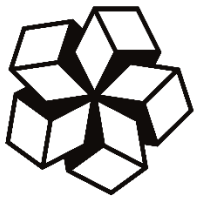


# EmisChain Whitepaper

*An application of blockchain technology for road-transport emissions monitoring to support an emissions market and an in-use emissions-based tolling system in the EU*

Beck R.,
Spasovski J.,
Gentile L.,
Manga Mukkamala A.

**Contact information**

European Blockchain Center

Name: Roman Beck

Address: Rued Langgaards Vej 7, 2300 København

Email: beck@itu.dk

# Contents

## Abstract

The Paris climate agreement requires to improve current solutions to reduce pollution and fight global warming. Different market-based approaches to face the problem are available, such as emissions trading. However, in order to increase effectiveness of these approaches, several challenges need to be addressed. Blockchain technologies may represent an opportunity to create an emissions monitoring system collecting a large amount of data about vehicles and an emission trading system that allows emissions permissions to be traded in a decentralized peer-to-peer system. However, the adoption of blockchain for massive large-scale systems has still to illustrate its applicability.

This report is primarily intended to evaluate existing Distributed Ledger Technology (DLT) systems and their readiness for an emission monitoring and permission trading system associated with road transportation in Europe. Initially, we analysed requirements of the emissions monitoring system, executed a comparative analysis of the available blockchain technologies and identified limits of current DLT systems to fight global warming.

After executing scalability and performance tests on permissioned public DLT systems to store carbon emission data for the approx. 300 million vehicles on European roads, we identified DLT systems that are capable to handle the necessary transactions per second under different consensus mechanisms.

Subsequently, the requirements and involved stakeholders for the emission trading system are discussed. Such a system needs to build upon the emission monitoring system and ideally provides an autonomous trading mechanism that seamlessly interact. The proposed DLT system would be again a permissioned public solution that allows for smart contracts to create a trading market place. As part of the emission trading mechanism, mechanism design and nudging techniques are discussed, such as a safety valve system and a feedback mechanism to incentivize users to behave in the intended way.

This work concentrates on the feasibility of rolling out an emission monitoring and trading system on a DLT system in Europe and highlights the specifications, design elements, stakeholders, as well as performance and scalability considerations as information base for further discussions regarding feasibility of DLT systems to fight global warming in Europe.

## Executive summary

If the Paris climate agreement is to effectively combat climate change, a market for trading emissions rights in the sector of traffic and transportation is needed to enable an economic incentive mechanism that will ultimately help reduce pollution. While some emissions-rights trading systems are already in place in certain countries or for specific industries, a Europe-wide system for enforcing emissions rights in traffic and transportation would face several challenges. Such a system would be very large; it would be responsible for tracking and tracing nearly 300 million vehicles on European roads, and would utilize onboard units to facilitate emissions rights management and auditing. Such a system would not only be one of the largest distributed computer networks in the world, but as a multinational system it would also face the complexities of enforcing the rules and norms that would ultimately reduce emissions across national borders. The use of a distributed ledger technology (DLT), commonly referred to as blockchain, would be one promising way of enforcing emissions rights in a multinational, decentralized system like this.

In this report, we introduce the organizational challenges of blockchain technologies. While the identity of the vehicles and owners would be known via national car registration systems, it is not clear what the governance structure of such a Europe-wide system would be, where the data would be stored, how the system would perform, and how such a system could provide incentive mechanisms to enforce, or, hopefully entice, vehicle owners to reduce emissions. Such a system would likely have to interact with other DLT and non-DLT system (e.g., national vehicle registration systems) in the logistics and transportation industries. As all vehicles would be also nodes in a large-scale blockchain system, we introduce the foundations of blockchain here to prepare the reader for the subsequent parts of the report, where we illustrate the "Emissions Chain" system (EmisChain for short), its functional and nonfunctional requirements, and evaluate existing DLT systems if they meet the defined criteria.

To understand the current state of blockchain applications in general, we briefly illustrate other large-scale blockchain systems that are in place or are under development, in order to illustrate how large-scale systems are currently designed and implemented, before we examine blockchain applications in the area of transport and logistics, since such applications are more relevant to the field of emissions-rights management. Subsequently, we introduce the high-level requirements and assumptions associated with EmisChain, which will be used in the following sections as a basis for the simulation and testing of different DLT systems in terms of their applicability for EmisChain. The emissions monitoring system comprises onboard units installed in 292 million vehicles on European roads, as well as all 115 thousand gas stations, which together will be used to record and triangulate gasoline consumption, driven miles, and emissions per vehicle. EmisChain is thus based on a network of units in vehicles and gas stations that confirms that the vehicle owner has the needed emissions rights when refuelling, and also measures the actual emissions of the cars and trucks in use.

In the following, we articulate the design and architecture of a blockchain system for metering and potentially reducing emissions. We also introduce the stakeholders of EmisChain, as well as the architectural configuration of EmisChain and the smart contracts involved. We describe the ledger system that tracks and traces the emissions and the market mechanism for trading emissions rights here as well. Since a large-scale blockchain-based system like this has never been implemented or even tested before, we must also evaluate the available DLT systems in other application areas. Some DLT systems promise high performance and scalability, while others feature a programming environment that allows for smart contracts to be coded for trading emissions rights. As the system will need to handle the reported emissions from nearly 300 million vehicles, the processing speed, or transactions per second, is an important feature, as is the corresponding consensus mechanism, guaranteeing the robustness of the system. Finally, the report offers conclusions and recommendations concerning considerations associated with a potential EmisChain roll-out.

# 1 Blockchain and other Distributed Ledger Technologies

## 1.1 Blockchain foundations

We are living in a digital economy, and our societies are continuously increasing levels of digitization by embracing technological innovation. According to the World Economic Forum [1], one of the top ten most disruptive technologies is "Blockchain"; in 2017 **it was estimated that by 2025 the estimated business value of blockchain will be approximately $176 billion, exceeding $3.1 trillion by 2030** [2]. A more conservative estimate from 2018 by IHS Markit, speculates that the business value of blockchain will grow from $2.5 billion in 2017 to $2.0 trillion in 2030 [https://ihsmarkit.com/topic/blockchain-technology-reports-analysis.html]. Blockchain technology first became prominent in 2009 with the advent of Bitcoin, a decentralized cryptocurrency representing a major innovation in digital currency, enabling the transfer of money within a peer-to-peer network without any central authority. Blockchain is the underlying technology of the cryptocurrency Bitcoin. Most importantly, since blockchain is a type of distributed ledger technology (DLT), maintained and governed autonomously, new data entries are validated through a consensus mechanism—the participants in the network follow a set of rules to reach a consensus regarding the validity of new transactions [3].

Stated simply, a blockchain is a ledger with a set of special features that provide several advantages over a traditional registry log. In its most basic form, blockchain technology is a "decentralized database that stores a registry of assets and transactions across a peer-to-peer network. It's basically a public record of who owns what and who transacts what. The transactions are secured through cryptography and over time that transaction history gets locked in blocks of data that are then cryptographically linked together and secured" [4]. This technology thus gives rise to a **highly tamper-resistant ledger that serves as a technological source of truth** among the peers.

Blockchain technology **decentralizes information storage**, **reduces or eliminates the need of third parties, and provides trust through technology**. Although Bitcoin was the first application to allow a global exchange of digital assets without the need for intermediaries, it is not the only one. Currently, various applications and platforms are being developed to reduce or eliminate friction in transaction-related processes. Blockchain offers an innovative alternative that opens the door to new ways of interacting, where trust is provided by technology.

Due to the disruptive properties of blockchain, such as removal of intermediaries (decentralized), all transactions are traceable (transparency) and permanent (immutable), and cryptographic protocols create a chronological chain of transactional data that **is extremely difficult to defraud** (tamperproof). Not surprisingly, therefore, blockchain technology has attracted much attention among academics and practitioners alike [5][6]. Another novel feature of blockchain technology involves computer protocols known as **smart contracts,** which are deployed and run on a blockchain **so that contractual clauses are automatically executed** (self-executed) when preprogramed conditions are fulfilled [7]—for example, Ethereum smart contracts. The blockchain, along with smart contracts, provides the building blocks for many new application areas. Indeed, potential applications of this technology are not limited to the financial sector; rather, they encompass a range of industrial and social sectors. Based on the requirements of the application area, it is possible to use **permissionless or permissioned blockchains, and public or private blockchains**. Permissioned blockchains, in contrast to permissionless blockchains, restrict who can read or write data or validate transactions on the blockchain. Private blockchains, in contrast to public blockchains, allow only a selected set of users to connect to the network and interact with the blockchain (according to the permissioned criteria).

Since a blockchain is composed of a significant number of nodes, there must be a mechanism to synchronize the information and reach an consensus that defines which transac-

tions are saved on the ledger and which are not. This mechanism is called a **consensus algorithm** [8].

Traditional distributed systems, such as databases, are known for using crash fault tolerant (CFT) consensus mechanisms—meaning that they can continue to function even if nodes within the system begin to fail or crash [9]. Most **blockchains use Byzantine fault tolerant (BFT) consensus mechanisms**, meaning the system can tolerate some nodes within the system acting maliciously or crashing [10]. A BFT consensus system can handle up to one third of all nodes acting maliciously [11]. Thus, one way to break BFT would be to hijack over one third of all nodes to take-over the system.

Distributed systems, while theoretically more scalable than centralized systems, often produce different results in practice [12]. **Blockchain technology suffers from several scalability issues, both in terms of physically storing the blockchain and in terms of the resources required for reaching consensus**.

Consensus algorithms within blockchains ensure that all machines in the distributed system agree with changes made at any point in time. By enabling BFT consensus, no single machine can succeed in malicious acts against a distributed system [11]. The three main consensus mechanisms used in blockchains are: proof of work (PoW), proof of stake (PoS), and proof of authority (PoA)—otherwise known as Byzantine voting.

**Proof of work (PoW)** first dates back to 1993. According to the original paper [13] the main idea was to "require a user to compute a moderately hard, but not intractable, function in order to gain access to the resource, thus preventing frivolous use". The paper puts this idea into context by suggesting that machines sending emails should be forced to complete a moderately difficult computation that can be easily verified in order to decrease the rate at which spam emails can be sent. In 1997 Back [13] invented the PoW algorithm hashcash with the purpose of countering spam emails using SHA1 hashing problems. Hashcash currently has a wide range of purposes, including prevention of DoS attacks, but it is best known today as the consensus algorithm that secures the Bitcoin blockchain. Bitcoin's version of hashcash works by creating SHA256 hashing based problems that can be verified in O(1) time but take O(2^k) time to solve, where k = 256 is the hash size. Miners on the Bitcoin blockchain solve the hashcash algorithm so that they can verify and add a block to the blockchain, and each block contains multiple transactions. The miners that successfully solve the hashcash problems and add the blocks to the blockchain are rewarded with Bitcoins.

**Proof of stake (PoS)** is an alternative to PoW involving no mining to achieve consensus; rather, the next node to create a block is selected based on its stake in the blockchain. The stake can vary depending on how the blockchain has implemented its consensus mechanism. In cryptocurrency blockchains, the stake is normally the number of coins the node holds. In non-cryptocurrency blockchains, alternative approaches are generally needed, as no stake exists by default. If cryptocurrency-powered blockchains were to use pure PoS then the richest node would be selected every time, meaning the blockchain would become centralized with a single entity controlling the blockchain consensus. This is why many cryptocurrencies such as Nxt, Blackcoin, and Peercoin use heuristics in their PoS algorithms. Nxt and Blackcoin add randomization into their selection formula, while Peercoin uses randomization combined with the practice of selecting only nodes that have not spent or received cryptocurrency for at least 30 days[14][15]. PoS does not require mining, thus allowing for lower energy requirements in contrast with PoW [16], comparable to running standard server equipment.

**Proof of authority (PoA)** or Byzantine voting is a commonly used consensus mechanism for permissioned environments where the validators of a network are known and trusted. Many private and public blockchains such as Hyperledger, Tendermint, Ripple, MultiChain, and Red Belly use PoA as the consensus mechanism [17][18][19][20][21]. PoA uses trusted validators for block creation, allowing the validators to simply vote on the validity of the block, and leads to high performance and scalability [22]. In selected

PoA implementations such as in Tendermint [17], voting power can be assigned to the validator nodes, making it possible to give some nodes more decision power over others.

The blockchain achieves a consensus via the built-in consensus mechanism as a governance system coded into the DLT system. This is the reason why it is important to apply a life-cycle approach when it comes to **DLT/blockchain system governance standardization**, which not only takes the design and implementation of a DLT system into account, but also considers the use and maintenance phase, and finally, the termination of the system. At this first level (I), deciding on a certain consensus mechanism—such as proof of work, proof of stake, or proof of authority—defines subsequent decision rights, and thus the overall governance system. At the second level (II), the governance of the DLT itself and the surrounding human and organizational agents must be considered. A consensus based on a single intersubjective and interorganizational reality must be established, in order to define how decisions will be made and how potential conflicts are to be resolved. At this level the code will decide who is allowed to participate, how to resolve disputes, and how votes or voting mechanisms work. The third level (III) is the governance structure, addressing the interoperability between and across different DLT/blockchain systems; governance and interoperability issues are addressed at this level (Figure 1).

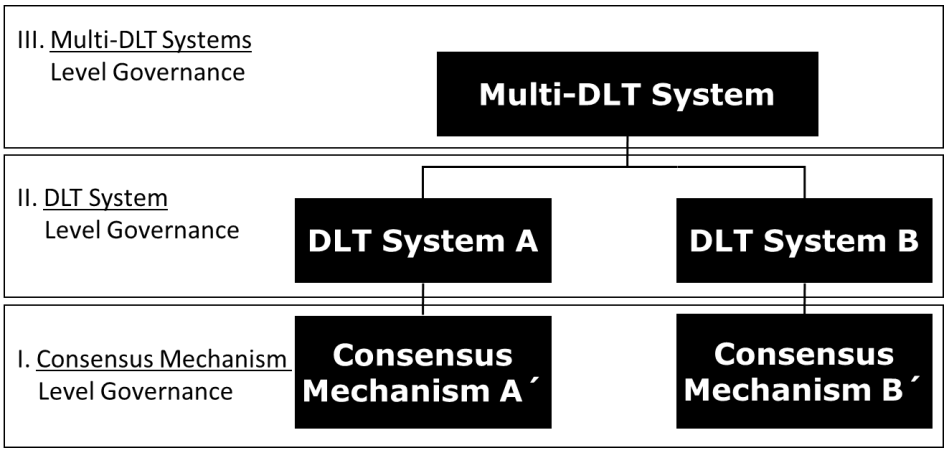


Figure 1: Levels of DLT/blockchain systems governance

DLT/blockchain governance systems reveal a tension between **resilience and scalability**. In this context, **resilience means the tolerance and even resistance** of a governance system regarding faulty or malicious behaviour, whether fraudulent or simply due to lack of consideration. **Scalability** is **the ability of a governance system to process a large number of decisions** in a given period, and to even increase its rate as more agents participate in the network.

The duality of DLT/blockchain systems also needs to be addressed here, in that **DLT can be viewed both as the governance system in and of itself and as the object needing governance**. Since DLT/blockchain face the commonly recognized challenges of collective decision-making environments, we used insights derived from them to guide our discussion of DLT/blockchain system governance. DLT/blockchain systems comprise sociotechnical aspects of DLT implementation that require different aspects of governance—exemplified, for instance, by permissionless and permissioned systems. We advocate for a single DLT/blockchain system where possible, but as we will see in this report, multiple DLT systems are sometimes needed to fulfil the functional requirements.

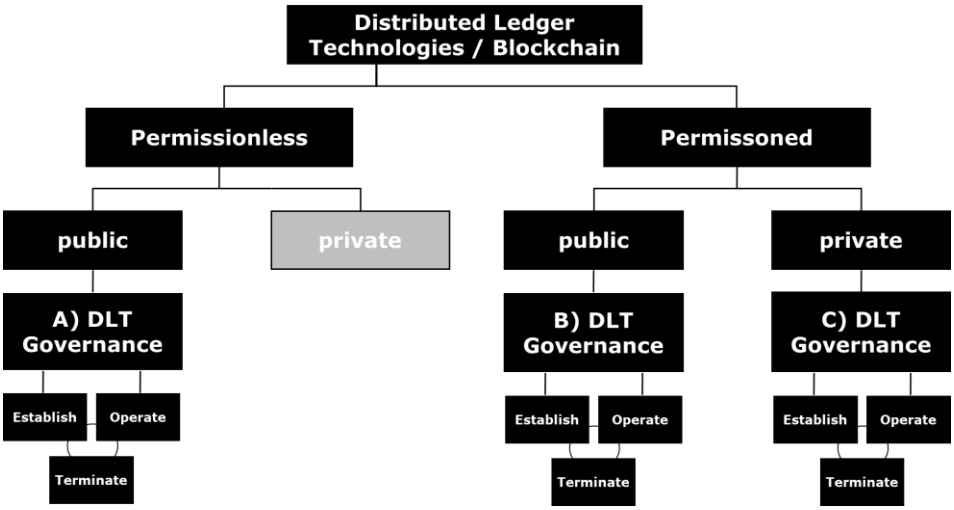


Figure 2: Types of DLT/blockchain systems governance

We focus on permissioned DLT systems as the object of **EmisChain governance**. In this document, DLT systems governance is structured along governance mechanisms and governance episodes for three different types of DLT/blockchain systems, which are illustrated in Figure 2.

The need for DLT-specific governance emerges along three different types, depicted as A) to C) in Figure 2. This classification helps clarify the **scope of the EmisChain DLT system governance**. In type A) of DLT systems governance, all nodes can read DLT data and submit transactions. All nodes can validate transactions along the governance mechanisms defined during the systems establishment phase. In type B), all nodes can read DLT data and submit transactions, but only predefined nodes can validate transactions and initiate changes in the governance mechanisms defined during the systems establishment and operation phase. In type C), only predefined nodes can read DLT data, submit transactions, validate transactions, and initiate changes to the governance mechanisms defined during the systems establishment and development phase. As all systems must eventually come to an end of some sort, any DLT systems governance standard must also consider the termination of the system.

A DLT system such as EmisChain will require **new forms of multistakeholder or decentralized governance**. As an extension of Figure 2, we now turn to a discussion of additional characteristics of DLT systems. Distributed ledgers have many participating nodes that operate under a wide variety of organizational contexts, which may include:

- **Permissioned/Private**: Nodes are separate IT systems that are all owned by a single organization. (Type C in Figure 2 above)
- **Permissioned/Public**: Nodes are operated by separate entities (e.g., departments or geographic divisions) owned by or responsible to a shared top-level organization (e.g., a parent company, or jurisdiction). (Type B in Figure 2 above)
- **Permissionless/Public**: Nodes are operated by separate parties (individuals or organizations) who may have no shared interests and who may not recognize or be recognized by a clear source of authority. (Type A in Figure 2 above)

Traditional approaches to governance of IT can be directly applied to Type B and Type C, although the detailed strategies, policies, and management systems for DLT/blockchain systems may be different from those for conventional systems such as cloud systems or enterprise IT in general. For Type B, accountabilities and responsibilities for an entity may arise contractually in an outsourcing arrangement, rather than through ownership

by a parent organization, but this kind of arrangement is accommodated by conventional approaches to governance of IT. For Type A, hierarchical approaches to governance of IT can be effective to the extent that all parties jointly recognize a shared source of authority for their shared IT infrastructure. However, how to govern a permissionless and public DLT system that is not dominated by a single governing body is a problem that can be addressed using multiple approaches. For example, the Ethereum blockchain does not offer a built-in democratic mechanism that would allow users to change its rules. If a set of users do not agree with the rules, they can create a partial or complete copy of the blockchain and establish different rules for it—i.e., a fork. Other users can continue using the version of the blockchain they prefer or can use both versions.

In contrast, the QTUM blockchain features a built-in democratic mechanism allowing users to partially change its rules. This is made possible by a voting procedure called the decentralized governance protocol [23][24]. This example shows how forks may be avoided in certain situations.

In our context, **on-chain** usually refers to activities like transactions and emissions records that occur on the blockchain, while **off-chain** are activities do not occur on the DLT/blockchain. There is also the term **side-chain,** denoting activities occurring on the blockchain, but not on the main chain, such as on a fork of an Ethereum platform. These terms can also be used to refer to the blockchain types themselves.

EmisChain DLT systems governance may be achieved through mechanisms intrinsic to a DLT system itself, as on the QTUM blockchain (**on-chain governance**), or through interoperability with mechanisms extrinsic to the system, as on the Ethereum blockchain (**off-chain governance**). On-chain governance relies on the design of DLT to provide the mechanisms for defining, changing, and enforcing the operational rules of a DLT system. Off-chain governance relies on mechanisms external to the DLT system itself. Due to the need to coexist with existing DLT and non-DLT legal and regulatory frameworks, standardized technology environments, and commercial paradigms, **we expect that the EmisChain DLT system will likely also interoperate with some degree of off-chain governance**.

Off-chain activities occur when a DLT transaction requires the intervention of other DLT or non-DLT systems. Governance of other DLT and non-DLT systems should incentivize these systems to encourage coherence with the DLT transaction purpose. For example, Oraclize [25] is a non-DLT system that is incentivized by payments encouraging users to provide information to smart contracts. This system belongs to the family of oracles, that will be explained in more detail in Chapter 3.

The transparency of governance arrangements for a DLT contributes significantly to the trust that participants and stakeholders place in that DLT. A benefit of on-chain governance is the increased transparency of DLT/blockchain systems governance mechanisms and the availability of the protocols for changing them, as well as a record of the history of such changes. Furthermore, on-chain governance may provide certainty in multijurisdictional spheres.

To explain the potential of blockchain technology, countless use cases of blockchain applications are discussed internationally with a focus on different sectors such as healthcare, financial services, the manufacturing and industrial sector, charity, retail, real estate, transport and tourism, media, and government [26]. In government and the public sector, more than 100 government-led blockchain projects have been initiated in more than 30 countries already [27]. Trust and transparency is the main tenet that could be useful for addressing real-world challenges like fraudulent behaviour [28], data sharing in healthcare [29], [30] personal user-data management [31], and so on. Especially in supply chains and transportation logistics, trust and transparency between the different stakeholders could be ensured by using a shared, immutable ledger to identify and track the goods throughout the supply chains [32][33].

## 1.2 Blockchain implementations in different industries

In this section we describe how blockchain can be applied to positively impact three main areas: finance, supply chain management, and medicine. Like EmisChain, these three areas are **characterized by high throughput as well as significant stability and safety requirements**. Although there are a large number of use cases that have been established, most of them have only been developed as proof-of-concept at the beta or alpha stage [34], and some are only prototypes. In 2017, IBM claimed to have worked with more than 400 customers on prototypes and proofs of concept in different industries [35]. However, only a very few have reached the commercial production phase.

Finance is probably the sector with most active blockchain applications, and is likely the one with the biggest market value during the last year [36]. This is partly due to the fact that the first commercial blockchain application was the Bitcoin electronic payment system. However, another important reason lies in the complexity of the financial world, a context involving numerous parties and significant trust issues, which also offers many opportunities for improvement, factors which makes finance a fruitful starting point for applying blockchain. Some finance applications include and might include:

**Cross-border payments**: Every year cross-border payments worth more than 20 trillion dollars are made [37]. In the area of B2B transactions alone, there are steep fees at both ends of the transaction that could potentially be eliminated through using a DLT system [38]. Additionally, transactions can take several days, during which the money is available to neither the issuer nor the recipient. Peer-to-peer applications based on blockchain would allow international payments to be sent and received at a faster rate, at a lower cost, and with greater transparency (traceability), and thus reduced risk. For example, Ripple has developed a DLT platform on which several payment initiatives are currently under development. In April 2018, Santander Bank launched One Pay FX, a remittance service based on the Ripple platform that allows transfers to several countries and reduces the transaction execution time from four days to just one day [39]. The same company created a product called xRapid that is being used to send US dollars from the United States to Mexico, where the recipient directly receives Mexican pesos [40]. The process takes only a few minutes and is significantly cheaper than a traditional remittance operation. The emissions market we describe in Chapter ☐☐ will also benefit from this cost- and time-reducing feature of blockchain technologies.

**Loans and mortgages**: Loan and mortgage processes are complex and involve several stakeholders. The required paperwork generates inefficiencies and sometimes errors. By making use of blockchain properties, a business network could deliver relevant information in real time to each stakeholder regarding the status of an asset and its related documents. Each stage of the sales process of an asset and a financing transaction could make use of smart contracts; for example, smart contracts could be used to enforce the rules of a business or automatically transfer and the ownership of an asset [41]. Additionally, during the process, the actual status of a payment could be easily tracked and would be verifiable with documentation at any point in time. This would allow financial institutions to provide added value and security to the participating transaction parties.

**Trade finance**: Trade finance operations require the certification (often manual) of numerous documents. These documents serve to prove that certain goods are at a certain destination and that their transport and load meets specific conditions. The parties involved include customs, port authorities, transporters, and sanitary authorities, among others. The complexity lies in handling and tracking the documentation used by these parties. A blockchain platform could integrate these tasks into a business network that digitally approves documentation and that would serve as a single source and location for all parties [42]. Insurance could be automatically issued and claims could be paid according to rules translated into the code of the relevant smart contract. This would significantly reduce delays by eliminating the need for manual handling of documents [43].

**Know Your Customer (KYC) and identity management**: anti-money laundering (AML) rules are becoming stronger and banks are being increasingly forced to perform

more validation activities to verify their clients [44]. This creates costs and frictions in financial processes and reduces the pace of business, which may also reduce the quality of the experience for the client. Blockchain has been presented as an alternative that is currently being analyzed by consortiums of financial institutions as it makes its way toward becoming a real application [45]. The blockchain application would verify a customer's information each time a bank account is opened, and an encrypted KYC record would be stored in a DLT system. Regulatory authorities and the financial services industry would have access to this information and allow KYC verification operations to be carried out quickly, while at the same time complying with AML regulations [46]. DLT/blockchain-based systems, in this case, would offer a unique and uniform source of data, improve efficiency by decreasing verification times, and provide greater transparency.

**Food industry:** There is a constant demand for greater food safety, availability, and freshness. When we buy food in a supermarket or restaurant, we trust its origin and safety. However, the difficulty of guaranteeing the origin of products that enter the supply chain and their proper handling across it represents a huge challenge for the food industry. DLT systems would make it possible to create a network involving producers, transporters, distributors, and even authorities. As such, the producer would register the products delivered to the supply chain, the transporters would register the transport conditions, and the authorities would register the controls they implement. The information shared would reduce friction and inefficiencies in the supply chain and would provide transparency to the industry and added value to the end user [47].

In this context, **blockchain is a system for storing supply chain data that is shared by everyone, but that no one entity completely controls**. This presents an advantage over traditional databases, because no one entity is responsible for managing the data. In the specific case of EmisChain, data would be shared among European countries, but none of them would be able to modify data in an arbitrary way or could be the only entity responsible for hosting or controlling the data. Data would be modified according to a predefined set of rules and all European countries would be responsible for hosting a copy of the data.

Currently, several companies have made successful blockchain prototypes in different countries. In a pilot project, Walmart used the platform developed by IBM Food Trust and was able to track a shipment of mangoes and obtain information on their origin in a couple of seconds, something that traditionally takes six days [48]. Nestlé has also tested a blockchain-based system to track the origin of food used in processed baby food [49]. These two companies are part of a consortium of more than 90 entities seeking to provide the end-consumer with greater transparency and safety [50].

Another potent use of DLT/blockchain would be to identify food implicated in food-poisoning incidents. In June 2018, after months of research, the FDA was able to identify the source of food that caused the hospitalization of 200 people and the death of five more [51]. This time and effort could almost certainly be significantly reduced by blockchain/DLT and would allow authorities to act in a more targeted manner to prevent further impacts during these types of events.

**Counterfeit prevention**: The manufacturing industry has fought tirelessly against the counterfeiting of goods, which not only negatively affects the economy, but sometimes even endangers individuals. Blockchain has the capacity to not only provide a mechanism for guaranteeing the origin of a product but could also determine its location and ownership in an efficient manner. Everledger is one of the pioneering examples of providing a mechanism to guarantee the origin of a product [52]. This company records a digital representation of a diamond on a blockchain, based on its unique physical characteristics. This guarantees the legal provenance of a diamond for the consumer and offers the industry a mechanism for combatting the negative consequences of the illegal diamond trade.

Provenance is an organization whose blockchain platform allows large and small producers to connect with transporters and other players in the supply chain [53]. Each member records information about a product that includes not only its origin, but also information about its impact on the environment and the working conditions of those who produced it. End consumers can use mobile phones to scan a product label, get detailed information about the product, and make a more informed purchasing decision.

**Logistics:** Every year, several trillion US dollars' worth of goods are distributed globally, and about 80% of them are transported by sea [54]. International trade documentation, sanitary controls, and monitoring procedures generate high costs and reduce the speed of such distribution. This is largely due to the fact that participants in the supply chain have generally independent systems that do not communicate efficiently or do not communicate at all, creating great friction and inefficiencies. A blockchain platform called TradeLens, created by IBM and Maersk, has been designed as a tool for increasing the speed of processing trade documents in the supply chain from end to end [55]. This tool connects exporters, transporters, ports, authorities, administrators, and importers in the network and provides visibility throughout the chain, allowing participants to communicate about events related to the cargo in real time. In addition, it digitalizes trade documentation and automates its completion while allowing authorities to quickly approve and stamp it at different stages and across different countries and borders. TradeLens is implemented on Hyperledger Fabric. More details on this technology are presented in Chapter 4. We discuss logistics and supply chains application in more detail in Section 1.4.

**Medical records:** Currently, medical records are typically stored in cloud-based databases belonging to hospitals and other medical service providers. Because of their importance to people's privacy, administrators spend large sums of money to ensure the security and integrity of such data. Additionally, access by other hospitals or health care providers is difficult because their systems may store information in different formats and communication is not always efficient. Blockchain could provide a solution: if medical records were directly or indirectly stored in a blockchain network involving physicians, hospitals, pharmacies, laboratories, insurance companies, and patients themselves, patients would have a full control over their records and could give consent for access and modification, and hospitals and other providers would have a single place where information was always updated and available. Estonia has developed this concept on a national blockchain platform that stores the e-Health records of its citizens [56]. It allows physicians to easily access patient records in real time while recording each time they are accessed, thus ensuring patient safety. In an emergency, any service can access critical information, such as blood type, allergies, recent treatments, or pregnancy, for example. Patients can access their records through their cell phone as well as manage the records of their children or of other individuals who have authorized access. Estonia has implemented this system on a private and permissioned version of KSI blockchain running on an Estonian government network [57].

**Pharma logistics**: The use of blockchain mentioned in the logistics industry could be extended to the drug supply chain. A blockchain platform integrating suppliers, logistic operators, wholesalers, and distributors would guarantee the provenance of a product. The authenticity of each product could be tracked and verified at every stage of the supply chain. Additionally, with the use of Internet-of-things (IoT) technology it would be possible to verify the transport conditions, and if a medicine were to break its cold chain or were subjected to improper environmental conditions, it could be returned immediately on the basis of improper handling. FarmaTrust [58] and MediLedger [59] offer two examples of how blockchain is currently being used to improve the pharmaceutical industry. Their solutions contribute to reducing the counterfeit drug problem responsible for the death of hundreds of thousands of people each year. In addition to providing patient safety, these applications have the ability to significantly reduce costs for reprocessing, transportation, and counterfeit losses, which could, in turn, reduce pharmaceutical prices in the marketplace.

**Efficient management systems**: Payers and providers of medical services face great challenges related to the efficient handling of claims. Companies must provide significant resources, expressed in time and manpower, to reconcile claims and make payments. A private blockchain network would integrate the actors involved and serve as a single, true source of real-time information concerning the filing, submission, and status of a claim. With millions of transactions per day, a health care network could thereby optimize its resources, streamline payments, prevent errors, and improve the overall settlement workflow. This would not only offer significant savings to the network, but would also improve workflow and service-provider satisfaction by reducing the time and effort necessary to receive payments. Change Healthcare has developed a solution applying these principles that promises to provide a mechanism for streamlining the interaction between hospitals, physicians, and payers [60].

## 1.3 Impact of blockchain on economic systems

Currently, multiple industries and sectors are working intensively with DLT/blockchain-based systems at different levels of maturity and at different stages of real-word implementation. Its potential to change business models and introduce significant transformations in industries, organizations, and governments will significantly impact both societies and the global economy. Bitcoin and the thousands of other cryptocurrencies that have emerged in recent years represent one of the greatest economic impacts of this technology at its nascent stages. The World Economic Forum (Sept. 2015) estimates that **by 2025 at least 10% of the global GDP will be stored on blockchain platforms**. The global economy is complexly connected as never before, with much of the economy substantially dependent on the US dollar, which currently serves as the world's reserve currency and the anchor currency for more than 60% of all nations [61]. As such, much economic power is centralized within the US government and economy, and it is precisely this central locus of power that cryptocurrencies could disrupt or significantly transform. As electronic payment methods based on blockchain are increasingly adopted, the dynamics of international trade, foreign relations, and diplomacy may change substantially.

However, the impact of blockchain may not be limited to the way we transfer monetary value on a global scale; rather, blockchain technology also **paves the way for the creation of other technologies** that would enable the **transfer of value in different ways** through new models of trust in common transactions. Through blockchain technology, value creators such as artists, composers, and designers would be able transfer this value to their clients or consumers simply and directly, with fewer intermediaries. This technology would make it possible to track and control the reproduction of a work, royalties, and advertising revenues, all on a consumption basis. In the same way that the music industry went from selling records to selling songs, blockchain would make it possible to bill customers according to how often or how long their music is played using more efficient payment systems. Intellectual property concerns could be managed on blockchain platforms that protect artists and producers and facilitate increased fairness in the trade of artistic works. As such, blockchain has the capacity to substantially disrupt the media industry through new micropayment-based pricing models, by limiting the possibilities of piracy, and by bypassing content aggregators, platform providers, and royalty collectors [62].

In recent years, **digitization has also facilitated the emergence of new business and consumer models, such as the sharing economy**. It is estimated that the revenues from this sector will reach 40.2 billion US dollars in 2022, up from 18.6 billion US dollars in 2017 [63]. Despite offering economic, social, environmental, and practical benefits, the sharing economy features centralized asset management, and business models are not fully equitable in the distribution of the value generated. This economic model has spawned giants like Uber and AirBnB. These kinds of companies accumulate value in an inequitable way and are subject to attacks that compromise the privacy and security of their users [64]. DLT systems and **blockchain would enable the inclusion of self-regulating and self-controlling elements** that would give users the opportunity to

manage and govern the platforms used, ensuring a more equitable distribution of value. Additionally, blockchain could facilitate **micropayment mechanisms**, which would improve efficiency and ameliorate security and privacy concerns for users. New blockchain-based applications are constantly under development. These new applications generate value in entirely new ways, increase the numbers of ordinary people involved in economic activities, and contribute to a more inclusive economy [65].

But how global is our economy really? According to the International Monetary Fund, as of 2016, nearly two billion people had no access to a bank account [66]. This problem excludes this population from the global economy, which is one reason that the financial services and telecommunication industries are seeking solutions; for example, the use of mobile phones for banking instead of actual bank accounts. However, **combining mobile communication with blockchain technology** could potentially lead to even greater improvements. Lower-cost direct international transfers, fraud prevention mechanisms that make bank accounts safer, and identity certification systems [67] are some of the blockchain-enabled features that could improve banking access for this population. Nevertheless, it remains difficult to assess whether blockchain will reduce the basic **problem of inequity** [68]. While Bitcoin and other blockchain-based payment mechanisms in theory may allow currently excluded individuals to become part of the global economy, with about 97% of Bitcoins currently concentrated in the hands of a few individuals it seems to be unlikely that Bitcoin is becoming an alternative for the unbanked [69]. Furthermore, there are also many nontechnical factors that would impact the possibility of a massive adoption of technology for fair and economically beneficial purposes.

## 1.4 Blockchain and DLT in supply chain

**Logistics and supply chains**: The logistics industry is very competitive and is also highly fragmented. Its value chain comprises countless players and stakeholders and faces many challenges, such as data silos, lack of transparency, unstandardized processes, and so on. The various regulatory requirements, in particular, create a huge administrative burden for this industry, as they are primarily paper-based, manual processes. To address this problem, Maersk and IBM joined forces to create TradeLens, a global blockchain-based system that helps digitize trade workflows and shipment tracking [70]. Other blockchain-based initiatives have tested alternative solutions [71] to manage the so-called *bill of lading*, which also plays a central role in international shipping regulations. Another use case is offered by Blockshipping, which is developing a blockchain-based global shared container platform to provide a global container registry along with real-time container location information [72] intended to not only reduce the number of empty containers shipped, but also reduce carbon emissions.

In general, a supply chain constitutes a complex network of different stakeholders; hence, products must travel through retailers, distributors, transporters, storage facilities, and suppliers. Reporting a product's tracking data on a blockchain would improve customer access, enhance transparency and traceability, and substantially reduce the massive problems of counterfeiting and food contamination. Thus far, experimental blockchain prototypes have been used to not only digitize workflows but also to trace counterfeit products and track the origin of products, which would improve the efficiency of supply chain management. For example, a blockchain-based system has been prototyped and tested in the garment supply chain of the textile industry to ensure the **transparency of ethical and sustainable business practices** and verify the garment's history. This application would allow consumers to scan the QR code or NFC-enabled label of a product with a smartphone app and then browse through the origin and history of the product [73]. Similarly, another company, Everledger, developed a blockchain-based system devoted to tracing and tracking the origin and ethical sourcing of high-end goods such as diamonds, wine, and artworks [73][74].

Retail giant Walmart, in collaboration with IBM, has completed two blockchain pilots based on Hyperledger fabric (pork in China and mangoes in the Americas) for food provenance [75], one of which successfully reduced the time needed to track mango ship-

ments from 7 days to 2.2 seconds. In August 2017, other food giants such as Kroger, Nestle, and Unilever joined Walmart in collaborating with IBM to use blockchain to improve food safety through tracing and tracking goods in enhanced supply chains [76]. Chinese e-commerce giant Alibaba has also used blockchain to fight counterfeit products on its platform: using QR codes, Alibaba customers can scan and read the history of product that is stored on blockchain system [77]. Recently, Accenture (a Dublin-based consultancy) and Thales (a French multinational aerospace and defence systems provider) partnered and presented a tailored blockchain prototype built on Hyperledger fabric to generate tamperproof cryptoseals appended to parts produced for the aerospace and defence industries. The purpose of this blockchain-based prototype is to verify the authenticity of parts and supplies across the complex and heavily regulated industry-specific supply chains [78]. Most of the prototypes are tested to evaluate feasibility in implementing blockchain-based systems in real-world scenarios. A number of industry-specific blockchain projects are currently being developed to improve transparency and traceability in supply chains. However, while many projects are in the experimentation phase, very a few large-scale applications are nearing implementation.

## 1.5 Large-scale applications of DLT systems

Everledger is a success story in this developing field, in that it has already digitally certified over one million diamonds and records every diamond's information on its blockchain indefinitely, offering a clear audit trail for stakeholders. "While Everledger does not provide technical details on their solution, it claims to use a hybrid model between a public/private blockchain to benefit from the permissioned controls in private blockchains" [79]. In China, Alibaba through its subsidiary Ant Financial, launched a private, proof-of-work blockchain to track charitable donations. The blockchain-based charity platform AntLove not only records the donations of approximately 450 million Alipay users, but also connects them to various charitable groups and nongovernmental organizations [80][81].

Dubai has launched a citywide blockchain strategy with a stated goal of being "the first blockchain-powered city by 2020" [82][83]. Singapore's central bank has completed a proof-of-concept trial of using DLT systems for domestic interbank payments and has announced that it is now ready to use the blockchain technology for interbank payments [84]. ID2020 is a project using blockchain technology to provide "**global identity or proof of identity**" to people who do not have official documents to identify themselves. The ID2020 alliance expects to move from prototype to implementation with the aim of supporting more than seven million refugees from 75 countries by 2020 [73]. It uses the *Enterprise Ethereum Alliance's* permissioned blockchain protocol [85]. Commonwealth Bank of Australia and its logistics clients launched a successful blockchain pilot to track the global shipment of almonds. The coalition successfully tracked and managed a shipment of 17 tons of almonds from Australia to Germany [86]. In another example, the number of Chinese electronic invoices is forecast to reach 54.55 billion by 2022. Since current electronic invoice systems in China face nearly intractable hurdles in the process of invoice circulation, China Aerospace Science and Industry Corporation is switching to a blockchain system for electronic invoices in order to ensure authenticated invoice issuance, and efficient, traceable, and cost-effective oversight for tax authorities [87].

# 2 Requirements for a blockchain-based emissions monitoring system

A **basic implementation of the emissions monitoring system in the EmisChain** project would include **onboard units fitted in all 292 million vehicles** currently registered in the EU. The onboard devices would register the distance travelled by vehicles twice per day. All of the EU's gas stations (approximately 115 thousand) [88] would require hardware units to register the amount of fuel consumed by each vehicle, thus confirming the general validity of the data registered from the vehicle's onboard unit. Numerical data would be sent from the gas stations and the onboard units and directly uploaded to the blockchain.

From a technical perspective, any **DLT or blockchain system supporting smart contracts can be tokenized**, meaning credits or currency can be incorporated into the system in the form of a token that symbolizes tracking and recording purposes [89]. This functionality can be used as a base for an economic model such as an auctioning mechanism for trading emissions rights. A future implementation of **the onboard unit would also be capable of capturing other data,** such as speed, time, location, and G-force, which could be provided as input to optimization algorithms that could then be used to suggest alternative driving routes or to implement other means of improving the carbon footprint of each vehicle.

Blockchains are tamper-resistant systems [31], meaning that it would require great effort to attempt to manipulate any saved data. Blockchains may be tamper-resistant, but they **do not safeguard against incorrect data being loaded onto the system** [90], meaning any data produced on hardware that has been tampered with could be loaded onto a blockchain. In our case scenario, having two points of data entry (the vehicle hardware and gas station hardware) would minimize the risk of incorrect data being loaded due to data corrupted by hardware tampering. The main risk to be considered would be a situation where both the gas station hardware and the onboard hardware were tampered with in an undetectable manner. Approaches like **auditing suspected onboard unit tampering** or video surveillance at gas stations could be used to prevent such malicious activity. The integrity of the transaction communications are assumed secure for testing purposes, but possibilities of real-word tampering is an important issue in need of further study.

The **data sent to the EmisChain blockchain would have to be scheduled** to help distribute the generated load, as all 292 million devices registering data concurrently could cause the cache storing the unprocessed transactions (referred to as a mempool) to overload. The **size of the mempool** in many blockchain implementations **is dependent on the size of the machines hosting the blockchain**. The **size of the data packages** sent to the blockchain also determines how fast the blockchain mempool fills. In a concrete example where we assume smaller data packages are sent, a mempool could easily store over one million unprocessed transactions using under 1GB of memory.

The test simulations in this report will help to approximate the **machine specifications** required **alongside the performance feasibility of this project.** The process of creating the test simulations can be divided into five steps. The first step sets up a blockchain environment replicating a potential blockchain environment hosted by the EU. The second step designs the synthetic load the blockchain would receive. The third step runs initial tests providing various testing parameters. The fourth step tests the blockchain environment using the synthetic load and parameters obtained from the previous step. The final step analyses the test results that contained critical performance and scalability data.

# 3 Analysis of a possible blockchain-based emissions trading system for road transport

Emissions trading is a **market-based approach for controlling pollution** [91]. In its most general form, a central authority allocates or sells a limited number of emissions allowances permitting the discharge of specific quantities of a specific pollutant in a specified period of time. Polluters are required to carry emissions allowances that are equal to their actual emissions and must purchase emissions allowances from others willing to sell them if they want to increase emissions. Polluters are thereby also incentivized to reduce their emissions, since they can sell any unused emissions allowances.

Figure 3 shows a high-level flowchart description of the **DLT-powered emissions trading system** that we propose. In order to understand how the proposed emissions trading system works, it will be useful to identify three phases: 1) **granting** emissions allowances to an initial list of allowed users; 2) **updating** the list of allowed users, taking into consideration requests to join the emissions trading system; and 3) **Dutch auction** as a mechanism for selling emissions allowances.

While the first two phases require the intervention of a regulator, the Dutch auctions to trade emissions allowances can be organized in a completely peer-to-peer manner among the users of the emissions trading system.

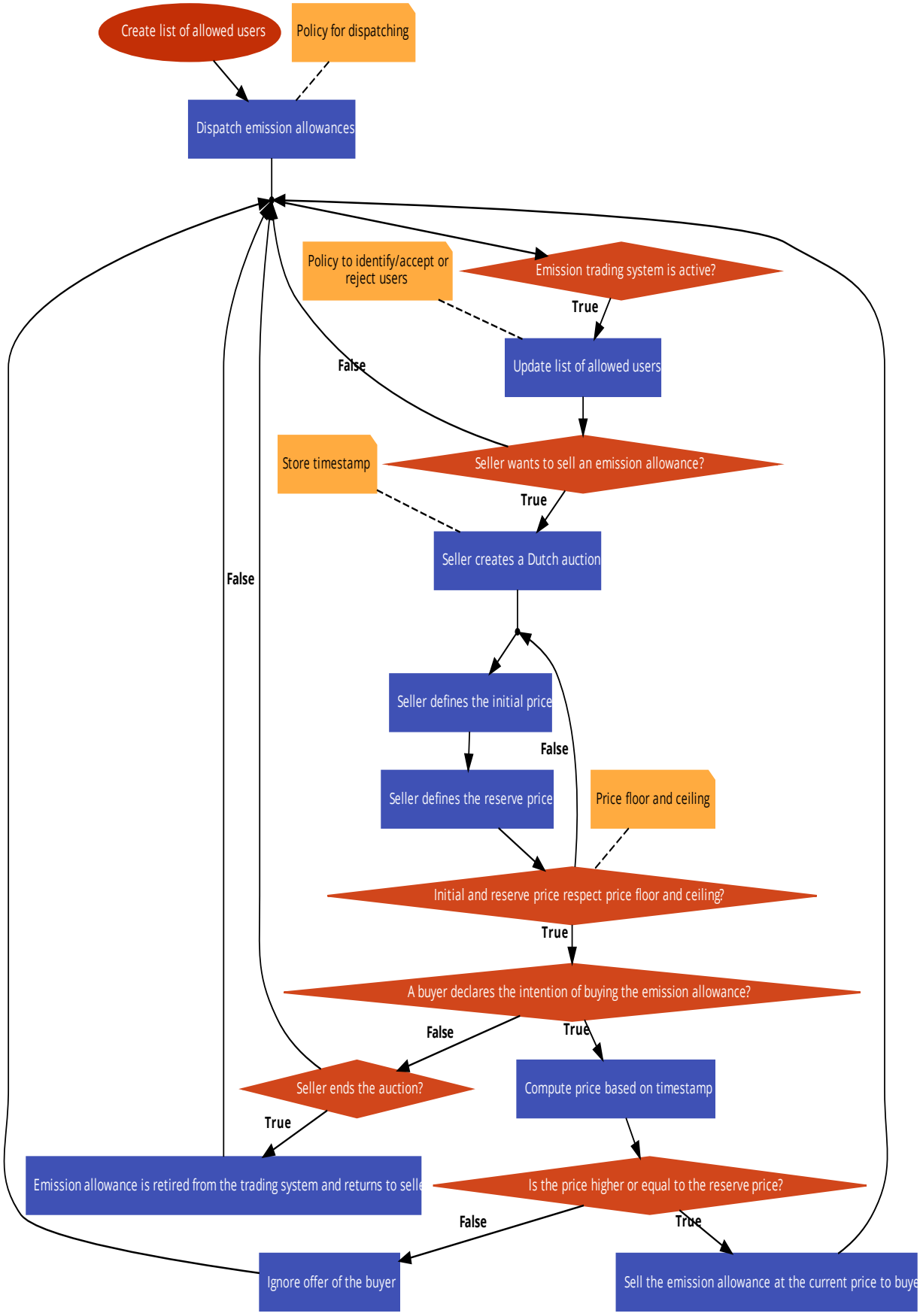


Figure 3: Flowchart of the proposed emissions trading system.

The suggested system is a **variation of the existing cap-and-trade system** known as the European Union Emission Trading Scheme [92]. This approach gives users an initial amount of emissions allowances. An emissions allowance permits the holder to emit one metric ton of CO2. If users comply with emissions allowances, the system guarantees a cap on the total emissions of CO2. Its adoption, however, has demonstrated that the system is afflicted by the following problems [93]:

- Due to the number of economical, technological, and social factors that influence future emissions, predicting the amount of emissions is a complex task. Since emissions caps are defined on the basis of future emissions predictions, faulty predictions may result in defining emissions caps that are not stringent enough to drive a significant reduction in emissions;
- Granting emissions allowances may not consider the different economic objectives among countries. This could increase disparities between developed and underdeveloped countries.

Increasing the accuracy of future emissions predictions and defining a politically viable policy of granting emissions allowances would require a tracking system with low granularity and a large amount of available data based on an immutable database like a blockchain.

Emissions allowances are traded by using a Dutch auction—i.e., an auction mechanism in which the auctioneer begins with a high asking price and lowers it until a participant accepts the price. This type of auction is good for auctioning goods quickly, since a sale never requires more than one bid. In the context of the blockchain implementation of an emissions trading system, it means that exactly one transaction is required to sell an emissions allowance. An auction mechanism such as a second-price sealed-bid auction would require many more transactions.

Without an available dominant strategy, the drawback of a Dutch auction is that if users seek to maximize their outcome by bidding strategically, they must use all available information about other users to estimate their expected bids. This could require a lot of analytical power. Moreover, it does not incentivize users to bid truthfully and it may result in a high variance in auction revenues.

However, in the context of a DLT or blockchain system, minimizing the number of transactions necessary for the system to work is essential, since transactions typically imply an explicit monetary cost dependent on the congestion of the network. Also, minimizing the effort of the network saves resources. This is why we suggest a Dutch auction mechanism. For a more detailed explanation of different auction mechanisms, see [94].

A seller is allowed to set an initial price and a reserve price for every emissions allowance to be sold. The reserve price is the minimum price at which the seller would sell the emissions allowance. This offers a certain degree of freedom to users. Since such a system must follow principles that are perceived as fair and just in order to reduce carbon emissions, the system suggested here partially limits the freedom of buyers and sellers by adopting a so-called **safety valve instrument** [95]. This means that from a market-engineering point of view, the regulator has a certain degree of control over the market. In particular, the regulator can set a **floor and ceiling price for emissions** allowances to prevent carbon emissions allowances from being traded at a price that is below a certain threshold that is necessary to reduce emissions effectively. In an extreme case, if polluters received emissions permits for free, they would have no incentive to reduce their emissions at all, because if they did so, they would most likely receive fewer pollution emissions allowances in the future [96].

Such an **undesirable incentive mechanism can be alleviated if permits are also auctioned** during the granting phase—i.e., sold to polluters, rather than given to them for free [97]. Again, we suggest the Dutch auction mechanism here. Revenues from auctions pass to the government and can be used for restructuring the economy to further

reduce emissions and increase sustainability [98] or to cut distortionary taxes, thus improving the efficiency of the overall cap policy [99].

Allocating allowances without cost could be also be used as a measure to protect domestic firms that are exposed to international competition [97]. In other words, a firm that pays for allowances may be at a competitive disadvantage to firms that are not subject to the same regulations. While this argument may have been valid in the past in the context of the European Union, the purpose of the proposed emissions trading system is to compensate for the drawbacks of auctioning emissions allowances by improving the fairness of how allowances are granted, which should lead to significant environmental advantages in the medium and long term.

The level of abstraction of the flowchart in Figure 3 shows how the proposed **emissions trading system fits with the *event-driven programming paradigm* that characterizes smart contracts**. In the context of smart contracts, the events that determine the flow of the program are external user actions called transactions.

The emissions trading system is based on the following smart contracts:

- The main **emissions trading system smart contract** manages the information and transaction flow of the emissions trading system
- The **user smart contract** represents a system user and is used by the main smart contract to manage users

A transaction must not necessarily be triggered or completed by a human being, as it can also be initiated by another system. The latter is usually the case in the context of "oracles", such as the one provided by Oraclize [25]. Since smart contracts, by design, cannot fetch external world information by themselves, this **information is provided by an external service called an oracle**. In our context, an oracle is required to provide travel information about vehicles coming from the emissions tracking system to the smart contracts of the emissions trading system.

Table 1 provides an initial list of potential stakeholders of the EmisChain system. We divide the stakeholders into direct stakeholders and indirect stakeholders according to their type (governmental, commercial, administrative, user).

**Direct stakeholders** are stakeholders who interact directly with the system, which is the reason why they are mentioned and modelled into the architectural schema of EmisChain in Section 3.1. **Indirect stakeholders** are stakeholders who still benefit from the system, but do not interact directly with it. Indirect stakeholders are vehicle producers—since they may have an incentive to produce low-emissions vehicles, if the market request increases—vehicle maintainers, and logistic companies, since they may have anonymized cumulative travel information that could be used to improve their processes. National law enforcement agencies represent a further indirect stakeholder group.

In the context of the emissions trading system a user may be any entity interested in trading emissions allowances (e.g., vehicles drivers, a private company, a state); however, **the emissions monitoring system focuses on vehicles alone**. For this reason, we will henceforth specifically consider the case scenario in which users are vehicle drivers.

| | Commercial | Government | Private | Administration |
|---|---|---|---|---|
| Direct stakeholders | **Gas stations** | **Regulator**: defines the functioning of the emissions monitoring system and the emissions trading system. It covers the following tasks:<br>Grant emissions allowances;<br>Define policy to identify, accept or reject users;<br>Create/update list of allowed users;<br>Define price floor and ceiling for emissions allowances;<br>Define any other rule of the smart contract (compute price, sell an emissions allowance). | **Vehicles drivers**: if they reduce their emissions, they receive a direct economic benefit through the opportunity to sell their unused emissions allowances in the emissions trading system. | **Oracle**: the system pays an oracle to provide off-chain information.<br>**EU agency** for the development and maintenance of the system. |
| Indirect stakeholders | **Vehicle producers:** they have an incentive to produce low emission vehicles, if the market request increases.<br>**Vehicle maintainers**<br>**Logistic companies:** they have anonymised cumulative travel information, that could be used to improve their processes. | **National law enforcement** | | |

Table 1: Stakeholders in an EmisChain environment

## 3.1 DLT systems architecture of the emissions monitoring system

The synergy of the defined emissions trading system with the emissions monitoring system described in Section 2 facilitates checking if each network user is in conformance with the emissions constraints in terms of the number of allowances purchased.

In Figure 4, we present a high-level description of how the two systems can be integrated.

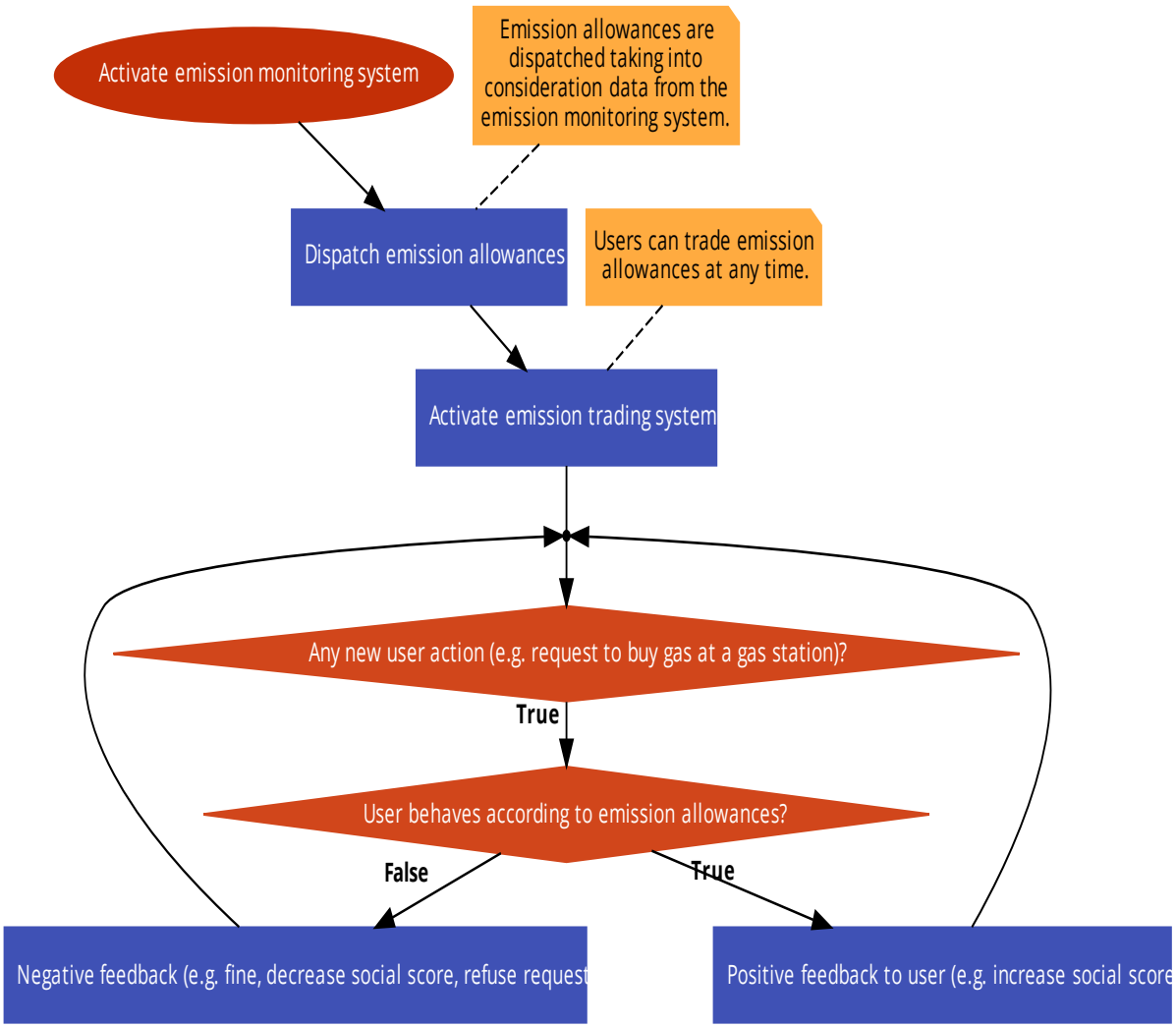


Figure 4: Integrated emissions monitoring and emissions trading system

A fine or a malus in terms of **social score can be adopted** as negative feedback, while a bonus in terms of social score can be adopted for positive feedback. The purpose of **the social score is rewarding or penalizing users** in the context of the emissions trading system, based on their behaviour. Note also that users are allowed to **trade emissions allowances at any time**. The system checks if users behave according to the number of emissions allowances they own every time they make a request to buy gas at a gas station. If this check fails, another type of negative feedback the system could impose on the user is refused of the request to buy gas.

Figure 5 provides an illustration of the entire **EmisChain architecture**, including the emissions monitoring system and the emissions trading system.

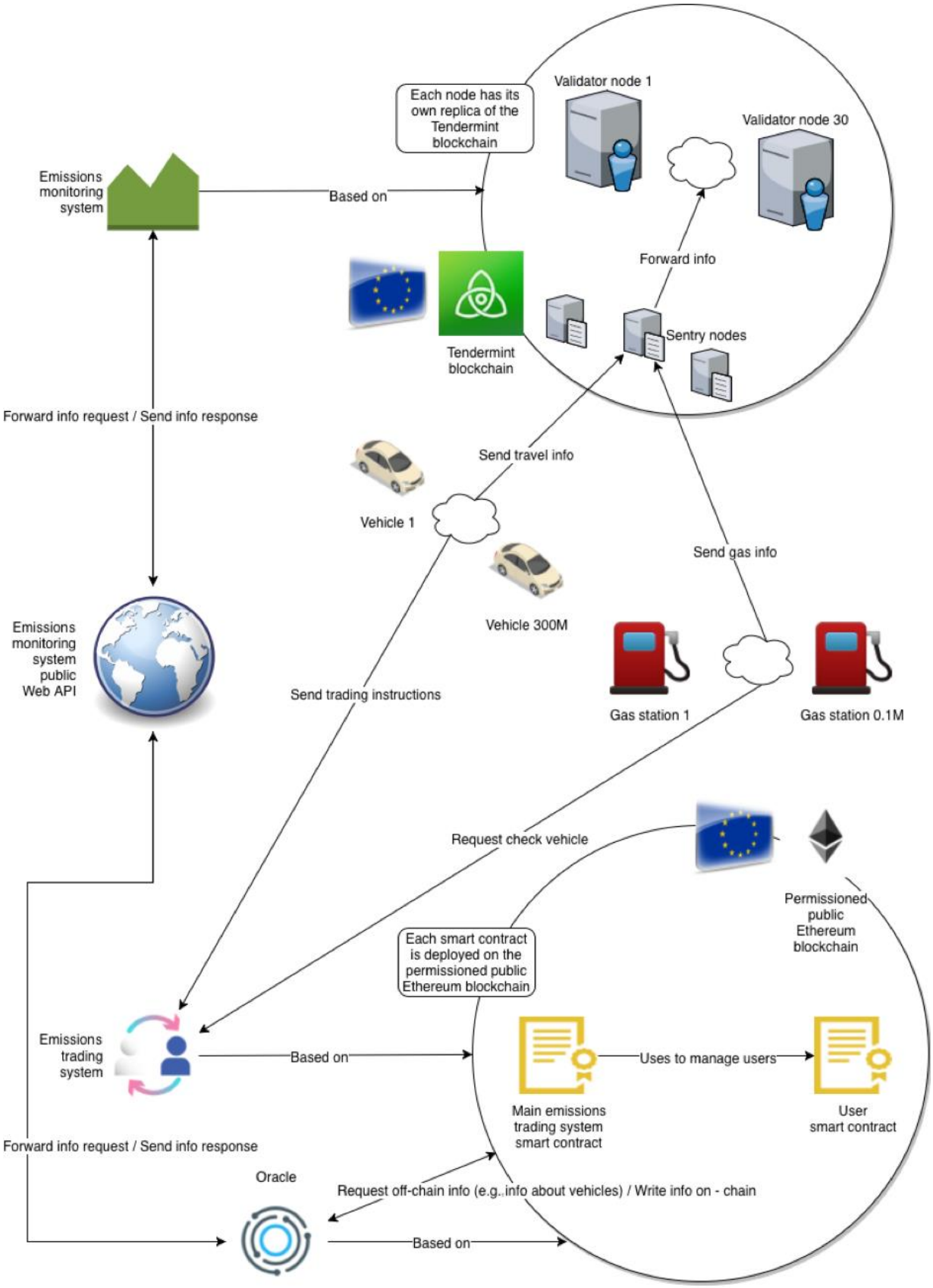


Figure 5: Architectural schema of EmisChain

The emissions monitoring system is based on the **Tendermint blockchain**, presented in more detail in Chapter 4.

The Tendermint blockchain acts as a data storage layer for the emissions monitoring system; all vehicle travel and gas usage information is stored on it. An estimated 300 million vehicles will join the network, while the number of gas stations is estimated at roughly 100,000 [100][101].

To test the emissions monitoring system, all **transactional data** from the vehicles and gas stations **will be validated by 30 validators**, with each member of the **European Union being represented by one validator**. There are more validators than actual EU member states in order to ensure a certain degree of flexibility.

To mitigate the problem of **distributed denial-of-service attacks** (DDoS) [102] on the validator network, a **sentry node architecture is proposed** as described in [103] and further discussed in the following chapter. Note that DDoS is a potential problem since private vehicles can interact with the system.

We now consider the emissions trading system. Any blockchain with full smart contract functionalities would be suitable for implementing the emissions trading system detailed in Figure 3. However, the blockchain should also include a Turing-complete scripting language. Since Ethereum is the most popular blockchain with the highest market cap that includes this feature, we would use the **Ethereum blockchain for our EmisChain emissions market place implementation**.

Bitcoin would not be suitable because its scripting language lacks Turing-completeness and blockchain-blindness [104]. Lack of Turing-completeness implies that loops are not available in the language; however, our emissions trading system requires a loop to verify the behaviour of all users. Blockchain-blindness means that blockchain data are not visible as a timestamp in the context of a script; our emissions trading system requires timestamps in order for the Dutch auction algorithm to function properly.

Taking into consideration that the European Union wants to control who can be a validator in the network, **we propose a permissioned version of Ethereum** that is public in the context of the European Union. More specifically, the European Union will define the rules of the governing body or agency overseeing EmisChain to decide who can join the network (and can see the data entries) and who can be a validator.

## 3.2 Design considerations for the implementation of an emissions trading system

Emissions trading systems have been strongly criticized in the past [93]. Taking this into consideration, we have designed the proposed system to anticipate problems regarding future emissions-prediction difficulties, as well as problems identified in past attempts regarding lack of functionality of emissions allowances from a market mechanism point of view. In particular, our system addresses the lack of fairness related to the distribution of emissions allowances. While scalability has been widely investigated in this work, a prototype of both the emissions monitoring system and the emissions trading system would be useful for:

- Validating and stressing the economical functioning and environmental effectiveness of the system;
- Optimally tuning the parameters of the system:
  - Weighting applied based on specific properties of the EU member states— e.g., GDP, population, etc.—in order to test different concepts of fairness related to granting emissions allowances;
  - Policy strictness regarding identifying, accepting, or rejecting users;
  - Price floor and ceiling related to emissions allowances;
  - Degree of positive and negative feedback given to users according to how well they comply with the constraints defined by the emissions allowances they own;

- Defining a policy for granting the Ether tokens required for interacting with the emissions trading system implemented on the EU permissioned public Ethereum blockchain;
- Understanding what user experience design choices might be best suited toward maximizing the usability of the system, by giving a selected list of users the opportunity to try the system;

In order to explore the key factors above, the prototype should be executed in different initial simulated scenarios.

Each scenario is characterized by:

- Countries:
  - CO2 level: amount of CO2 measured in the country;
  - Emissions trading market policy: when the country should buy or sell emissions allowances;
  - Owned emissions allowances: amount of emissions the country can emit;
  - CO2 emissions: amount of emissions the country emits;
- Vehicles:
  - Emissions-trading market policy: when the vehicle buys or sells emissions allowances;
  - Owned emissions allowances: amount of emissions the vehicle can emit;
  - CO2 emissions: amount of emissions the vehicle emits;
- Gas stations:
  - Feedback policy: the type and degree of positive or negative feedback the gas station should give to users according to how well they comply with the constraints defined by the emissions allowances they own;

Scenarios change according to events—e.g., a vehicle goes from a place to another, a vehicle buys gas, an emissions allowance is traded. The key factors above make it possible to test the response of the CO2 level of a certain country following system adoption, how quickly the CO2 level decreases, and how effective the feedback policy of a gas station is in relation to a set of vehicles following the same emissions-trading market policy.

# 4 Maturity analysis of DLT systems for emissions monitoring

## 4.1 DLT systems for metering emissions transactions

DLT and blockchain systems promise to solve a critical problem in traditional transactional systems, which are controlled by a single authority rather than a governing body or all entities involved in the transactions [105]. Blockchain systems are classified as distributed systems but generally differ from traditional distributed systems in two major areas: how consensus is achieved and how data are stored [106].

Traditional transaction systems are typically centralized, with a single party controlling and managing all data. The primary goal of DLT systems is to create a politically and geographically decentralized (distributed) environment with no third party in control of the data. Data tampering on a blockchain is easily detected through the data structure—the most common structure is called the Merkle tree [107]. Since the data structure can easily detect any data tampering, the consensus mechanism checks the validity check of all data at every block insertion [108].

In cases where a single party possesses the data write privileges, it would make most sense to use a traditional centralized distributed database for performance and scalability reasons [79]. Given that EmisChain will mostly likely be run by a consortium of EU countries, or by the EU itself, using a blockchain would make the system virtually **immune to fraudulent activities and would fortify it against hacking**.

The type of blockchain needed for a specific system falls into one of the following three categories: Permissionless public (e.g., Ethereum and Bitcoin), permissioned public (e.g., Ripple and Stellar) or permissioned private (e.g., Hyperledger and Tendermint). The write/read privileges of a system determines which category of blockchain is required [79].

**EmisChain will most likely require a permissioned public or private DLT system**. First, state is needed since there are data that need to be saved. Second, there will be multiple writers consisting of all the registered vehicles in the system. Third, we do not wish to use a single trusted third party (TTP). Fourth, all writers will be known but not necessarily trusted. Finally, the read permissions of the system will be either private or public. This setting can be easily changed in any permissioned system, as it simply requires allowing or revoking public read access.

The project requirements of the onboard units require that **data are sent twice per day from all 292 million vehicles**—i.e., 584 million transactions per day. The project requirements of the gas stations require that data are sent every time a vehicle refuels, which is estimated at once a week per vehicle, or 42 million transactions per day for all 292 million vehicles. Assuming that all 580 million plus 42 million transactions are scheduled, **the system would have to handle 7,200 transactions per second processing nonstop**. It is therefore important that the transactions are scheduled to some extent, so that the mempool of the blockchain does not overload. How such a system is to scheduled remains outside of the scope of the blockchain implementation.

Table 2 presents is a **survey of performance claims of BFT blockchain systems**. Earlier in this section we argue that BFT is a fundamental part of securing a distributed system, therefore **this survey does not include blockchains that are not BFT**. By following the flowchart from Figure 3 we concluded that this project will require a permissioned blockchain; thus, the focus of this survey has been on permissioned DLT systems. To this author's knowledge all suitable permissioned blockchains under active development with well-documented performance claims have been included in this survey. In order to compare the effectiveness of the PoA consensus mechanism we have included the two largest PoW blockchains and the first PoS blockchain.

| Name | Consensus | Permisionless/ Permissioned | Open Source | Throughput (transaction/second) | Response time (seconds) |
|---|---|---|---|---|---|
| Bitcoin | PoW | Permisionless | Yes | 3-5 | 4,680 |
| Ethereum | PoW | Permisionless | Yes | 15-30 | 360 |
| NXT | PoS | Permisionless | Yes | 4.5 | 60 |
| Hyperledger Fabric | PoA | Permissioned | Yes | 80,000 | < 1 |
| MultiChain | PoA | Permissioned | Yes | 1000-1500 | 5-10 |
| Quorum | PoA | Permissioned | Yes | 835 | 5 |
| Tendermint | PoA | Permissioned | Yes | 4,000-10,000 | < 1 |
| Redbelly | PoA | Permissioned | No and not in production | 660,000 | 2-4 |
| Kadena | PoA | Permissioned | No and not in production | 8,000 | < 0.1 |

Table 2: Survey of performance claims for various blockchain systems [109][110][14]

As seen in Table 2, the PoW blockchains (Ethereum and Bitcoin) have a low throughput and high response time compared with the PoA blockchains. The PoS blockchain (NXT) has a slightly faster response time, compared with the PoW, but fails to compete with the PoA blockchains in terms of throughput or response time. The project requirements mentioned in the previous section require a **throughput of at least 7,200 transactions per second**; thus, of the surveyed blockchains, **there are only four possible candidates,** and of the four possible candidates **only two are currently available and open-source**—namely, **Hyperledger Fabric** and **Tendermint.**

The following section summarizes **Hyperledger Fabric** and **Tendermint**; thereafter, we articulate our decision of which to use for our scalability tests. A summary of the **Redbelly** blockchain will also follow as it seems to be the most promising future candidate that is backed by academic research in terms of performance and scalability.

Hyperledger Fabric is an open-source permissioned blockchain technology maintained by IBM and hosted by the Linux foundation [18]. Hyperledger features smart contracts, which allows the functionality of an application to reside on the blockchain, thus facilitating high levels of decentralization. Hyperledger has two built-in interchangeable consensus mechanisms, the first is called "solo", which replicates a centralized solution and is used for development [18]. The second interchangeable consensus mechanism is based

on Apache Kafka, which is Crash Fault Tolerant (CFT) [85] [86]. Hyperledger also features a proof-of-concept consensus mechanism based on BFT-SMaRt that is Byzantine fault tolerant (BFT) [18].

Over the past few years, IBM researchers have published multiple, perhaps exaggerated performance claims, the most significant being in 2016 when they stated that experiments had demonstrated that Hyperledger's BFT consensus mechanism (BFT-SMaRt) is capable of a throughput of about 80,000 transactions per second [110]. However, performance experiments in collaboration with IBM in 2018 using Hyperledger's CFT consensus mechanism (Kafka) only reached 2,250 transactions per second [112]. The aforementioned **CFT consensus mechanism features improved performance over BFT consensus mechanisms at the cost of security**, in that it can be disrupted by a single malicious node [11][113].

Tendermint is an open-source permissioned blockchain technology created by Jae Kwon in 2014. Tendermint uses a BFT consensus mechanism, which is similar to the practical Byzantine fault tolerant consensus [17]. Tendermint is relatively lightweight since its BFT consensus method is proof-of-authority, using a voting mechanism, as opposed to the more computationally expensive proof-of-work consensus mechanism [17]. Two different node types exist on the Tendermint blockchain; namely, validator and nonvalidator nodes. Validator nodes are part of the consortium that votes to agree on consensus, while nonvalidator nodes are restricted to reading and proposing transactions on the blockchain. All nodes on the Tendermint blockchain communicate over a persistent encrypted TCP P2P gossip protocol. **Unlike Hyperledger, Tendermint does not have smart contract functionality**. The Tendermint blockchain is only responsible for data storage and achieving irrefutability through its Merkle tree data structure BFT consensus mechanism.

Performance benchmark tests were conducted on Tendermint in a detailed paper by the CTO of Tendermint [109], hereafter referred to as *the previous Tendermint benchmark tests*. The previous Tendermint benchmark tests reveal that Tendermint is capable of handling over 4,000 transactions per second with a network consisting of 32 validators spanning seven data centers and five continents [17]. Given that the Tendermint blockchain has evolved since 2016, it is difficult to know if the performance claims from 2016 are still accurate. We will use these previous Tendermint benchmark tests as a guideline and refer to them throughout this report.

Redbelly blockchain was designed by Dr. Vincent Gramoli from Sydney University and is currently not open source. Experiments run on a single data center show that the Redbelly blockchain is capable of handling over 660,000 transactions per second on a network consisting of 300 validators. Running experiments on a single data center is commonly used when benchmarking as network latency is nonexistent. Blockchains are decentralized, therefore the nodes constituting the blockchain network must be distributed over multiple physical locations, which introduces network latency [65]. The latest test runs by Redbelly blockchain from September 2018 used 1,000 validator nodes on 300 machines in 14 geographical regions, including: Europe, South America, North America, and Asia Pacific. The aforementioned experiment yielded results indicate that this blockchain is capable of **handling 30,000 transactions per second** with an **average response time of three seconds per transaction** [114].

The Redbelly blockchain is a very promising technology, because it also has the security of BFT and maintains high levels of scalability and performance [20]. **Like Tendermint, the Redbelly blockchain is only responsible for the consensus and data storage of the blockchain, thus it does not have a smart contract layer**. Unfortunately, there is no information regarding the release of this blockchain to the public.

## 4.2 High level technical description of the EmisChain architecture

Given the current state of blockchain and DLT systems and the multiple real-world examples given in the first chapter, it is evident that **blockchain is mature enough to be**

**used for EmisChain**. However, one of the biggest challenges will be how to design such a system and how to choose a blockchain implementation capable of meeting the performance requirements for the emissions trading market, in addition to tracking and tracing the carbon emissions through the ledger system.

The survey presented in this chapter reveals that **highly scalable permissioned blockchains generally use the PoA as the consensus mechanism** [22]. The main requirement to run such a PoA blockchain for EmisChain is a trusted consortium that can run validator nodes. This consortium might, for example, consist of the 28 countries that make up the EU, where each country would host its own validator node. The analysis of the performance claims from the survey revealed that Tendermint seems to be the most scalable and promising permissioned blockchain available, assuming that the results from the previous Tendermint benchmark tests are still valid.

Tendermint consensus [109] is achieved through a set of identifiable validators that each hold and maintain a full replica of the entire blockchain. Validators take turns proposing new blocks (batches of transactions from its mempool), for each height (or round) of the blockchain. After a new block is proposed by a validator, the remaining validators then vote on the validity of the block proposal. Votes on the validity of a proposed block occurs over two phases; namely, the prevote and the precommit. Each phase of the voting must be approved by over 2/3 of all validators in order to be committed. Figure 6 offers a visualization of the Tendermint consensus process from the proposal stage to the commitment stage.

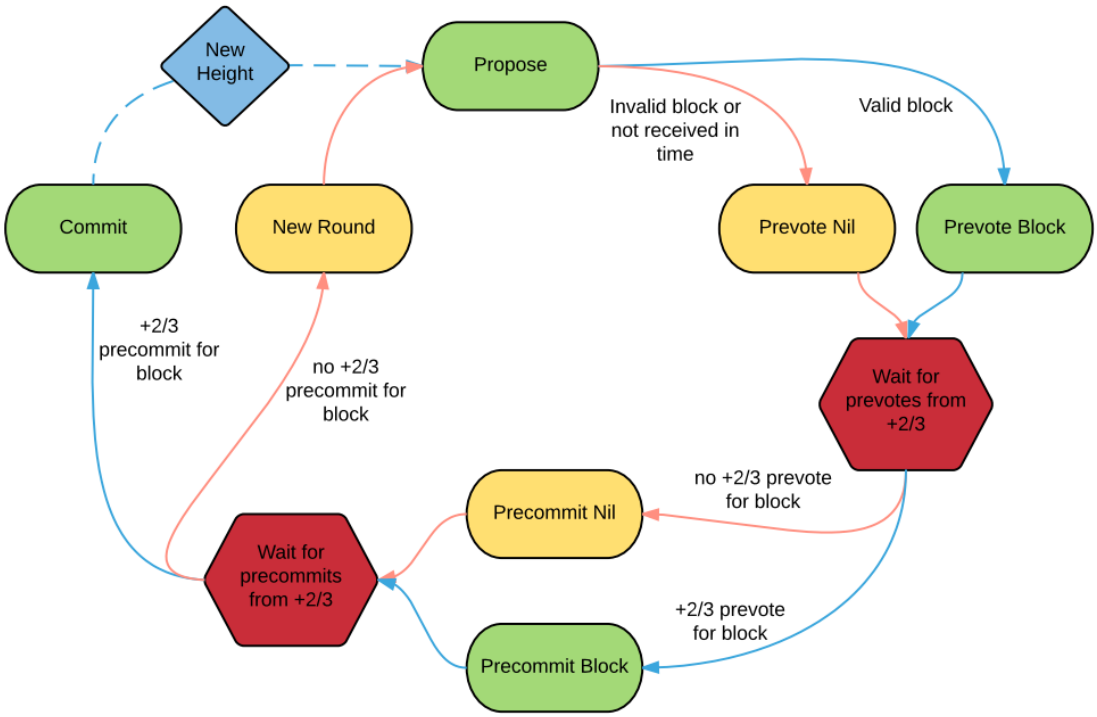


Figure 6: Tendermint consensus process [109]

When transactions are first received by a Tendermint node, they are placed in an in-memory cache known as a mempool. Since the mempool runs on memory, the maximum size of a mempool is restricted by the amount of RAM available. The mempool works as an ordered list where transactions stay until they are proposed in a block. Each node has its own mempool, and the default setting allows nodes to broadcast the transactions stored in their mempool to other nodes. Broadcasting transactions in this manner makes the system more resistant to failures and can decrease the amount of time it takes for a transaction to be added to the blockchain. If large amounts of transactions are being

added to the mempool, this broadcasting feature should be disabled [17]. The Tendermint protocol also maintains a cache used for filtering any transactions that the node has already seen [17].

The Tendermint blockchain features a web-based RPC protocol with an API that runs in each instance on port 26657. There are three different RPC endpoints that allow transactions to be added to the blockchain [115], and they are as follows:

The *broadcast_tx_async* endpoint returns immediately without waiting to find out if the transaction is even valid. It simply conveys the transaction to a validator, which then adds it to the mempool. The *broadcast_tx_sync* endpoint returns with the result of running the transaction through a built-in function called CheckTx. This CheckTx function checks the validity of the transaction on that single machine and then adds it to the mempool. The *broadcast_tx_commit* endpoint waits until the transaction has been committed and added to the blockchain and only then returns.

Tendermint uses blocks when storing transactions, which has multiple benefits. By batching transactions and storing them together in a block, Tendermint optimizes both throughput and data integrity. The consensus protocol requires that each commit fulfils two rounds of communication across all validators, thus allowing the cost of all transactions in a block to be amortized [109]. All blocks other than the first block (genesis block) are interlinked in that they store the previous block's block hash. A block hash is a combined hash of all the transactions and can be used to verify if any transactions have been changed. By combining batched hashing of transactions and the interlinking of the blocks, Tendermint is capable of efficiently validating the current state of the blockchain at any time and maintaining data integrity.

Similar to Bitcoin, Tendermint uses the Merkle tree data structure to implement blocks and block hashes [3][109].

In Figure 7 we introduce the architecture of the performance tests on the emissions monitoring system. A local machine connects via remote desktop to the master testing VM, which is hosted on the same Azure virtual network as the slave testing VMs. The master testing VM loads a test scenario that is run and synchronized on all of the slave testing VMs. The slave testing VMs follow the commands in the testing scenario, which tells the slaves to send https requests to the Tendermint validators through the RPC that accepts HTTPS requests. The testing scenario is also used for defining parameters such as the number of concurrent threads running, length of the tests, and size and content of the transactions being sent to the validators.

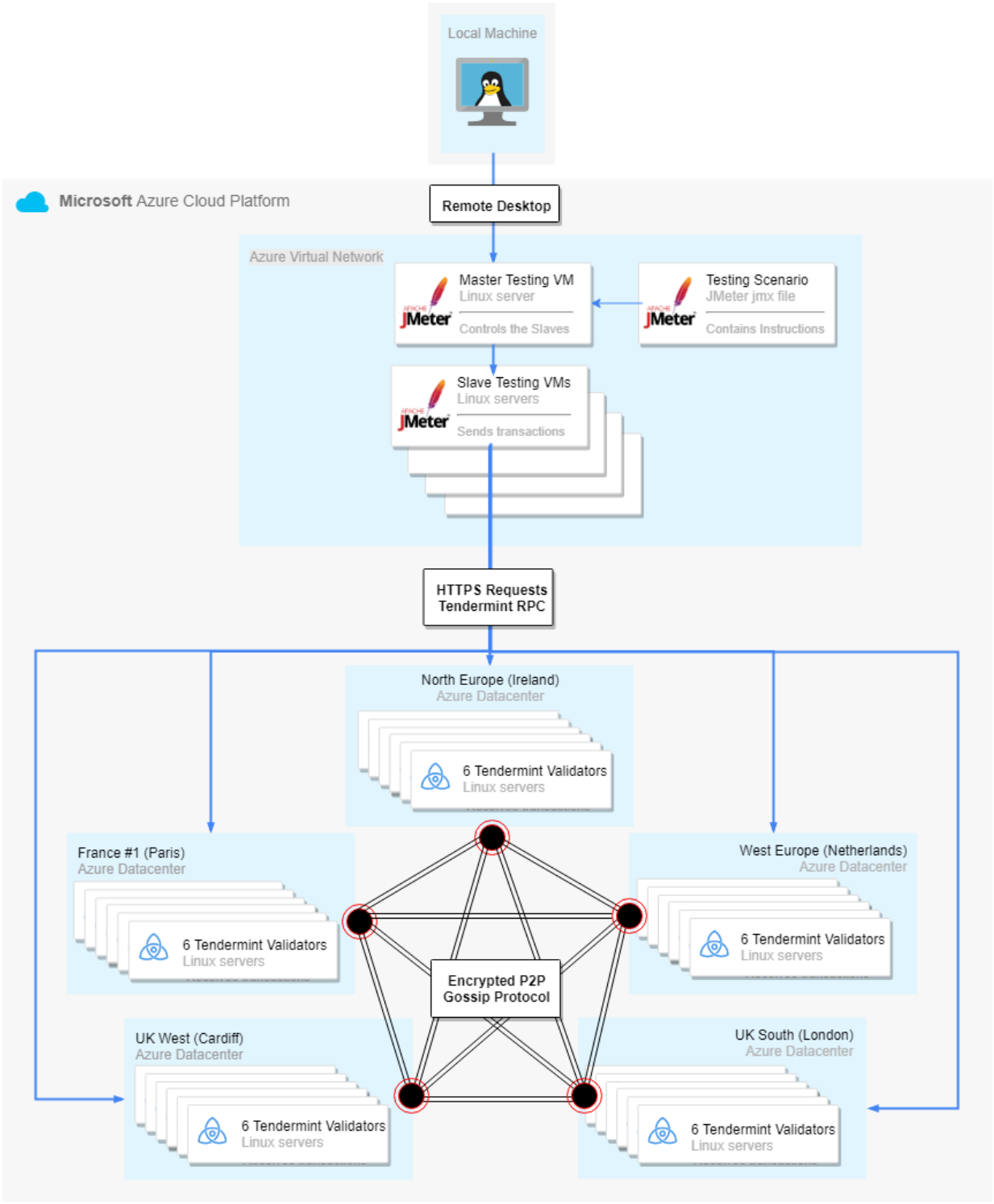


Figure 7: Performance-testing architecture for the emissions monitoring system

**The architecture used for the validator nodes in this simulation aims to replicate the EU consortium project, which will host validator nodes on cloud computing servers geographically spread across the EU**. Since the Azure cloud platform unfortunately does not have data centres in every EU country, we placed six validator instances in each of the five data centres found in the EU: Dublin, Paris, Cardiff, London, and Amsterdam.

All Tendermint validator virtual machines are hosted on 30 instances of Azure's F2sv2 series, which feature dual-core Intel® Xeon® Platinum 8168 processors with a single core frequency of 3.4GHz and a maximum turbo frequency of 3.7GHz. Each instance also features 4 GB of RAM with SSD storage running Debian version 9.6.

The main change made to the configuration was the disabling of mempool sharing. By default, Tendermint uses mempool sharing to force all validator nodes to broadcast their mempool transactions in to distribute the load between validators. Since the load in our tests is equally distributed across the various validators, enabling mempool sharing would cause an unwanted performance overhead [109]. The max number of open connections allowed by the Tendermint RPC was also increased to 9,000 in the configuration file. The size of the mempool and cache was also increased to 200mb to allow for a buffer of unprocessed transactions. We left the block size used in our tests at the default of 22mb due to the previous Tendermint benchmark tests that indicated that no performance gains are obtained by using larger block sizes.

We replicated the synthesized load of the onboard devices from the vehicles and gas stations through a distributed network of cloud computing servers running the Apache JMeter load testing software. Jmeter is an open-source load testing software created by Apache in the Java language. Jmeter synthesizes the load by running threads that concurrently send requests to specified targets. In our tests the targets are the Tendermint validators and the load being generated is equivalent to the HTTPS requests. Each validator runs a built-in Tendermint web API that accepts HTTPS requests via port 26657 (as designed by Tendermint).

The Java programming language relies on an automatic process called garbage collection to free up unused memory during run time. If garbage collection runs in the middle of a test it corrupts the test results; therefore, it is important that the Java virtual machine (JVM) that runs Java is properly configured. We logged of all garbage collection activity to improve visibility if tests were corrupted by garbage collection.

In an attempt to additionally bypass the complications of garbage collection, we distributed the load tests over multiple cloud virtual machines (VMs) called testing slave VMs, these slaves are controlled by a single VM called the testing master VM. All testing VMs are on the same virtual network so that the software can schedule and synchronize the entire load without the high latencies that would otherwise disrupt the test results.

Each of the testing slave VMs are hosted on four instances of Azure's F2sv2 series which feature dual-core Intel® Xeon® Platinum 8168 processors with a single core frequency of 3.4GHz and a maximum turbo frequency of 3.7GHz. Each instance also features 4 GB of RAM with SSD storage running Debian version 9.6.

The testing master virtual machine is hosted on one instance of Azure's F4sv2 series which features quad-core Intel® Xeon® Platinum 8,168 processors with a single core frequency of 3.4GHz and a maximum turbo frequency of 3.7GHz. This instance also features 8 GB of RAM with SSD storage running Debian version 9.6. All the aforementioned testing virtual machines are hosted at the West Europe Azure data centre.

We expected that our tests would not return the same high level of throughput as the previous Tendermint benchmark tests. The aforementioned benchmark tests were only run for a small sample size of 16 blocks. Given that block creation takes roughly one second according to their results [109], their tests would be based on a sample taken over roughly 18 seconds. All data was also preloaded locally to each validator in the benchmark tests from 2016; therefore, the time it takes to send transactions to the validators is not included in their results. Since the previous Tendermint tests are a benchmarking test, they did not have a motivation for including the cost of sending and receiving transactions across the Internet. Because our tests sought to simulate a real implementation for EmisChain, we did not preload any data. Instead, all transactions were sent from the Azure data centre in Holland.

The testing scenario starts by creating 40, 80, 160, 320, 640, 1,280 or 2,560 threads. Each thread concurrently sends HTTPS requests containing a single transaction to each of the 30 validator nodes using the selected RPC endpoint. **Each thread is only capable of handling one request at a time**, meaning that each thread must wait for each request to return before the next can be started.

The timeout of each request is **500 milliseconds to connect and five seconds to return**. The connection timeout value was chosen based on a study performed in 2014 [116] showing that the average latency across Europe is 27ms; therefore, using 500 milliseconds ensured that we had a buffer. The **return timeout value was chosen because it takes approximately one second to add a transaction to the blockchain** [17]. Each scenario runs for a total of 120 seconds, which provides a much larger sample size than the previous Tendermint benchmark tests, while also being short enough to avoid relying on virtual machines with large amounts of RAM allocated for the mempool. The contents of each transaction must be unique in order to be added to the blockchain; therefore, each transaction contains a thread number unique to each thread and an internal counter that iterates for each response. Each transaction is sized at 100 bytes, as this allows for storage of 100 characters per transaction. Since this project requires that only numerical emissions data are stored, **we decided on the 100-byte transaction size as an overestimate of the storage needed**. Tendermint's performance claims are based on tests with 250-byte transactions, which directly influenced our decision to use a comparable transaction size to make the analysis of the results more comparable. Testing with lower transaction sizes could improve performance and should be further studied.

The functionality of the emissions monitoring system requires that each onboard unit or gas station that sends a transaction knows whether the transaction was successfully added to the blockchain. Therefore, the requests made in the initial test are made using the broadcast_tx_commit endpoint, because this endpoint does not return until the transaction is added to the blockchain. This initial test was run with 40 to 2,560 threads; but regardless of the number of threads, **the throughput only reached an average of 750 transactions per second**. The **average response time for adding a transaction to the blockchain was 2.6 seconds**. This initial test failed to satisfy the project requirements and our expectations, which used Tendermint's performance claims as a guideline.

Given that the initial test results using the broadcast_tx_commit endpoint did not meet the project requirements, we instead looked toward the broadcast_tx_async as a possibility for achieving a higher throughput. In contrast to the broadcast_tx_commit endpoint, the broadcast_tx_async endpoint does not wait for each transaction to be added to the blockchain before returning. This endpoint simply queues a transaction and returns, meaning 640 threads were capable of queuing transactions at a rate of 12,800 transactions per second. The throughput results for this test in isolation merely confirm how many transactions can be queued per second; therefore, a separate Apache JMeter instance was used to query the blockchain at 10-second intervals, asking how many transactions had been added to the blockchain.

As the emissions monitoring system is expected to handle more than 600 million transactions per day, the size of each transaction will have a great impact on the potential performance and growth of the blockchain. **Since blockchains are immutable, there is no way of removing old data; thus, long-term data storage could be a potential problem** [117]. Each of the transactions sent from either the gas stations or the onboard devices only contain a number; therefore, we chose to test using a transaction size of 100 bytes (or 100 characters), which will allow for future expansion.

Each of the validator nodes only have limited RAM shared between running the operating system and the Tendermint blockchain, which includes the mempool and cache. When initially running the tests, **it became evident that the mempool became overloaded in a short amount of time, which made it impossible to run tests for longer periods of time**. In the production environment, each machine running a blockchain valida-

tor would require a large amount of RAM as a buffer to prevent such overloading. A single GB of RAM can store over 10 million transactions at a size of 100 bytes before it overloads, meaning a 64GB RAM could be a viable option.

| Threads | Average Throughput |
|---|---|
| 640 | 2,127 tps |
| 320 | 2,518 tps |
| 160 | 2,126 tps |
| 80 | 1,650 tps |
| 40 | 1,147 tps |

Table 3: Average throughput using multiple threads

The following graph in Figure 10 compares the test results of the aforementioned test scenario run with five thread settings—namely, 40, 80, 160, 320, and 640. The results are plotted such that the number of transactions committed is shown over a 120-second time frame. Table 3: Average throughput using multiple threads presented in Table 3 reveals the average transactions per second for the same test results that are plotted in Figure 10.

Figure 10 demonstrates that the **highest throughput was achieved in the test with 320 Threads, with an average of 2,518 transactions committed per second**. The test with 640 threads could not process as many transactions as the test with 320 threads, this was due to validator nodes that crashed, causing the mempool to overload. The throughput of transactions being queued with 640 threads was too high, such that validators could not commit transactions fast enough to prevent the mempool from overloading. With 320 threads it was possible to queue transactions at a rate that was faster than transactions could be committed, and 120 seconds was a short enough time frame to avoid mempool overload. Since the number of transactions queued per second with 320 threads was much greater than the number of transactions committed, we can be certain that the we reached the maximum average throughput of transactions committed per second. It is also visible in the graph from Figure 10 that the runs using less than 320 threads were not queueing enough transactions to meet the maximum throughput of 2,518 transactions per second. From the tests run with 320 threads, we can confirm that the maximum average throughput for this test setup is 2,518 transactions per second.

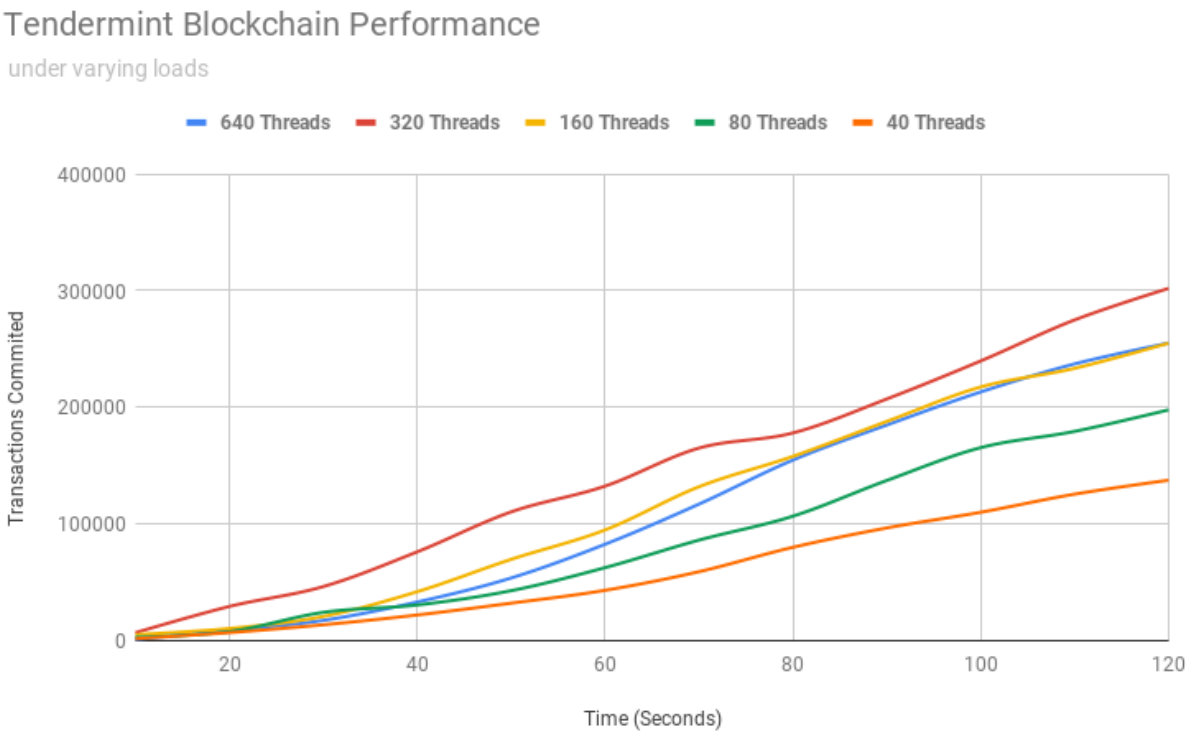


Figure 8: Transactions committed over 120 seconds using multiple threads

The previous Tendermint benchmark tests were capable of committing over 4,000 transactions per second with 32 validators spread over seven data centres spanning five continents. The size of the transactions in these previous tests were set to 250 bytes; but unlike our tests, all transactions where preloaded onto each validator node. The preloading of the tests disregards the two-way latency involved with sending and receiving requests. The sample size of the previous Tendermint benchmark tests is also only 16 blocks or ~16 seconds, which is potentially too small to return a realistic result. Finally, the previous tests were also run on a version of Tendermint that was over two years old. The variance in our results compared with the previous Tendermint benchmark tests could come down to any or a combination of the abovementioned differences.

The test results revealed that the **Tendermint blockchain is only capable of handling 2,518 transactions per second**, but in order to meet the project requirements we would require a blockchain capable of handling over 7,000 transactions per second. This lack of performance implies that **running the whole system on a single blockchain is not feasible for this project**, although alternative approaches, such as scaling the blockchain horizontally, remain viable options. We discuss horizontal scaling, also known in database terminology as sharding, in Chapter 4.3.

## 4.3 EmisChain system specifications and requirements

The test results analysed in Chapter 4.2 confirmed that by running tests with the broadcast_tx_commit RPC, a throughput above 750 transactions per second cannot be achieved. This prompted us to test with the broadcast_tx_async RPC, which allowed us to reach a throughput of 2,518 transactions per second. The broadcast_tx_async endpoint is missing an important piece of functionality; namely, it does not confirm whether a transaction has been added to the blockchain. This missing functionality could be supplemented with a query call that takes place a certain amount of time (*n* minutes) after a transaction is initially queued, if after *n* minutes the transaction is not added then it

would be requeued. This procedure could repeat until the transaction is confirmed as added to the blockchain. **Querying the blockchain would take place on nonvalidator (sentry) nodes, thus not using the valuable resources of the validator nodes**. Requeuing transactions in this manner can only operate in a blockchain like Tendermint where replica transactions cannot exist.

As mentioned in the previous section, the use of **multiple blockchains could be used to obtain a higher level of performance**, meaning the **load could be split over multiple blockchains running in parallel. This is commonly referred to as sharding** [118]. Sharding could help lower the performance and scalability requirements of this project by distributing the load.

An example of a possible sharding scenario would be if **each of the 28 countries that make up the EU country ran 28 validator nodes with each node running a separate blockchain.** This would allow for each country to have a separate blockchain containing only their data, but because each of the 28 blockchains would have 28 validators, it would ensure the same level of security as using a single blockchain. This approach would allow for a **separation of concerns** [119] **regarding each country's data storage** while maintaining a decentralized network where no single validator node is capable of change the data.

By using the sharding approach, **the scalability and performance requirements would be set by the country with the most vehicles**. As of January 2018, based on data from the KBA [120], Germany had a total of 63.7 million registered vehicles. By using the project requirements from Chapter 2, the system would therefore have to handle two transactions per day per vehicle and one refuelling transaction per week per vehicle. We can thus estimate that **Germany alone will require a total of 136.5 million transactions per day**. 136.5 million transactions, if processed over a 24-hour period would **equal 1,580 transaction per second**.

Our simulation results reveal that Tendermint runs in a similar environment as that needed by the EU and can handle an average of 2,518 transactions per second. **If the sharding approach is used, the project requirements would drop to 1,580 transactions per second, thus making Tendermint a feasible option.** Such a system could be further sharded by creating separate blockchains for each type of vehicle.

Scheduling algorithms are known for being difficult to optimize and not entirely reliable [121]; therefore, we cannot assume that all transactions will be perfectly scheduled to ensure a stable 1,580 transactions per second over 24 hours. Queues are currently used in Tendermint to keep track of all transactions in the mempool waiting to be inserted into the blockchain. Using machines with large amounts of RAM and using a configuring Tendermint to use a large mempool would offer a buffer to accommodate nonoptimal scheduling and would improve the system's ability to withstand malicious attacks when the mempool is overloaded.

The transactions that are inserted to the blockchain will come either from the onboard vehicle device or from a gas station. It is possible to roughly schedule the transactions from the onboard devices, as they are fixed at twice daily, but **gas station transactions are too unpredictable** to schedule. **It is therefore important that the system can handle use cases where all gas stations would be concurrently queueing transactions**. A statistical report for the year 2016 [88] indicates that Germany has 14,510 gas stations, the most in the EU. Not counting transactions from gas stations, German onboard devices would require 1,475 transactions per second, and given that Tendermint can handle 2,518 transactions per second, 1,043 (2518-1475) of throughput would remain available for gas stations. Since no data are available for the number of pumps at gas stations in Germany, we estimate that each gas station has eight pumps capable of processing payments. **If all gas station pumps in Germany were to concurrently send transactions, the system would require at least 78.4 seconds between each vehicle engaged in refuelling to stay within the throughput limit of 1,043 transactions per second**. We can thus safely assume that the system can be config-

ured with a large enough mempool to withstand any such scenario, especially given the unlikely event that every gas station pump in Germany were to be concurrently engaged in refuelling, and also considering the time it would take for each vehicle to refuel a vehicle and pay for the gas.

As the system is currently implemented for testing in its current state, it is **vulnerable to DDoS** attacks due to the **validator nodes being publicly accessible on the Internet**. The only way **to overcome a DDoS attack on Tendermint is to use sentry node architecture** [103], such that nonvalidator nodes act as a proxy by obfuscating the real location of the validator nodes. These sentry nodes would hold a full copy of the blockchain and be connected to the validator nodes via Tendermint's encrypted p2p protocol. Sentry nodes are allowed to propose transactions but do not participate in the validation. Sentry nodes should be placed on the same network as validators so that latency overhead would be almost nonexistent and have little impact on performance. The mempool of the Sentry nodes also acts as a queue for all transactions waiting to be added to the blockchain; therefore, it is important to have sufficient nodes with sufficient RAM allocated for the mempool.

One attack potential for this application is **tampering with the physical onboard devices**. Tampering with the software running the onboard devices could allow incorrect data to be sent to the blockchain in an attempt to cheat the system. **Thus, gas stations must also submit transactions in order to validate the data sent from the onboard devices**. If the software that sends transactions from the gas stations is tampered with, it would potentially leave the system vulnerable to incorrect data being uploaded via corrupted onboard devices. If such an attack were to occur, it would perhaps be hard to detect, but since data stored on the blockchain are immutable, we can be confident that hypothetical attackers would not be able to modify data to cover their tracks on the blockchain.

System failures in large-scale systems can be difficult to predict; as the renowned computer scientist Dijkstra once stated, "Testing shows the presence, not the absence of bugs" [122]. We cannot plan for what we do not understand; therefore, it is important to know how long the recovery time for such a system would be if it were to fail. Below we provide a formula to calculate exactly how many hours would it take for the blockchain to recover and catch up with missing transactions.

*n * TSPH / (ATPH-TSPH)*

*n = hours of failure*

*TSPH = Transactions sent per hour*

*ATPH = Average throughput per hour*

Below is a concrete example illustrating 24 hours of failure using the project specifications for this project with sharding:

*24 * 1580 / (2518-1580) = 40.42 hours to recover*

The storage capacity needed for this project is feasible, even though all data on the blockchain are immutable. **If 100 characters were to be stored per transaction (100 bytes) using the abovementioned system and project specifications, with sharding it would cause the blockchain to increase at a rate of 13.65 gigabytes per day (4.98 terabytes per year).** As the prices of data storage are steadily decreasing, while the sizes of drives are increasing [123], the cost of storage will not be problematic. As the blockchain grows in size, the time required to synchronize will also increase. For example, if a validator node must format its hard drive and must therefore synchronize with the blockchain in its current state, this would mean the whole blockchain would have to be downloaded and verified. The Tendermint blockchain has an optimized synchronizing feature called fast sync [124], but if the blockchain contains terabytes of data, it could take days or even weeks to download and synchronize. It is im-

portant to note that the system will continue to function as normal while synchronizing is taking place, as long as over two thirds of all validators continue to validate.

**In the following, we provide an overview of the proposed system which is based on the research conducted for this report.**

The main technical observation from this report is that a permissioned public blockchain that is sharded would be an optimal design choice. We propose that **the 28 countries that make up the EU would each run 28 Tendermint validator nodes.** Each validator node would contain data for only one of the countries. Each country should also run as many sentry nodes (nonvalidator nodes) as possible, which will queue and buffer all incoming transactions. These sentry nodes will need to be on the same virtual network as the validator nodes. All onboard devices are scheduled to send transactions to the sentry nodes in that country twice per day. All gas stations will send transactions to the sentry nodes as each vehicle refuels. The sentry nodes will transfer all transactions to the validators.

The machines running the validator nodes must reach the required system requirements from the Tendermint documentation [125]. Machines running the sentry nodes will require the same system requirements as validator nodes, but with much more RAM. The size of the RAM will depend on how many sentry nodes are created and how much of a buffer is desired.

The size of the mempool and cache must be adjusted accordingly in the configuration file to assure it matches the RAM. Two potential technical issues that may need further investigation include: the data integrity of transactions and retesting with different transaction sizes.

# 5 Recommendations and Conclusions

Blockchain is a technology that enables various industries to gain a competitive advantage over those that rely only on traditional technologies like databases. As blockchain is a young technology, the adoption for large-scale applications in production is not yet common. There is explicit interest in adopting blockchain for large-scale applications, indicated by the number of pilot projects and the general investment in development using blockchain.

Given the requirements for EmisChain, we have demonstrated and outlined a guideline of how to implement a blockchain-based monitoring system and how to determine which blockchain technology is best-suited for a given project, in light of its requirements. We further determined that the EmisChain project would require a permissioned public blockchain. The monitoring system specifications make assumptions regarding the integrity of the data sent and the security of the communication; these two important subjects require further research.

The tests described in this report demonstrate the performance, various bottlenecks, and feasibility of using a permissioned blockchain to store all carbon emissions data for over 300 million vehicles. Using the analysis of the test results, we proposed the architecture and functionality of the EmisChain project using the permissioned blockchain called Tendermint. The proposed architecture and functionality assume that all transactions are scheduled, which is a key subject that also requires further research.

As of December 2018, our recommendations for the proposed architecture and functionality for implementing such a system are current; however, one must keep in mind that in the near future these recommendations may become outdated in favour of blockchains like the RedBelly blockchain discussed above. From a security perspective, in order to further develop the EmisChain project, more research should also be done in the areas of tamperproof hardware and protection against cyberattacks.

Regarding emissions trading, the proposed system has been designed to address problems regarding future emissions-prediction difficulties, the fairness of granting emissions allowances, and issues concerning data resiliency and the potential for data manipulation invoked by previously attempted solutions. This has been done both by exploiting blockchain features and by creating an ad hoc mechanism for trading.

The proposed emissions trading system is a variation of a so-called cap-and-trade system. This approach requires granting users an initial amount of emissions allowances. Assuming users comply with their emissions allowances, the system guarantees a cap on the total emissions of CO2.

The proposed implementation using smart contracts allows emissions allowances to be traded in a completely peer-to-peer manner among the users of the emissions trading system. The suggested mechanism to trade emissions allowances is a Dutch auction. In the context of a blockchain, it means that exactly one transaction is required to sell an emissions allowance and the workload of the system is kept as low as possible.

While a seller is allowed to set an initial price and a reserve price for every emissions allowance she or he wants to sell, a safety valve system is recommended. In other words, the regulator can set a floor and ceiling price for emissions allowances to prevent carbon emissions allowances from being traded at a price that is below the threshold needed to reduce emissions effectively.

In order to incentivize users of the system to behave according to the amount of emissions allowances they own, we propose different potential feedback mechanisms from the system: fines, a social score mechanism, and the inability to purchase gas in certain situations.

As of December 2018, we recommend implementing the described emissions trading system on Ethereum, which is currently the most commonly used blockchain with smart contract functionality.

Taking into consideration that the European Union wants to control who can serve as a validator in the network, we propose a permissioned version of Ethereum that is public in the context of the European Union.

Finally, we suggest implementing a prototype of both the emissions monitoring system and the emissions trading system so that the economical functioning and environmental effectiveness can be validated in different scenarios. Further load testing with an increased parameter space (such as transaction size) of the above-mentioned prototypes would reduce the likelihood of system failure in production, while also providing an increased understanding of how to optimize these systems.

## References


[1] World Economic Forum's Meta-Council on Emerging Technologies, "Top 10 Emerging Technologies of 2016," 2016.

[2] Gartner, "Forecast: Blockchain Business Value, Worldwide, 2017-2030." .

[3] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[4] B. Warburg, "How the blockchain will radically transform the economy," *2016*, 2017.

[5] R. Beck, "Beyond Bitcoin: The Rise of Blockchain World," *Computer (Long. Beach. Calif).*, vol. 51, no. 2, pp. 54–58, 2018.

[6] "Blockchain technology: Beyond bitcoin," *j2-capital.com*.

[7] X. Xu *et al.*, "A taxonomy of blockchain-based systems for architecture design," in *Software Architecture (ICSA), 2017 IEEE International Conference on*, 2017, pp. 243–252.

[8] The Linux Foundation, "Blockchain: Understanding Its Uses and Implications," 2018. [Online]. Available: https://www.edx.org/course/understanding-blockchain-and-its-implications.

[9] F. Cristian, "Understanding fault-tolerant distributed systems," *Commun. ACM*, vol. 34, no. 2, pp. 56–78, 1991.

[10] B. . Castro, M., & Liskov, "U.S. Patent No. 6, 671, 821. Washington, DC: U.S. Patent and Trademark Office.," 2003.

[11] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," *ACM Trans. Program. Lang. Syst.*, vol. 4, no. 3, pp. 382–401, 1982.

[12] I. Sommerville, *Software engineering (1st ed.)*. 2011.

[13] C. Dwork and M. Naor, "Pricing via Processing or Combatting Junk Mail," in *Advances in Cryptology — CRYPTO' 92*, Berlin, Heidelberg: Springer Berlin Heidelberg, 1992, pp. 139–147.

[14] Nxt Community, "Nxt Whitepaper," 2014.

[15] P. Vasin and B. Co, "BlackCoin's Proof-of-Stake Protocol v2."

[16] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Big Data (BigData Congress), 2017 IEEE International Congress on*, 2017, pp. 557–564.

[17] E. Buchman, "Tendermint: Byzantine fault tolerance in the age of blockchains," 2016.

[18] E. Androulaki *et al.*, "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *Proceedings of the Thirteenth EuroSys Conference*, 2018, p. 30.

[19] G. Greenspan, "MultiChain Private Blockchain-White Paper."

[20] V. Gramoli, "From blockchain consensus back to byzantine consensus," *Futur. Gener. Comput. Syst.*, 2017.

[21] P. Todd, "Ripple Protocol Consensus Algorithm Review," 2015.

[22] M. Vukolić, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," in *International Workshop on Open Problems in Network Security*, 2015, pp. 112–125.

[23] D. Patrick, N. Mahi, J. Earls, and A. Norta, "Smart-Contract Value-Transfer Protocols on a Distributed Mobile Application Platform." [Online]. Available: https://qtum.org/user/pages/01.home/Qtum whitepaper_en v0.7.pdf.

[24] M. Bhutoria, "Qtum," 2018. [Online]. Available: https://www.circle.com/marketing/pdfs/research/circle-research-qtum.pdf.

[25] "http://www.oraclize.it/." .

[26] B. Marr, "35 Amazing Real World Examples Of How Blockchain Is Changing Our World," 2018. .

[27] J. MyungSan, "Blockchain government-a next form of infrastructure for the twenty-first century," *mdpi.com*, vol. 4, p. 7, 2018.

[28] Y. Cai and D. Zhu, "Fraud detections for online businesses: a perspective from blockchain technology," *Financ. Innov.*, vol. 2, no. 1, p. 20, Dec. 2016.

[29] P. Mamoshina *et al.*, "Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare," *ncbi.nlm.nih.gov*, vol. 9, pp. 5665–5690, 2018.

[30] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control," *J. Med. Syst.*, vol. 40, p. 218, 2016.

[31] G. Zyskind, O. Nathan, and A. "Sandy" Pentland, "Decentralizing privacy: Using blockchain to protect personal data," *IEEE*, pp. 180–184, 2015.

[32] M. Iansiti and K. R. Lakhani, "The truth about blockchain," 2017.

[33] T. Feng, "An agri-food supply chain traceability system for China based on RFID and blockchain technology," *2016 13th Int. Conf. Serv. Syst. Serv. Manag.*, pp. 1–6, 2016.

[34] Gartner, "Top Trends in the Gartner Hype Cycle for Emerging Technologies, 2017," 2017. .

[35] Developerworks IBM, "Develop, govern, and operate your business network with the IBM Blockchain Platform," Mar-2018. .

[36] Statista, "Block chain market share by sector 2018 | Statistic," *Statista*, 2018. .

[37] Accenture, "International Payments in a digital world," 2017. .

[38] L. Myler, "Transparent Transactions: How Blockchain Payments Can Make Life Easier For B2B Companies," *Forbes*, 2017. .

[39] Santander, "Santander launches the first blockchain-based international money transfer service across four countries," 2018. .

[40] Ripple, *xRapid Brings on Three New Exchange Partners*. 2018.

[41] PwC, "Financial services qa. Blockchain in mortgage," 2016. .

[42] Deloitte, "How Blockchain Can Reshape Trade Finance." .

[43] M. Gupta, "Blockchain For Dummies®, 2nd IBM Limited Edition," p. 51, 2018.

[44] T. ACAMS, "The Future of Anti-Money Laundering Compliance.," 2018. .

[45] N. Patel, "R3 Reports. Blockchain KYC/AML utilities for International Payments," 2017. [Online]. Available: https://www.r3.com/wp-content/uploads/2018/02/blockchain_kyc_aml_utilities_R3.pdf.

[46] KPMG International, "Could blockchain be the foundation of a viable KYC utility?," p. 8, 2018.

[47] Deloitte, "When two chains combine. Supply chain meets blockchain," 2017. .

[48] IBM, "Blockchain for Food Safety," Aug-2017. .

[49] K. S. Nash, *Farm to Cradle: Nestlé Experiments with Tracking Gerber Baby Food on the Blockchain*. 2018.

[50] J. Henderson, "94 companies sign up to IBM/Maersk blockchain initiative," 2018. .

[51] The Washington Post, "Five dead, nearly 200 sick in E. coli outbreak from lettuce. And investigators are stumped.," *Washington Post*, 2018. .

[52] Everledger, "Everledger | A Digital Global Ledger," 2018. .

[53] Provenance, "Every product has a story," *Provenance*, 2018. .

[54] M. White, "Digitizing Global Trade with Maersk and IBM," *Blockchain Unleashed: IBM Blockchain Blog*, Jan-2018. .

[55] K. Nærland, C. Müller-Bloch, R. Beck, and S. Palmund, "Blockchain to Rule the Waves - Nascent Design Principles for Reducing Risk and Uncertainty in Decentralized Environments," p. 17, Dec. 2017.

[56] e-Estonia, "e-Health Records," *e-Estonia*, 2018. .

[57] "KSI Blockchain." [Online]. Available: https://e-estonia.com/solutions/security-and-safety/ksi-blockchain/.

[58] FarmaTrust, "FarmaTrust Whitepaper v10." Mar-2018.

[59] MediLedger, "MediLedger - Blockchain solutions for Pharma companies," 2018. .

[60] Change Healthcare, "Change Healthcare Announces General Availability of First Enterprise-Scale Blockchain Solution for Healthcare," *Default*, Aug-2018. .

[61] World Economic Forum, "No currency can compete: Here's why the US dollar still rules," *World Economic Forum*, 2017. .

[62] Deloitte, "Blockchain @ Media. A new Game Changer for the Media Industry?," 2017. .

[63] Juniper Research, "Sharing Economy Revenues to Double by 2022, Reaching Over $40 billion," 2017. .

[64] S. Williamson, "Blockchain Solutions Are Changing the Sharing Economy," *NASDAQ.com*, May-2018. .

[65] D. Tapscott and A. Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. Portfolio, 2016.

[66] R. Maino, "International Monetary Fund. Leveraging Financial Technology for the Underbanked," *IMF*, 2018. .

[67] BBVA, *Blockchain opens the door for those who still do not have a bank account*. 2018.

[68] M. Novak, "The Implications of Blockchain for Income Inequality," *SSRN Electron. J.*, 2018.

[69] C. Brennan, B. Zelnick, M. Yates, and W. Lunn, "Cryptocurrencies are only the beginning. Credit Suisse," 2018. .

[70] "Maersk and IBM Unveil First Industry-Wide Cross-Border Supply Chain Solution on Blockchain." [Online]. Available: https://www-03.ibm.com/press/us/en/pressrelease/51712.wss.

[71] "ZIM's Groundbreaking Blockchain-Based Bill of Lading," 2017. .

[72] Blockshipping, "The Blockshipping ICO white paper," 2018.

[73] D. T. Research, "Blockchain in Logistics," 2018.

[74] C. Gutierrez, "A Close Look at Everledger—How Blockchain Secures Luxury Goods," 2017. .

[75] R. Kamath, "Food Traceability on Blockchain: Walmart's Pork and Mango Pilots with IBM," *J. Br. Blockchain Assoc.*, vol. 1, pp. 1–12, 2018.

[76] C. R. Portal, "19 Corporations Working On Blockchain And Distributed Ledgers," 2018. .

[77] E. Xiao, "Alibaba, JD tackle China's fake goods problem with blockchain," 2017. .

[78] A. Stanley, "Accenture Showcases Blockchain Prototype For Aerospace Supply Chains At Farnborough Air Show," 2018. .

[79] K. Wust and A. Gervais, "Do you need a Blockchain?," *2018 Crypto Val. Conf. Blockchain Technol.*, pp. 45–54, 2017.

[80] Christina Luchetta, "A Revolution in Trust: Distributed Ledger Technology in Relief and Development," 2017.

[81] B. Perez, "Alibaba affiliate Ant Financial to accelerate blockchain initiatives," 2017.

[82] *Dubai - The First City on the Blockchain*. 2017.

[83] "Deloitte National Transformation in the Middle East A Digital Journey."

[84] M. Tegos, "Singapore's central bank is ready to use the blockchain for inter-bank payments," 2017. .

[85] Jeremy, "Microsoft And Accenture Aid ID2020 Partnership With Enterprise Ethereum Alliance Permissioned Blockchain Protocol," 2017.

[86] A. Makadiya, "Commonwealth Bank of Australia Ships Almonds in Blockchain Pilot," 2018. .

[87] Marie Huillet, "Chinese State-Owned Aerospace Firm Turns to Blockchain to Manage Billions of Invoices," 2018. .

[88] N. Eu, "Statistical Report 2017-Marketing Infrastructures Unit: Number of petrol stations."

[89] J. Dai and M. A. Vasarhelyi, "Toward blockchain-based accounting and assurance," *J. Inf. Syst.*, vol. 31, no. 3, pp. 5–21, 2017.

[90] E. Gaetani, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, "Blockchain-based database to ensure data integrity in cloud computing environments," 2017.

[91] R. N. Stavins, "Experience with market-based environmental policy instruments," in *Handbook of environmental economics*, vol. 1, Elsevier, 2003, pp. 355–435.

[92] A. D. Ellerman and B. K. Buchner, "The European Union emissions trading scheme: origins, allocation, and early results," *Rev. Environ. Econ. policy*, vol. 1, no. 1, pp. 66–87, 2007.

[93] C. C. Committee and others, "Building a low-carbon economy-the UK's contribution to tackling climate change," *Station. Off. London*, 2008.

[94] N. Nisan, T. Roughgarden, E. Tardos, and V. V Vazirani, *Algorithmic game theory*. Cambridge University Press, 2007.

[95] M. L. Weitzman, "Prices vs. quantities," *Rev. Econ. Stud.*, vol. 41, no. 4, pp. 477–491, 1974.

[96] International Monetary Fund. March 2008. pp. 25–26. Retrieved 2010-04-26., "Fiscal Implications of Climate Change (PDF)." .

[97] C. Hepburn, "Regulating by prices, quantities or both: an update and an overview," *Oxford Rev. Econ. Policy*, vol. 22, no. 2, pp. 226–247, 2006.

[98] "Climate change; The greening of America. The Economist. 2007-01-25. Retrieved 2009-04-03." .

[99] B. S. Fisher *et al.*, "An economic assessment of policy instruments for combatting climate change," 1995.

[100] "ACEA Report Vehicles in use Europe, European Automobile Manufacturers Association," 2018.

[101] "Number of petrol stations in Europe end of 2016. National Oil Industry Associations, FPS Economy, DG Energy." [Online]. Available: https://www.fuelseurope.eu/wp-content/uploads/2015/06/Graphs_FUELS_EUROPE-_2017_-52.pdf.

[102] "Understanding Denial-of-Service Attacks. US-CERT. 6 February 2013. Retrieved 26 May 2016." .

[103] "https://forum.cosmos.network/t/sentry-node-architecture-overview/454." .

[104] V. Buterin and others, "Ethereum white paper, 2014," *URL https//github. com/ethereum/wiki/wiki/White-Paper*, 2013.

[105] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology?—a systematic review," *PLoS One*, vol. 11, no. 10, p. e0163477, 2016.

[106] M. Sharples and J. Domingue, "The blockchain and kudos: A distributed system for educational record, reputation and reward," in *European Conference on Technology Enhanced Learning*, 2016, pp. 490–496.

[107] Y. Yuan and F.-Y. Wang, "Towards blockchain-based intelligent transportation systems," in *Intelligent Transportation Systems (ITSC), 2016 IEEE 19th International Conference on*, 2016, pp. 2663–2668.

[108] S. Bano *et al.*, "Consensus in the age of blockchains," *arXiv Prepr. arXiv1711.03936*, 2017.

[109] E. Buchman, "Tendermint: Byzantine fault tolerance in the age of blockchains," The University of Guelph, 2016.

[110] C. Cachin and M. Vukolić, "Blockchains consensus protocols in the wild," *arXiv Prepr. arXiv1707.01873*, 2017.

[111] "Apache Kafka." [Online]. Available: https://kafka.apache.org/. [Accessed: 17-Oct-2018].

[112] P. Thakkar, S. Nathan, and B. Vishwanathan, "Performance Benchmarking and Optimizing Hyperledger Fabric Blockchain Platform," *arXiv Prepr. arXiv1805.11390*, 2018.

[113] J. Kreps, N. Narkhede, J. Rao, and others, "Kafka: A distributed messaging system for log processing," in *Proceedings of the NetDB*, 2011, pp. 1–7.

[114] C. Chelvan, "Next generation blockchain boosts speed and energy efficiency on global scale," 2018. [Online]. Available: https://www.csiro.au/en/News/News-releases/2018/Next-generation-blockchain-boosts-speed-and-energy-efficiency-on-global-scale. [Accessed: 29-Sep-2018].

[115] "Using Tendermint | Tendermint Documentation." [Online]. Available: https://tendermint.com/docs/tendermint-core/using-tendermint.html#broadcast-api. [Accessed: 09-Nov-2018].

[116] S. Limited, "Quality of Broadband Services in the EU," 2014.

[117] S. A. Abeyratne and R. P. Monfared, "Blockchain ready manufacturing supply chain using distributed ledger," 2016.

[118] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, "A Secure Sharding Protocol For Open Blockchains," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS'16*, 2016, pp. 17–30.

[119] W. L. Hürsch and C. V. Lopes, "Separation of concerns," 1995.

[120] Henk Bekker, "2018 Germany: Total Number of Registered Cars - Car Sales Statistics," 2018. [Online]. Available: https://www.best-selling-cars.com/germany/2018-germany-total-number-registered-cars/. [Accessed: 11-Oct-2018].

[121] A. Allahverdi, C. T. Ng, T. C. E. Cheng, and M. Y. Kovalyov, "A survey of scheduling problems with setup times or costs," *Eur. J. Oper. Res.*, vol. 187, no. 3, pp. 985–1032, 2008.

[122] J. N. Buxton and B. Randell, *Software Engineering Techniques: Report on a Conference Sponsored by the NATO Science Committee*. NATO Science Committee; available from Scientific Affairs Division, NATO, 1970.

[123] G. Nagle and L. Geosystems, "Image Archiving: An Opportunity and a Burden."

[124] "Fast Sync | Tendermint Documentation." [Online]. Available: https://tendermint.com/docs/tendermint-core/fast-sync.html. [Accessed: 08-Dec-2018].

[125] "Running in production | Tendermint Documentation." [Online]. Available: https://tendermint.com/docs/tendermint-core/running-in-production.html#hardware. [Accessed: 08-Dec-2018].