network, the software provides a web-based interface as well as the relatively easy API gateway of Multichain. It also connects to SAP's Enterprise Resource Planning (ERP) software.

TruBudget does not offer smart contracts that would run automatically once an event triggers its execution. Usually, such events would originate from off-chain sources. Due to the absence of smart contracts, the secure use of off-chain data sources (e.g., external oracles, IoT devices) can be left to the users. In order to ensure the accountability of data origins, TruBudget works with a credential management system. A login is necessary to ensure that data uploads are linked to a specific network identification. Transparency and the immutability within the network guarantee that the group of participants controls the quality of the data.

Concluding Remarks on TruBudget Governance

TruBudget is a tool aimed at improving project transparency. Tools like TruBudget also have the capacity to provide transparent stakeholder consultation. This is especially relevant in cases where project participants need to prove compliance with environmental or social standards.

Recipient countries do not always appreciate increasing the transparency of decision-making processes with direct budget implications. This especially true for areas with weak governance structures. Donor countries can pressure counterparts and insist on using tools such as TruBudget as a mandatory condition of implementation, however, that is usually not attractive due to the need for long-term collaboration with these counterparts. Current strategies to convince partner countries include identifying local champions in relevant government agencies.

4. Governance challenges at the national level: Regulatory framework for blockchain-based projects for climate action

Projects using blockchain for climate action need to comply with existing laws. However, blockchain is a disruptive technology with characteristics that raise difficult legal questions. In addition, some existing national laws need to be adapted in order to better enable blockchain applications for climate action. The following chapter discusses national regulations on blockchain and climate action, ultimately elaborating on the different legal challenges related to blockchains.

4.1 National regulations

4.1.1 National blockchain and climate change laws

National regulations and oversight of markets can facilitate or hinder the use of blockchain. Most countries apply a "technology-neutral" approach to laws and regulations, and, as a result, have been reluctant to adopt blockchain-specific laws. Their focus has rather been on ensuring existing laws and regulations still work when faced with new possibilities and technologies such as blockchain. As a result, most countries have focused on analysing the activities and ensuring existing regulations of those activities sufficiently deal with new methods and possibilities offered by new technologies.

Some countries have adopted blockchain-specific legislation[74] (e.g., Liechtenstein), made blockchain specific changes to the existing financial market and other laws (e.g., Switzerland) or simply tweaked existing laws to ensure legal certainty when carrying out a particular task using a blockchain (e.g., Luxembourg).

Where blockchain applications are used to improve existing processes, current legislation often suffices.[75] Nonetheless, some existing laws might still pose problems, e.g., when they require paper documents. Highly disruptive projects are more difficult to fit clearly into current legislative frameworks, particularly those which change the underpinnings of centralised institutional infrastructure.

In regard to climate action, blockchain applications tracking agricultural goods from the field to the customer are often viewed as interesting projects that improve existing processes. Not only can such an application help significantly reduce the time and effort for tracking goods along supply chains, in the example of Walmart mango tracking decreased from 7 days to 2.2 seconds,[76] such applications could be used to help track carbon emissions caused by consumption.

In other sectors relevant for climate action, such as housing, blockchain can be a promising application for smart homes, helping to reduce energy consumption or stabilise electricity networks with renewable energy sources. Current legislation often suffices, although more guidance via consistent communications of legal interpretations is required to allow for improved understanding among practitioners

[74] International Finance Corporation, World Bank Group 2018.
[75] International Finance Corporation, World Bank Group 2018.
[76] Hyperledger: Case Study on Walmart.

on how existing laws and regulations can and should be applied in the context of blockchain applications.

The energy sector is an important area of climate action. In many countries, energy transitions are only at the beginning stages, with national grid infrastructure as well as energy sector regulations still designed for a system of centralised infrastructure based around large power producers. These older grid infrastructures and regulations are not well suited to newer concepts of decentralised power generation and peer-to-peer electricity markets of "prosumers". Prosumers both produce and consume energy, e.g., by having solar panels on their roof that produce energy that can be used by both themselves and fed into the grid for others. Highly disruptive projects such as this require changes to traditional grids and legislation. For example, since 2019, Portugal allows direct exchange between two or more prosumers and the development of micro-grids as well as various collective self-consumption business models.[77]

4.1.2 Experimentation via "sandboxes"

Another promising way to incentivise testing of blockchain projects for climate action is to allow for regulatory "sandboxes" to enable experimentation within a supervised environment and trusted business partners. Although there are differences across jurisdictions, sandboxes typically have the following features[78]:

- Case by case rules for each project or sector, waivers or modifications to existing rules
- Limitations on the number of customers/clients and time period
- Safeguards for consumer protection (e.g., requirement to obtain informed consent)
- Restricted authorisation/licensing
- No enforcement action letters

Regulatory sandboxes have been in use in different countries since 2016.[79] For example, there is a Dutch sandbox program with the goal of increasing the production of sustainable and decentralised electricity. It explicitly provides for the relaxation of certain regulatory framework conditions from the electricity generation and use. These include deviations in the structure and level of grid charges and tariff rules or allowing a company to build and operate its own low-voltage grid in a new neighborhood.[80] Several developing countries such as Mauritius, Sierra Leone, Mozambique or Malaysia have also used sandbox approaches, so far primarily focused on fintech applications.[81]

Because blockchain is still a rather new technology, an active exchange between projects and leaders from academia, civil society, business and governments is necessary to inform dialogue on blockchain applications.[82] Informed dialogue is an important step to achieve understanding of the technology, the interpretation of

[77] Campos et al. 2020.
[78] Agarwal, Khushboo 2018.
[79] World Bank Group 2020.
[80] Swiss Federal Office for Energy 2020.
[81] World Bank Group 2020.
[82] CLI 2020.

existing laws to blockchain applications as well as necessary modifications to existing laws or the introduction of new laws.

The advantages of sandbox experimentation must however be weighed against the anti-competitive aspects of a sandbox. By their nature, sandboxes advantage certain selected actors by allowing them to provide products or services on conditions which are not generally available to other market entrants or even incumbents who are not exempt from regulations.

4.1.3 Legal coordination across borders

On the international scale, there are very different laws and regulations across different countries. Many blockchain platforms and projects are being operated across countries. "Legal interoperability" across borders would be desirable due to the cross-border nature of blockchain infrastructure. Guidelines and codes of conduct are necessary to help with greater coherence and overcome inevitable differences that exist across jurisdictions.[83]

4.2 Legal challenges related to blockchains

4.2.1 Applicable laws in cases of conflicts

It is recommended to include choice of law, arbitration/dispute resolution and choice of forum clauses in agreements. However, not every possible litigant will have signed a contract, let alone one with such clauses. For these cases, *private international law*, also called *conflict of laws*, determines which law to apply in case of disputes that touch multiple jurisdictions. This can be challenging when transactions touch different countries, with nodes operating in further countries by parties located in different countries and blockchain governance located at another place entirely. This may result in multiple legal systems making a valid claim to have jurisdiction.

Even with these clauses in place, some mandatory laws cannot be waived by contract. This is particularly true for criminal law and most regulatory frameworks. In order to become de facto standards, some regulations have an intentionally broad reach, such as the General Data Protection Regulation *GDPR* of the European Union or financial regulation of the US. As the GDPR has developed into an international benchmark, the discussion of data protection laws (see Chapter 4.2.6) will focus on the GDPR.

4.2.2 Blockchain-based entries as legal evidence

Blockchain technology can be used to store and/or verify reporting (1.2), for registries and tracking (1.3, 2.6) as well as climate finance (1.4). In all three scenarios, some basic questions need to be answered:

a) Is an entry accurate?

b) Is an entry unique?

c) By whom or by which device has it been created? Is this person or device authorised to do so?

d) Is a climate credit used multiple times (double spending)?

e) Is it final – protected against manipulation?

[83] CLI 2020.

Blockchain technology provides a high level of immutability. Entries on a blockchain might be altered in the context of governance actions or forks only in very limited cases. This high degree of immutability warrants the above points (d) and (e). However, Blockchain can only provide very limited guarantees regarding the accuracy (a) of an entry. Usually, only the time of the reporting can be verified and a public/private key-pair can be identified as a source (c). However, it cannot typically be verified whether this key has been used by the authorised person or device. Blockchain can provide solid protection against double spending of tokens (d), which has been proven by the very first blockchain, Bitcoin. Blockchain can also be used to create transparency to detect double reporting (b), for example when one or more entities report the same emission reduction multiple times.

Because blockchain governance can, in some rare case, alter entries on blockchain, it does not provide perfect finality of transactions (e).This leads to two legal questions:

- Will an entry be recognised as evidence in front of a court?
- What legal remedies exist if an entry is not accurate or authentic and there is no blockchain governance procedure available to rectify it? On the other hand, what legal remedies exist if blockchain governance has altered entries that should not have been altered?

The evidence accepted by a court, as well as the appropriate procedures for presenting and verifying this evidence, depend on the jurisdiction. Expert witnesses might be asked to testify regarding a blockchain entry. Some countries (e.g., Italy) have passed laws to facilitate electronic evidence, while others (e.g., the UK) have pilot projects and numerous courts have accepted electronic evidence that can be verified through blockchain technology[84]. The

United Nations Commission On International Trade Law (UNCITRAL) Model Law on Electronic Transferable Records[85] was adopted in 2017 but countries have been slow regarding its implementation.

4.2.3 Validity of electronic signatures

When a blockchain entry has been signed by a natural person, it can also be regarded as an *electronic signature*. Although an UNCITRAL Model Law on Electronic Signatures[86] was passed 20 years ago, the validity of electronic signatures is still limited to specific jurisdictions[87]. According to Art. 25 of the eIDAS regulation[88] of the European Union, for example, a *qualified electronic signature* has the equivalent legal effect as a handwritten signature. However, this regulation only recognises foreign qualified *electronic signatures* from countries in the European Economic Area (EEA)[89] as there are not yet any mutual recognition agreements between the EU and other countries. Even qualified *electronic signatures* from Switzerland that are based on the Swiss ZertES law[90] are currently not fully recognised under the eIDAS regulation. The eIDAS regulation distinguishes between different types of *electronic signatures*:

[84] Pollaco, Alexia 2020.
[85] UNCITRAL 2017.
[86] UNCITRAL 2001.
[87] Heidel, Thomas et al. 2021.
[88] eIDAS
[89] See https://esignature.ec.europa.eu/efda/home/#/screen/home for a list of certified trust service providers.
[90] ZertES

- An *electronic signature* that solely indicates the name of the person that has signed a document.
- An *advanced electronic signature* that is linked to something under the sole control of the signatory and a mechanism that is able to detect subsequent changes in the data. This can already serve as proof of the signing.
- A *qualified electronic signature* that is based on a *qualified certificate* that has been issued by a *qualified trust service provider* and meets special requirements. Only *qualified electronic signature*s have the equivalent legal effect of handwritten signatures.

Because most signed blockchain transactions do not qualify as qualified electronic signatures, they do not have the legal effect of a handwritten signature. However, they might qualify as advanced *electronic signature*s and can usually still be recognised as evidence. This issue often relates to legal certainty and the weight of proof, including the ability to assume binding and ability to question the signature. It is worth noting that it is also possible to implement *qualified electronic signatures* on a blockchain[91].

4.2.4 Blockchain-based assets and registries

Initial Coin Offerings introduced blockchain tokens that represent all kinds of assets, including climate-related tokens[92]. After a series of Initial Coin Offerings (ICOs) in the years 2017-2019 that were mostly unaffected by regulation, financial regulators have tightened the application of financial regulation on the issuance and trading of tokens. Some countries also introduced laws that regulate the issuance and transfer of assets based on electronic registries on a blockchain; examples include Liechtenstein[93], Switzerland[94] and to some extent Germany[95]. While the mere blockchain-based documentation of carbon emission reductions and carbon sequestrations should not be viewed as uncertificated securities, the tokenisation of those certificates might, under some circumstances, be regarded as securities resulting in the possible application of financial regulations. The EU is currently preparing a new Market in Crypto Assets Regulation (MiCA) to regulate crypto assets[96].

4.2.5 Smart contracts and their legal status

The term Smart Contract was initially coined by Nick Szabo[97] and Vitalik Buterin[98] and is currently used to mean a number of different aspects, typically including one or more of the following:

a) The conclusion of a legal contract by executing computer program code, especially code being executed by a blockchain.

[91] LuxTrust 2018; Bärtschi, Harald 2019.
[92] See for example tokens offered by climatetrade (www.climatetrade.com) or Veridium (www.veridium.io) or Power Ledger (www.powerledger.io) or the D-RECs initiative (www.d-recs.energy/)
[93] Liechtenstein Blockchain Act.
[94] Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register.
[95]Gesetz zur Einführung elektronischer Wertpapiere
[96] Market in Crypto-Assets Regulation.
[97] Szabo, Nick 1997.
[98] Buterin, Vitalik 2013.

b) The execution of a legal contract by executing computer program code, especially code being executed by a blockchain.

c) The technology of programs/scripts that are being executed by a programmable blockchain and execute transactions.[99]

The third definition, smart contract technology (c), is used for most blockchain use-cases. A standardised blockchain is used to program specialised transactions, assets, proofs etc. Smart contracts can authenticate actors through their private keys. They can store hash-values as a fingerprint of digital objects to timestamp and sign those objects. Smart contracts can help trace supply chains and make sure that no step can be undone, removed from the documentation or added later-on. Finally, smart contracts are used to create and define the parameters of tokens. Using the Solidity Smart Contract Language for Ethereum, for example, it only takes very few pages of code to define a new token together with the rules for the transactions. Those rules might set conditions that transactions need to meet in order to be executed. For example, transactions could be limited to a specific time interval, to specific parties or could require validation by third parties. These rules are programmed into the smart contract which will automatically enforce them.

When smart contract technology is used to conclude or execute legal contracts (cases (a) and (b) above), there is typically no 1:1 relation between a smart contract program and a legal contract. A legal contract might need a series of smart contract programs to be executed, or a smart contract program can be used to conclude or execute many legal contracts. Often the author of a smart contract program is not a party to the legal contracts concluded or executed by the smart contract program. Calling a computer program a "smart contract" has led to confusion and Buterin has since apologised for it[100].

Often smart contracts are used to execute contractual obligations. Using a blockchain has the advantage that the code can be transparent and that its execution cannot be (easily) manipulated by either contracting party. The smart contract takes the role of a neutral trustee. Smart contract programs might also be used to conclude legal contracts in very specific situations as most contracts entered into do not depend on a specific form or language. For example, a gesture at the bakery may be sufficient to enter into a contract for buying a bagel. Most jurisdictions allow contracts to be written in any language that is understood by the contracting parties. Therefore, it should be possible to conclude a contract using a smart contract coding language like Solidity.

However, smart contract code is not identical to a legal contract. A legal contract is an abstract legal instrument. Even a paper contract is not identical to the legal contract that it represents. Clauses that contradict binding law might be void. Errors can usually be corrected based on the legal principle of *falsa demonstratio non nocet*.[101] The legal interpretation of a paper contract does not necessarily follow it word-by-word, and the legal interpretation of smart contract code can differ from its automatic execution.

Transactions by a blockchain-based smart contract are intended to be final, unless blockchain governance is able to reverse them. This, however, is not a new feature in contracts as many contractual obligations cannot be reversed or executed at a later

[99] ITU, A.7.
[100] Buterin, Vitalik 2013.
[101] Latin: a false description does not vitiate

stage. If a frozen wedding cake is delivered to the wrong address, for example, it might not be possible to take it back nor to deliver a new one to the correct address in time. Contract law offers damages to compensate for the lack of proper execution of a contract. Some blockchain environments, like EOS, offer on-chain or off-chain dispute resolution to deal with a contract that is not executed according to its legal interpretation as part of its blockchain governance.

Although legal contracts can in principle be concluded via smart contracts, there are some aspects that advise caution. Not all contract types can be concluded using a programming language, e.g., contracts regarding real estate often require a special form or procedure in front of a notary, consumer contracts may require specific language that might be difficult to meet using code. Even when it is legally possible, usually only the operationalisable clauses can be expressed more efficiently in program code. Moreover, only those parts of a legal contract that become more precise when expressed in program code should be expressed in program code. Finally, the main purpose of a documented contract is to ensure clarity of the understanding between parties (and win a legal dispute about this if one arises). Parties to a contract, as well as judges, currently understand legal writing better than program code. Therefore, it is advisable to have a basic legal contract in standard legal language as a master agreement that clearly defines the purpose and the scope of the coded smart contracts concluded on-chain.

4.2.6 Ensuring data protection

Data protection refers to the processing of personal data. In many cases, the General Data Protection Regulation of the European Union (*GDPR*)[102] is applicable, even when the data processing takes place outside the EEA. This depends on multiple factors - e.g., where the controller or processor is located or if it involves the processing of data of persons in the EU in the context of offering services or monitoring their behavior. The application of the GDPR, however, does not depend on where the processing is done. The GDPR is applicable in many situations where data is processed outside the EU.

The GDPR defines personal data as any information relating to an identified or identifiable natural person. This definition is very broad and includes data that can only be indirectly identified with a natural person like an IP address or a public blockchain address as long as those refer to a natural person. Therefore, even transactions or reports that are not directly related to a natural person might still be considered personal data. When personal data is being processed, there are four main potential conflicts with GDPR:

a) Information stored on a blockchain is close to being immutable. However, data protection laws include the right to be forgotten and obligations to erase personal data where there is no longer a justification to continue storing this data.

b) Data protection laws require accountability for the processing of personal data. In distributed data processing where there is a limited influence from numerous actors, the identification of accountable actors is very complex.

c) GDPR also regulates when natural persons are subject to automated decision making. It is not yet settled as to what extent this affects smart contracts or even simple blockchain transactions[103].

[102] GDPR.
[103] Finck, Michèle 2019; Erbguth, Jörn 2019a; David, Klaus et al. 2019.

d) Most blockchains have nodes in several countries (including countries outside the EEA). Transfer of personal data to these "third countries" is heavily regulated.

Legal literature regarding blockchain and GDPR consists of a diverse range of views according to numerous sources including a report from the European Blockchain Observatory and Forum[104], a European Parliament Research Service report[105] and several journal articles[106]. The European Data Protection Board announced blockchain as a possible topic for 2019/2020[107], but has not yet published a statement. The French data protection authority CNIL published a statement in 2018[108] regarding GDPR and blockchains. A particularly interesting point relates to the identification of controllers of blockchain transactions.

While data protection often relies on proper manual enforcement of rules, GDPR also includes a provision for data protection by design that protects personal data by technical means, e.g., pseudonymisation, data minimisation or encryption. DIN SPEC 4997[109] is a technical specification of the German standards organisation DIN that shows ways to use privacy enhancing technology to enhance privacy protection by proper design of systems using blockchain technology. While, for example, Bitcoin is public and only provides some degree of pseudonymity, privacy coins like Zcash or Monero offer a much higher degree of privacy protection. However, there is still a lack of legal certainty around basic questions regarding technology and privacy: For example, when is a hash-value of personal data considered to also be personal data?[110]

There are different ways to deal with GDPR compliance. However, none of these ways completely avoid legal uncertainty:

- Avoid processing of personal data (on-chain and off-chain). If no personal data is processed, GDPR does not apply. However, the definition of personal data is very broad. Removing names does not render data anonymous, but only pseudonymous. GDPR is applicable on pseudonymous data like IP addresses or blockchain public keys when they reference natural persons. It is necessary to be particularly prudent with so-called *special categories of personal data* which are considered sensitive and enjoy a higher level of data. This includes, for example, data concerning health, a natural person's sex life, data revealing racial or ethnic origin and biometric data, for example, identifiers calculated from fingerprints (2.4).

- Use privacy enhancing technology, such as described in DIN SPEC 4997. The simplest approach is to process personal data only off-chain as described in 3.5.2, for example. Off-chain data can be deleted and does not have to be shared with all nodes. Only timestamps, signatures or certificates will be stored on-chain. It depends on the use-case if this is a possible system design. Depending on the system design, even hash-values of personal data might be considered personal data in specific circumstances. A detailed analysis is therefore required to determine if the hash values on-chain are considered personal data.

[104] EU Blockchain Observatory & Forum 2018.
[105] European Parliamentary Research Service, Scientific Foresight Unit (STOA) 2019.
[106] See for example: Erbguth, Jörn 2019b.
[107] EDPB 2019.
[108] CNIL 2018.
[109] Beuth 2020.
[110] Finck, Michèle et al 2019; Erbguth, Jörn 2019c.

- If processing of personal data on a blockchain is unavoidable for the use-case, it should be based on a permanent justification. GDPR authorises the processing of personal data in many cases; the best-known is consent. However, consent can always be withdrawn and therefore processing on blockchains should not be based on consent. Contracts and legal obligations are other bases that cannot be withdrawn. For example, payment with Bitcoin often involves processing of personal data but can be permanently justified by an underlying contract. A legal obligation to publish information can also be justification to make it permanently available on a blockchain.

The entity determining the purpose and means of the processing of personal data is called the *controller*. The controller is responsible for GDPR-compliance. In case of GDPR-violations, the controller can be fined up to 20 million € or 4% of worldwide annual turnover (whichever is higher). The French CNIL differentiates between use-cases to consider who can be considered a controller in distributed blockchain systems. Depending on the type of blockchain, this could be the party that signs and publishes a transaction, the members of a consortium or even the smart contract developer that can influence the processing by updating the smart contract code. When permissioned blockchains are used, it is advised to have a consortium legal entity to remove some liability from the consortium members.

Smart contracts and even basic blockchain transactions involve simple automated and autonomous decisions. GDPR, however, limits the ability to base decisions solely on automated processing. Even when permitted, Art. 22 of the GDPR requires inclusion of at least the right to obtain human intervention. It is still unclear whether the application of simple rules from smart contracts will already be considered a decision.[111] Dispute resolution mechanisms that are able to remedy smart contract executions that do not comply with the law are recommended.

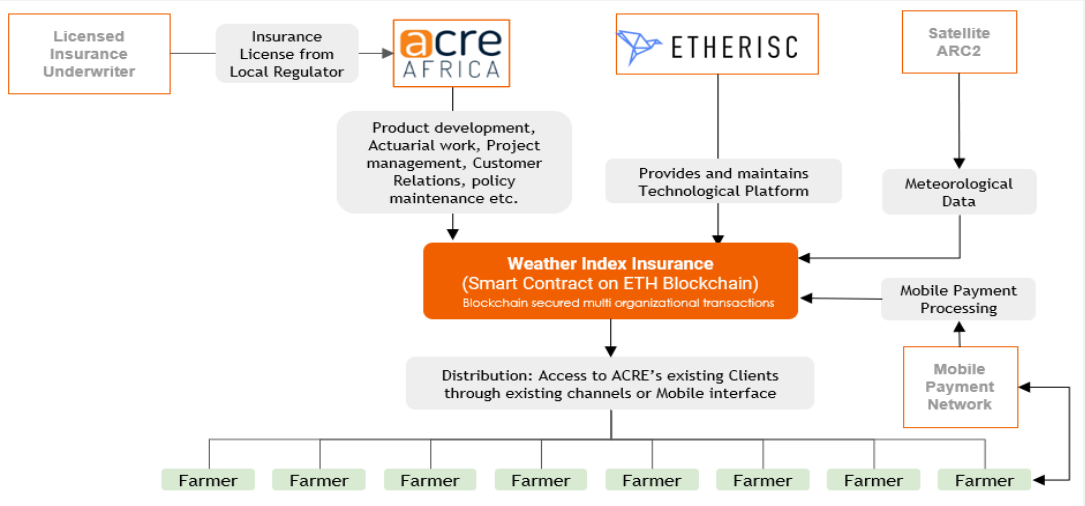
When nodes are in third countries with no valid adequacy decision of the EU Commission (such as the USA), processing involves additional barriers. A public blockchain might be privileged, since the European Court of Justice suggested in Lindqvist[112] that published data readable anywhere should not be subject to the limitations of third country rules. Otherwise, given the implications of the ruling of the European Court of Justice in *Schrems II*[113], there are only limited situations where the transfer could be based on explicit consent or on a contract that requires this data to be transferred.

If the processing of personal data is justified, GDPR still imposes many obligations like informing data subjects, making a list of all processing activities, entering into a contract with data processors and in some cases performing a *data processing impact analysis* (DPIA).

[111] Finck Michèle 2019; Jörn Erbguth 2019a.
[112] European Court of Justice 2020.
[113] European Court of Justice 2003.

Use case: Etherisc weather insurance in Kenya

Figure 7: System and relevant actors of the Etherisc Weather Index Insurance in Kenya



Source: Etherisc

Accessible and affordable crop insurance is crucial for smallholder farmers to protect their livelihoods and increase their resilience to the effects of climate change. Unfortunately, traditional insurance is not able to provide sufficient protection. In Sub-Saharan Africa, only three percent of smallholder farmers have access to agricultural insurance.[114] Insurance can be expensive, and there is little trust in traditional insurers due to histories of delayed or even absent pay-outs.

With the support of blockchain giants Chainlink and the Ethereum Foundation, Etherisc and Acre Africa launched a project in Kenya in October 2020. The purpose of the project is to make climate risk insurance cheaper, faster and more transparent, based on blockchain technology. Etherisc provides its blockchain platform, the "Generic Insurance Framework" or GIF, as a solution to automate an existing insurance product by ACRE Africa, which is distributed in cooperation with village-based agents and farm input suppliers, through scratch cards and a USSD telecommunication service. When planting seeds, the farmer can register the code using the SMS/USSD function on their feature phone to provide necessary personal and agricultural information. The basic insurance premium is prepaid, included in the price of the seeds. Top-up payments can be made through M-PESA to increase the cover.

Once the insurance smart contract is active, it will autonomously track the weather data relevant to the farmer's policy. Such data is sourced from satellite weather data "oracles" in real time. The smart contract can automatically execute the pay-out through an API connecting to the mobile

[114] Climate Policy Initiative and IFAD 2020; ISF 2018.

payment network as soon as the agreed conditions for drought or flood are met as defined in the farmer's respective policy. Such instant payments solve an existential cash-flow problem that farmers have with the delays between their claim and the insurance pay-out. The solution has the potential to achieve premium reductions of up to 30% and to reduce claim cycles from 3 months to 1 week.[115] The pay-outs are done through M-PESA directly to the farmer's mobile phone.

Governance related to the international level

The project is particularly aligned with the Paris Agreement's goal to increase "the ability to adapt to the adverse impacts of climate change and foster climate resilience" (Article 2). Weather index insurance can directly enhance the adaptive capacity of smallholder communities, strengthen their resilience and reduce their vulnerability to climate change (see Article 7). The project can contribute to the Paris Agreements aim of enhancing climate finance flows from a wide variety of sources, instruments and channels (Article 9, see Section 1.4).

With over 50% of the global annual food production coming from smallholder farmers,[116] many of whom live in regions most affected by climate change, improving the uptake of agricultural insurance by this group makes an important contribution in terms of improving food security and avoiding farmers falling in poverty. The main purpose of the project in Kenya is to prove that blockchain technology has the potential to solve the problems that have so far prevented uptake of climate risk insurance at a massive scale. With a successful proof of scale in Kenya this new, innovative insurance solution could be made available globally.

Governance related to the blockchain level

Etherisc's Generic Insurance Framework (GIF) is an open-source framework to develop and operate blockchain-based insurance products. It consists of a system of smart contracts running on the Ethereum blockchain and a system of microservices running in a kubernetes container. The basic idea behind the GIF is to abstract the generic parts shared across multiple different insurance products and leave only product-specific parts, such as risk model, pricing and pay-out configurations, to be adjusted. In its core, the GIF accumulates a number of components: core smart contracts, core microservices, product-specific smart contracts and product-specific microservices. Essentially, the GIF consists of two major layers for smart contracts and utility.

The smart contracts layer reflects the information and mechanisms relevant purely to the lifecycle of the actual insurance product. All steps from premium collection, policy issuance and claims payment are managed through smart contracts and safely stored on blockchain.

[115] See study by Global Innovation Lab for Climate Finance 2019.
[116] IFAD and UNEP 2013.

The utility layer allows for other applications (and humans if need be) to share, communicate and work with the information from the smart contract layer, similar to back-office functions of an insurance company. This includes, for example, statistical monitoring of weather events triggered by contracts, making e-mail or instant messenger notifications, accepting fiat payments for policies as well as making fiat pay-outs.

The smart contracts layer is designed in a way that any insurance product built on top of the GIF can be easily implemented into any network supporting the Ethereum Virtual Machine. The utility layer can contain any number of off-chain utility services supplementing on-chain functionality.

Governance related to the national level

Building on lessons learned in a first small-scale pilot together with AON, Oxfam and Sanasa in Sri Lanka in 2019, the team of Etherisc Impact B.V. regards Kenya as an ideal market to roll out blockchain-based climate risk insurance at a larger scale due to its well-developed insurance market, widespread use of mobile payments, forward-looking regulator and strong existing partnerships on the ground. For the project, ACRE and Etherisc have selected one of ACRE Africa's existing insurance products which has been offered in the market successfully for several seasons with approval from the Kenyan regulator.

ACRE is in discussions with the Kenyan regulator to join the regulatory sandbox program. The sandbox is intended to drive innovation in the insurance sector by allowing new products and services based on novel technologies to be tested in the local market under scrutiny and guidance of the regulator. A successful completion of the program may result in a permission to operate in the market under lighter-touch requirements with further potential for additional cost savings.

Concluding remarks

Etherisc's project in Kenya aims to provide smallholder farmers with access to affordable crop insurance to increase their resilience to the effects of climate change. The blockchain-based solution brings premiums down to an affordable level. It helps to eliminate asymmetric access to information and increases transparency. The automated payments increase speed of transactions, lower operational costs and avoid conflicts of interests for the insurer. This helps to build trust that claims will be paid when farmers need them most urgently.

Once the technology has undergone its proof of scale with a target of 250,000 farmers in Kenya, Etherisc is planning to build on the experience to help improve agricultural insurance in other non-OECD countries around the globe. Conducive environments for blockchain-based solutions to climate risk insurances are a supportive legal and regulatory environment for blockchain technology, availability of microinsurance, a high adoption rate of mobile money and public support.

5. Conclusions

The aim of this report was to provide an overview of the most relevant governance challenges facing blockchain-based climate action. This ranges from the appropriate technical design of such systems to compliance with legal regulation. However, the publication did not attempt to discuss governance issues exhaustively.

While blockchain works without a central authority, this does not mean there is an absence of governance. Governance is defined as an allocation of power, risks and responsibilities and thus is also key to blockchain-based climate actions. Different governance challenges have to be carefully addressed in order to build trust and create confidence in the technology and particularly its usage for climate action.

Governance challenges have been structured along three different levels: the international, national and blockchain level. While the focus of the first two levels is on complying with existing national and international laws, the latter is about actively defining rules that will then be automatically enforced. Three use cases in the publication provide insights into how the governance issues have been addressed in practice.

Governance at the international level: Blockchain fits well with the decentralised structure of the Paris Agreement. The UN Climate Change Secretariat has recognised the role that blockchains could play in the implementation of the Paris Agreement. This report specifically identifies the implementation of provisions related to MRV, decentralised market mechanisms and enhancing finance and clean energy as suitable to be supported through blockchain-based projects. Non-party stakeholders, such as local governments, companies or NGOs already play an important role in the implementation of the Paris Agreement and more generally in climate action. This is recognised by the "Non-State Actor Zone for Climate Action" established in conjunction with the Paris Agreement.

Governance at the blockchain level: While simple sounding, it should first be well considered if blockchain is the right technology for the project or if a centralised database would suffice. Similar to any other large IT project, to guarantee proper functioning of a blockchain project, it is then important to establish the management and governance, including, for example, setting up a legal entity and deciding on the day-to-day project oversight and management.

The active definition of on-chain governance plays a significant role in determining who maintains power and responsibilities. This begins with the decision of having a private or public permissioned or permissionless blockchain, the choice of consensus mechanism and how the blockchain interacts with other blockchains and more broadly the outside world. The choice of the proper participation mode and governance structure strictly depends on the use-case characteristics.

In the context of climate action, the energy consumption of consensus mechanism is of particular interest. The report shows that there are possibilities to balance energy consumption with node scalability, throughput and latency, depending on the project.

Another issue of particular interest in the climate action context is the technical interoperability, i.e., using data from the outside world. While data from the outside

world can be manipulated, there are options to overcome this such as using cryptography, multiple data sources and credential management systems to increase security and credibility. Another challenge in the interoperability context is the interaction between blockchains. Various areas of potential conflicts exist because of different governance solutions between blockchains. Under the current circumstances where there are no industry-wide standards, governance arrangements between blockchains will continue to require solutions on a case-by-case approach.

Governance at the national level: Blockchain projects for climate action need to comply with national regulations. The more disruptive a blockchain application is, the more difficulties it will face in complying with the current legislative framework. This report shows that for climate action, national energy laws are especially a challenge because they are usually designed for a system of centralised infrastructure based around large power producers.

Although legal uncertainty has been decreasing over the past years, many issues remain unsettled as of yet, thus posing an unnecessary risk to innovation. An important way to decrease uncertainty is to ensure consistent communication of legal interpretation, particularly by public authorities. Some countries have also adopted blockchain-specific legislation or made changes to laws. Another possibility can be the adoption of regulatory "sandboxes" that enable experimentation and learning by business and government on blockchain for climate action. Finally, ensuring "legal interoperability" across borders through soft-law instruments such as guidelines and codes of conduct would be desirable, particularly for global projects common in climate action.

This report shows the importance of addressing governance issues from the very beginning of a project on all three levels when using blockchain for climate action. On the one hand, this ensures that perspectives from the blockchain, climate change and legal community are brought together. On the other hand, this allows for the establishment of projects that build trust and create confidence in using blockchain for climate action.

In order to support the growing recognition of the topic of governance, exchange and mutual learning should be encouraged. In addition, it is important to support and study use cases in order to test the application of solutions to governance challenges in practice.

Figures

Figure 1: Important Paris Agreement elements and related information flows 14

Figure 2: Centralised vs. decentralised technology 16

Figure 3: Climate finance flows 17

Figure 4: The Climate Warehouse as publicly accessible meta-data layer within a carbon market ecosystem 20

Figure 5: When to use blockchain, and which type, instead of adopting a traditional database system 27

Figure 6: Consumption level of consensus categories 32

Figure 7: System and relevant actors of the Etherisc Weather Index Insurance in Kenya 50

Tables

Table 1: Examples of climate related services on different blockchain networks 20

Table 2: Three main types of blockchains 24

Table 3: Further classification of permissioned blockchains 25

Table 4: Summary about consensus performance 32

Table 5: Approaches to ensure credible application of oracles 35

Table 6: Interoperability between blockchains and governance challenges 36

Literature

Agarwal, Khushboo 2018: Playing in the Regulatory Sandbox, Blog Post, New York University, Journal of Law & Business, online: https://www.nyujlb.org/single-post/2018/01/08/Playing-in-the-Regulatory-Sandbox [29.01.2021].

Alhabib, Abdulhakim et al. 2020: Bridging the Governance Gap: Dispute resolution for blockchain-based transactions, online: http://www3.weforum.org/docs/WEF_WP_Dispute_Resolution_for_Blockchain_2020.pdf [08.04.2021].

Bärtschi, Harald 2019: First-ever qualified electronic signature for blockchain, News ZHAW of January 28, 2019, online: https://www.zhaw.ch/en/about-us/news/news-releases/news-detail/event-news/first-ever-qualified-electronic-signature-for-blockchain/ [08.04.2021].

Belotti, Marianna et al. 2019: A vademecum on blockchain technologies: When, which, and how, IEEE Communications Surveys & Tutorials 21.4 (2019): 3796-3838.

Beuth 2020: DIN SPEC 4997:2020-04, Privacy by Blockchain Design: Ein standardisiertes Verfahren für die Verarbeitung personenbezogener Daten mittels Blockchain-Technologie, online: https://www.beuth.de/de/technische-regel/din-spec-4997/321277504 [08.04.2021].

Buterin, Vitalik 2013: Ethereum White Paper, online: https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf [08.04.2021].

Buterin, Vitalik 2018: Twitter, October 13, 2018, online: https://twitter.com/VitalikButerin/status/1051160932699770882 [08.04.2021].

Campos et al. 2020: Regulatory challenges and opportunities for collective renewable energy prosumers in the EU, Energy Policy 138, online: https://doi.org/10.1016/j.enpol.2019.111212 [29.01.2021].

CLI 2018: Navigating Blockchain and Climate Action, An Overview, online: https://www.climateledger.org/index.html?cmd=countFile&file=CLI_Report-January19.pdf [04.01.2021].

CLI 2020: Navigating Blockchain and Climate Action, State and Trends, online: https://www.climateledger.org/index.html?cmd=countFile&file=CLI_Report_2020_state-and-trends.pdf [08.04.2021].

Climate Policy Initiative and IFAD 2020: Examining the Climate Finance Gap for Small-Scale Agriculture, online: https://www.ifad.org/documents/38714170/42157470/climate-finance-gap_smallscale_agr.pdf/34b2e25b-7572-b31d-6d0c-d5ea5ea8f96f [18.03.2021].

CNIL 2018: Blockchain and the GDPR, Solutions for a responsible use of the blockchain in the context of personal data, November 6, 2018, online: https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data [08.04.2021].

David, Klaus, Kurt Geihs, Martin Lange, Gerd Stumme 2019: INFORMATIK 2019, 50 Jahre Gesellschaft für Informatik – Informatik für Gesellschaft, Bonn: Gesellschaft für Informatik e.V. (S. 421-434). DOI: 10.18420/inf2019_59

EDPB 2020: Work Program 2019/2020, online: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-02-12plen-2.1edpb_work_program_en.pdf [08.04.2021].

Erbguth, Jörn 2019a: Smart contracts und die DSGVO, GI 2019, 412, online: https://doi.org/10.18420/inf2019_59 [08.04.2021].

Erbguth, Jörn 2019b: Five ways to GDPR-Compliant Use of Blockchains, EDPL 2019, 427, online: https://edpl.lexxion.eu/article/EDPL/2019/3/19 [08.04.2021].

Erbguth, Jörn 2019c: Datenschutzkonforme Verwendung von Hashwerten auf Block-chains, MMR 2019, 654, online: https://beck-onli-ne.beck.de/?vpath=bibdata%2fzeits%2fMMR%2f2019%2fcont%2fMMR%2e2019%2eH10%2egl2%2ehtm [08.04.2021].

EU Blockchain Observatory and Forum 2018: Blockchain and the GDPR, October 16th, 2018: https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf [08.04.2021].

EU Blockchain Observatory and Forum: FAQ, online: https://www.eublockchainforum.eu/faq [3.11.2020].

European Court of Justice 2003: C-101/01 - Lindqvist, November 6, 2003, ECLI:EU:C:2003:596, online: http://curia.europa.eu/juris/liste.jsf?language=en&num=C-101/01 [08.04.2021].

European Court of Justice 2020: C-311/18 - Facebook Ireland and Schrems, July 16, 2020, ECLI:EU:C:2020:559, online: http://curia.europa.eu/juris/liste.jsf?num=C-311/18 [08.04.2021].

European Parliamentary Research Service, Scientific Foresight Unit (STOA) 2019: Block-chain and the General Data Protection Regulation, Can blockchains be squared with European data protection law? PE 634.445, July 2019.

Finck, Michèle 2019: Smart contracts as a form of solely automated processing under the GDPR, International Data Privacy Law, Volume 9, Issue 2, May 2019, Pages 78-94, online: https://doi.org/10.1093/idpl/ipz004 [08.04.2021].

Finck, Michèle and Frank Pallas 2019: The Who Must Not Be Identified - Distinguishing Personal from Non-Personal Data Under the GDPR, Max Planck Institute for Innova-tion & Competition Research Paper No. 19-14, online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3462948 [08.04.2021].

Finck, Michèle 2019: Blockchain and the General Data Protection Regulation, online: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf [08.04.2021].

Global Innovation Lab for Climate Finance 2019: Blockchain Climate Risk Crop Insurance, Lab Instrument Analysis, online:

https://www.climatepolicyinitiative.org/wp-content/uploads/2020/08/Blockchain-Climate-Risk-Crop-Insurance_instrument-analysis.pdf [18.03.2021].

Heidel, Thomas, Hüßtege, Rainer, Mansel, Heinz-Peter, Noack Ulrich 2021: Bürgerliches Gesetzbuch: Allgemeiner Teil, EGBGB, BGB § 126a Rn. 40

Hyperledger: Case Study: How Walmart brought unprecedented transparency to the food supply chain with Hyperledger Fabric, online: https://www.hyperledger.org/learn/publications/walmart-case-study [29.02.2021].

ICAO: Carbon Offsetting and Reduction Scheme for International Aviation (CORSIA), online: https://www.icao.int/environmental-protection/CORSIA/Pages/default.aspx [08.04.2021].

IFAD and UNEP 2013: Smallholders, food security, and the environment, online: https://www.ifad.org/documents/38714170/39135645/smallholders_report.pdf/133e8903-0204-4e7d-a780-bca847933f2e [18.03.2021].

Institute on Governance: What is Governance?, online: https://iog.ca/what-is-governance/ [3.11.2020].

International Finance Corporation, World Bank Group 2018: Blockchain Governance and Regulation as an Enable for Market Creation in Emerging Markets, EM Compass, Note 57, Sept. 2018, online: https://www.ifc.org/wps/wcm/connect/b0c5e494-ae55-4a7b-852c-a574278fb34c/20180921_EMCompass-Note-57-Blockchain-Governance_v1.pdf?MOD=AJPERES&CVID=mnZCoNv [29.01.2021].

ISF 2018: Protecting Growing Prosperity, Agricultural Insurance in the Developing World, report supported by Syngenta Foundation for Sustainable Agriculture, online: https://www.raflearning.org/file/1414/download?token=1i4u5GwD [18.03.2021].

ITU: Focus Group on Distributed Ledger Technology, 2019, Technical Specification FG DLT D1.1, Distributed ledger technology terms and definitions, https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d11.pdf [07.05.2021].

Kohli, Anik 2015: Making Sense of Transparency and Review in the Paris Agreement, Yearbook of international Environmental Law, Vol. 26, No. 1 (2015), pp. 46-67, doi:10.1093/yiel/yvx005.

LuxTrust 2018: Luxembourg based company InTech launches innovative blockchain-based on-line service “EDDITS” for associating strong digital identities with ethereum addresses, in partnership with LuxTrust, Electronic Identity, News of 29 March 2018, online: https://www.luxtrust.com/luxembourg-based-company-intech-launches-innovative-blockchain-based-on-line-service-eddits-for-associating-strong-digital-identities-with-ethereum-addresses-in-partnership-with-lux/ [08.04.2021].

Lyons, Tom and Ludovic Courcelas 2020: Governance of and with Blockchains, a thematic report prepared by the European Union Blockchain Observatory & Forum, online: https://www.eublockchainforum.eu/sites/default/files/reports/report_governance_v1.0_0.pdf [04.01.2021].

Maupin, Julie et al. 2019: Blockchain: A World Without Middlemen, online: https://www.giz.de/en/downloads/giz2019-EN-Blockchain-A-World-WIthout-Middlemen.pdf [08.04.2021].

Mota, Miguel 2019: Evolution of Blockchain Components to Off-Chain Models, online: https://medium.com/@miguelmota/evolution-of-blockchain-components-to-off-chain-models-ca3649fe2c83 [07.04.2021].

Nazarov, Sergey and Punit Shukla 2020: Bridging the Governance Gap: Interoperability for blockchain and legacy systems, online: http://www3.weforum.org/docs/WEF_Interoperability_C4IR_Smart_Contracts_Project_2020.pdf [08.04.2021].

Ondera, Marcio 2019: Navigating Blockchain and Climate Action 2019, online: https://www.climateledger.org/resources/CLI_Report-2019-State-and-Trends.pdf [08.04.2021]..

Pollaco, Alexia 2020: The Interaction between Blockchain Evidence and Courts – A cross-jurisdictional analysis, BCAS, April 23, 2020, online: https://blog.bcas.io/blockchain_court_evidence [08.04.2021].

Radcliffe, Mark 2019: Consortium blockchain governance: four critical issues for enter-prise blockchain projects, guest blog on Ledger Insights, online: https://www.ledgerinsights.com/consortium-blockchain-governance/ [4.01.2021].

Sedlmeir, J. et al. 2020: The energy consumption of blockchain technology: beyond myth, Business & Information Systems Engineering, (2020), 62(6), 599-608.

Schalatek, Liane 2017: Why Climate Finance Actions Need Gender Justice to Succeed, Heinrich Böll Foundation North America, online: https://www.ctc-n.org/sites/www.ctc-n.org/files/liane_schalatek-_why_climate_finance_actions_needs_gender_justice.pdf [08.04.2021].

Swiss Federal Office for Energy 2020: Regulatory Sandboxes, Best Practices für die Schweiz, Freiräume für neue Lösungen und digitale Innovation in der Stromversor-gung, online: https://pubdb.bfe.admin.ch/de/publication/download/10074 [29.01.2021].

Szabo, Nick 1997: The Idea of Smart Contracts, online: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html [08.04.2021].

UNCITRAL 2001: Model Law on Electronic Signatures, online: https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures [08.04.2021].

UNCITRAL 2017: Model Law on Electronic Transferable Records, online: https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_records [08.04.2021].

UNFCCC 2018: UN Supports Blockchain Technology for Climate Action, Article of 22 Jan, 2018, online: https://unfccc.int/news/un-supports-blockchain-technology-for-climate-action [13.11.2020].

United Nations 2001: UNCITRAL Model Law on Electronic Signatures, 2001: https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures [08.04.2021].

United Nations 2017: UNCITRAL Model Law on Electronic Transferable Records, 2017: https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_records [08.04.2021].

United Nations 2021: Paris Agreement, United Nations Treaty Collection, online: https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=XXVII-7-d&chapter=27&clang=_en [06.04.2021].

WEF 2020: Redesigning Trust, Blockchain Deployment Toolkit, Supply Chain Focus, online: https://widgets.weforum.org/blockchain-toolkit/pdf/WEF_Redesigning_Trust_Blockchain_Deployment%20Toolkit.pdf [05.01.2021].

World Bank 2019: Simulation on Connecting Climate Market Systems, Summary Report, online: https://documents.worldbank.org/en/publication/documents-reports/documentdetail/128121575306092470/summary-report-simulation-on-connecting-climate-market-systems [08.04.2021].

World Bank Group 2020: Global Experience from Regulatory Sandboxes, Fintech Note No. 8, online: http://documents1.worldbank.org/curated/en/912001605241080935/pdf/Global-Experiences-from-Regulatory-Sandboxes.pdf [29.1.2021].

WRI 2020: CAIT, online: https://cait.wri.org/source/ratification/ [13.11.2020].

Legal Sources

Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register (not in force yet), September 25, 2020, online: https://www.admin.ch/opc/de/federal-gazette/2020/7801.pdf [08.04.2021].

Decision 1/CP.21 Adoption of the Paris Agreement, online: https://unfccc.int/sites/default/files/resource/docs/2015/cop21/eng/10a01.pdf [15.04.2021].

eIDAS, Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS) and repealing Directive 1999/93/EC, online: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN [08.04.2021].

GDPR, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR), online: https://eur-lex.europa.eu/eli/reg/2016/679/oj [15.04.2021].

Gesetz zur Einführung elektronischer Wertpapiere (Draft), December 16, 2020, online: https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RegE_Einfuehrung_elektr_Wertpapiere.pdf?__blob=publicationFile&v=3 [08.04.2021].

Liechtenstein Blockchain Act, Unofficial Translation of the Government consultation Report and the Draft-Law on Transaction Systems Based on Trustworthy Technologies (Blockchain Act): https://www.naegele.law/files/Downloads/2018-10-05-Unofficial-Translation-of-the-Draft-Blockchain-Act.pdf [08.04.2021].

MiCA, Proposal for a regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM/2020/593 final: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593 [07.05.2021].

Paris Agreement, online: https://unfccc.int/sites/default/files/english_paris_agreement.pdf [15.04.2021].

ZertES (Federal Law on Electronic Signatures), Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifi-kate March 18, 2016: https://www.admin.ch/opc/de/classified-compilation/20131913/index.html [08.04.2021].

INATBA CLIMATE LEDGER INITIATIVE

CLIMATE LEDGER INITIATIVE

Contact details:

Website inatba.org
climateledger.org

Contact contact@inatba.org
info@climateledger.org