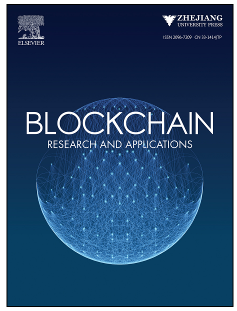
Journal Pre-proof



Blockchain-based internet of musical things

Luca Turchet, Chan Nam Ngo

PII: S2096-7209(22)00024-0

DOI: https://doi.org/10.1016/j.bcra.2022.100083

Reference: BCRA 100083

To appear in: *Blockchain: Research and Applications*

Received Date: 18 August 2021

Revised Date: 16 March 2022

Accepted Date: 2 April 2022

Please cite this article as: L. Turchet, C.N. Ngo, Blockchain-based internet of musical things, *Blockchain: Research and Applications* (2022), doi: https://doi.org/10.1016/j.bcra.2022.100083.

Blockchain-based Internet of Musical Things

Luca Turchet[1,*], Chan Nam Ngo[2,*]

Abstract

Blockchain technology is impacting several industries, including the creative industries and those operating in the Internet of Things (IoT). Lately, researchers' attention has been devoted to the application of blockchain in the recorded music industry. However, thus far, no research has investigated the use of such technology in the Internet of Musical Things (IoMusT). The IoMusT is a new area emerging in the industry and in the academy as the extension of the IoT to the musical domain. The IoMusT itself, as the IoT, is a distributed network of Musical Things, which are objects augmented with information and communication technologies serving a musical purpose. The IoMusT vision requires, above all, IoT features such as decentralization, seamless authentication, transparency, data integrity and privacy, and self-maintenance, as well as the musical domain's feature such as efficient handling of copyrights and speed of royalties payment. Such features can be brought by blockchain. In this paper, we investigate the integration of blockchain technology with the IoMusT, and we name such synthesis as "Blockchain-based IoMusT". We present a vision for this new paradigm in terms of the novel opportunities that are enabled, as well as we propose a set of application scenarios enabled by the technological integration. Finally, we outline the open research directions in this promising area.

Keywords: Internet of Musical Things, Blockchain, music industry, privacy, security, Internet of Things

1. Introduction

The Internet of Musical Things (IoMusT) [1] is a branch of the Internet of Things (IoT) that specifically targets the musical sector and its many stakeholders (including performers, amateur musicians, audience members, music students and teachers, studio producers, labels, publishers, sound engineers). It is an emerging field of research positioned at the confluence of IoT-related disciplines (such as electronics engineering and telecommunications) and music technology disciplines (such as Music Information Retrieval and New Interfaces for Musical Expression). Specifically, the IoMusT refers to the network of Musical Things, which are objects augmented with information and communication technologies serving a musical purpose. Examples of Musical Things include smart musical instruments [2], smartphones used in participatory contexts [3], and wearables for extended reality [4] or for haptic-based communications [5].

As of today, security and privacy are mostly unrealized in IoMusT research, with methods specific to such application field. This lack of attention by researchers in the field may hamper the wide adoption of the IoMusT and its social acceptability. Whereas some of the IoT methods can be applied to the IoMusT, the latter differentiates from the former for its artistic focus, which requires music-specific methods. The paradigm of IoMusT is paving the way for a world, where many Musical Things will be connected and will interact with their user and environment to collect information and automate certain tasks. Such a vision requires, above all, the IoT features such as decentralization, seamless authentication, transparency, data integrity and privacy, and self-maintenance, as well as the musical domain's feature such as efficient handling of copyrights, speed of royalties payment, etc. Such features can be brought by blockchain.

Blockchain technology has been applied extensively in the fields of finance, real estate and supply chain, and has been identified as a disruptive technology that can strongly affect several other industries. One of these, object of the present article, is the music industry [6], which is worth an estimated $45 billion, of which approximately $15 billion relates to recorded music [7]. The application of blockchain to music is of particular interest because it appears to offer solutions to problems musicians have highlighted for decades. These include transparency, the sharing of value, and the relationships with intermediaries that are placed between the artist and fan.

In a different vein, the potential of blockchain technology in IoT contexts has been advocated by a number of authors, leading to the vision for a Blockchain-based IoT (BIoT). For instance, researchers have focused on the definition of possible BIoT architectures as well as on the application and deployment of BIoT solutions (for recent reviews see [8, 9, 10, 11]). Meanwhile different blockchain platforms suitable for creating IoT applications have emerged and are in rapid progress [9].

However, thus far, to the authors' best knowledge no research has investigated the use of blockchain technology in the IoMusT. In this vision paper we focus on showing potential disruption of IoMusT ecosystem using blockchain technology and

*Corresponding author
Email address: luca.turchet@unitn.it (Luca Turchet)
[1]Department of Information Engineering and Computer Science of University of Trento.
[2]Faculty of Mathematics, Informatics, and Mechanics of the University of Warsaw

possible challenges in development of so-called *Blockchain-based IoMusT (BIoMusT)* applications. Firstly, we present the IoMusT concept and identify its stakeholders. Secondly, we describe the key features of blockchain technology and its current applications within the music industry. Thirdly, we present our vision for the BIoMusT in terms of involved stakeholders and exchanged data, and exemplify it through scenarios. Finally, we discuss current challenges in the integration of blockchain and IoMusT.

2. The IoMusT vision

The IoMusT is an emerging field that extends the Internet of Things paradigm to the musical domain. In [1] the IoMusT was defined as *"the collection of ecosystems, networks, Musical Things, protocols and associated music-related information representations that enable services and applications related to musical content and activities, in physical and/or digital environments. Music-related information refers to data sensed and/or processed by a Musical Thing, and/or communicated to a human or another Musical Thing for musical purposes. A Musical Thing is a device capable of sensing, acquiring, actuating, exchanging, or processing data for musical purposes"*.

Musical things are connected by a networking infrastructure that enables multidirectional communication, both remotely and locally. The IoMusT technological infrastructure enables an ecosystem of interoperable Musical Things that connect musicians with each other, as well as with audiences, record labels and other music-related stakeholders. Different kinds of Musical Things prototypes have been developed by the IoMusT community, along with frameworks to connect them (see e.g., [12, 13]). Notably, Musical Things are devices envisioned to be context-aware and to be able to support proactively various musical activities. These features are enabled by big data analysis techniques.

One of the most prominent instances of Musical Things are the so-called Smart Musical Instruments, an emerging category of IoT devices characterized by sensors, actuators, wireless connectivity, and embedded intelligence [2]. Such instruments are the result of the integration of various technologies including sensor- and actuator-based augmented instruments, IoT, self-contained instruments, networked music performance systems, as well as methods for semantic audio, audio pattern recognition, and sensor fusion. Such novel types of musical instruments are also fostering the emergence of innovative services, such as those related to the wireless interaction of the instrument with other connected devices [14] or with cloud-based repositories [15].

Other instances of Musical Things include wearable devices used for musical purposes. These include headsets for virtual or augmented reality if used in networked musical applications and in conjunction with other Musical Things (see e.g., [14, 16, 4]). Musical Haptic Wearables are an emerging category of wearable devices comprising haptic stimulation, tracking of gestures and/or physiological parameters, and wireless connectivity features. These wearables were devised to enhance communication between musicians as well as between musicians and audiences by exploiting the sense of touch in both remote and co-located settings [5]. They were also conceived for enriching the musical experience of audience members of music performances by integrating haptic stimulations, as well as for providing novel capabilities for creative participation via a control interface [17].

An important factor distinguishing IoMusT from IoT is latency, which must be kept constantly below 30 ms to support realistic musical interactions enabling geographically displaced musicians to play together [18, 19]. Several IoMusT applications require a fast exchange of musical content between geographically displaced musicians interacting over the network. Such requirement is not necessary in the vast majority of IoT applications.

3. Blockchain and its application in the musical industry

3.1. Key Features of Blockchain

Distributed Ledgers are ledgers that are not maintained by a single individual but a network of independent (and often anonymous) nodes. Such distributed ledgers are usually built with the blockchain technology.

A blockchain comprises a graph of interconnected data units called blocks (whereas each block is composed by a block header and a block data) [20]. However, at a certain point in time, the majority of nodes agree on a longest sequence of the blocks, called the main chain. Such blocks along the main chain record the transactions of the distributed ledger digitally in chronological order in their block data. Each block points to its previous block along the chain using the hash of the previous block's header.

The key feature of the blockchain technology is that it provides its users a way to carry out transactions with another person or entity without having to rely on third-parties. Blockchain technology allows its users to track, coordinate, and execute transactions, in a peer to peer manner, as well as store information from a large number of devices, which enables the creation of applications that require no centralized entities. Such a technology focuses on making data easily accessible to its (possibly anonymous) users over a peer-to-peer network, and at the same time ensures the confidentiality and integrity of data using cryptographic mechanisms.

In summary, the blockchain technology has the following key characteristics:

- Decentralization: it is maintained by a network of nodes instead of a single entity. It enables the validation of the transaction between two peers without the authentication, jurisdiction, or intervention performed by a central entity. Thus no trusted entity is required. Hence, attacks such as insider threats can be avoided.

- Immutability: a blockchain cannot be changed without the efforts from the majority of nodes and hence is unchangeable (unless redactability is made a feature [21]). Since every link between blocks in the chain is an inverse hash point of the previous block, any change performed on a block causes the invalidation of all the subsequently generated blocks.

- Traceability: users can verify and trace the origins of historical data items thanks to the chronological order of the transactions saved in the blockchain.
- Non-repudiation: a cryptographically signed transaction can not be denied by the initiator of the transaction. This is the consequence of the fact that the private key (which is only known to the initiator) is utilized to sign the transaction. This can then be accessible and verified by other users through the corresponding public key.
- Transparency: each user is allowed to access and interact with the blockchain network with an identical right. In addition, each new transaction is available for every user, since it is validated and saved in the blockchain.
- Pseudonymity and anonymity: blockchain systems have the ability to preserve a certain degree of anonymity by using public key as pseudonymous addresses for users. Additional cryptographic techniques such as Commitment Scheme [22] and Zero-Knowledge Proof [22] are required for full anonymity.

An important aspect related to blockchain technology is that of *smart contracts* [23]. These are pieces of self-sufficient decentralized code, which get executed in autonomous way whenever a certain condition occurs. Devices are allowed to call public code functions in a smart contract. On the other hand, such functions can also trigger events, while applications can listen for them to properly react to the event triggered. In order to change the state of the contract (i.e., to modify the blockchain), it is necessary to publish a transaction in the chain. Each transactions is signed by a sender and needs to be accepted by the chain.

Decentralized storage [24] can be used along with the blockchain technology to provide storage for data that are too large to store in a block, e.g. a Bitcoin block can only contains at maximum 2MB of data. In this case, large files are stored in the decentralized storage and their URI (e.g. the hash of the file) will be stored in the blockchain to refer to the large file in an application.

Different kinds of blockchains exist, which can be classified according to the managed data, the availability of such data, and what actions a user is allowed to conduct. A blockchain may be public or private, and permissioned or permissionless. In the case of public blockchains, anybody is allowed to join the blockchain without the approval of third-parties and each node keeps its own copy of the ledger. Conversely, in private blockchains, the network access is restricted by the owner. In permissioned blockchain only authorized entities are able to act on a ledger, whereas in permissionless blockchains anyone can act on a ledger. Notably, many, but not all, private blockchains are also permissioned, in order to control which users can carry out transactions, execute smart contracts or act as miners in the network.

Consensus protocols are the main components that facilitate the main feature of decentralization of the blockchains mentioned above. The classic paper on consensus protocols, i.e., Byzantine agreement on synchronous system [25] focuses on three properties that an agreement protocol must hold: (i) Validity: inputs must be initially proposed by honest nodes. (ii) Agreement: Every honest nodes must agree on the same output. (iii) Termination: The agreement must be reached in finite time. The FLP impossibility result [26] showed that agreement cannot be achieved in asynchronous settings even with a single faulty participant. Thus, researchers introduced techniques such as randomization [27] or assume partial synchrony [28]. In such systems, safety is always prioritized over liveness. Recent advances in consensus protocols achieve agreement based on leader election, either with computational power, i.e. Proof-of-Work [29], or with financial capacity, i.e. Proof-of-Stake [30].

3.2. Blockchain and the music industry

In recent years, various scholars have discussed about the potential applications of blockchain technology in the music industry [31]. A particular focus has been placed on the record music industry, identifying different use cases [32, 33, 34, 35, 36, 37].

The first use case consists of the creation of a networked database of copyright ownership that would help solving issues with music licensing. To date, to own products via ownership rights and benefit from royalty distribution represent a big challenge for the music industry. Ownership rights are required to monetize digital music products. Blockchain and smart contracts could be utilized to generate an extensive and accurate decentralized database of music rights. A database based on the blockchain would include all the information distributed in various proprietary databases, and thanks to the blockchain technology all the data would be updated in an automated and instant fashion, and would be available to every user.

The second use case relates to the utilization of smart contracts to manage royalties. Meantime, the ledger can be utilized to provide a transparent information concerning the royalties of artists as well as real-time distributions to all the labels involved. Digital currency can be used to make the payments according to the contracts' terms. Micropayments could be made through smart contracts, which makes payments with lower transaction costs and quicker. Today royalty payments to artists are slow (they typically occur a few times a year), but via smart contracts they could occur immediately after the consumption of a musical piece.

The third use case relates to the solution of the issues of transparency within the value chain. Nowadays it is not easy for artists to judge the level of efficiency with which payments are processed by record labels, collective management organizations, or publishers; due to the aforementioned copyright information problems, often a non negligible amount of revenues does not reach the artists, but it ends up in black boxes in which it is not possible to identify in accurate way who are the rightful owners of royalty revenue.

The use cases illustrated above are supported also by a plethora of whitepapers produced by music technology companies, as discussed in [31]. However, such use cases only discuss issues in the recorded music industry [32], which is only one component of the industries in the music sector. The present article investigates broader issues, which are related to a large variety of musical activities, stakeholders, devices, and data types for which blockchain technology could represent a viable solution.

4. BIoMusT vision

The IoMusT refers to a network of wearable and non-wearable musical devices, which continuously gather music-related data about different kinds of stakeholders. However, part of this data is sensitive and private, or is protected by copyright. Therefore, it is necessary to ensure that data related to users is handled in a secure and confidential way. In addition, several issues hamper the music industry and its supply chain as reviewed in Section 3.2.

In this section we promote our vision for a BIoMusT, which can make the IoMusT more secure and its related industry more transparent and fair. We first list who are the stakeholders of BIoMusT, secondly we list the sources and the types of the data involved in BIoMusT. Subsequently, the BIoMusT vision is proposed in terms of opportunities resulting from the integration of the IoMusT and the blockchain. In part, the content of this section builds upon the works of different scholars who investigated the integration of IoT and blockchain [8, 9, 10, 11], and complements those results with a music-specific focus.

4.1. BIoMusT stakeholders

In Table 1 we identify the relevant parties and their roles in the BIoMusT domain, and we provide a comparison with their roles in the IoMusT. We show how the BIoMusT will benefits some of the IoMusT stakeholders, whereas other stakeholders will not be benefitted because they will play a less relevant role (e.g., they will have less responsibility) or will even disappear.

4.2. IoMusT data to be exchanged in the blockchain

In reference to the Musical Things described in Section 2 and the BIoMusT stakeholders identified in Section 4.1, we identified the following types of data that can be exchanged in the blockchain and its decentralized storage.

Some of the data reported below should be stored in the blockchain's decentralized storage, as they are larger than the typical block size of the blockchain. The reasons for storing such data using blockchain mechanisms can be manifold. For instance, users would like to share data produced by their Musical Things but keep it anonymous, without revealing their identity. In addition to this, users could be interested in monetizing this data, by selling it to other stakeholers such as companies performing big data analysis to provide personalised services. Moreover, compared to traditional databases, data stored in the blockchain can be accessed in an easier way by interested parties, and it is possible to trace in a transparent way who made use of the data. The scenarios reported in Section 4.5 illustrate the advantages of using blockchain technology to store data produced by IoMusT applications.

Musical signals. The most prominent kind of data is the sound produced by musicians during a given musical activity (performance, recording, composition, rehearsals, etc.). Such signals may also be created by audience members of a participatory concert involving a technology-mediated audience participation system [3].

Digital scores. These documents, related to intellectual property, are produced via dedicated software for writing music and are the result of the composition or arrangement process of composers, arrangers or producers.

Biometric signals. A variety of body-related signals can be tracked by wearable devices utilized by users of IoMusT services. These include EEG, heart rate, galvanic skin response, muscle activity, eye tracking, respiration. For instance, such data can be generated during live music concerts to track and repurpose the emotions felt by audiences, or during rehearsals in order to monitor the progresses of an individual musician or a band.

Gestural data. This data relates to the gestures of musicians interacting with the sensors embedded in a smart musical instrument's sensor interface (the player's gestures are tracked by such sensors and can then repurposed in multiple ways, such as the control of sound effects or stage equipment). Gestural data can also refer to signals captured by inertial sensors (e.g., accelerometers) or other kinds of sensors embedded in wearable devices utilized by audience members.

Error signals. In IoMusT pedagogical applications, data related to a learning activity of a music student can be tracked by smart musical instruments or other Musical Things. Then such data is compared to reference values (i.e., score with notes and sensors indications) to determine the presence of errors made during a practice study session.

Musical Things can be used for collecting users data, in a rapid and instantaneous way. Although IoMusT devices have inadequate resources, they generate big data by means of the embedded sensors and intelligence, which can then be coupled with blockchain technology to provide important use cases in the music industry domain. Nevertheless, in some cases the kind of data reported above poses important issues related to privacy and copyright of intellectual property, which blockchain technology could successfully handle.

Other types of data, as they are small, but important, should be stored directly on the blockchain.

Metadata to the exchanged data. The blockchain must store the pointer or an URI to the data that is stored in the decentralized storage, along with any related information such as size, date of creation, and other necessary metadata.

Ownership of exchanged data. The ownership of the above mentioned exchanged data such as the musical signals, digital scores, etc. must be assigned to the related stakeholder. Such data is small enough and important enough to be stored on the blockchain.

Access to the exchanged data. Besides the owner, who should have full access to the data, the blockchain also stores the list of stakeholders and their rights on the exchanged data. Some of the stakeholder may get access (rate-limited or unlim-

Stakeholder	Role in IoMusT	Role in BIoMusT
Musicians	They can use IoMusT services, as well as create and copyright the compositions, lyrics and/or arrangements, or contribute to concerts and recordings by providing vocals or playing instruments. They can have diverse expertise (beginner, intermediate, expert) and professional level (amateur, professional). They can further be categorized into performers, composers, music students and teachers.	They cover the same role than in IoMusT. They are one of the main sources of BIoMusT data, including data related to the use of BIoMusT services as well as copyrighted music and lyrics.
Audience members and listeners	They can use IoMusT services during live or recorded concerts, and recorded music in general. They are the consumers who utilize a published or unpublished music work in many ways, including streaming, live performance, buying CD or vinyl.	They generate BIoMusT data resulting from the use of BIoMusT services during the attendance of live or recorded concerts, as well as during the listening of streamed music.
Audio engineers	They are responsible for controlling the sound production resulting from a live concert or a recording. They can be classified as live sound engineers and studio producers.	Live sound engineers and studio producers use BIoMusT services (and produce associated data) during work in live concerts or recording studios.
Record labels and publishers	These are entities whose role is to promote composition and its usage via many distribution channels, including streaming platforms and CD stores. Typically, composers have to transfer ownership of their copyright to a publisher for exchange.	The parties may play a less relevant role in the BIoMusT because the need of a middleman between artists and consumers is decreased given the fact that artists could not transfer the ownership of their copyright to them.
Rights societies	These are parties whose task is pursuing royalty payments for every performance and usage of composition, anywhere in the world.	These entities which handle royalty payments will play a less relevant role or may even disappear, because blockchain technology allows artists to be remunerated directly and immediately after their music is consumed by a listener. However, Right Societies may still be needed as regulatory bodies in the BIoMusT.
Distributors and aggregators	These are actors in the music industry supply chain who are responsible for logistics, for physical products (CD, vinyl) or digital distribution (via streaming services).	These IoMusT parties, related to logistics for physical products or digital distribution, will keep their role in the BIoMusT.
Musical Things manufacturers and IoMusT service providers	They are companies that produce musical IoT devices, such as smart musical instruments and musical haptic wearables, or that provide services associated to Musical Things.	They can leverage data generated by Musical Things and associated services to improve their design and understand users' behaviours.
Music venues	They comprise big and small organizations and places where live concerts take place, such as concert halls, pubs, stadiums, and theaters.	They can exploit data generated by Musical Things and associated services to monitor users' behaviours so to provide better services to them during live music concerts.

Table 1: Comparison of stakeholders' roles in IoMusT and BIoMusT.

ited) to the exchanged data provided that they pay certain fee.

Consumption of exchanged data Related to the ownership of the exchanged data, any stakeholder that uses or subscribes the data belongs to another stakeholder must pay a certain amount of fee. Such data should also be stored on the blockchain.

Registration of Musical Things. The identity of each of the musical thing can be stored on the blockchain, which can be used later for seamless authentication purpose.

Updates of Musical Things. Software updates of Musical

Things can be stored in the decentralized storage and its MD5 hash can be stored on chain for integrity.

4.3. Opportunities of integrating blockchain with IoMusT

The IoMusT is starting to reshape the current musical industry to a "smart" musical industry featured with networked interactions and data-driven decision-making. Nevertheless, the intrinsic features of the IoMusT result in a number of challenges, such as decentralization, poor interoperability, privacy, and security vulnerabilities. Blockchain technology provides opportunities for addressing not only such challenges that are also common to the general IoT field, but also others that are music-specific. Potential improvements and benefits that such integration can bring include (but are not limited to) the following, where the first two challenges are music-specific and the rest are IoT-generic.

Copyright, licensing, and speed of royalty payments. So far the focus of applications of blockchain technology to the musical domain has been that of coping with issues related to the supply chain of the recorded music industry, such as revenue calculation, revenue share between many authors, reward delay, copyright and licensing issues. The IoMusT presents the same issues of the recorded music industry, but involves others related to IoMusT services, as illustrated below. Blockchain technology, which exploits the power of peer-to-peer networks, could be a more sustainable model for artists and producer of IoMusT content, realizing the revolutionary potential of disintermediation and direct-to-fan/user models. For example, the copyright of the digital scores can be registered on the blockchain, any party that wants to use that digital score must obtain a license for that score; such a subscription can also be recorded on the blockchain for verification per usage of the score. Payment for the subscription or the usage of the score is instantaneous due to the peer-to-peer nature of the blockchain. We refer the reader to the further discussion in Scenario 1 in Section 4.5.

Enhanced interoperability of IoMusT systems. Interoperability refers to the capability of interacting with Musical Things and exchanging information between IoMusT systems through a common language [38]. In an interoperable IoMusT ecosystem, technology platforms and software applications should be able exchange data, communicate seamlessly, and use the shared data across stakeholders. Nevertheless, IoMusT stakeholders today struggle with fragmented data, delayed communications and gapped workflows caused by vendor specific and incompatible IoMusT systems. This prevents the creation of efficient and effective services. A fundamental problem is the lack of a trusted link that can connect these independent IoMusT systems together to establish an end-to-end reachable network.

Blockchain, being a decentralized peer-to-peer architecture, can improve the interoperability across Musical Things, IoMusT ecosystems and industrial music sectors, by transforming and storing IoMusT data into blockchains. In this process, heterogeneous types of IoMusT data are converted, processed, compressed and finally stored in blockchains. Thanks to the blockchain, musical services providers and the users of such services would have access to the same information in a trusted manner. Furthermore, the use of blockchain in the IoMusT would ensure continuous availability and access to real-time data. Real-time access to (shared and trusted) data can improve communication and payments between stakeholders, as well as facilitate the emergence of innovative services. Different approaches are emerging in the healthcare domain to enhance data interoperability via the blockchain [39, 40]. Such approaches are also relevant to the IoMusT and can be coupled with a shared IoMusT data representation such as the one offered by the IoMusT Ontology [38].

Decentralized bootstrapping of IoMusT connection. Decentralized communications allow peer-to-peer connections between Musical Things thus removing central points of failures and reducing the performance bottleneck at the central agency (even though one node is compromised, the global system should continue to work) [41]. Note that only the establishment of the connections are done via blockchain, where the authentication of the Musical Things are performed utilizing the information written on the blockchain such as devices IDs, public keys, after that the musical things can be connected via their peer to peer channel and thus no burden for the blockchain during their communication. Moreover, decentralization will help prevent situations in which a few powerful organizations control the processing and storage of the information of a big number of IoMusT stakeholders, e.g. the removal of the Recording Studios as discussed in Scenario 7 in Section 4.5.

Scalability. An additional benefit that comes with the decentralization of the architecture is an improvement of the scalability of the IoMusT system [42], i.e. by moving the heavy computation from the smart devices in the IoMusT to the full nodes in the blockchain system in a secure way.

Autonomy. Autonomic interactions refer to the ability of Musical Things and IoMusT systems to interact with each other without the arbitration of a trusted third party (e.g., a server). Blockchain technology makes possible the development of such intelligent autonomous assets. IoMusT applications could benefit from this functionality to offer device-agnostic and decoupled-applications. Such autonomy may be achieved by smart contracts enabled by blockchains, for instance by the automatic execution of clauses embedded in smart contracts when a given condition is met, e.g. when the digital scores are downloaded from an online music repository (please see the further discussion in Scenario 3 in Section 4.5).

Identity. Through a blockchain system IoMusT stakeholders are capable of identifying every single Musical Thing [43]. Data inserted into the blockchain is immutable and uniquely identifies the data that was generated by a Musical Thing. Moreover, blockchain technology can offer trusted distributed authentication and authorization of Musical Things, which would represent an improvement for the IoMusT field and its stakeholders. Therefore, IoMusT stakeholders would be able to trust the blockchain infrastructure because it would automate the integrity of the data exchange. Not only would stakeholders know if their data had been manipulated, but also they would see exactly how it was done.

Traceability of IoMusT data. Traceability refers to the ability to trace and verify the spatial and temporal information

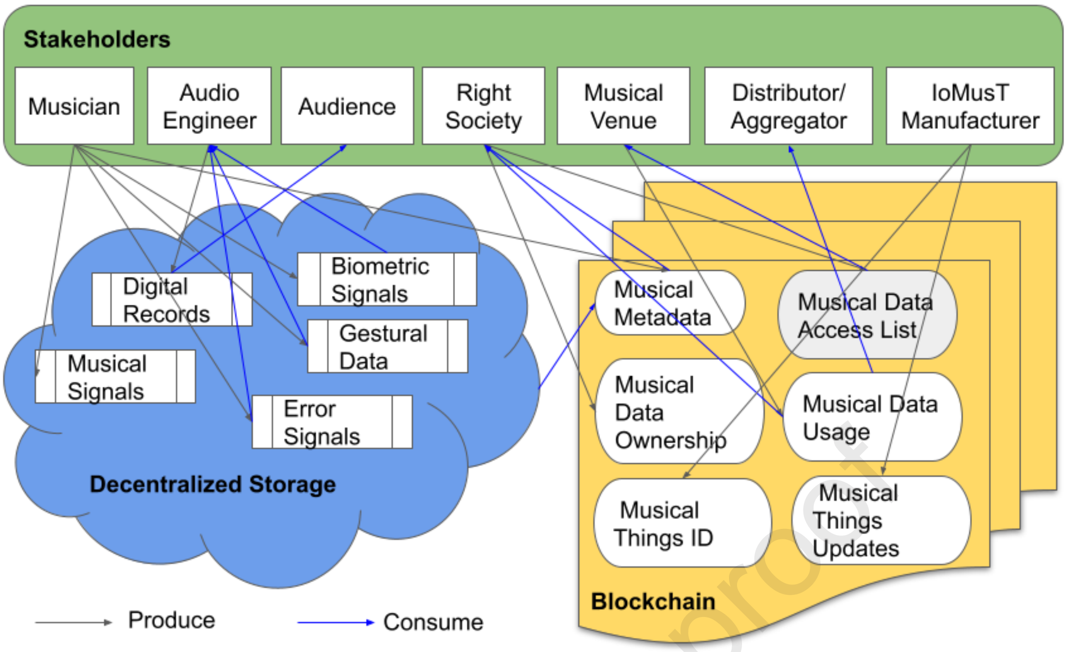


Figure 1: Types of data stored in the decentralized storage or on chain, and their corresponding producers and consumers

of a data block stored in the blockchain. Every data block stored in a blockchain is traceable to each user thanks to the attached timestamp. This also confers IoMusT data with reliability. We refer the reader to the further discussion in Scenario 4 in Section 4.5.

Reliability and Accountability of IoMusT data. Data reliability is the quality of data being trustworthy while accountability is to hold responsibility of the data provider in case of fraudulence (e.g. when a musician claim copyright of another's piece). In a blockchain IoMusT data can persist immutable and distributed over time. Such immutability of blockchains ensures the reliability of IoMusT data since it is extremely difficult to falsify or alter a transaction stored in a blockchain. The identity or pseudonymity of the data provider are treated the same way. Reliability and accountability can be assured by the integrity enforced by cryptographic mechanisms inherent in blockchains, such as hash functions, asymmetric encryption algorithms, and digital signature. Moreover, the authenticity of blockchain data can be identified and verified anytime and anywhere by participants of the blockchain system.

Security. Blockchain can lead to improved security of IoMusT systems. Blockchain technology ensures security of data and communications when these are stored as transactions of the blockchain, which are encrypted and digitally signed by cryptographic keys. Message exchanges between Musical Things can be treated by the blockchain as transactions, validated by smart contracts. In this way the communications between Musical Things is made secure. Existing standard protocols for security utilized in the IoT [44] can be optimized with the application of blockchain also in the IoMusT. In addition, integrating IoMusT systems with blockchain technologies (such as smart contracts) can be useful to increase the security level of IoMusT systems by automatically updating the firmwares of Musical Things in order to remedy vulnerable breaches [45]. We refer the reader to the example of Scenario 5 in Section 4.5.

Market of services. Blockchain technology has the potential to speed up the creation of IoMusT ecosystems of services and data market-places, in which transactions between stakeholders are possible without any intermediate authority. Microservices can be easily deployed in such ecosystems and micropayments can be safely made in a trustless environment. We refer the reader to the further discussion in Scenario 7 in §4.5.

Secure code deployment. Thanks to the secure and immutable storage capability of blockchain, code can be securely uploaded into Musical Things [46]. In addition, manufacturers of IoMusT systems are able to track states and updates with a high level of confidence.

Although blockchain can benefit IoMusT in the ways listed above, a number of challenges need to be addressed before the potentials of BIoMusT can be fully unleashed. Section 5 illustrates the most prominent challenges and open research questions in BIoMusT.

4.4. Determining the need for using a blockchain within IoMusT applications

Whereas the previous section explored how to make use of a blockchain for IoMusT applications, in first place it is necessary to highlight that a blockchain may not be the best solution for a given IoMusT scenario. To establish whether the usage of a blockchain is appropriate, a developer should determine whether the following features are necessary for a certain IoMusT application:

Latency. The very first criterium to determine the suitability of the blockchain for a certain IoMusT application is its lack of low-latency requirements. As a matter of fact, blockchain is a time-consuming technology, whereas several IoMusT applications are not latency-tolerant (e.g., networked music performances). In those scenarios, conventional methods can be utilized to ensure for instance the security of a musical communication.

Decentralization. Some IoMusT applications demand decentralization in absence of a trusted centralized system. Nevertheless, many IoMusT stakeholders may still prefer trusting certain firms, government agencies or banks. In those cases of mutual trust, a blockchain is not required.

Robust distributed system. The need of a distributed system in an IoMusT application scenario is not a sufficient motivation for utilizing a blockchain: indeed it is necessary that at least one node of the distributed system lacks trust towards another node.

Peer-to-peer exchanges. In the IoMusT several kinds of communications occur between Musical Things and remote servers (e.g., [15]). Peer-to-peer communications also occur, especially in applications such as co-located or remote networked music performances [18, 19].

Payment system. In some cases, an economic transaction with a third party may be required by an IoMusT application, while this is not a requirement for other applications. In addition, economic transactions can still be accomplished via conventional payment systems, even though they typically result in the payment of transaction fees and require to trust banks or middlemen.

Micro-transactions records. Like for the IoT, some IoMusT applications may require to maintain a record of each transaction to keep traceability (for instance, to support auditing). In such situations, a blockchain may be useful. However, for other applications it is not necessary to store any collected value.

Figure 2 illustrates a flow diagram that can support a developer in the decision-making process about the kind of blockchain that is needed depending on the features of a given IoMusT system (the figure builds upon the related figure reported in [8]).

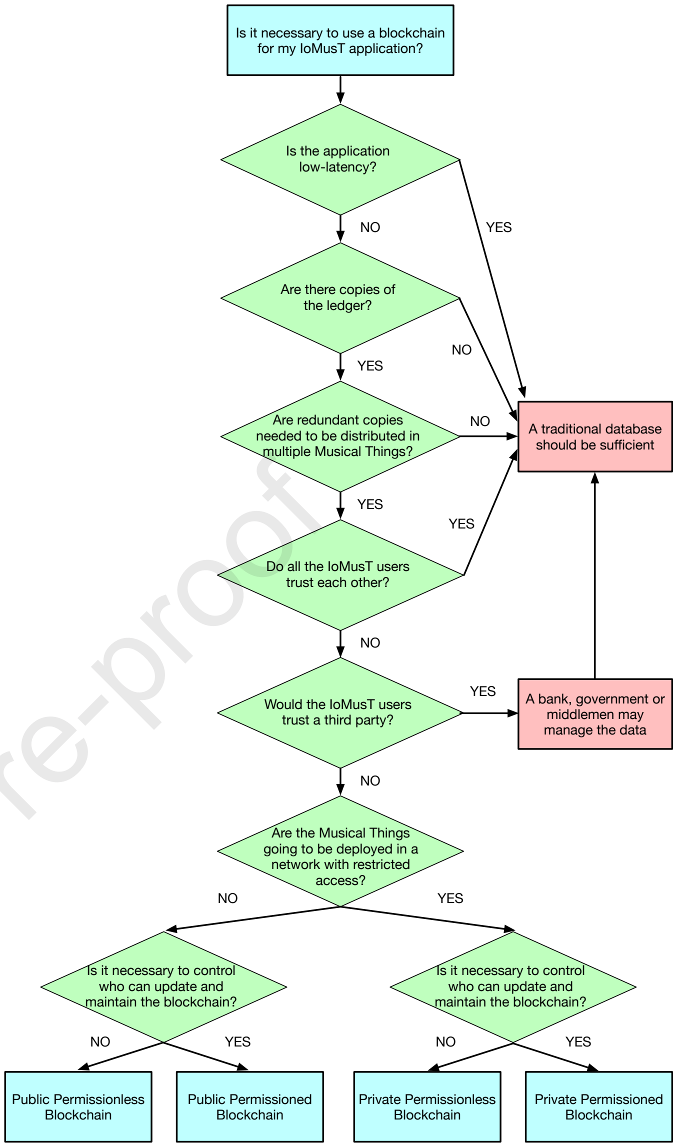


Figure 2: Flow diagram for deciding when to use blockchain in an IoMusT application (adapted from [8]).

4.5. BIoMusT scenarios

Blockchain technologies have the potential to bring many benefits to the IoMusT, but, as they have not been devised explicitly for IoMusT environments, it is necessary to adapt the different components that comprise them. To foster their optimization, we propose a series of application scenarios that in the near future could be implemented as well as assessed under the performance standpoint. The role of these scenarios is also that of enabling a debate about the potential of the BIoMusT and of identifying capabilities that at present are missing.

Scenario 1: Cover song identification. An ad-hoc Musical Thing, equipped with microphones and intelligence dedicated to the identification of cover of songs, is utilized by an inspector of a national Rights Society at a music venue during a live concert. The songs automatically identified (thanks to music information retrieval techniques [47]) are then matched to the song titles declared by musicians in the list to be sent to the national Rights Society. This verification assesses the correctness of what declared by musicians, and at the same time ensures the correct payment of royalties to the composers. Such a Musical Thing can be deployed in several music venues to guarantee an effective monitoring of the reported cover songs, whereas the blockchain can facilitate the interoperation of such devices. As soon as the match is verified then the composers can be immediately rewarded thanks to the use of a smart contract deployed on such blockchain.

Scenario 2: Royalties payment via smart musical instruments. Thanks to the blockchain, when a concert occurs at a music venue, the music venue organization pays only the performers, not the composers: the payment to the composers is ensured by smart musical instruments of the performers, which understand what music has been played and automatically make the payment to composers. Therefore, there is no need for the music venue to pay also a Right Society handling the rights of composers. In this context, the composers do not depend on the

Right Society any more, as all the above operations are automated by a smart contract deployed on the blockchain.

Scenario 3: Interaction with online music repositories. This is yet another possible scenario which is facilitated by blochchain where the intermediary is replaced. A smart guitar, such as that reported in [15], is utilized to query and download copyrighted content from a music repository (e.g., Spotify). Each time that a new download on the smart guitar is accomplished, the instrument notifies through the blockchain the composer(s), who will immediately receive the royalties payment.

Scenario 4: Monetization of musicians' data. Musicians produce several data through their Musical Things. These data are relevant to musical instruments manufacturers and services providers, which are interested in exploiting this data (e.g., to do some big data analysis to understand the collective use of a given product or service). Thanks to the blockchain musicians possess and are in control of their data, and can decide to monetize such data by sharing it with the wanted parties. Blockchain technology also allows to preserve the privacy of these users by making them not identifiable by the companies.

Scenario 5: Privacy of audience's data collected via wearables. The privacy of biometric data, captured by wearables worn by audience members participating in a live concerts, is ensured thanks to the embedded blockchain technology. These collected data are repurposed in many ways (both in real-time during the concert and offline at a subsequent stage dealing with big data analysis) without however revealing sensitive information about the user. For instance, biometric data can be used to infer the emotional state of audiences, which provides indications about the level of engagement experienced. This information can be exploited by the concert venues organizers to create better performance conditions, as well as by performers to understand how to amend their lineup in order to enhance the experience of the audience.

Scenario 6: Enhanced music pedagogy. Blockchain technology is coupled with Musical Things to enable remote consultation of a student with a teacher. Sensors on a smart bracelet and other wearables continuously gather and monitor the student's stress level or mental state during the study practice. They also generate an alert when a threshold is crossed, upon which a transaction is generated in the blockchain and the teacher is informed. The teacher examines the student's data and provides the appropriate study directions accordingly. We note that, data such as sensors value, and the inferred stress level or mental state of the student, are not necessarily be stored in real time on the blockchain, as the teacher only need to observe those data after the studying session in order to plan to the next one.

Scenario 7: Audio engineers market of services. Thanks to blockchain, a novel and fair market of services related to audio engineering works will be possible. Audio engineers could promote themselves and offer specific services to musicians, thus becoming fully independent from Recording Studios typically offering those services. In particular, audio engineers will become visible to musicians, instead of being shadowed by the Recording Studios as before. This brings tremendous fairness in competition between audio engineering services.

5. Challenges in blockchain–IoMusT integration

Blockchain technology may be beneficial to the IoMusT in terms of security, privacy, and royalties payment as shown by the scenarios envisioned in Section 4.5. Nevertheless, the integration of the two technologies represents a non trivial task and faces numerous challenges due to some conflicting requirements in these two technological paradigms. For instance, blockchain technology was conceived for an Internet scenario with powerful computers, and this is far from the IoMusT reality, which mostly relies on embedded systems.

The sweet spot, as always, is in the middle. Permissioned blockchains may bring an improved level of trust, which is still missing in the music world where stakeholders do not trust each other. A way of achieving this could involve the integration of cloud resources and IoMusT devices at the edge of the Internet [48]. Blockchain ha the potential to pave the way to a world in which the use of trusted third parties is not the sole way to arbitrate a set of entities. The capability of establishing trust via permissioned blockchains allows one to shift the control from the datacenters to the edge, truly accomplishing the promises of edge-centric computing.

In order to reach maturity and achieve efficiency it is necessary to address numerous open issues that currently prevent the adoption of BIoMusT. The challenges, some of which are common to the general IoT field, include the following.

Latency. IoMusT applications generally require a real-time response for which a fast consensus protocol is necessary. On the contrary, blocks creation is time-consuming; some existing blockchain implementations can solely process a few transactions per second (for instance, in Bitcoin, every 10 minutes 1MB is created per block), so this is a potential bottleneck for some IoMusT applications. It is challenging to group such streams of data on blocks while respecting real-time requirements. Such problem has been addressed in the blockchain application to the Internet of Medical Things by eliminating the consensus protocol [49] or by using a lightweight consensus mechanism [50] to meet the real-time requirements. Other authors suggested to adapt blockchain, and especially its consensus protocol, to augment the bandwidth and reduce the latency of its transactions [51].

Privacy. Privacy and protection of data are key challenges for the IoMusT. The adoption of blockchain technology can alleviate the problem of identity management in IoMusT. Several IoMusT applications are envisioned to function with confidential data. When the Musical Thing is linked to a specific user it is essential to address the problem of data privacy and anonymity. For instance, this is the case of a wearable device with the capability of hiding the identity of the user when sending personal data (e.g., for real-time musical applications or for subsequent big data analysis), or smart musical instruments that safeguard the privacy of the intellectual property of composers. Different solutions are emerging in the BIoT field which can also be utilized for BIoMusT (see e.g., [43, 52]). Securing the Musical Thing in order to store data in a secure way and to prevent their access without permission is a challenge because it necessitates the integration of a security application into the device. Developers aiming at these improvements are required to consider carefully the limitation of resources of the Musical Things as well as the restrictions related to economic viability. Notably, the use of ad-hoc hardware for cryptography could speed up cryptographic operations and circumvent the overload of complex secure software protocols.

Security. Security is a major challenge for IoMusT applications that need to handle security problems at different levels, but with additional limitations due to the lack of performance and high heterogeneity of resource-constrained devices. Musical Things are limited in terms of computational and memory resources and, therefore, are not capable of affording the high resource requirements of traditional security algorithms which are complex and heavyweight. Moreover, the centralization utilized in the current and most widespread security frameworks, is not well suited for some distributed IoMusT applications because of the large distributed scale of IoMusT networks and single point of failure. There is the need of proposing novel blockchain technology schemes optimized for IoMusT, in order to successfully solve the security challenges as well as preserve IoMusT users' privacy. Many experts see blockchain as a key technology to improve security in IoT, and IoMusT is no exception. However, the reliability of the data produced by the IoT is a challenge for BIoT and consequently for BIoMusT: while blockchain ensures that data in the chain are immutable and can trace their transformations, it will keep data corrupted if this arrived in such a form. Therefore, it is crucial to thoroughly test Musical Things before their integration with blockchain and to include mechanisms to identify Musical Things failures as soon as they happen.

Processing. In blockchain the mining process and the complexities of cryptography are resource-hungry tasks, which demand intensive computation and consumption of a high amount of energy. Resource-constrained devices such as Musical Things cannot afford such demands. Note, however, that in our vision the main blockchain-related computations will not happen directly onto the Musical Thing, but on the miners' node. Certain computations happen at the device (e.g., signing transactions) others not (e.g., aggregation of statistical data).

Storage and scalability. Musical Things can produce large amounts of data with huge flow. It is necessary to store such data in the blockchain so to ensure its integrity. This poses a non negligible challenge: blockchain technology relies on its nodes to provide a distributed storage, which can not be afforded by Musical Things having limited storage capabilities. As reported in [9], storage capacity and scalability of blockchain are still under discussion, but in the context of IoMusT applications the intrinsic capacity and scalability limitations make these challenges much greater. Blockchain is not designed to store huge quantities of data like those generated in the IoMusT. Musical Things can produce gigabytes of data in real-time, and this is a limitation representing a barrier to the IoMusT-blockchain integration. As such, large data should be only stored in decentralized storage, and only meta data and other data related to interactions between stake holders should be stored onchain. Still, BIoMusT research needs to tackle these challenges when performing the integration of blockchain and IoMusT.

Energy efficiency. Musical Things are typically based on resource-constrained embedded systems that are powered by batteries [2]. Consequently, energy efficiency is a crucial factor to facilitate a long-lasting deployment of an IoMusT node. However, the vast majority of blockchain implementations are power-hungry, where a vast part of the consumption is caused by cryptographic operations and P2P communications.

Traffic overhead. The nodes in the blockchain communicate continuously to achieve synchronization, which creates weighty overhead traffic. This cannot be affordable by bandwidth- and throughput-limited Musical Things. Therefore, a challenge relates to the creation of methods to improve bandwidth consumption and support network bandwidth for blockchain transactions and updates.

Lack of standards. Current solutions in BIoT, which could be also utilized in the BIoMusT, are fragmented and proprietary [53]. The definition of standard protocols capable of adapting heterogeneous technologies and promoting interoperability is currently missing, which prevents the adoption of such solutions. Therefore, providing platform-agnostic solutions that govern the interaction between Musical Things, blockchain, and IoMusT stakeholders is of paramount importance.

Programming abstractions. BIoMusT opens the door to various important applications in the music field. Nevertheless, the BIoMusT adoption is a complex matter and necessitates in-depth interdisciplinary knowledge at both high-level (e.g., storing, sharing, and treating IoMusT data) and low-level (e.g., the management of Musical Things and configuring blockchain to meet IoMusT requirements). Therefore, it is paramount to devise an abstraction layer capable of masking all such complexities and of providing developers with novel application programming interfaces and middleware thatt allow them to implement in an easy way decentralized and secure musical applications leveraging the BIoMusT.

Mobility. Blockchain technology was conceived for a fixed network topology. Nevertheless, Musical Things such as wearable devices or smart musical instruments are constantly in movement, and therefore the topology is continuously changed. This may represent a challenge to the technological integration envisioned in the BIoMusT.

Legal issues. The IoMusT domain, like the IoT, is subjected to a country's laws or regulations concerning data privacy (e.g., the European Union's GDPR). The emergence of blockchain requires the revision of such legal framework. The creation and adoption of novel laws and standards can facilitate the certification of security features of Musical Things and, therefore, it can contribute to create more secure and trusted IoMusT ecosystems. Laws that deal with information handling and privacy are still an unsolved and scarcely addressed challenge to be addressed in IoMusT and, therefore, will constitute an even more significant challenge when the IoMusT is combined with the blockchain.

6. Conclusion

This paper proposed a synthesis of two different technologies, IoMusT and blockchain. This synthesis was illustrated via a number of application scenarios that could be implemented in the short- and medium-term. The presented scenarios showed not only how the blockchain can be an enabler for IoMusT applications not possible otherwise, but also how it can positively impact a range of stakeholders (from musicians to audiences, from music venues to Rights Societies).

The aim of this study was to assess the practical limitations of such technological integration, identify directions for further research, as well as inform developers about some of the issues that will have to be addressed before deploying the next generation of BIoMusT applications. Through the adopted methodological approach, the present study sought to contribute to the advancement of the state of the art in IoMusT research, not only by shedding new light on a scarcely addressed technological integration, but also by enabling a debate about the potential of the BIoMusT and identifying capabilities that are present are missing.

In some cases, IoMusT data are sensitive, heavy and necessitate high degree of security. With the emergence of blockchain technology, researchers' attention could be devoted to adopting blockchain strategies to bring security to IoMusT applications. Other benefits provided by the BIoMusT include the efficient handling of copyrights, licensing, and royalty payments. However, at present such integration represents a non-trivial task due to the diverse requirements in these two technologies. Nevertheless, the use of the BIoMusT paradigm enables a wide number of potential applications that could disrupt the music industry. Unprecedented services for musical stakeholders and, as a consequence, new markets in the music sector can be envisioned following the development and widespread use of such technological enabler. Nevertheless, the adoption of the BIoMusT will be fostered by companies providing such services, which are driven not only by technological considerations, but also by ideological (e.g., unfairness of royalties payment to artists) and market-related considerations (e.g., benefits of cryptocurrencies), as recently shown in [31].

The IoMusT can benefit from the functionalities provided by blockchain, which may help to further develop and improve current IoMusT technologies. Even though the convergence of blockchain and IoMusT brings several opportunities in improving the musical industry, there are many research challenges that must be addressed before the potentials of BIoMusT can be fully unleashed. Such challenges include technical (e.g., latency), sustainability (e.g., energy efficiency), economic (e.g., monetization), and regulatory aspects (e.g., privacy and legal issues). This research topic is still in a preliminary stage and calls for more research capable of providing effective solutions to bridge the current gaps.

Acknowledgment

The authors wish to thank Prof. Alberto Montresor for the useful discussions on the content of this work.

[1] L. Turchet, C. Fischione, G. Essl, D. Keller, M. Barthet, Internet of Musical Things: Vision and Challenges, IEEE Access 6 (2018) 61994–62017.

[2] L. Turchet, Smart Musical Instruments: vision, design principles, and future directions, IEEE Access 7 (2019) 8944–8963.

[3] O. Hödl, C. Bartmann, F. Kayali, C. Löw, P. Purgathofer, Large-scale audience participation in live music using smartphones, Journal of New Music Research 49 (2) (2020) 192–207.

[4] L. Turchet, R. Hamilton, A. Çamci, Music in extended realities, IEEE Access 9 (2021) 15810–15832.

[5] L. Turchet, M. Barthet, Co-design of Musical Haptic Wearables for electronic music performer's communication, IEEE Transactions on Human-Machine Systems 49 (2) (2019) 183–193.

[6] A. Lerch, The relation between music technology and music industry, in: Springer Handbook of Systematic Musicology, Springer, 2018, pp. 899–909.

[7] R. Rethink Music, Fair music: Transparency and payment flows in the music industry, Berklee Institute of Creative Entrepreneurship.

[8] T. M. Fernández-Caramés, P. Fraga-Lamas, A review on the use of blockchain for the internet of things, IEEE Access 6 (2018) 32979–33001.

[9] A. Reyna, C. Martín, J. Chen, E. Soler, M. Díaz, On blockchain and its integration with iot. challenges and opportunities, Future generation computer systems 88 (2018) 173–190.

[10] H.-N. Dai, Z. Zheng, Y. Zhang, Blockchain for internet of things: A survey, IEEE Internet of Things Journal 6 (5) (2019) 8076–8094.

[11] M. A. Uddin, A. Stranieri, I. Gondal, V. Balasubramanian, A survey on the adoption of blockchain in iot: Challenges and solutions, Blockchain: Research and Applications (2021) 100006.

[12] A. Fraietta, O. Bown, S. Ferguson, S. Gillespie, L. Bray, Rapid composition for networked devices: HappyBrackets, Computer Music Journal 43 (2) (2019) 89–108.

[13] B. Matuszewski, A web-based framework for distributed music system research and creation, Journal of the Audio Engineering Society 68 (10) (2020) 717–726.

[14] L. Turchet, M. Benincaso, C. Fischione, Examples of use cases with smart instruments, in: Proceedings of Audio Mostly Conference, 2017, pp. 47:1–47:5.

[15] L. Turchet, J. Pauwels, C. Fischione, G. Fazekas, Cloud-smart musical instrument interactions: Querying a large music collection with a smart guitar, ACM Transactions on the Internet of Things 1 (3) (2020) 1–29.

[16] B. Loveridge, Networked music performance in virtual reality: Current perspectives, Journal of Network Music and Arts 2 (1) (2020) 2.

[17] L. Turchet, T. West, M. M. Wanderley, Touching the audience: Musical Haptic Wearables for augmented and participatory live music performances, Journal of Personal and Ubiquitous Computing (2021) 1–21.

[18] L. Gabrielli, S. Squartini, Wireless Networked Music Performance, Springer, 2016.

[19] C. Rottondi, C. Chafe, C. Allocchio, A. Sarti, An overview on networked music performance technologies, IEEE Access 4 (2016) 8823–8843.

[20] Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, An overview of blockchain technology: Architecture, consensus, and future trends, in: 2017 IEEE international congress on big data, IEEE, 2017, pp. 557–564.

[21] G. Ateniese, B. Magri, D. Venturi, E. Andrade, Redactable blockchain–or–rewriting history in bitcoin and friends, in: 2017 IEEE European symposium on security and privacy (EuroS&P), IEEE, 2017, pp. 111–126.

[22] O. Goldreich, Foundations of cryptography: volume 2, basic applications, Cambridge university press, 2009.

[23] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, J. Kishigami, Blockchain contract: Securing a blockchain applied to smart contracts, in: 2016 IEEE international conference on consumer electronics (ICCE), IEEE, 2016, pp. 467–468.

[24] D. Vorick, L. Champine, Sia: Simple decentralized storage, Nebulous Inc.

[25] L. Lamport, R. Shostak, M. Pease, The Byzantine Generals Problem, ACM Transactions on Programming Languages and Systems 4 (3) (1982) 382–401.

[26] M. J. Fischer, N. A. Lynch, M. S. Paterson, Impossibility of Distributed Consensus with One Faulty Process, Journal of the ACM 32 (2) (1985) 374–382.

[27] M. O. Rabin, Randomized Byzantine Generals, in: 24th Symposium on Foundations of Computer Science, IEEE, 1983, pp. 403–409.

[28] C. Dwork, N. A. Lynch, L. Stockmeyer, Consensus in the Presence of Partial Synchrony, Journal of the ACM 35 (2) (1988) 288–323.

[29] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, `https://bitcoin.org/bitcoin.pdf`. Accessed: 2019-05-01 (2008).

[30] P. Vasin, Blackcoin's proof-of-stake protocol v2, `https://blackcoin.org/blackcoin-pos-protocol-v2-whitepaper.pdf`. Accessed: 2019-05-01 (2014).

[31] D. Chalmers, R. Matthews, A. Hyslop, Blockchain as an external enabler of new venture ideas: Digital entrepreneurs and the disintermediation of the global music industry, Journal of Business Research 125 (2021) 577–591.

[32] M. O'Dair, Z. Beaven, The networked record industry: How blockchain technology could transform the record industry, Strategic Change 26 (5) (2017) 471–480.

[33] S. Zhao, D. O'Mahony, Bmcprotector: A blockchain and smart contract based application for music copyright protection, in: Proceedings of the 2018 International Conference on Blockchain Technology and Application, 2018, pp. 1–5.

[34] C. Sitonio, A. Nucciarelli, The impact of blockchain on the music industry, in: R&D Management Conference 2018 – "Designing Innovation: Transformational Challenges for Organizations and Society", 2018, pp. 1–13.

[35] O. Gough, Blockchain: a new opportunity for record labels, International Journal of Music Business Research 7 (1) (2018) 26–44.

[36] A. Kim, M. Kim, A study on blockchain-based music distribution framework: Focusing on copyright protection, in: IEEE International Conference on Information and Communication Technology Convergence, IEEE, 2020, pp. 1921–1925.

[37] P. Kudumakis, T. Wilmering, M. Sandler, V. Rodríguez-Doncel, L. Boch, J. Delgado, The challenge: From mpeg intellectual property rights ontologies to smart contracts and blockchains [standards in a nutshell], IEEE Signal Processing Magazine 37 (2) (2020) 89–95.

[38] L. Turchet, F. Antoniazzi, F. Viola, F. Giunchiglia, G. Fazekas, The internet of musical things ontology, Journal of Web Semantics 60 (2020) 100548.

[39] R. Jabbar, N. Fetais, M. Krichen, K. Barkaoui, Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity, in: 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies, IEEE, 2020, pp. 310–317.

[40] G. Kamau, C. Boore, E. Maina, S. Njenga, Blockchain technology: Is this the solution to EMR interoperability and security issues in developing countries?, in: Proceedings of 2018 IST-Africa Week Conference (IST-Africa), IEEE, 2018, pp. Page–1.

[41] K. Yeow, A. Gani, R. W. Ahmad, J. J. Rodrigues, K. Ko, Decentralized consensus for edge-centric internet of things: A review, taxonomy, and research issues, IEEE Access 6 (2017) 1513–1524.

[42] O. Novo, Blockchain meets IoT: An architecture for scalable access management in IoT, IEEE Internet of Things Journal 5 (2) (2018) 1184–1195.

[43] D. W. Kravitz, J. Cooper, Securing user identity and transactions symbiotically: Iot meets blockchain, in: 2017 Global Internet of Things Summit, IEEE, 2017, pp. 1–6.

[44] M. A. Khan, K. Salah, Iot security: Review, blockchain solutions, and open challenges, Future Generation Computer Systems 82 (2018) 395–411.

[45] K. Christidis, M. Devetsikiotis, Blockchains and smart contracts for the internet of things, IEEE Access 4 (2016) 2292–2303.

[46] M. Samaniego, R. Deters, Hosting virtual iot resources on edge-hosts with blockchain, in: IEEE International Conference on Computer and Information Technology, IEEE, 2016, pp. 116–119.

[47] J. Serra, X. Serra, R. G. Andrzejak, Cross recurrence quantification for cover song identification, New Journal of Physics 11 (9) (2009) 093017.

[48] P. G. López, A. Montresor, A. Datta, Please, do not decentralize the Internet with (permissionless) blockchains!, in: Proc. of the 39th Int. Conference on Distributed Computing Systems, ICDCS'19, 2019.

[49] A. Khatoon, A blockchain-based smart contract system for healthcare management, Electronics 9 (1) (2020) 94.

[50] V. Malamas, T. Dasaklis, P. Kotzanikolaou, M. Burmester, S. Katsikas, A forensics-by-design management framework for medical devices based on blockchain, in: 2019 IEEE World Congress on Services, Vol. 2642, IEEE, 2019, pp. 35–40.

[51] I. Eyal, A. E. Gencer, E. G. Sirer, R. Van Renesse, Bitcoin-NG: A scalable blockchain protocol, in: 13th {USENIX} symposium on networked systems design and implementation ({NSDI} 16), 2016, pp. 45–59.

[52] A. Dorri, S. S. Kanhere, R. Jurdak, Towards an optimized blockchain for iot, in: 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation, IEEE, 2017, pp. 173–178.

[53] F. Ellouze, G. Fersi, M. Jmaiel, Blockchain for internet of medical things: A technical review, in: International Conference on Smart Homes and Health Telematics, Springer, 2020, pp. 259–267.

Declaration of interests

☒ The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

☐The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: