NATIONAL TECHNICAL UNIVERSITY OF ATHENS
SCHOOL OF ELECTRICAL AND COMPUTER ENGINEERING
DIVISION OF COMMUNICATION, ELECTRONIC AND INFORMATION ENGINEERING
DISTRIBUTED KNOWLEDGE AND MEDIA SYSTEMS GROUP

Blockchains beyond Digital Currencies: Privacy-Oriented Implementations of Industrial Architectures

Doctoral Dissertation

by

Nikolaos E. Kapsoulis

Submitted to the School of Electrical and Computer Engineering
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

at the

NATIONAL TECHNICAL UNIVERSITY OF ATHENS

Supervisor: Prof. Theodora Varvarigou

Athens, Greece
October 2023

This page is left blank by design.

.....

Nikolaos E. Kapsoulis

Doctor of Electrical and Computer Engineering N.T.U.A.

This page is left blank by design.

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΕΠΙΚΟΙΝΩΝΙΩΝ, ΗΛΕΚΤΡΟΝΙΚΗΣ & ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΕΡΕΥΝΗΤΙΚΗ ΟΜΑΔΑ ΚΑΤΑΝΕΜΗΜΕΝΩΝ ΣΥΣΤΗΜΑΤΩΝ ΔΙΑΧΕΙΡΙΣΗΣ ΓΝΩΣΗΣ

Αλυσίδες-κορμού πέραν των Ψηφιακών Νομισμάτων: Υλοποιήσεις Βιομηχανικών Αρχιτεκτονικών Προσανατολισμένων στην Ιδιωτικότητα

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

Νικόλαος Ε. Καψούλης

Συμβουλευτική Επιτροπή : Καθηγήτρια Θεοδώρα Βαρβαρίγου (Επιβλέπουσα)
Καθηγητής Εμμανουήλ Βαρβαρίγος
Καθηγητής Συμεών Παπαβασιλείου

Εγκρίθηκε από την επταμελή εξεταστική επιτροπή την 16η Οκτωβρίου 2023.

…….	…….	…….
Θεοδώρα Βαρβαρίγου	Εμμανουήλ Βαρβαρίγος	Συμεών Παπαβασιλείου
Καθηγήτρια Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.
…….	…….	…….
Αναστάσιος Δουλάμης	Δημήτριος Ασκούνης	Ιωάννης Ψαρράς
Αν. Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.

…….
Κωνσταντίνος Τσερπές
Αν. Καθηγητής Χαροκόπειο Π.

Αθήνα, Οκτώβριος 2023

This page is left blank by design.

.....

Νικόλαος Ε. Καψούλης
Διδάκτωρ Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

For the family

Preface

The presented doctoral dissertation was achieved from September 2019 to October 2023 at the Distributed Knowledge and Media System Group laboratory of the School of Electrical and Computer Engineering at the National Technical University of Athens. During this time period, I was lucky enough to be able to dive deeper into the dynamic, cutting-edge and interesting for me technologies of blockchains and distributed ledgers, and their ever evolving applications.

I am feeling that I was adequately blessed to obtain highly valuable support from people that helped me along my journey. First of all, I would like to greatly thank my supervisor, Professor Theodora Varvarigou for her trust, her support, and the amazing opportunity provided to really grow as a professional throughout my years of studying in the lab.

I would also like to thank a lot my advisory committee, Professors Manos Varvarigos and Symeon Papavassiliou for their highly appreciated support and valuable advice along my degree journey.

I am notably grateful to my colleague, Professor Antonios Litke for his constant faith in me and trust, his immense support and uninterrupted help along my journey, his detailing guidance and skillful teachings, and his ubiquitous professionalism in every kind of situation.

I am forever thankful to my colleague, Dr. Alexandros Psychas for his unconditional help and thorough guidance throughout my degree, our endless scientific discussions on research topics and future, and his acute honesty applied

to every thing.

My grand appreciation is expressed for Professor John Soldatos for his charismatic leadership and timeless advice that helped me move forward on my path as a professional.

I would also like to thank my colleagues for their support and help throughout my years, Dr. Vrettos Moulos, Efstathios Karanastasis, Achilleas Marinakis, Senior Researcher and Dr. Vassiliki Andronikou, Dr. Efthymios Chondrogiannis, Orfeas Voutyras, and Dr. George Palaiokrassas.

My sincere acknowledgments are also destined to my colleagues, Assistant Professor Nima Afraz, David Boswell, and Assistant Professor Vipin Rathi.

I am more admiring to my Patricia for her abundant confidence in me, and her eternal care and encouragement for my chosen path, a force of nature that matured me as an individual.

Finally, I am hugely thankful to my parents, Eleftherios and Vaia, and my sister, Foteini, for their tremendous support on this personal journey, and their unceasing help and love that aided me complete my degree.

Please forgive my any omissions.

« La lutte elle-même vers les sommets suffit à remplir un cœur d'homme. »

— Albert Camus, Le mythe de Sisyphe. Essai sur l'absurde (1942)

Nikolaos E. Kapsoulis

October 2023, Athens

Table of Contents

Table of Figures

Index of Tables

Abstract

Blockchain applicability has evolved beyond the cryptocurrency landscape over the past decade. The next generation Internet demands that different industrial applications are built on top of strong data privacy requirements. This doctoral dissertation studies the applicability of data privacy in blockchains and distributed ledgers through architecting and deploying dissimilar industry use cases. The enabling of privacy-oriented implementations over common industrial needs that concern user identification, copyright management, and cloud computing, enhances the ways data privacy is applied in each use case individually with regards to corresponding blockchain qualities. Particularly, in terms of user identification processes, a decentralized architecture with Know Your Customer processes preserving data privacy is implemented and analyzed throughout this work. Regarding copyrights management, the dissertation studies a related deployed implementation of consortium blockchain smart contracts on music industry rights management, while the latest presented use case of cloud computing proposes an unbiased Service Level Agreements assessment procedure leveraging smart contract isolation. Data privacy elaboration respects each of the aforementioned industrial architectures defining particular blockchain privacy layers. Conclusively, the dissertation discusses individually each use case's outcomes and future dimensions, and deduces a holistic architectural paradigm blockchain stack that envisions

privacy applicability in next generation Internet.

Keywords: Distributed Systems, Application Development, Privacy Preservation, Data Protection, Distributed Ledger Technology, Next Generation Internet

Περίληψη

Οι δυνατότητες ανάπτυξης εφαρμογών σε αλυσίδες-κορμού έχουν επεκταθεί την τελευταία δεκαετία σε μεγάλο βαθμό πέρα από τα κρυπτονομίσματα. Το Διαδίκτυο επόμενης γενιάς απαιτεί οι διάφορες βιομηχανικές εφαρμογές να βασίζονται σε ισχυρές απαιτήσεις απορρήτου και ιδιωτικότητας δεδομένων. Σε αυτήν την διδακτορική διατριβή μελετάται η εφαρμοσιμότητα της ιδιωτικότητας δεδομένων σε δίκτυα αλυσίδας-κορμού μέσω της αρχιτεκτονικής σχεδίασης και ανάπτυξης ανόμοιων και ενιαίων εφαρμογών. Παρουσιάζονται σχετικές υλοποιήσεις με γνώμονα την προστασία της ιδιωτικότητας των δεδομένων σε κοινές βιομηχανικές αρχιτεκτονικές που αφορούν αναγνώριση της ταυτότητας χρηστών, διαχείριση πνευματικών δικαιωμάτων καθώς και συμφωνίες επιπέδου υπηρεσίας υπολογιστικού νέφους, ενώ αναλύονται οι τρόποι με τους οποίους εφαρμόζεται το απόρρητο δεδομένων ξεχωριστά σε κάθε περίπτωση χρήσης και ανάλογα με τις αντίστοιχες ιδιότητες της εκάστοτε αλυσίδας. Ειδικότερα, όσον αφορά τις διαδικασίες αναγνώρισης ταυτότητας χρηστών, μελετάται η ιδιωτικότητα διαδικασιών Know Your Customer σε συγκεκριμένα πλαίσια αποκεντρωμένης αρχιτεκτονικής αλυσίδας-κορμού και υλοποιείται αντίστοιχα στην παρούσα διατριβή. Όσον αφορά τη διαχείριση πνευματικών δικαιωμάτων, η διατριβή μελετά μια αποκεντρωμένη εφαρμογή έξυπνων συμβολαίων αλυσίδας-κορμού κοινοπραξίας που αφορά τη διαχείριση δικαιωμάτων στη μουσική βιομηχανία. Σχετικά με την περίπτωση χρήσης υπολογιστικού νέφους, προτείνεται μια αμερόληπτη διαδικασία αξιολόγησης

συμφωνιών επιπέδου υπηρεσίας που αξιοποιεί την απομόνωση έξυπνων συμβολαίων σε επίπεδο υποδομής. Η ανάλυση της ιδιωτικότητας δεδομένων σε καθεμία από τις προαναφερθείσες βιομηχανικές αρχιτεκτονικές ορίζει συγκεκριμένα επίπεδα ιδιωτικότητας για την τεχνολογία της αλυσίδας-κορμού. Εν κατακλείδι, η διατριβή εξετάζει ξεχωριστά τα αποτελέσματα κάθε ενιαίας εφαρμογής και τις μελλοντικές τους διαστάσεις, και συνάγει μια ολιστική αρχιτεκτονική στοίβα της τεχνολογίας η οποία οραματίζεται τους διάφορους τρόπους εφαρμοσιμότητας της ιδιωτικότητας για το Διαδίκτυο επόμενης γενιάς.

Λέξεις-κλειδιά: Κατανεμημένα Συστήματα, Ανάπτυξη Εφαρμογών, Διατήρηση Ιδιωτικότητας, Προστασία Δεδομένων, Τεχνολογίες Κατανεμημένης Λογιστικής, Διαδίκτυο Επόμενης Γενιάς

1

Introduction

1.1 Decentralization, Blockchain, and Privacy

Centralized systems have been the foundation of Web2.0 Internet providing the novel convenient way of information distribution and user participatory experience since the first appearing forms of global Internet, i.e., Web1.0. However, the worldwide establishment of the technology and increased and unlimited adoption has generated a lot of pain points and pitfalls from the perspective of participants and data. For instance, a main risk of centralization constitutes the lack of user and data privacy. When users entrust their data to centralized systems, they are always dependent on their provider and their policies. On the other hand, they receive no guarantees regarding any privacy vulnerabilities. For example, is their personal information as shielded as they are promised, or does it become susceptible to unintended exposure? Centralized systems also present security vulnerabilities as they succumb to various cyber-attacks and need to be constantly and sufficiently fortified against ever evolving cyber threats. A single system breach could shatter

security and reveal classified documents exposing participants and sensitive information. Moreover, centralized systems are extremely dependent on installation infrastructure. The more a system relies on the same basis of hardware and software containers and components, the more easy it is to attack and exploit. A twin risk constitutes the single point of failure in centralization. In the event of a catastrophe, are there any fail-safes in place in order to ensure continuity and redundancy, or will the entire system collapse? Additionally, as central authorities are administering these kinds of infrastructures, clients and users should always rely and trust the actors in charge regarding all kinds of matters and issues. For instance, users should be aware of market monopoly risks that could be cast in terms of data governance and decision-making. Is there any kind of provable transparency upon relevant results? With regards to censorship and information control, what if the trusted parties ever manipulate information flow or alter customer data to align with their own interests? It may also be the case where such responsible positions have been hijacked by malicious external entities with disagreeable intentions. How well-guarded are centralized systems against a spectrum of attacks targeting to obtain entire control of the system and manipulate any kind of internal activity? Are stakeholders and users at risk as well? Is it always the case that defenses are robust enough to thwart new and sophisticated phishing, ransomware, and DDoS assaults? The frequency and importance of the aforementioned risks present the need for more resilient systems and infrastructures that address adequately these risks inheriting decentralization

principles, as are blockchains and distributed ledgers examined during this doctoral dissertation.

Blockchains and distributed ledgers offer robust system security through distributed consensus algorithms that are executed by a network of nodes. Particularly, data governance and control is distributed across a network of nodes mitigating the aforementioned risks of centralization since all parties agree to a common view of the data without any single points of failure. Alternatively, parties that disagree with the shared open source consensus protocol are excluded from the network. Consensus mechanisms as well as cryptographic techniques fortify network security, thwarting common breaches and attacks to the distributed nodes making blockchains systems more resilient. Furthermore, decisions concerning the network behavior and activities are publicly carried out through transparent, inclusive and collaborative activities among the parties ensuring a more democratic and open ecosystem and preventing censorship while building trust within the community. Blockchains and distributed ledger architectures also follow principles of diversity and redundancy in terms of adopted network infrastructures and functionalities, while they excel regarding technological innovation by creating decentralized solutions applied beyond the limits of centralization and third-party authorities control.

Blockchain technology has seen significant scientific progress as the bedrock of cryptocurrencies through repeated adoption across the globe over the past decade. Decentralized currency presented the first applicable outcome

of this technological breakthrough [1] and setup the landscape for the scientific revolution that followed. Permissionless networks with their own native tokens appeared creating their own communities around the world [2,3,4,5]. However, within a few years, the next era of programmable logic contracts, i.e., smart contracts, appeared, changing entirely the current status of the transactional logic, allowing for automated software that is executed by all the nodes of the blockchain network at specified points in time [6]. Smart contracts integrated with decentralized applications (dApps) forming end-to-end utility applications while bringing onboard a variety of use cases. Nowadays, novel and cutting-edge chains are still being created covering different needs of the market, ecosystem, builders and community [7,8].

In general, the openness and transparency of blockchain networks slowly started to create the first privacy concerns leading to the adoption of permissioned networks [9,10], which constituted the initial idea behind this doctoral dissertation. Particularly, blockchain's foundational principle of transparency ensures that all transactions are publicly recorded and shared eliminating important privacy rules. For instance, sensitive data and personal information can be revealed to anyone that participates to the network. Data that is stored on-chain is tamper-proof and immutable while at the same time it is exposed permanently creating significant issues around privacy. Moreover, blockchains and distributed ledgers provide full traceability of financial and transactional histories even allowing for the identities of the involved parties to be disclosed. The frequent adoption of account pseudonymity through

cryptographic addresses can still expose users' real identities. Finally, blockchain transparent nature strongly contradicts with privacy regulations like GDPR [11], which advocate for the right to be forgotten and personal data protection.

1.2 Contribution and Innovation

In this doctoral dissertation, three (3) industrial architectures oriented around privacy have been investigated, designed, and implemented in the context of decentralization. The first use case refers to a Know Your Customer (KYC) privacy-preserving architecture that utilizes blockchain smart contracts in order to enable and deliver user data privacy [12]. In centralized systems, KYC processes lack important privacy principles that usually lead to unnecessary exposure of sensitive information and personal data. The developed framework protects the privacy of KYC user data incorporating two distinct types of smart contracts, a public one operating for the registration, submission and validation of KYC documents, and a private one responsible for the Create, Read, Update, Delete (CRUD) operations on the documents. The end result constitutes an innovative system that regulates data transparency and protects users privacy through a decentralized structure that ensures users have control over their data.

The second use case introduces an advanced end-to-end decentralized application on a permissioned blockchain environment, especially tailored for

the purpose of governing and managing musical rights through smart contracts utilization [13]. In the context of music industry, the architected use case innovates by governing conflicting musical rights held by diverse domain entities applying private smart contract methods. At the same time, the proposed implementation unifies disparate business sectors within the industry and connects various consortia and nonprofit blockchain associations in a cohesive manner.

The third investigated use case examines Cloud Service Level Agreements (SLAs) assessment procedures [14]. Given the disproportionate influence of large corporations that tend to monopolize measuring methods for SLA metrics and Key Performance Indicators (KPIs), clients and consumers result inside controlled environments with impartial SLA assessments. Towards SLA self-assessment, the presented architecture introduces a fair approach to SLA assessment procedure with inherent transparency and privacy by harnessing permissioned blockchains equipped with Trusted Execution Environments (TEEs). The use case deploys isolated smart contracts that allow for secure data calculations and enclaved computations. In the outcome ecosystem, Infrastructure as a Service (IaaS) providers and their consumers are collectively agreeing to pre-approved SLA rules and regulations that define an SLA's metrics and guarantees, are submitted on-chain and are audited in a decentralized and fair way, while the system has been discussed and accepted within the Hyperledger Open Source Community of The Linux Foundation [15].

The examined architectures are approaching the matter of privacy applicability on blockchain in various ways. In an overall and holistic view, the following layers are offering an important advantage to ecosystem administrators or application designers and builders that aim to apply privacy to their blockchain use case or dApp. The doctoral dissertation envisions the standardization of the blockchain privacy stack through the examined use case-driven investigations as depicted in Figure 1.

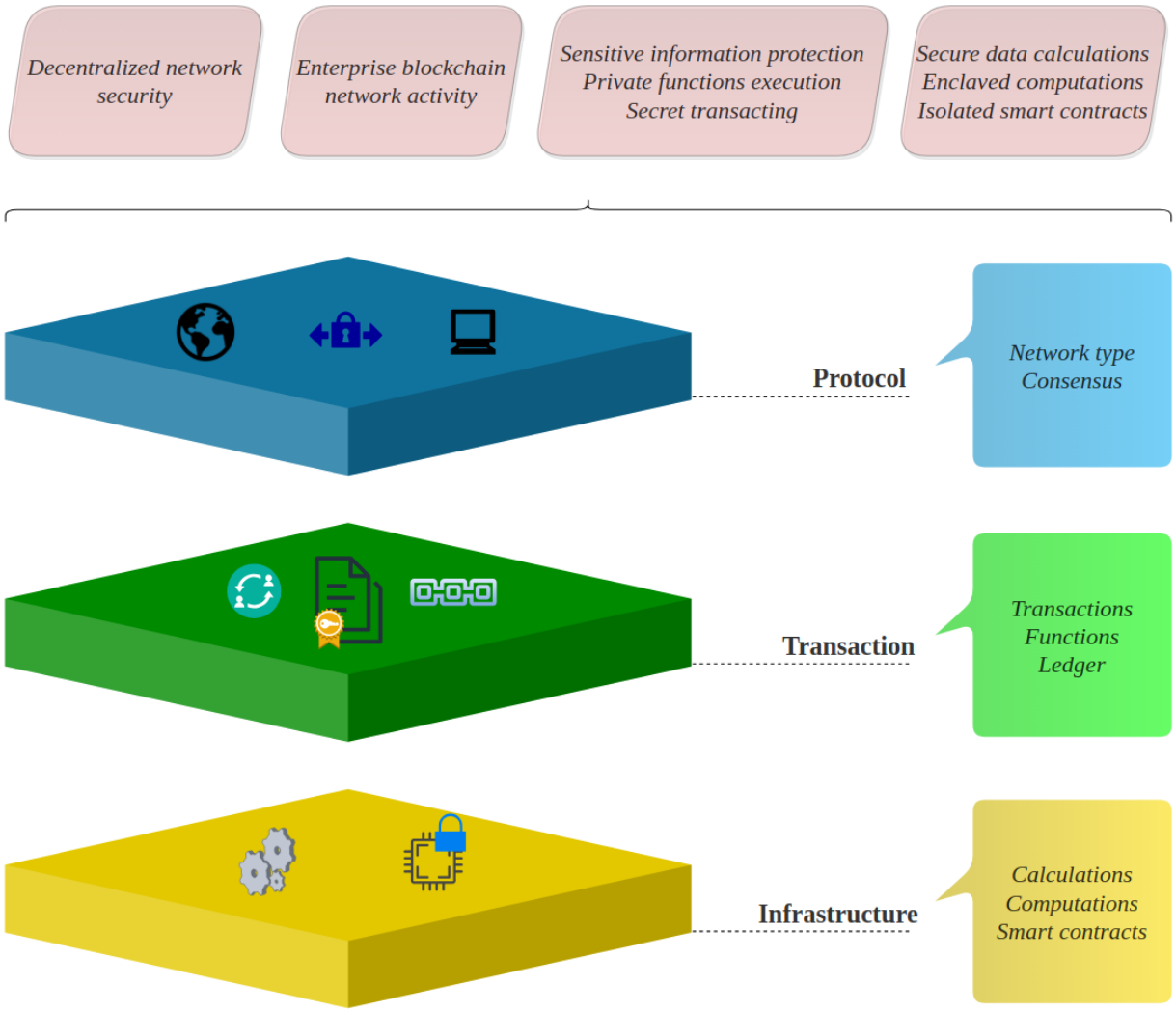


Figure 1: Envisioned Blockchain Privacy Stack for Web3.0

In the envisioned blockchain privacy stack for the next generation Internet of Web3.0, the privacy layers holistically provide the following:

- Decentralized network security.
- Enterprise blockchain network activity.
- Sensitive information protection with private function execution and secret transacting.
- Secure data calculations and enclaved computations with isolated smart contracts.

1.3 Structure

The doctoral dissertation continues with the literature review of relevant architectural deployments in chapter 2, introducing related research works and use cases on blockchains and distributed ledgers. Chapter 3 examines a decentralized architectural deployment on user identification systems with KYC processes orienting around privacy. Chapter 4 presents consortium copyright governance for a music industry use case through dedicated smart contracts on permissioned blockchain with enabled privacy features. Chapter 5 introduces a cloud computing architecture with strong enabled privacy through smart contract isolation resulting in an honest and legitimate system of SLA assessing metrics for the Cloud, as featured as well in Hyperledger Foundation. Chapter 6 discusses the conclusions of the dissertation around the

envision blockchain privacy stack for Web3.0 as well as the different future research directions of the presented architectures.

2

Literature Review on Relevant Architectural Implementations

Initially introduced as the underlying framework for cryptocurrencies, blockchain appeared in the technology sector through the creation of Bitcoin in 2009 [1]. Bitcoin presented an innovative peer-to-peer (p2p) electronic cash system that is focused on establishing a secure and decentralized ledger for recording and validating digital transactions. Following Bitcoin's popularity, dissimilar cryptocurrencies appeared in the technological field, offering slightly different characteristics [2,3]. However, as research and development within the field progressed the upcoming years, a deeper comprehension of blockchain's potential began to emerge beyond its application in the financial realm [16]. Blockchain technology inherent properties, such as transparency, immutability, and distributed consensus, paved the way for releasing its full potential of decentralized applications (dApps) with Ethereum around 2014 [6]. Consequently, the possibilities exploded into a myriad of industries, spanning supply chain management, healthcare, identity verification, and beyond [17,18,19]. Blockchain decentralized trust, data management, and transactional processes promoting the development of innovative solutions that

operate under a common network of rules without requiring the decision-making of intermediate entities. Therefore, the creation of various architectural deployments comprised of both transactional and application-oriented use cases that combined the aforementioned properties delivering the complete potential of blockchain.

A plethora of distributed applications (dApps) have been proposed within academic research, spanning sectors such as government [20,21], funding mechanisms [22], and beyond. The convergence of blockchain technology with Internet of Things (IoT) has showcased various successful applications' instances [23]. Decentralized applications have been also conceptualized to address the IoT sensors data sharing [24]. In a similar context, Papadodimas et al. [25] have introduced a platform built on the Ethereum blockchain that acts as a marketplace for IoT weather sensor measurements, facilitating transactions through the Sensing-as-a-Service (S2aaS) model for the purpose of data monetization and value extraction.

In recent years, a multitude of smart contract deployments have implemented digital tokens as well. The exploration of diverse smart contracts, including payment tokens and asset management, originate from media industry domain. Blockchain technology along with user-generated multimedia content has created a suitable venue for creators to monetize their content [26]. With respect to the examined use cases in the doctoral dissertation, their related literature review is discussed as follows.

2.1 Literature on KYC User Identification Systems

Regarding identification systems, various blockchain-based identity management and authentication frameworks have been proposed. Particularly, research works [27] and [28] target the blockchain potential of decentralizing credential ownership and furnishing a universally accessible protocol for validating records within the immutable data chain. Mikula et al. [29] introduced a proof-of-concept system for authorization and authentication that is strategically aligned with identity management rooted in Electronic Health Records, a context that demands an immutable and auditable history for patient data. Widick et al. [30] proposed a blockchain-oriented authentication and authorization framework that controls resource access to IoT devices. Simultaneously, the research investigation by Mudliar et al. [31] combines blockchain technology for the deployment of a national identity use case.

The aforementioned works implement value exchange protocols through blockchain transactions and smart contracts that ultimately require the adoption of KYC processes. In this direction, the presented user identification use case in chapter 3 successfully deploys smart contracts for exchanging value within the media industry in a decentralized manner, integrating KYC process handling for on-chain and off-chain data. Recent research studies data management and KYC within the realm of blockchain applications. Shbair et al. [32] contributed a blockchain-based KYC proof-of-concept system and orchestration tool geared towards private blockchain environments. Their work

prompts for new extended research regarding security and privacy of blockchain applications. Norvill et al. [33] proposed a system that streamlines the KYC process through automation and permissioned document sharing. Similarly, Zhang and Yin [34] explored a blockchain-based digital copyright management system that uses PBFT consensus mechanisms enhanced by Tendermint [35], and that allows for user account management strategies and applications for digital rights management. Their work focuses on designing and implementing decentralized smart contracts for KYC processes.

Moreover, despite the facilitation of security deployed with blockchain in such systems, it is often the case that the trade-off between blockchain transparency and privacy should be well-designed. Bhsaskaran et al. [36] presented a smart contracts architecture engineered to orchestrate consent-driven, double-blind data sharing within a Hyperledger Fabric blockchain network. Their work eases data submission, validation, and retention within the transaction ledger, accommodating varied consent rules and privacy policies. Vishwa et al. [37] proposed a decentralized data management system that deploys data privacy and control for multimedia files. In their presented architecture, an external data lake positioned as a centralized data storage solution within a cloud environment hosts the transaction details of all blockchain activity. As users access the blockchain, they activate the identification process by broadcasting their ID. After they obtain system acceptance through the consensus node majority, the system triggers the allocation of a new identity and the associated access permissions. Their

approach also leverages the added utility of InterPlanetary File System (IPFS) [38] in order to output a decentralized application that encapsulates successful smart contract deployments and related software components that automate the KYC process.

2.2 Literature on Copyrights Governance

The broader application of blockchain technology extends to the development of Digital Rights Management (DRM) mechanisms. DRM employs information security technology in order to ensure legitimate usage of digital media content, protecting content producers' income [39]. Thanks to the inherent decentralization, tamper-resistance, and scalability, blockchain technology presents high potential for resolving issues related to digital copyright registration, a crucial aspect of securing original creators' rights [40]. For instance, Xu et al. introduced a DRM scheme that deploys consensus mechanisms, smart contracts, digital signatures, and hash chains to ensure real-time copyright validation and verification [41]. In order to tackle issues of free consumption and unauthorized spreading, Ma et al. proposed a blockchain-based DRM scheme that aligns the right content with the right users while ensuring trust and conditional traceability [42]. Nevertheless, implementing blockchain-based DRM systems introduces important challenges, such as end-to-end latency, which can be mitigated through customizing the proof-of-work algorithm as presented in [43]. Beyond

technical considerations, legal implications also arise from system architects whether digital content should be stored on-chain, alongside ownership metadata, or off-chain [44].

In music industry, various blockchain-based copyright management implementations have emerged to enhance copyright data accuracy and availability, with ultimate goal to foster the sustainability of music careers [45]. For example, BMCProtector utilizes the Ethereum blockchain to protect music copyrights and ensure income for content owners while tackling piracy through encryption and watermarking [46]. Furthermore, Gomaa introduces a digital currency on a permissioned blockchain to securely share and track digital content, facilitating lower barriers for musicians and equitable royalty payments [47]. Chen et al. leverage blockchain's core features and properties in order to address music copyright issues like ownership disputes [48]. Similarly, Ouyang et al. have created a copyright management platform using blockchain technology in order to combat music plagiarism [49]. On the other hand, Ito et al. accurately stress that effective blockchain usage requires proper incentive mechanisms design for intellectual property management systems [50].

In this context, the presented copyright management implementation details an end-to-end blockchain-based framework for musical rights governance, aligned with CMO objectives in the music industry. The solution encompasses conflicts detection originating from multiple copyright claims for the same music asset. The framework also incorporates a monetary incentive mechanism to discourage exploitative behaviors related to claims submission

and reduce conflicts.

2.3 Literature on Blockchain SLA Assessment

With respect to scientific research around Cloud SLA assessment and blockchains, this section mentions and analyzes relevant works.

To begin with, Nguyen et al. [51] suggested an SLA related architecture for assessing and enforcing tourism SLA agreements using distributed ledger software. The authors' presented method revolves around preserving the integrity of the SLA assessment process through the inherent immutability of the underlying technology. In their approach, an automated SLA monitoring and computation process takes place within the blockchain infrastructure, ensuring successful SLA evaluation with specific acknowledgment for end-users. On the contrary, the respective SLA assessing solution in doctoral this dissertation introduces the notion of self-assessment for SLAs architecting and implementing a technological framework where SLA intelligence unfolds in a fully decentralized and private manner that is distinct from third-party on-chain involvement.

Furthermore, Ranchal and Choudhury [52] proposed an autonomous and trustworthy framework for continuous SLA monitoring within a multicloud ecosystem. Their approach leverages blockchain and smart contract properties in order to concretely identify SLA violations in a hierarchical system structure. As outlined in their work, their solution tackles the SLA assessment

process in a multi-tiered cloud environment with diversely installed rules and regulations. Additionally, Alowayed et al. [53] proposed a blockchain-based network provider evaluation system based on providers' adherence to their SLAs regarding interconnection agreements. In their technological framework, a metric measurement mechanism verifies SLA scores for each provider, which are later evaluated on-chain. At the same time, their strategy incorporates a privacy-preserving protocol for SLA agreements, aiming to objectively define a network provider's SLA score and privately store it on-chain for authorized end-user access. On the other hand, the approach presented in chapter 5 relies strictly on an SLA intelligence mechanism agreed upon between the customer and the provider. This mechanism takes into account respective algorithmic drivers for SLA monitoring and computation, while it is executed on-chain as per the mutual agreement.

Additionally, Uriarte et al. [54] proposed an SLA management framework facilitating the specification and enforcement of dynamic SLAs in order to track and define service parameters that lead to SLA modifications over time. Their two-level blockchain-based architecture converts an SLA into its smart contract equivalent, guiding dynamic service provisioning on the first level. On the second level, their solution generates objective measurements for SLA assessment through a federation of monitoring entities that scales for multiple nodes. In a similar direction, Alzubaidi et al. [55] presented a blockchain-based approach to assess SLA compliance and enforce consequences through a diagnostic accuracy method for dependability validation. Their approach

assumes trust in service providers to acknowledge SLA breaches and execute relevant compensations. Another previous work of theirs [56] proposed a conceptual blockchain-based framework to address limitations associated with traditional SLA management approaches. Their rationale argues that SLA management should occur in a distributed environment that is not controlled by a few central third-party authorities. In similar alignment, the corresponding SLA consensus solution presented in this doctoral dissertation builds a system based on the same principles, employing on-chain private smart contract structures to protect SLA business intelligence from third-party participants in the blockchain network.

Furthermore, D'Angelo et al. [57] analyzed challenges and requirements for enforcing accountability in Cloud infrastructures where SLA violations are significant and frequent. The authors suggest that smart contracts and blockchain technologies are offering a crucial contribution to accountable Clouds. Finally, W. Tan et al. [58] introduced a performant and secure SLA model where blockchain ensures trust among IaaS providers, clients, and third-party monitoring entities. The authors highlight the lack of an effective supervision mechanism for third-party monitoring and an efficient compensation mechanism for SLA breaches. Their presented model effectively supervises service providers on the blockchain using dedicated smart contract mechanisms. In this dissertation, the respective SLA consensus solution includes similar concepts as it presents an approach where providers and customers participate only at the beginning and end of the workflow. This

ensures fair and private SLA monitoring and computation throughout the entire SLA business intelligence process.

3

Public and Private Smart Contracts for User Identification Systems

3.1 Introduction

User identification systems and identity management are strongly linked with the rules around KYC procedures forming the bedrock of anti-money laundering endeavors for organizational and financial institutions. This technological domain presents high interest and applicability nowadays, particularly in the context of financial technology applications implementations on blockchain platforms. In this direction, KYC processes maintain the responsibility of harmonizing robust identity management with privacy-enhanced techniques, ensuring the alignment of such applications with regulatory frameworks such as GDPR [11]. The major motivation behind the current research aims at the deployment of novel, streamlined, and efficient KYC processes respecting privacy and specifically tailored for decentralized applications on blockchain networks. In order to fulfill this objective, the architected and implemented framework combines highly decentralized

technologies, including IPFS and a Quorum blockchain [59] deployment. Leveraging dedicated smart contracts, the presented framework facilitates the execution of multi-party KYC processes within the blockchain network enabling user privacy protection with two (2) types of developed smart contracts.

In particular, a public smart contract facilitates the registration and submission of KYC information by the users. The data is stored on an integrated IPFS storage system while the corresponding blockchain transactions occur inside the permissioned blockchain network of Alastria (T Network) [60]. The public smart contract also enables administrative users to assess the expiration dates of users' KYC documents. Additionally, a private smart contract operates in terms of CRUD operations on KYC document entries inside the corresponding file repository (IPFS). In general, the private contract ensures the secure handling of the related decentralized activities. The outcome constitutes an innovative system that enables a streamlined approach to operations, through a simplified schema structure and seamless integration of diverse technological elements. In principle, the architecture emphasizes the pivotal role of blockchain technology, which is integral to the system's overall clarity and effectiveness. This framework is carefully designed in order to achieve optimal transparency within its blockchain structure.

3.2 KYC Authorization Architecture

In this section, the analysis revolves around how user authorization functions within a blockchain environment, specifically concerning KYC standards. The central focus here is to ensure user privacy through the utilization of a permissioned blockchain framework. This is ultimately accomplished by employing two (2) distinct types of smart contracts. The first, known as the "KYC Smart Contract," handles various tasks including CRUD operations on user data through the corresponding blockchain transactions. Conversely, the second one, namely "KYC Admin Smart Contract," manages transactions linked to the user data repository that is hosted within IPFS.

The integration of blockchain technology with KYC processes standards, in sync with carefully developed business-logic smart contracts, establishes a streamlined, enterprise-oriented framework that is characterized by its simplicity and operational efficiency. Within this section, a systematic breakdown is provided, encompassing the process of authorizing users as per KYC standards within the blockchain network. Privacy considerations for users are highlighted along with the application's architecture, the dedicated smart contract implementations, and the concrete outcomes originating from a real-world use case.

3.3 KYC & Protecting User Privacy

KYC procedures own a very important role when it comes to maintaining security inside permissioned blockchain networks of companies and institutions while registering diverse clients across different worldwide

jurisdictions. However, in order to ensure legit security, it is required to adhere to specific conditions regarding user privacy. The presented KYC process initiates by enabling the client registration, which marks the first step of the onboarding process. As a legitimate client enters their details into the KYC Registration scheme of the broader blockchain ecosystem, several actions unfold as follows. The authorization procedure concerning users that enter a company or a consortium blockchain network subjects to security measures maintained by the KYC mechanism. For instance, the entity or group owning the blockchain network should verify that the user is a legal citizen and possesses a background that is appropriate for entry in the network. At this point, an external entity comes into play, namely the KYC Document Evaluator. Acting as a third-party non-profit validator, the entity approves the submitted KYC documents, bringing operational simplicity to the system. Consequently, the business network is secured against money laundering, identity theft, or other illegal activities, such as global terrorist finance. The aforementioned steps form the bedrock of the KYC authorization process of users that participate to blockchain transactions within global enterprise networks, whether cryptocurrencies are involved or not. At the same time, through the presented system, the users themselves avoid the risk that their personal information being shared or sold to third-party entities or intelligence agencies. Their sensitive information regarding identity, family, property status, or financial records – which are requested during user authorization and network entry as part of the onboarding process – remain shielded from

immoral trading and unethical data swaps.

Furthermore, within the decentralized structure of the presented system, a decentralized method for storing KYC-related documents of network members is employed. This decentralized method is akin to BitTorrent-like peer-to-peer architectures and protects customer data privacy as of paramount importance. Customer information is protected using a one-way functions, namely hashes. In the end, the entity possessing the data and the one-way function can obtain the permitted information, yet they are unable to access it holistically and physically. Simultaneously, the system offers seamless compatibility with blockchain technology.

An essential aspect of the system's overall development involves the sustained presence of users within the network. Clients are able to maintain access to the blockchain network for a specific and predetermined period of time. After this duration, their validity expires and they are excluded from the network. Instances of users exclusion follow a specified number of appropriate warnings, coupled with options for extending their expiry date through re-evaluation of newly submitted KYC documents.

3.4 Architectural Approach

The aforementioned landscape of KYC systems in sync with the respective privacy requirements described in the previous section, led to the conceptualization and construction of the blockchain-based KYC system.

Figure 2 depicts the implemented application architecture and outlines the various processes in a vector graphics diagram.

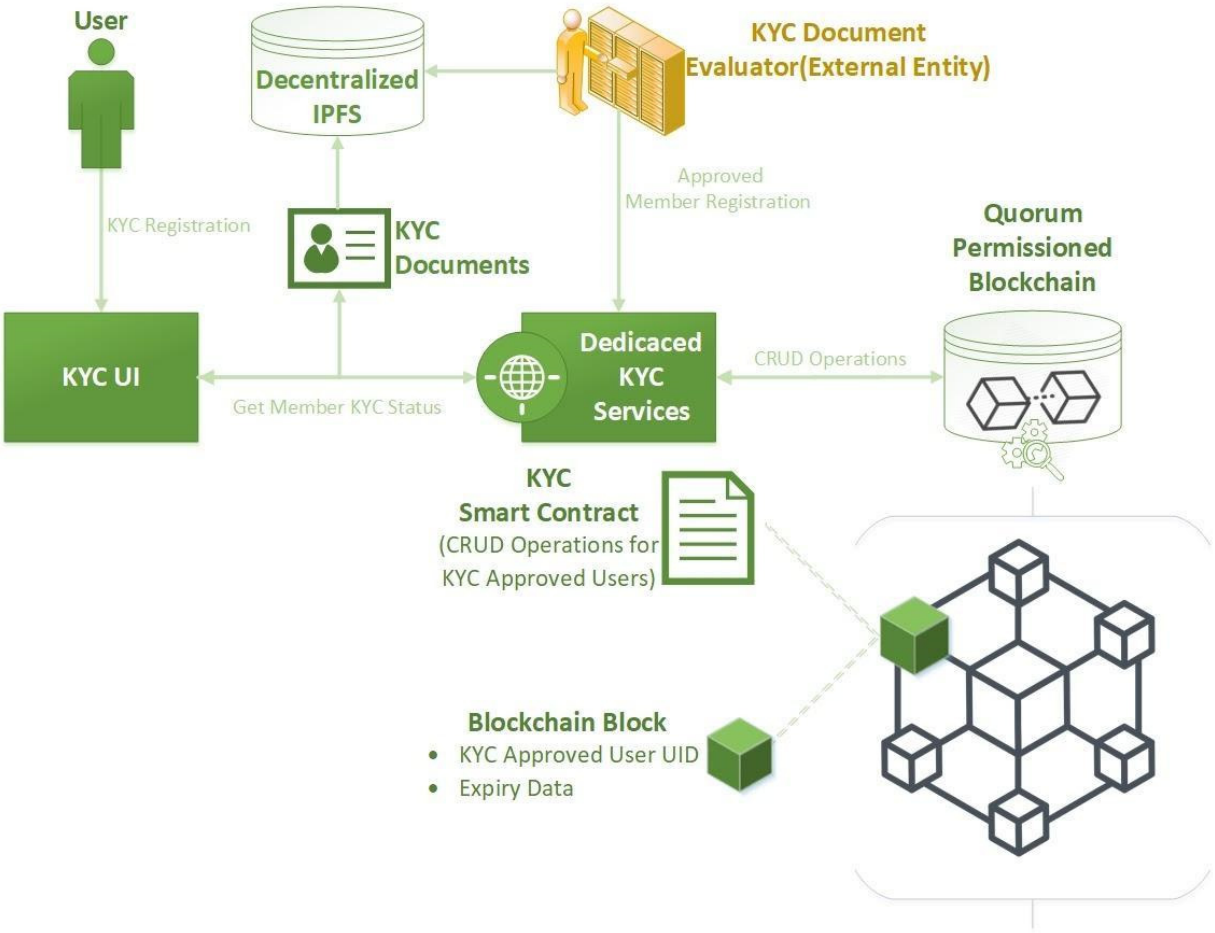


Figure 2: Architectural development and processes elaboration

The overall architectural approach of the system centers on operational simplicity while emphasizing on blockchain technology. The system's components and entities functionalities are explained through the logical flow of the KYC procedure in this system. Initially, the user, being a prospective customer of the system, engages in the "KYC Registration" process by submitting their KYC documentation through a user-friendly interface called

"KYC UI" (Figure 2). Notably, users are responsible for accurately providing the required information from their side, while a new scanning mechanism is designed to identify any possible misconduct and promptly exclude inappropriate users from the process as explained below.

Upon successful document submission, the KYC documentation is stored within the decentralized, peer-to-peer, blockchain-friendly repository of IPFS. IPFS protocol establishes a resilient system for file storage within a decentralized peer-to-peer network which is blockchain-compatible. However, IPFS employs special security measures for the stored data, relying on cryptographic hashing techniques and mechanisms. Each data chunk stored on IPFS obtains a distinct address derived from a specialized data-hashing process. The latter utilizes an one-way function that transforms input data into a singular hash, without the ability to reverse this process. Similarly, IPFS content addressing assigns a single hash, such as "QmVHVH9WeGy9tTNN9dViqvDn7N79XJJUseKXD1rpyLVckK" which serves as a pathway to the content data. Accessing the content data requires knowledge of the corresponding Content Identifier (CID).

Following the secure storage and validation of KYC data, a process is initiated to store specific information within the blockchain. This information encompasses only the essential details required to identify the KYC-approved user, along with the validity period proposed by the candidate client. Consequently, sensitive information is not stored within the blockchain

ensuring that network members can't access the user's sensitive data, only their membership validity. Subsequently, the process continues by interacting with the blockchain network and storing the aforementioned data. The latter interaction demands specific libraries and dedicated drivers that establish connections and facilitate information exchange between the involved components. The "Dedicated KYC Services" component provides the necessary software and drivers to establish connection and interaction with the blockchain, as well as the associated smart contracts.

Regarding the blockchain implementation, the system employs a Quorum blockchain. The selection of Quorum was driven by several factors, notably its foundation on the established Ethereum blockchain [59]. Quorum's capability to create smart contracts using Solidity [61,62], coupled with its security and permission features led easier to its adoption. As previously stated, the data stored in the blockchain, particularly within a smart contract, is designed to be sufficiently redundant for user identification while maintaining the anonymity of the user. Engaging with the dedicated smart contracts requires that the development of specific functions is accessible to the "Dedicated KYC Services" component which provides the appropriate data to confirm a given user account KYC approval.

3.5 Implementation of Smart Contracts with IPFS Storage

Both IPFS and Quorum are aiming to establish a decentralized system that not only protects but also enhances the privacy and security of user personal information. As detailed in the previous section, IPFS serves as the decentralized repository that hosts all member-related sensitive information. As illustrated in Figure 3, IPFS protocol divides KYC files into fragments, generating an endpoint object that links the various segments of a user's KYC files.

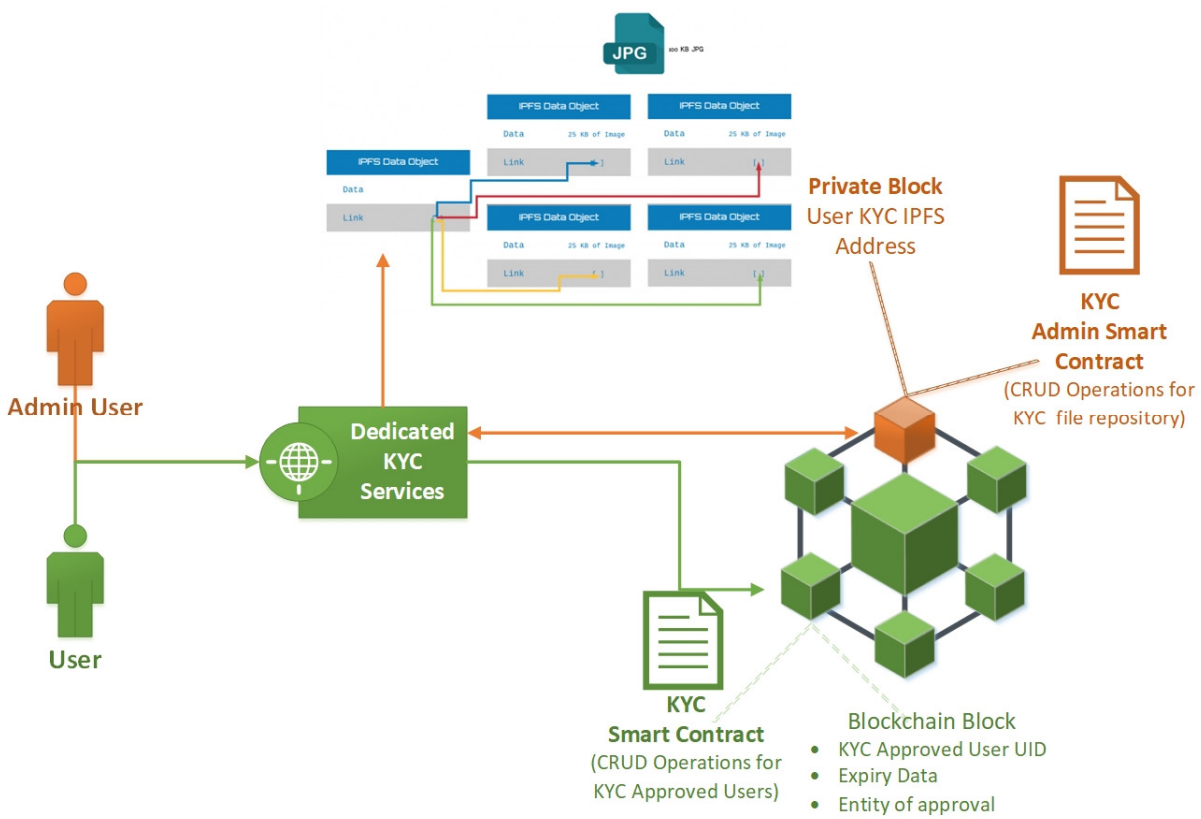


Figure 3: Public (user) and private (admin) KYC smart contracts.

In order to access the data contained inside IPFS, one must possess the corresponding address of the endpoint object. Quorum permissioned blockchain facilitates the creation of private or permissioned blocks,

accessible solely to specific users, while simultaneously broadcasting only the hash of these private contracts and blocks to the rest of the blockchain. This broadcast is designed to validate the integrity of these blocks across the entire blockchain. As depicted in Figure 3, the Quorum blockchain network deployment hosts both private and public smart contracts, each providing different levels of information access.

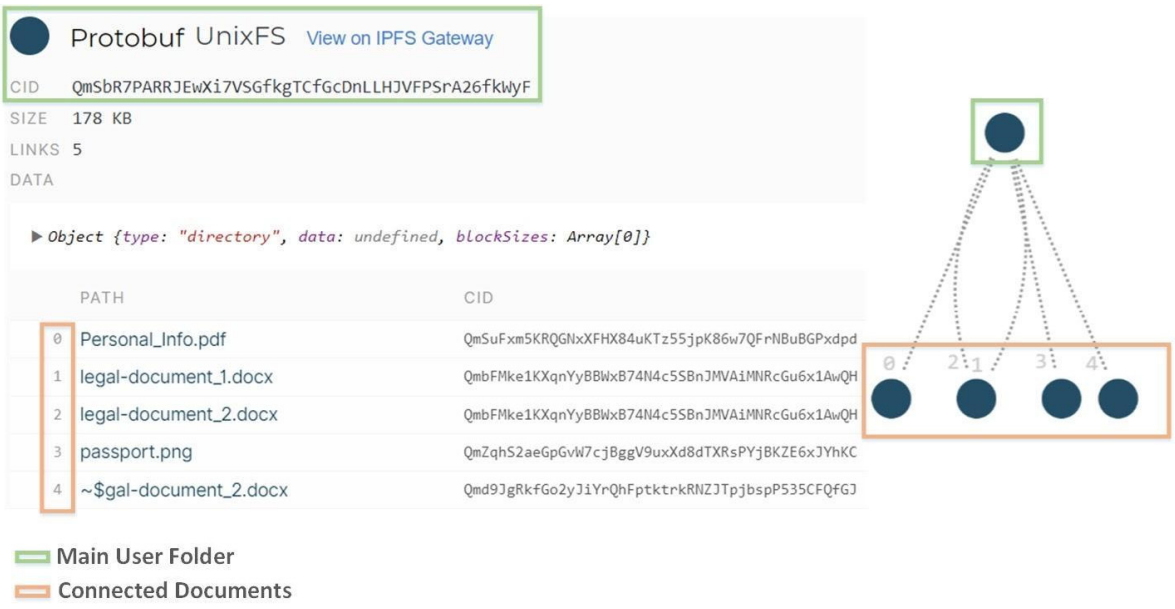


Figure 4: IPFS content-addressed file system.

As described in Table 1, the public KYC smart contract incorporates all the detailed functions that are necessary in order to facilitate the CRUD operations of the users information being stored within the corresponding smart contract's structures.

Function Name	Description	Input	Response
GetKYCMemberApproval()	This function is responsible for delivering basic KYC information upon request. All the data returned from this function do not contain any sensitive information about the user, only the minimum amount of information in order to identify the User and the time period this Member is approved for.	**Address:** User account address	**Date:** Expiration date of the KYC approval. **String:** Entity that approved the member
UpdateKYCMember()	KYC approval of an account needs to be updated when the approved period has passed, and also there are cases in which an approved member needs to be banned due to malicious activities. This function is responsible for updating the KYC information stored in the blockchain.	**Address:** User account address **Date:** Renewed expiration date **String:** Entity that approved the member **String:** Admin account private key	Success message
CreateKYCMember()	When a new member is approved by the system, the KYC info must be stored in a structure inside the Smart Contract. This method is responsible for creating a new record with the KYC info of a new member.	**Address:** User account address **Date:** Renewed expiration date **String:** Entity that approved the member **Bytes32:** Admin account private key	Success message

Table 1: Public smart contract methods descriptions.

On the other hand, private smart contracts grant access to the KYC documents that are stored in IPFS, enabling document evaluation or other kinds of updates. To access a user's KYC documents in IPFS, admin users require the corresponding CID.

Function Name	Description	Input	Response
GetUserCID()	This function is responsible for returning the CID of the folder containing the KYC documents. It is important to mention that in order to access the functionality of this method, the smart contract requires the user accessing this method to be in the pool of users that have security clearance to access this smart contract. Moreover, the function also requires the hashed private key of the user accessing this method.	**String:** User account ID **String:** Admin hashed private key	**String:** Corresponding CID
CreateUserCID()	When the KYC documents are successfully stored in the IPFS, this method is called to store the KYC CID in order to make them discoverable and accessible to the admin users of the private smart contract.	**String:** User account ID **String:** Folder CID **String:** Admin hashed private key	Success message

Table 2: Private smart contract methods descriptions.

Particularly, the CID is assigned by IPFS nodes to the respective file system folder containing the user's KYC files. IPFS links these files together, allowing admin users to access and modify them through a single entry point, as depicted in Figure 4.

Similarly, the security of these CIDs is guaranteed within the private KYC smart contract as they can be accessed exclusively by authorized admin members. These network members possess enough authorization and are able to invoke smart contract methods returning CIDs of users, thus, granting access to their corresponding files. In Table 2, the outlined functions are callable only by specific blockchain nodes with administrator privileges.

3.6 Use Case Outcomes

This section presents the implementation and outcomes of the use case through a gradual elaboration of the system's followed end-to-end procedure. Operating within an enterprise blockchain framework where every new user (i.e., a customer organization) requires accurate validation, the proposed KYC privacy-focused architecture introduces a direct and secure decentralized approach that is crucial for managing user data protection in permissioned blockchain networks. When it comes to sensitive user data, such as financial records and family and property status, the general absence of user data privacy among network participants constitutes a major challenges in permissioned blockchain networks. The presented architecture offers an automated solution for securing sensitive user data, thereby ensuring high-

level user privacy within permissioned blockchain networks. The development of a well-structured implementation that hosts business intelligence smart contracts necessitates for the achievement of such a setup. The targeted outcome is a fully operational scheme that can benefit any consortium requiring data privacy within their own blockchain network, while also incorporating various state-of-the-art technologies, such as public-permissioned blockchains and IPFS.

The following gradual step sequence details the use case's implementation and outcomes. Initially, a new user inputs their information through "KYC UI" (Figure 1), which involves the uploading of their KYC documents and specifying the desired validity period if approved (i.e., the expiration date until which they maintain eligibility within the blockchain network). Afterwards. the External Entity ("KYC Document Evaluator") examines the uploaded documents, and upon validity confirmation, an admin member invokes the private smart contract method "CreateUserCID()" in order to initiate user approval. Subsequently, the KYC documents are stored in the IPFS repository, while the private contract method "GetUserCID()" returns the corresponding CID to the admin profile. Next, the user obtains approval to enter the permissioned blockchain network. Concurrently, the public smart contract method "CreateKYCMember()" establishes the new member's network details and sets the corresponding expiration date. These details are stored on-chain within the corresponding smart contract member structure. Finally, the new user gains access to the permissioned network.

When admin members require to check a member's identification or verify the user's expiration date, they invoke the public smart contract method "GetKYCMemberApproval()", receiving only the necessary information as response from the IPFS decentralized storage also including the External Entity's name that approved the member. The response data does not fetch sensitive user information like family status or financial records from IPFS, while it is stored within the smart contract's storage, as depicted in Figure 5:

```
struct registeredMember {
    address memberAddr;
    uint256 time;
    string approveEntity;
}
```

Figure 5: Member non-sensitive information is stored in the blockchain block (on-chain).

Sensitive information is stored on the content-addressing IPFS file-system and accessed only by authorized admin members. Similarly, for instances where a member's approved period expires or if their behavior within the network is malicious, admin members are authorized to call the public contract method "UpdateKYCMember()" in order to renew or shorten the validation period in the context of a warning action. This smart contract function updates a member's "time" and "approveEntity" fields, either by extending their expiration date through the same approving entity or a different one, or by reducing the validation period for misbehaving members. The latter smart contract methods can be useful and contribute to every process executed within the proposed system. The public “KYC Smart

Contract” and the private “KYC Admin Smart Contract” are deployed on the Alastria Network through the Quorum Maker Utility [63] in order to monitor smart contracts and other blockchain activities and statistics. Figure 6 presents both the public "KYC Smart Contract" and the private "KYC Admin Smart Contract" from the perspective of application monitoring.

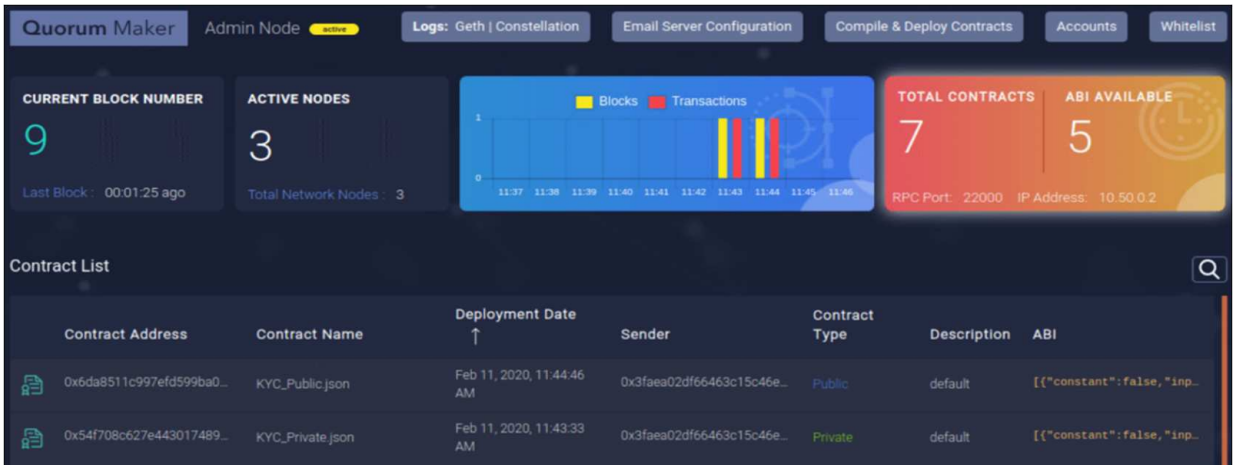


Figure 6: Quorum Maker Utility to monitor smart contracts.

From a technical point of view, the developed smart contracts are deployed onto the popular public-permissioned blockchain network of Alastria. This network is built on Quorum, an Ethereum-based blockchain implementation, and holds necessary permissions in order to accommodate decentralized applications. The compilation and deployment of smart contracts use the "Truffle Suite," and the Solidity version ^0.5.11. The Quorum and IPFS integration within the entire presented project represents a substantial research effort, paving the way for future directions in user information storage and blockchain-based management.

4

Consortium Smart Contracts for Copyright Governance

4.1 Introduction

The music industry encounters deep-rooted challenges that are related to managing copyrights and allocating royalties. These issues have been enhanced by digital transformation and the rise of streaming platforms. Efforts to address these problems have often fallen apart and short. One notable example is the Global Repertoire Database (GRD), a collaborative project involving various organizations such as music labels, software companies, collective management organizations (CMOs), and multinational unions. Unfortunately, the GRD dissolved in 2014 after four years of growth and conflicts, leaving behind a debt of $13.7 million [64]. Music work copyrights domain suffers from issues due to the involvement of numerous stakeholders and the lack of coordinated communication among them [65]. As shown in a simplified manner in Figure 7 the relationships between the involved industry stakeholders can lead to diverse copyrights and royalty documents distributions, complicating the process of tracking and verifying accurate

copyright data for CMOs.

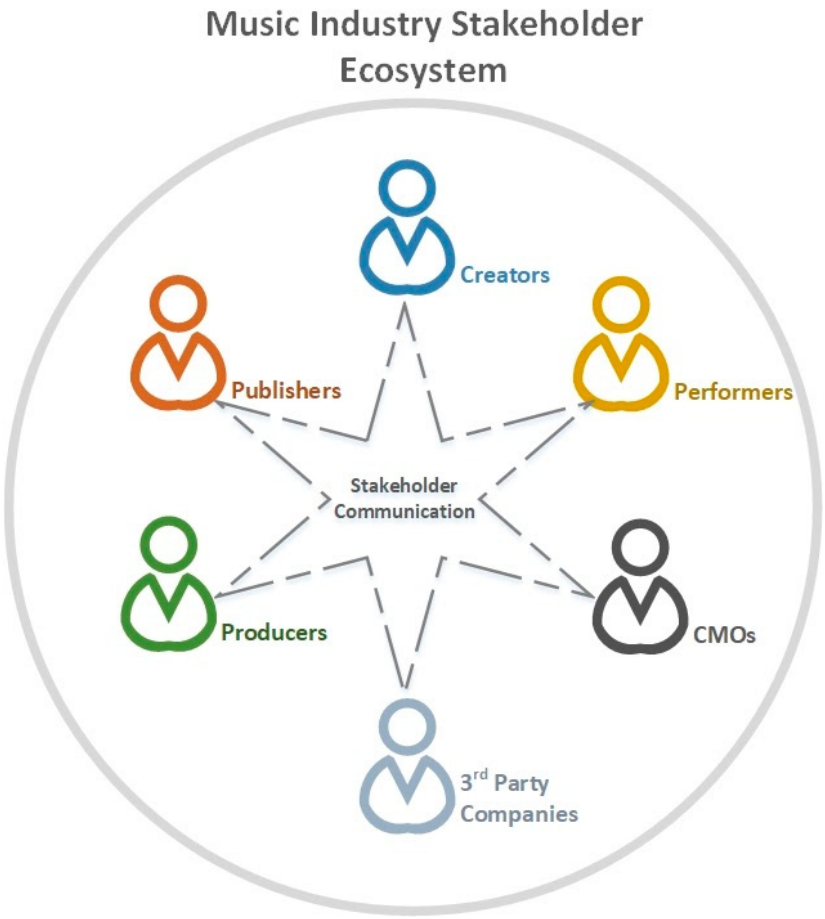


Figure 7: The ecosystem of music industry stakeholders.

Given the ecosystem's nature and the complete digitization of music creation and distribution, modern solutions for managing copyrights and distributing royalties have gained increased traction. Blockchain technology emerges as a promising tool to tackle such kinds of challenges [66]. Essential blockchain concepts like transparency, decentralization, and immutability can establish a stronger and more accessible system for all involved parties. The presented architectural implementation introduces a blockchain framework for

governing and managing musical rights.

The framework aims to simplify the entire music rights management process, ranging from declaring copyright ownership to promptly sharing up-to-date information with all stakeholders. It also includes a mechanism to resolve conflicts among registered stakeholders on a blockchain-based network, resulting in significant improvements of related organizational processes:

- Transparency: Anyone interested can participate and verify the status of their assets.
- Trust: No one is able to manipulate statements.
- Traceability: Ability to track the claims an asset has received over time.
- Decentralization: The database isn't controlled by a single entity; contributions come from a distributed group of parties.
- Conflict resolution: Unification of assets in a comprehensive view detects conflicts at early stages.
- Efficiency: Simplification through an interoperable solution sharing information among stakeholders and integrating with their backend systems.

The decentralized framework for managing music rights encompasses essential blockchain features and capabilities. The main functions include creating, updating, and identifying conflicts in music rights, while it is important to note that all the business intelligence (program blocks) responsible for identifying conflicts and managing music rights is

strategically integrated into the blockchain using smart contracts (Figure 8).

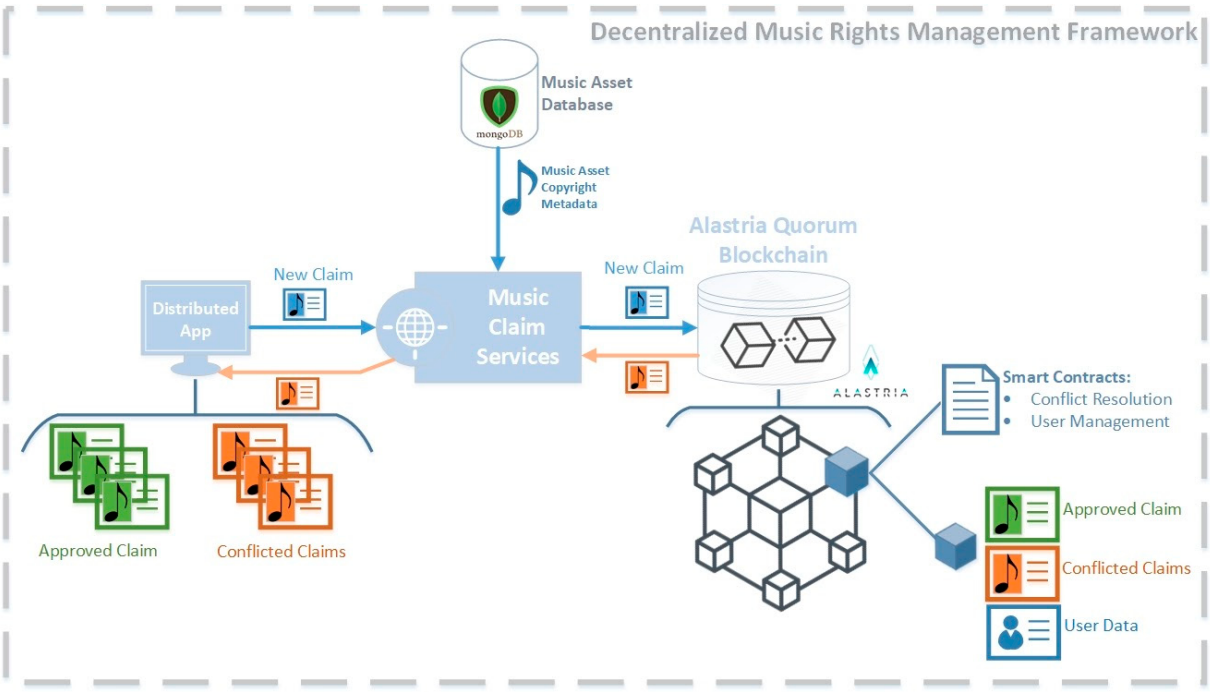


Figure 8: Decentralized music rights management framework.

The presented approach aims to create a genuinely decentralized system that is accessible to different stakeholders and their applications, resulting in a unified framework that handles the complex landscape of music rights management. As depicted in Figure 8, the dApp connects with the blockchain and visually displays stored copyright information enabling stakeholders to be able to manage their claims. Musical Claim Services are integrating both the blockchain logic and network with the metadata-enriched database of music works.

4.2 Public-Permissioned Platform

Blockchain technology is positioned at the forefront of technological advancements, leading to the creation of diverse blockchain platforms and frameworks [67]. However, not all of these platforms are capable of addressing the requirements of every use case. As depicted in Figure 9, various blockchain technologies offer distinct perspectives, particularly concerning the aspect of trust. Public blockchains lack control over network participants and operate with complete transparency. While this is a fit for cryptocurrencies, the nature of music industry rights management demands a degree of decentralization tailored to specific stakeholder participation. On the other hand, enterprise solutions offer high levels of trust but might compromise the required decentralization. Therefore, the optimal solution lies in the middle. Public-permissioned blockchains can provide the necessary security, trust, and privacy features of permissioned blockchains without sacrificing the essential decentralization [68].

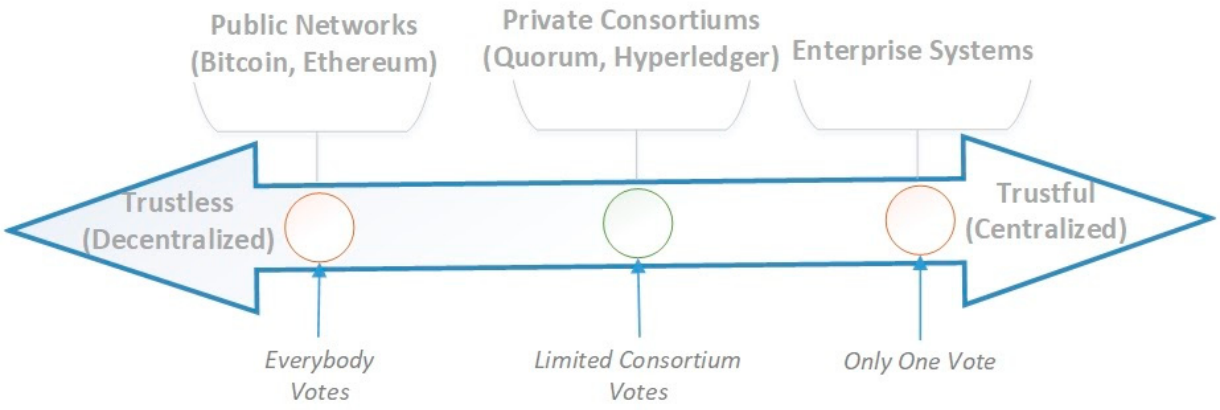


Figure 9: The trust continuum in state-of-the-art networks.

The blockchain network employed within the proposed framework is

based on a Quorum blockchain deployed within the Alastria T Network [60]. Quorum blockchain is essentially an Ethereum network enhanced with an additional security layer [59]. This layer ensures the necessary privacy and security for managing how music stakeholders access and interact with the blockchain. All operations remain transparent and can be endorsed by the consortium through broadcasting of transaction hashes. Furthermore, this security layer has the capability to monitor and control which consortium members can access and modify smart contracts. The operational blockchain framework provided by the Alastria node facilitates the testing, deployment, and execution of the proposed framework within a fully operational blockchain network. The current implementation of Quorum within Alastria utilizes the Istanbul Byzantine Fault Tolerance (IBFT) consensus algorithm, a variant of Practical Byzantine Fault Tolerance (PBFT) [69]. For a public-permissioned network like Alastria, IBFT is more suitable than algorithms used in public-permissionless networks such as Proof of Work (PoW) or Proof of Stake (PoS). IBFT offers superior efficiency and transaction throughput, exceeding the requirements of public networks. Additionally, IBFT ensures deterministic transaction finality, a crucial aspect for legal commercial transactions. The efficiency and throughput advantages of IBFT originate from a reduced set of validator nodes that are responsible for executing the consensus algorithm. These nodes exclusively determine block contents and transaction order in the ledger. Regular nodes in the network receive blocks generated by validator nodes and apply them to the blockchain, subject to transaction validation and

execution.

4.3 User Hierarchy

This section outlines the essential elements of the business hierarchy and the developed application modules. The aim is to establish a solid comprehension of the participating entities and components. In this dApp, there exists three (3) categories of users: Super Admins, Admins, and Users. Super Admins represent personnel from the participant CMOs, while Admins and Users are affiliated with the Members associated with those CMOs. In Figure 10, a clear visual is demonstrated with regards to the user hierarchy within the application.

In particular, each CMO maintains the capability of introducing new Members (e.g., an affiliated music rights company) through a Super Admin profile, while new participants can request to become Admins of an existing Member (pending approval by a Super Admin of their CMO or an Admin of their Member), or they can become regular Users (approval granted by an Admin of their Member). Additionally, the CMO possesses a comprehensive view of Member activities via the Super Admin accounts, enabling them to employ relevant changes as elaborated later in section 4.5. Conversely, a Member is empowered to create, modify, and delete music asset claims through the respective Admin and User profiles.

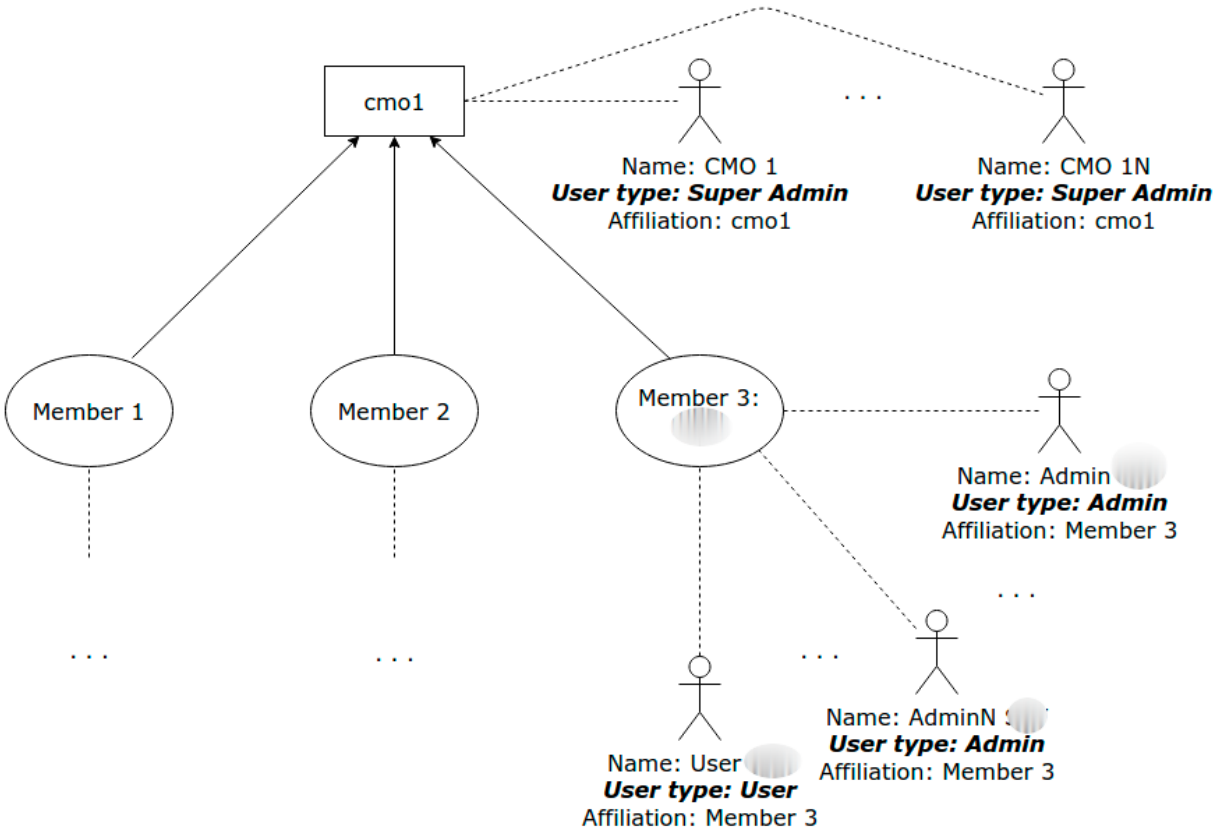


Figure 10: The user hierarchy with connections to business actors.

Notably, considerable attention is focused on the underlying framework and detection of the music asset claims. Such claims are submitted onto the blockchain through the dedicated smart contract, encapsulating copyrights data that includes parameters such as time span, territory, rights industry type, and right shared percentage. The complete structure and purpose of Solidity are later examined in the context of Conflicting Rights Governance (section 4.5).

4.4 Technical Overview

The complete connection and integration of technical architectural components follows as being built within a single system. The presented application combines an Alastria node, a key part of the blockchain network, an external NoSQL database where music asset data is accessed through the dedicated API service, and the core application that unites and harmonizes these elements.

In Figure 11, the core application, known as the Decentralized Rights Management App, is illustrated along with its interactive elements. The Alastria node, whose functionality is described in section 4.2, enables direct and efficient communication between the application and the smart contracts that are deployed on the Alastria blockchain. When initiating a new claim, the application interacts with a dedicated API in order to retrieve relevant music asset data from an external NoSQL database (MongoDB). Additionally, users only create claims for the music assets within their authorized collections that exist in the repertoire database. This database feature relates with the presented Decentralized Rights Management App since it is also configured on-chain for the CMOs, enabling their Members to access specific collections from the external database.

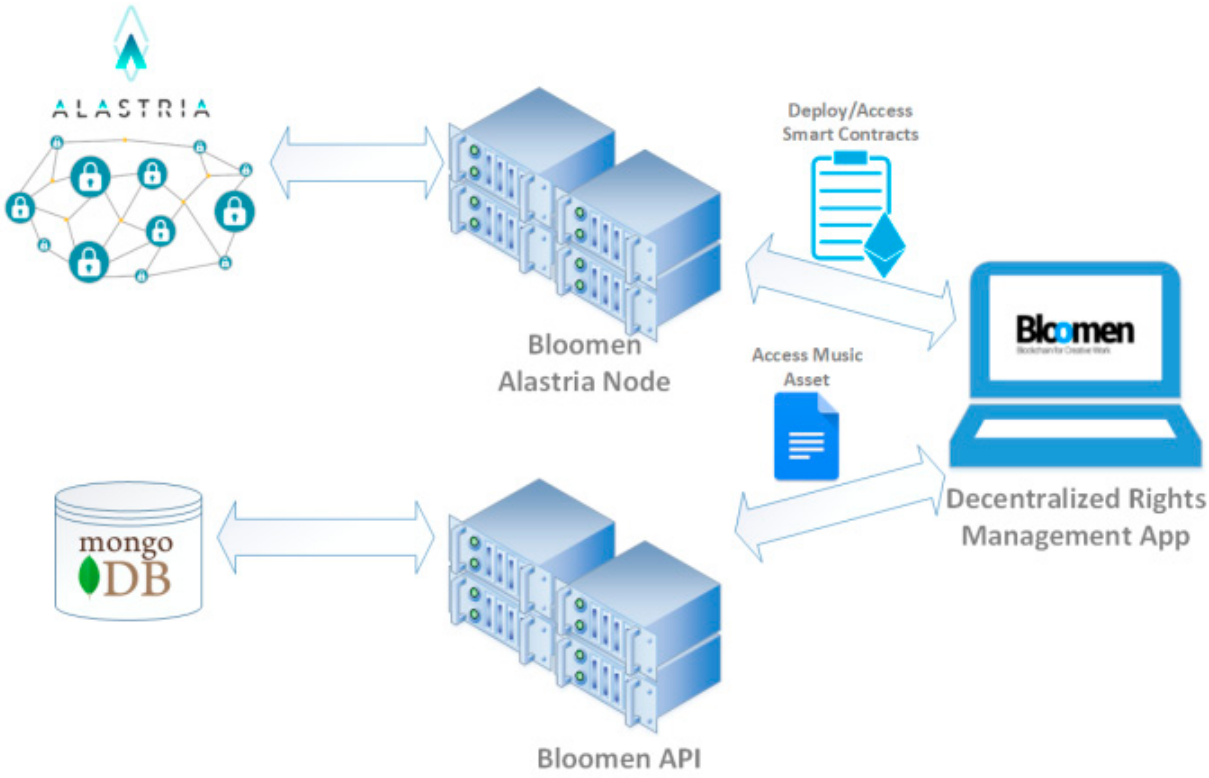


Figure 11: Technical architectural view of all the components.

Particularly, the REST API offers RESTful services responsible for seamlessly integrating the application layer with the blockchain. This REST API provides the application layer with all necessary blockchain and off-chain functions, ensuring a smooth user experience for the blockchain platform users.

Furthermore, Figure 12 displays the technology stack and architecture of the entire platform. The backend is divided into two parts: the off-chain and on-chain components. The off-chain segment consists of the data storage layer managed by a Node.js application built using the Express.js web framework, which exposes a RESTful API. MongoDB serves as object storage, primarily

for non-blockchain data, while the Apache Solr server functions as a full-text search engine. This part is hosted on the Heroku PaaS using Amazon Web Services, namely Amazon S3 cloud storage to store binary files.

As far as the on-chain part of the backend is concerned, the blockchain infrastructure is based on a Quorum instance, operating within the Alastria ecosystem. Particularly, a series of smart contracts written in Solidity are deployed on the blockchain network, while interactions and communication with the blockchain is implemented using JavaScript with the web3.js library [70].

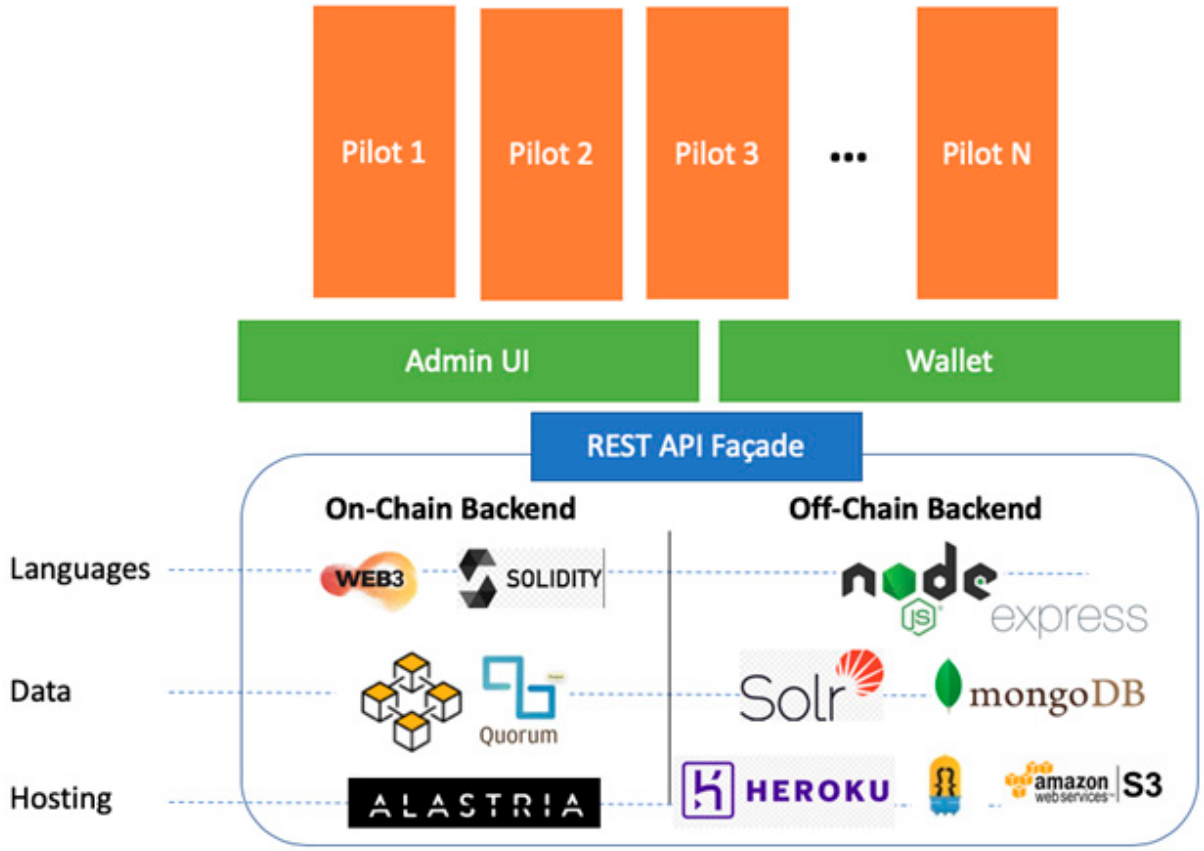


Figure 12: Technology stack from the REST API view.

Additionally, an extra logical layer synchronizes calls between the off-chain and on-chain portions of the backend by exposing a RESTful API for consumption by the musical rights governance use case, while other kinds of pilots could be deployed and integrated in the entire platform.

In terms of security, a robust authentication mechanism is designed and implemented using JSON Web Token (JWT) tokens for every call, ensuring all transactions are stateless. Following RESTful principles, client applications do not store sessions, instead, a server-signed JWT token is exchanged with each request. This token is typically stored in the browser's local storage and passed in the authorization header of the HTTP request. The JWT token allows the server side to authenticate the request sender and verify its validity and authorization. The highlight of the solution is the innovation of detecting conflicting copyright claims through the developed, deployed, and maintained smart contracts on the public-permissioned network of Alastria. A description of the innovation's rationale and analysis follows.

4.5 Conflicting Rights Governance

In this section, the approach to dealing with conflicting copyright governance is introduced, defined, and explained. This aspect constitutes the main part of the application's business intelligence and is developed and executed throughout the appropriate methods and function calls within the related Solidity smart contracts.

In the context of managing, detecting, and resolving conflicting claims over contradictory declared asset rights, the solution of the Decentralized Rights Management App introduces a unique and innovative approach. Specifically, all music rights claims submitted to the blockchain are organized within a dedicated smart contract submitted on the Alastria network. This contract outlines the necessary methods that are applied to the on-chain claims through function calls invoked by the application. The smart contract name is "Claims" and it represents each musical asset claim using a corresponding Solidity structure called "struct Claim." The struct comprises of distinct attributes, as illustrated in Figure 13.

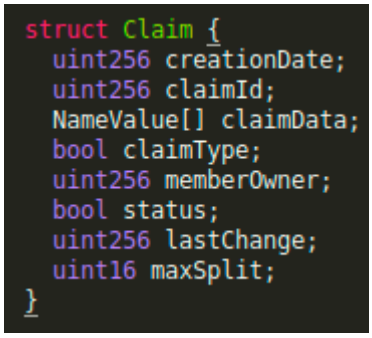


Figure 13: Solidity smart contract structure representing a claim.

Claim struct includes a status indicator that can be either represent a claimed right, in case there is no disagreement on the rights declaration compared to other on-chain submitted claims of the same asset, or a conflicted one, in case of overlapping rights within the claim declaration.

Specifically, the claim data field, named "claimData," is stored as a pair array of strings known as "NameValue type." It includes the main rights areas

where copyright conflicts could arise between musical assets. Claim struct also includes the percentage split of rights, the start and end dates of rights, the territories where rights are valid, and the type of rights, as depicted for a sound recording claim in Figure 14. Notably, the International Standard Recording Code (ISRC) is used for the sound recording type of musical asset, while the International Standard Musical Work Code (ISWC) is used for the musical work type of musical asset.

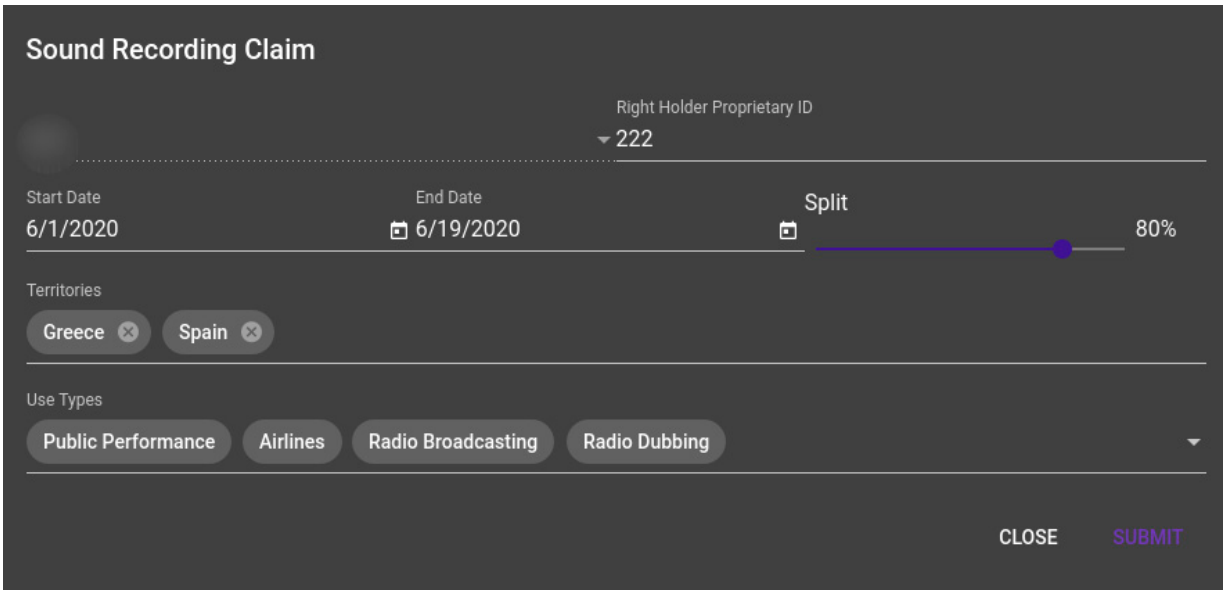


Figure 14: Claim overview with claim data when updating a claim.

Additionally, the claim Solidity structure includes logistical details such as creation and last change dates, claim type either sound recording or musical work, claiming Member, and a unique claim identification (claim ID). This claim ID is used on-chain to distinguish claims from one another. These elements have significant roles in the overall workflow of conflicting rights governance and its processes that are executed through corresponding smart

contract methods.

An important part of the conflicting copyrights governance and its dedicated data privacy constitutes the calling of the private method "checkClaimStatus()" inside the Claims smart contract. The checkClaimStatus() method has access to the private claims mapping within the smart contract where the claims declared on the system are stored. This kind of privacy ensures that the method and the mapping cannot be accessed directly by any other smart contracts or the application itself, allowing for strong privacy of the claims within the blockchain network. Furthermore, the private method checkClaimStatus() constitutes a Solidity algorithm that reads new claim information and interacts with all previously blockchain-submitted claims. It determines whether a new conflict occurs, thus, the status of one or more claims is updated within this method by modifying the dedicated claims mapping. If the new claim cancels out conflicting rights, the corresponding claim status information is updated accordingly.

The data field of a claim comprises of an array of name-value pairs, therefore, a special mechanism to effectively handle this data structure is required within Solidity. To accommodate this, and considering its applicability to future music or data types, the respective Solidity RLPReader library is employed [71]. The checkClaimStatus() method extensively uses the Ethereum RLP decoder library (RLPReader) to translate claim data information into an internal data structure suitable for conversions into desired data types, such as bytes, strings, and integers.

Moreover, the checkClaimStatus() method uses the private mapping of claims to identify claims with the same international standard code (ISRC or ISWC). For each pair of overlapping claims, their data is compared in order to determine whether there is overlap in terms of dates, use types, or rights types. If overlap exists, the method executes a code segment in the smart contract designated for overlapping claims. In general, when this method is privately called within the Claims contract, users are able to create, update, and delete new or existing claims.

The management of overlapping claims is closely tied to the "max split" field of a claim (uint16 maxSplit, Figure 13). The max split value indicates the total sum of the claim's own percentage split and the percentage splits of all its overlapping claims. If a claim's max split exceeds 100, it is marked as conflicting (Figure 15). Otherwise, it is marked as claimed (Figure 16). When two overlapping claims are detected, their max split values are recalculated on-chain, and their statuses are updated accordingly.

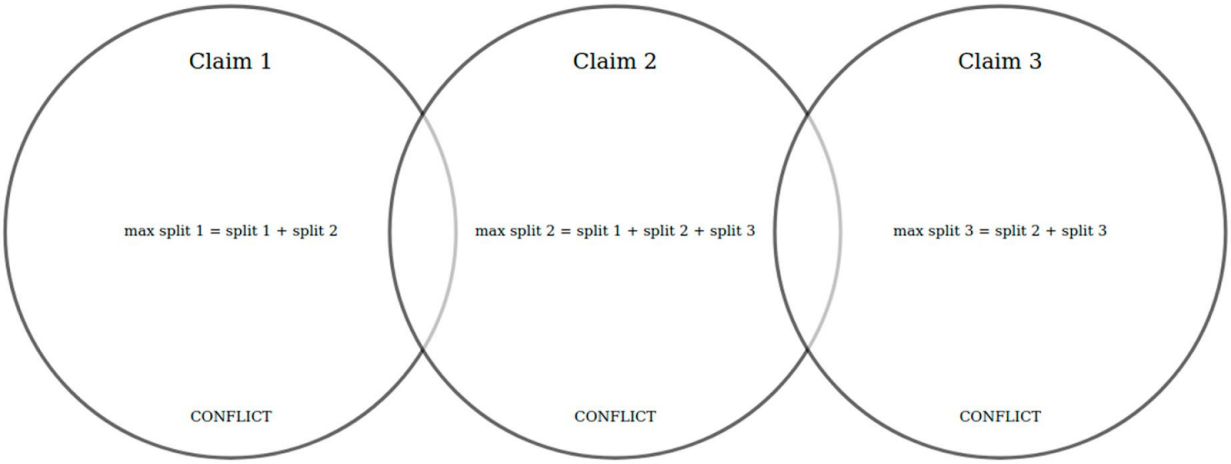


Figure 15: Max split explanation in a Venn diagram. All Conflict.

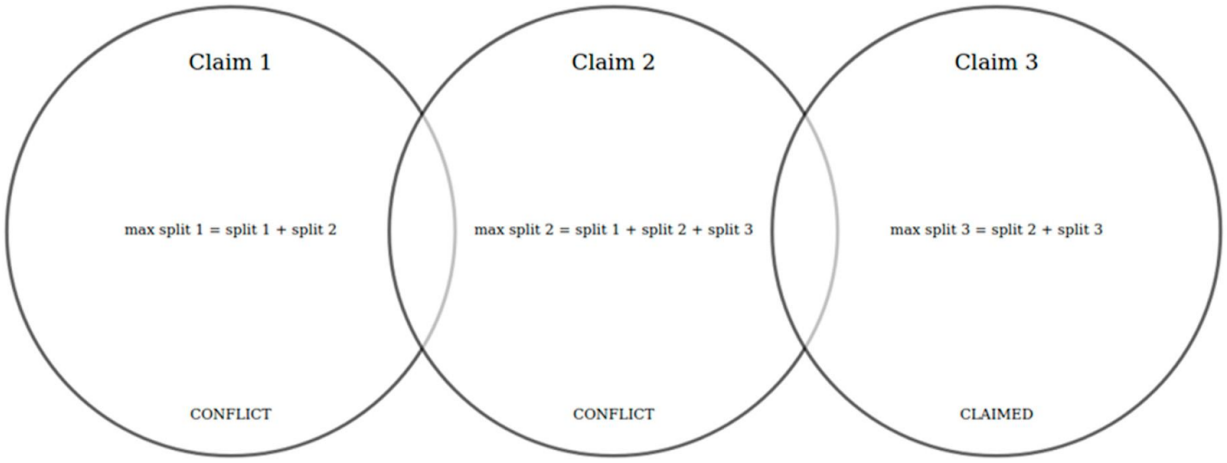


Figure 16: Example with Conflict and Claimed.

In parallel with the handling of max split percentages by this method, the user's claim inbox on the dApp UI is updated through the corresponding Solidity smart contract. When new conflicting claims arise, they are added to the user's inbox. Once conflicting claims are resolved, they are removed from the inbox. These operations are facilitated by the interoperability of the Claims contract with the Users contract, allowing the first contract to call methods in the second one in order to configure the user inbox when needed.

In conclusion, the on-chain governance of conflicting rights in the presented application is based on the immutability of permissioned blockchains and privacy protection of the Claims contract in order to create a secure system. This system enables clear and secure exchange of musical rights information and storage of claim data for CMOs and their Members. The presented framework has the potential to be applied to various use cases across different industries, while the comprehensive evaluation of the entire

system is discussed in section 4.7. Finally, the conflicting rights governance introduced includes a respective monetary incentive mechanism, as discussed in the next section (4.6).

4.6 Monetary Incentive Mechanism

In the context of a valuable application from a business perspective, a monetary incentive mechanism has been developed and is elaborated upon in this section. The general intention is to encourage users to engage with the platform in a sensible and rational manner by offering this incentive mechanism in a direct structure. As detailed in the following paragraphs, any user can execute the necessary transactions for the mechanism's regular operation and completion of procedures using a specific smart contract that is created specifically for this purpose.

In essence, the dedicated Solidity smart contract for managing user accounts throughout the system is labeled as "Users." Within this contract, each user is represented on-chain and can submit transactions permitted by the system, based on their role as a Super Admin, Admin, or User. For instance, an Admin of a Member can initiate a new claim by submitting a transaction or can delete an existing one.

The monetary incentive mechanism simplifies user-initiated claim transactions by introducing the concept of user token balance. When a user

attempts to submit a new transaction and has an adequate balance amount, the transaction is submitted, and the user's tokens are reduced by the value of the transaction's cost. A specific transaction cost associated with any claim transaction for creation, update, or deletion is defined. This framework encourages already authorized users to manage their claims account legitimately and carefully.

It's worth noting that the token balance attribute is applicable only to Admin and User user types. In this version of the application, no token balance is assigned to Super Admins, as they are not eligible to initiate claim-related transactions. Super Admins, who represent CMOs, obtain a vital role in the scenario as they control the claim submission authority of their Members, explained as follows.

To enhance the overall value and coherence of the system, the mechanism defines that each Member company is allocated a specific token amount, which is then allocated to its existing and new users. When a Member spends their token balance, the responsible CMO might recharge it through a Super Admin user. Primarily, Super Admins, who represent CMOs, have the authority to adjust a Member's token balance in order to facilitate transactional value for their users.

The principal aim of constructing and implementing the incentive mechanism is ultimately to mitigate accidental user errors or deliberate misuse of the claim submission process. For instance, accidental claim deletion or ill-advised claim creation and updates are prevented. In a wider music industry

context, this helps avoid unnecessary network congestion while boosting the overall value of transactions and enhancing the user experience. Ultimately, CMOs, positioned at the top of the business hierarchy, exercise diligence in this regard, contributing to the overall value of the system.

4.7 Evaluation of Music Rights Framework

In this section, the entire rationale of the presented framework is evaluated and followed by an outline of the results from an assessment of batch claim uploads.

Modern applications and platforms for managing music industry copyrights typically employ centralized systems that utilize distributed replication database servers in order to ensure fault tolerance and high availability. Therefore, each stakeholder business entity deploys their own database, while it is possible that a few distinct entities share the same technological components. However, the music industry stakeholder ecosystem as a whole (Figure 7) is characterized with abundant diversity, particularly in the technological frameworks used for data storage, retrieval, and processing. The various database systems endorse different methods of organizing information, encompassing data format, database type, and query structure. Within this context, data sharing between stakeholder business entities often poses challenges, and one of the primary reasons for the failure of the GRD lies in the multitude of distinct data sources [56]. The implemented music

rights framework tackles this diversity issue by leveraging blockchain infrastructure. The presented solution establishes a unified network in which all information is securely stored and shared among approved participants. As mentioned, the framework utilizes dedicated smart contracts deployed on a Quorum-based permissioned blockchain network to provide data transparency, traceability, and decentralization, while ensuring participant trust and effective resolution of claim conflicts. Additionally, the blockchain's immutability guarantees data integrity, while eliminating risks associated with centralized storage, data protection, and cyberattacks. It is important to note that in the current use case, the notion of blockchain ledger as a database replacement is applicable only when storing relatively small amounts of data using a Solidity structure. Each claim is primarily represented by its metadata (Figure 13), utilizing a manageable data volume suitable for on-chain storage. Blockchain is not well-suited for storing larger files, such as multimedia files. Ultimately, the music industry ecosystem operating within the proposed framework offers stakeholder business entities a securely shared network, facilitating seamless music copyright governance that spans from ownership assessment to royalty distribution and copyright validation, all while ensuring data availability, protection, and privacy. The following sections present the analysis results from an experiment involving the batch upload of claims.

To evaluate the system's response under real-world demanding loads, batch files were generated in CSV format, each containing a series of claims to be processed by the system and subsequently stored on the blockchain. The

batch files varied in size (ranging from 100 claims to 10,000 claims) to assess system responsiveness across different claim creation rates. The evaluation presents two (2) graphs.

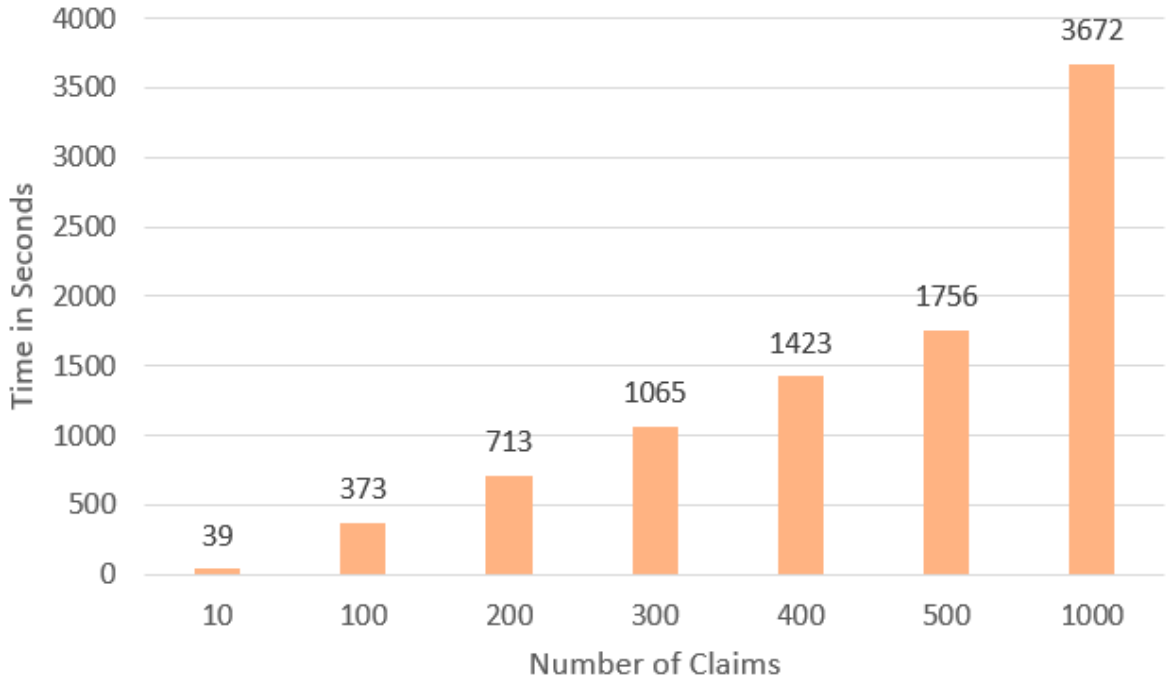


Figure 17: Time needed to process the different batch files.

The first one (Figure 17) illustrates the time required to process various-sized batch files, while the second graph (Figure 18) showcases the average time taken by the system to process an individual claim.

Given the limitations in block creation containing transactions (i.e. claims) along with the sequential processing of claims, the total batch time is relatively efficient. Although processing 10,000 claims takes approximately 10 hours, a usual workload in the music industry, the system is able to identify conflicts in less than a day, representing a significant improvement in the

dedicated scenario. In a production environment, claims can be batch-stored by the system rather than processed linearly.

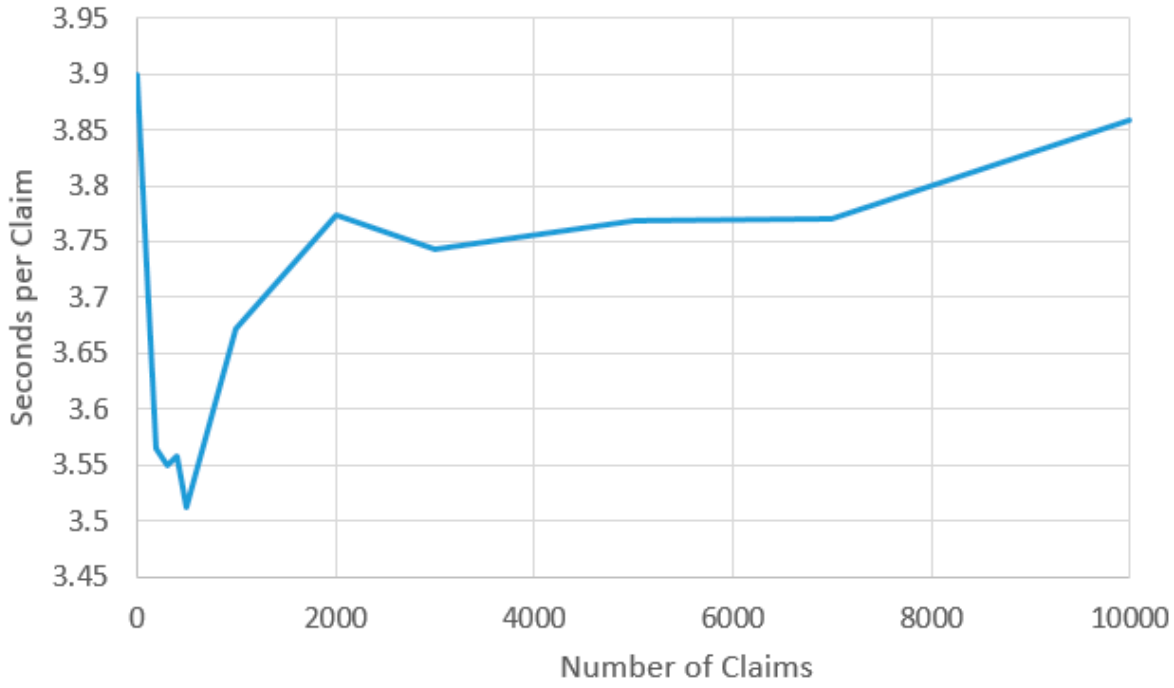


Figure 18: Average time needed to process claims.

This approach is often utilized in production blockchains like Bitcoin and Ethereum that accommodate millions of transactions daily.

Notably, the average time required to process a claim remained consistent (around 3.7 seconds) across different workloads (claim quantities). This stability indicates a robust system without any underlying bottlenecks. In Figure 18 graph, the respective spike is evident in the smaller batch files (3.9 seconds) and is caused by latency during the initialization of the blockchain communication. This latency is reducing as the number of claims increases.

5

Cloud SLA Self-Assessment through Smart Contract Isolation

5.1 Introduction

Cloud IaaS SLAs have been present since the inception of public Cloud infrastructure market. The rationale for SLA usability lies in the necessity of a legally binding agreement between service consumers and providers, especially in cases like Cloud computing and infrastructure where services are provided between both actors. SLAs have obtained a pivotal role in establishing trust between Cloud providers and their clientele. In private Cloud solutions, IaaS providers assess SLAs internally and communicate measurement outcomes to customers. In contrast, many public Cloud providers, including major corporations like Amazon EC2, don't actively monitor default SLA parameters, such as availability, which is reasonable given their vast user base and reputation. However, failure to address mishandled breaches could lead to significant financial losses [72].

Numerous tools, frameworks, and software components are available to

monitor, evaluate, and address performance and Quality of Service (QoS) issues related to cloud resources. Notably, public Cloud providers like Amazon, Microsoft, and Google have developed their own tools and frameworks [73,74,75] for assessing and orchestrating their own Cloud services and those of others.

In essence, these tools provide access to a comprehensive range of metrics and KPIs that assist cloud users in efficiently managing and assessing their cloud resources, particularly when utilizing tools provided by the Cloud provider. These metrics, such as CPU/RAM utilization, network traffic, and hard disk I/O, are widely accepted as performance and QoS metrics for both virtual and physical resources. Although these metrics are valuable for evaluating Cloud infrastructures' performance, they cannot be directly employed as SLA assessment metrics. This is due to the fact that SLA contracts generally outline explicit service guarantees in a predominantly verbal manner. For instance, one of the most prevalent metrics used among popular public IaaS providers is Availability. Although this metric is valuable for assessing a Cloud infrastructure's stability and robustness, it's also one of the easiest guarantees for IaaS to fulfill. Conversely, other metrics like those mentioned earlier, which are more critical for performance and QoS evaluation, are challenging to guarantee. This is because they are influenced by various external factors beyond the direct control of IaaS providers, such as software quality, internet provider capabilities, and significant workload fluctuations.

Although the availability metric might seem straightforward in terms of computation, there are numerous variables that contribute to standardizing the process to calculate this metric. Particularly, the process of SLA monitoring involves addressing specific questions, as depicted in Figure 19.

1. Which SLA parameters are contained in the SLA?
2. How are these parameters computed?
3. Is the computation of the parameters in line with the definition of the IaaS?

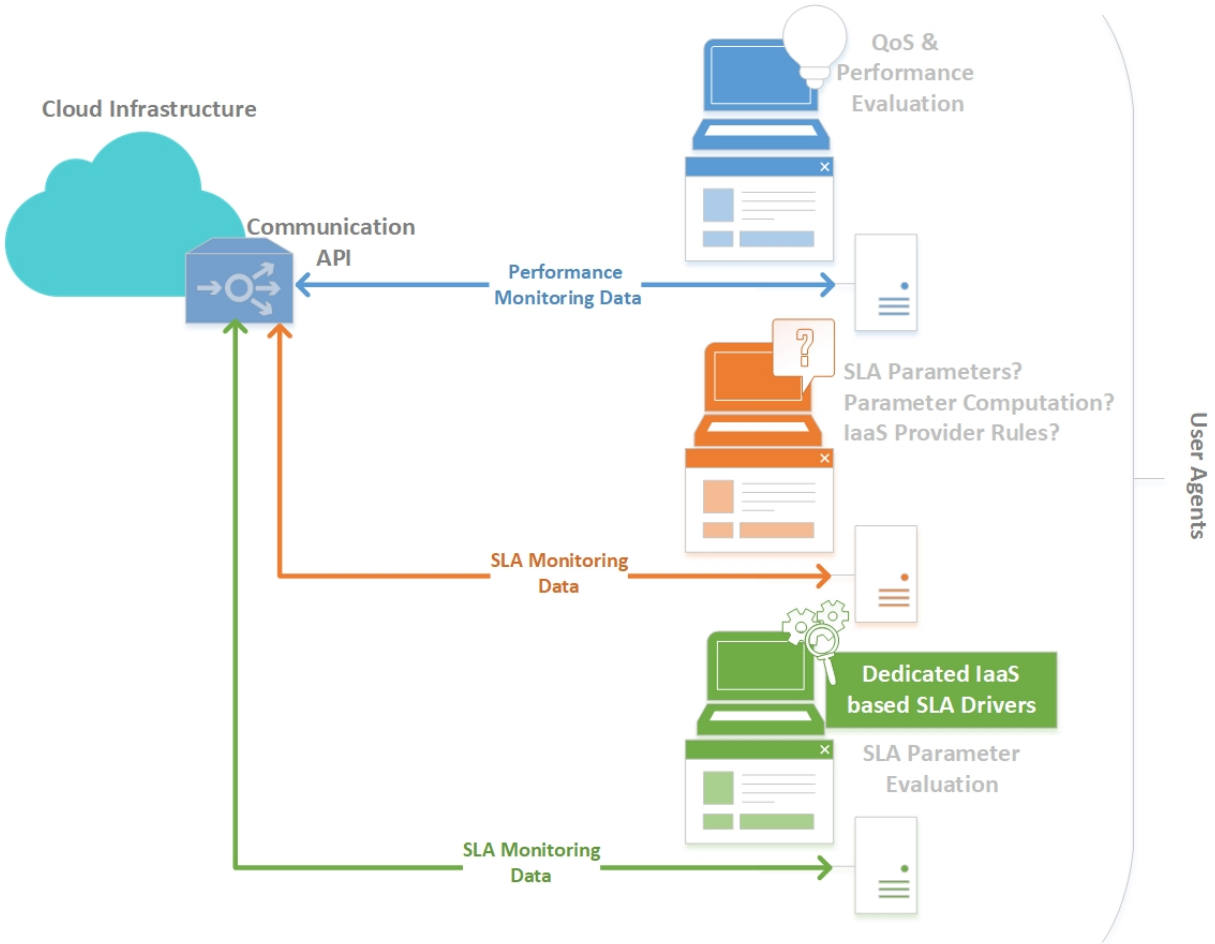


Figure 19: Standard SLA monitoring process.

Usually when it comes to availability, an SLA parameter is easily defined, but determining the parameter value that designates when a Cloud Service is unavailable and how this value is calculated are crucial steps that define the validity of the SLA monitoring process. In addition, factors like sampling rate, evaluation period, and the formula used for parameter calculation play a vital role in metric computation.

The presented system introduces a new approach to address the aforementioned uncertainties in SLA assessment. Visualizing the concept of SLA self-assessment, the presented use case creates a secure computational environment within an immutable decentralized ecosystem. Specifically, the solution leverages permissioned blockchains with isolated execution environments to establish a comprehensive SLA consensus without biased entities or intermediaries. Both IaaS providers and their clients engage in an ecosystem where SLA monitoring and computation are based on mutual pre-agreed contractual terms.

In particular, IaaS providers are able to propose various parameters defining specific SLA attributes. Simultaneously, clients participate in a secure and confident ecosystem where data and service utilization are characterized by accuracy and integrity. In order to ensure transparent and private computational flows within the permissioned blockchain-based environment, the proposed SLA consensus design and mechanism incorporates TEE capabilities [76]. The chosen TEE in this use case ensures secure and isolated on-chain SLA monitoring and computation and guarantees strong

privacy of smart contract data as SLA intelligence unfolds within the isolated smart contracts.

Both IaaS providers and clients experience precise and unbiased SLA assessment through a transparent algorithmic process that is approved and mutually agreed upon prior to the signing of the agreement. As SLA consensus operations initiate dedicated smart contract workflows, the SLA consensus life-cycle reaches completion while maintaining privacy of calculations and computations through the implemented TEE. In the context of digital trust, the on-chain validation of TEE specifications constitutes a crucial aspect of secure and isolated computation, providing global confidence across the permissioned ecosystem.

The proposed solution incorporates diverse technical concepts, resulting in dedicated and advanced components. These components adhere to interoperability and integration rules in order to achieve automated SLA consensus with an enterprise-scale vision.

5.2 Blockchain SLA Consensus

As blockchains gain wider adoption among numerous industrial enterprises, digital trust obtains a crucial role for stakeholder transactions. In the context of SLA self-assessment, the SLA business intelligence occurs within secure boundaries that enable both operational transparency and privacy of computations within the respective environments.

In brief, the presented framework outlines the key qualities of SLA consensus through the process of SLA Trusted Monitoring which ensures fair SLA operations within the Cloud SLA scenario. On one hand, the infrastructure provider involves their clientele in a secure system that ensures operational transparency and privacy of computations. Transparency primarily originates from the SLA parties consensus on the on-chain submitted Algorithmic Driver (elaborated in section 5.3) responsible for monitoring SLA logs, while computational privacy is established through the properties and capabilities of TEE [76]. On the other hand, customers benefit from a secure platform where a trusted SLA consensus procedure is applied. Particularly, the customers have confidence that the provided SLA computations follow an agreed calculation scheme that is commonly acknowledged with the infrastructure provider prior to signing the agreement.

The entire process of SLA Trusted Monitoring takes place within a permissioned blockchain network that utilizes Distributed Ledger Technology (DLT) features along with on-chain TEEs. Specifically, the solution is based on the Hyperledger Fabric distributed ledger software [77], incorporating on-chain TEE capabilities through a dedicated module, namely Fabric Private Chaincode (FPC) [78]. The latter extends the framework on-chain, allowing the deployment of smart contracts executed within protected isolated environments.

Moreover, Figure 20 provides a comprehensive overview of the solution's ecosystem architecture, illustrating the SLA consensus process with

a focus on operational transparency and privacy of computations. Both IaaS providers and their clientele navigate the ecosystem's standardized workflow which mainly involves the on-chain scheme with explicit off-chain interactions. A brief overview of the process and component interactions follows, while a more detailed analysis is presented later in section 5.4.

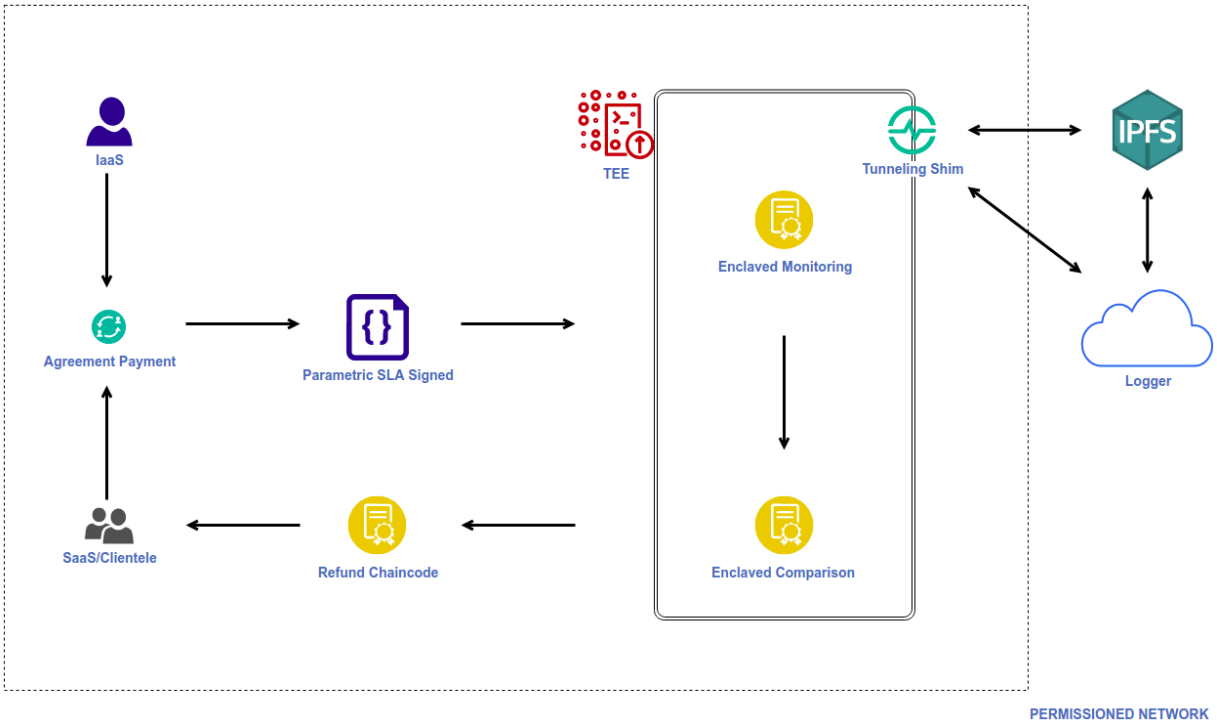


Figure 20: Blockchain SLA consensus architecture.

In Figure 20, the architectures' foundation relies on a permissioned blockchain network where its main actors are blockchain participants, i.e. the IaaS and their clients. Therefore, when an IaaS offers an SLA product to be purchased by a SaaS or other type of client, the corresponding Agreement Payment takes place as a transaction between the involved parties. This Agreement Payment constitutes a blockchain transaction verified through the

respective parties' signatures and includes the product acquisition details. During this process, the agreed Parametric SLA template digital document is signed by both parties and introduced to the on-chain TEE as a signed document, as depicted in Figure 20. This signed document includes essential SLA data defined during the Agreement Payment and validates the participation of the actors through their digital signatures.

Following the aforementioned signing, the on-chain TEE adds it as a new agreement to its portfolio of SLAs where specialized enclaved operation services are provided consistently. As illustrated in Figure 20, the TEE is supported by the Enclaved Monitoring, which calculates SLA metrics through the Tunneling Shim, a special integrator of Cloud and IPFS that securely manages the blockchain network's dedicated interoperability points with the external world.

Furthermore, the TEE encompasses the Enclaved Comparison component, responsible for computing SLA violations on behalf of the TEE. Upon SLA violation detection, this component activates the Refund Chaincode for the compensation workflow. In particular, the latter addresses SLA violations and satisfies the economic or other relations initially agreed between the IaaS and their clients as of the signed agreement.

5.3 SLA Standardized Monitoring

In order for the Parametric SLA to function correctly, it needs to include

all the necessary information from the SLA document as established in the agreement with the IaaS provider. This information should follow a standardized data schema format, while this use case adheres to the ISO 19086-2 SLA [79] standard for the Parametric SLA. This standard provides the appropriate guidelines for creating the core components of the schema. This process converts the SLA document into a JSON format, which then serves as input to the Algorithmic Drivers for SLA Evaluation.

Developing the parametric SLA involves specifying several crucial details that shape the JSON Schema representing the SLA. These specifics encompass:

- Metrics: This class embodies all the service-related objectives relevant to SLA guarantees. As discussed in section 5.1, for example, Availability stands as a popular metric used in SLAs. Moreover, this class includes basic metric-related information, mostly aimed at facilitating monitoring and measurement of a given metric.
- Parameters: This class complements each individual metric, offering comprehensive details about the respective parameters of a specific metric. Additionally, it encompasses the variable types that express a metric and their ways of measurement.
- Rules: In SLA contracts, there exist specific rules governing not only the specified guaranteed metrics but also the rules dictating metric measurement. To elaborate, these rules define how metrics should be interpreted. A typical rule scenario involves defining what signifies

failure or success for a specific metric. For instance, in the context of availability, Amazon Web Services (AWS) SLA [80] considers a service unavailable when it cannot be accessed in two (2) availability zones aiming to prevent a single point of failure.

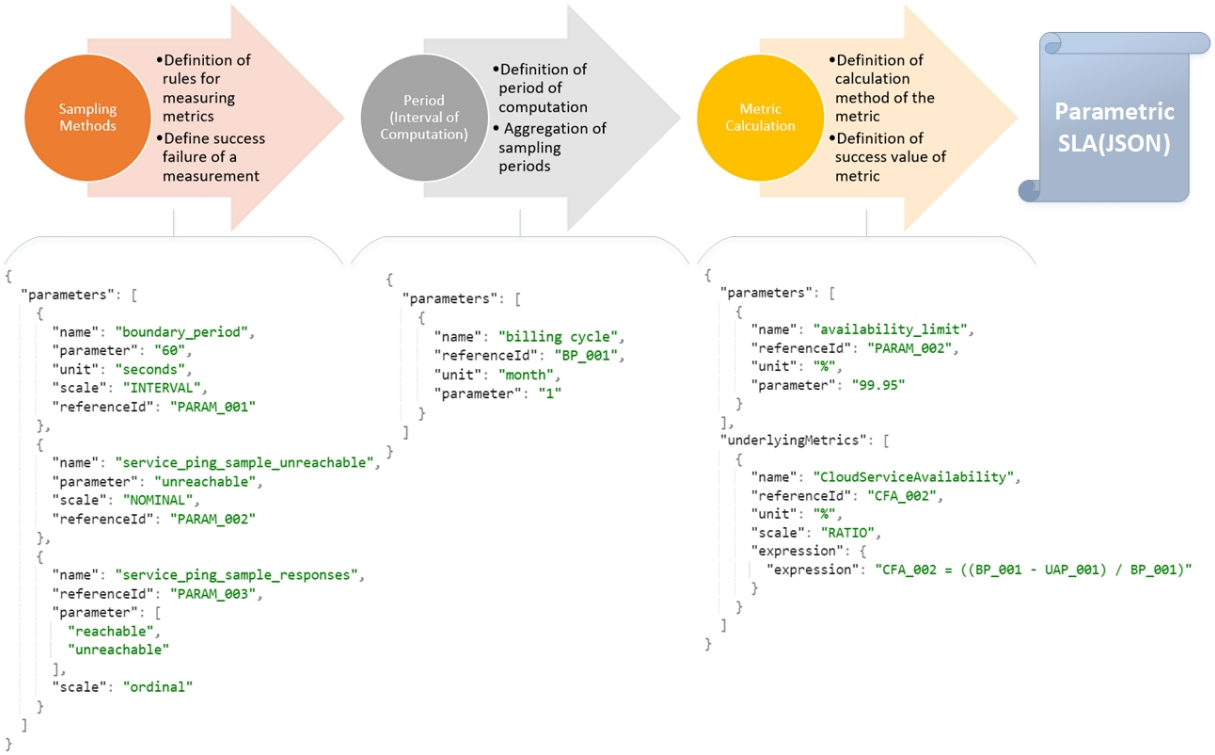


Figure 21: Layered configuration of Algorithmic Driver.

Both the parameters and their rules play a pivotal role in shaping the Parametric SLA schema since they significantly influence the actual computation of SLA metrics, including the algorithmic drivers (Figure 21). For algorithmic drivers to assess an SLA, they must take into account all the information provided by the Parametric SLA. The rules can have an important impact on metric calculations to the extent that different algorithmic drivers might be necessary even if they compute the same metrics for various IaaS

providers. Similar to the Parametric SLA, algorithmic drivers adopt a standardized approach in their development aligning with the SLALOM cloud specification model [81].

The Sampling Methods layer, as illustrated in Figure 21, assumes responsibility for designing methods that collect and assess the validity of sample data which is pivotal for metric computation. The constraints derived from the rules manifest in Boolean form and dictate whether a specific sample is retained for metric computation or discarded due to non-compliance with measurement constraints.

The Interval of Computation layer governs the frequency at which data is sampled for metric computation. It also defines the intervals at which SLA Metrics are computed and assessed. An SLA contract typically includes details about the billing cycle and, consequently, the SLA evaluation cycle. There exist services that compute their SLA parameters on a monthly basis or other, like biennial.

The Metric Calculation layer targets on the task of actually computing the metrics within a given time interval. Specified functions, which take into consideration metric definitions and associated rules, process the sampled data and generate the numerical values for SLA metrics.

Following successful configuration, the Parametric SLA becomes the SLA agreement proof that is stored on-chain. The proof includes necessary data, such as the wallet addresses of involved parties, SLA metrics details, and the applicable Algorithmic Drivers during the enclaved operations. Alongside

the submission of the signed agreement on the ledger, the TEE acquires a new agreement entry. Next, the TEE incorporates the new agreement entry into its dedicated enclaves portfolio where it is monitored and utilized by the SLA Trusted Monitoring along with other agreements as follows.

5.4 SLA Trusted Monitoring

Upon announcement of the signed parametric SLA within the on-chain TEE, the SLA Trusted Monitoring process is initiated for this new agreement. As this entire process occurs on the blockchain, the data pertaining to the SLA agreement is both trusted and transparent to the IaaS provider and their customers. Furthermore, confidentiality is maintained for SLA monitoring and computation as it is protected inside the enclaved environment the business intelligence occurs.

Once the Enclaved Monitoring module incorporates the new agreement into the designated enclaves portfolio, the most recent SLA logs are retrieved and processed within the TEE. Enclaved Monitoring functions automatically within the implemented FPC structure, which adheres to a well-defined smart contract structure [78]. FPC ensures strong privacy for the operations that are carried out by hosted elements, namely, the smart contract frameworks of Enclaved Monitoring and Enclaved Comparison. In particular, FPC exploits the inherent capabilities of TEEs by isolating smart contract calculations and computations on a hardware level. Thus, activities occurring within the FPC

are isolated and protected from other blockchain entities that participate in the network and access the shared ledger.

Enclaved Monitoring primarily consists of dedicated smart contract functions. These functions acknowledge the newly signed agreement and fetch the latest corresponding agreement logs from the IPFS network through the assistance of the Tunneling Shim integrator. The entire workflow is executed within an enclaved smart contract inheriting the aforementioned privacy features.

Moreover, throughout the solution workflow lifecycle, the Logger Cloud module consistently shares new log files related to the agreement on the IPFS network. Eventually, the returned IPFS CID is utilized by the Tunneling Shim to retrieve agreement logs. The latter component introduces custom integration functionalities that facilitate interoperability between the Enclaved Monitoring and IPFS nodes. Through the Tunneling Shim, the latest SLA logs for a specified agreement are retrieved and then transferred to Enclaved Monitoring. Subsequently, Enclaved Monitoring distributes the SLA logs to Enclaved Comparison, another well-defined smart contract structure that resides inside the FPC and is triggered automatically.

Enclaved Comparison's smart contract structure executes SLA computations that involve the calculation of potential SLA breaches. It utilizes all the relevant agreement information, including SLA agreement metrics, actual metrics from the log files, and the agreement's algorithmic driver. This process determines whether an SLA violation has occurred or not. The

aforementioned computation is executed within the private and isolated environment of the FPC, while being completely shielded from third-party entities that participate in the blockchain network. The outcome of Enclaved Comparison's calculations might or might not indicate the case of an SLA violation. The exported outcome of the system decision constitutes an unbiased result that is derived according to the predefined rules of the initially well-established and mutually acknowledged SLA agreement.

In the event of an SLA violation, the Enclaved Comparison component triggers the execution of the Refund Chaincode for compensation purposes. The latter, after receiving all the necessary data of the SLA agreement, fulfills its system role as follows. The purpose of the Refund Chaincode is to address the terms of an SLA violation occurrence as outlined in the agreement. The component consists of a smart contract that carries out a set of functions regarding primarily the execution of the violation corresponding compensations as well as other related actions defined in the SLA. The latter actions might include adjustments to parties' reputations, product scores, and others. When an SLA violation occurs, the clientele of the provider receive a refund payment as a compensation for the SLA breach, while the IaaS is charged for the same violation respectively. The Refund Chaincode serves as the final component of the solution's lifecycle during the SLA violation process workflow.

5.5 Experimentation Results

The previously mentioned ideas and processes of the SLA consensus system are applied and evaluated within the described architectural framework (Figure 20). Regarding the deployed technology, the blockchain infrastructure underneath relies on a Hyperledger Fabric permissioned network that hosts a TEE and technical communicates with it through a corresponding specialized enabler, namely Hyperledger FPC v1.0.0-rc1. In particular, the underlying Hyperledger Fabric network executes a fault-tolerant consensus algorithm that enables the network to handle a large number of transactions per second [82]. Inside the blockchain network, FPC manages the confidential business logic within enclosed smart contract structures. Particularly, the logic is executed within the aforementioned private structures is kept confidential from the blockchain participants and their transactional and contractual network activities.

The utilized TEE receives each new agreement in the ISO/IEC 19086-2:2018 format for a t2.nano Amazon testing instance [83] and processes it through the appropriate specification-compliant functions of the smart contract structures, as explained in section 5.4. Additionally, the TEE connects and integrates with the off-chain world through the Tunneling Shim component, a designated connector facilitating interoperability with the IPFS network (v0.9.0) and the public Cloud which is referred to as the Logger component within the architecture. The private smart contract structures are executed

inside the TEE, as being isolated within the endorsed FPC. Regarding network transactions, FPC achieves complete privacy against submitted transactions and other blockchain activity, especially for those that are external to the TEE. FPC constitutes a consolidated smart contract package armored with infrastructure level privacy and task isolation. When an SLA violation occurs, the designated smart contract, namely the Refund Chaincode, is triggered through an on-chain broadcast received from the enclaved computation smart contract. Moreover, all smart contract structures are coded in Golang 1.14.12 and make use of the standard Hyperledger Fabric Go API [84] for invoking transaction operations and chaincode triggers.

In the context of the SLA violation workflow, once the SLA product transaction is finalized, the TEE operations occur sequentially, beginning with Enclaved Monitoring followed by Enclaved Comparison. The TEE triggering originates externally from the enclosed environment, supported by strong encryption measures for secure bilateral interactions [85,86]. Within the TEE, SLA log data is securely retrieved through the Tunneling Shim which interacts with the IPFS network. The interoperability happens within the TEE and is completely protected and isolated from third-party entities, such as unauthorized chaincodes, the blockchain network, or other consensus nodes. The retrieved SLA logs are processed within the TEE, i.e. on the corresponding chaincode memory, and the resulting SLA intelligence exits the private isolated environment concluding the SLA Trusted Monitoring lifecycle. In case an SLA violation occurs, the Refund Chaincode is triggered and

executed across the entire permissioned network.

Figure 22 displays the experimental results of the solution illustrating the time required for the system to process and verify the existence of an SLA violation. The proposed approach assesses the timing performance difference when a violation is present compared to when it is not. The experimental results confirm that within the presented framework the dedicated SLA assessment system can efficiently detect an SLA violation because of the deployed isolated and private SLA intelligence environment.

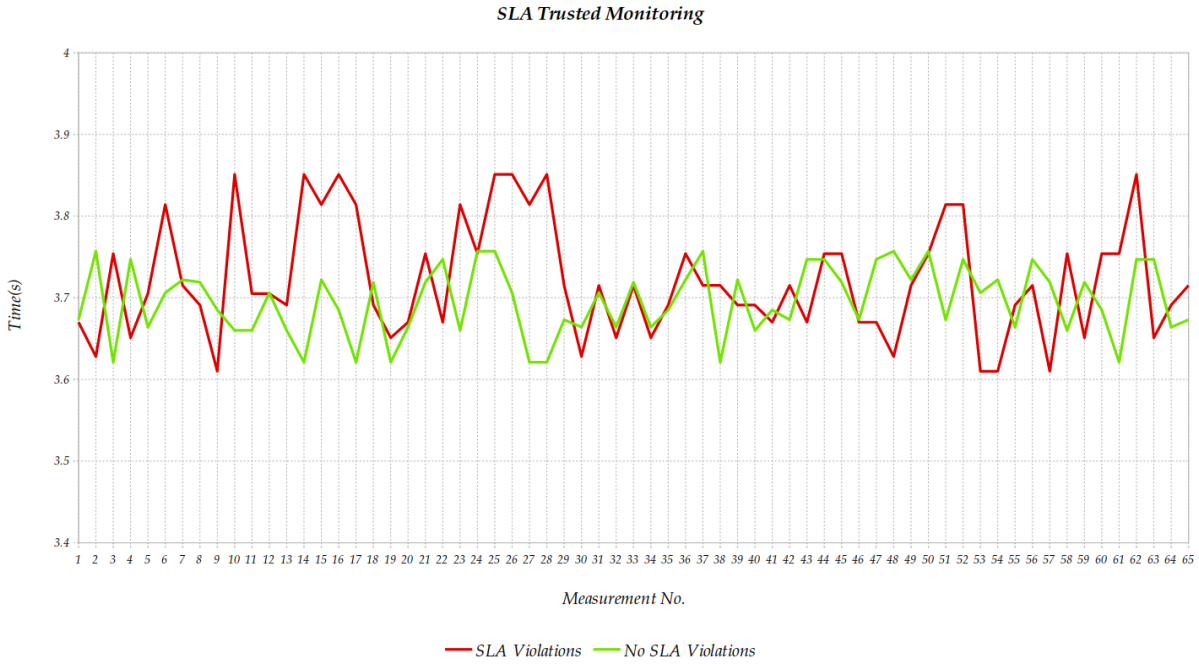


Figure 22: SLA violations time performance shift in SLA Trusted Monitoring.

In general, the time needed for resolving and submitting private chaincode transactions within the enclosed environment varies depending on whether a violation occurred or not. As shown in the experimental results (Figure 22), in both scenarios the solution's timing performance falls within a

certain range, while a bit wider time range is observed in the case where a violation is detected. Particularly, when there is no violation, the system outputs results more quickly than when a violation is present. It is worth noting that during a violation additional private chaincode computations are required leading to a longer execution time.

In the presented solution, specific and immutable smart contract structures are executed in order to complete the violation determination workflow, thus, their performance time remains within measured thresholds. The latter is attributed to the high transaction throughput and transactional mechanics of the underlying permissioned blockchain of Hyperledger Fabric that includes a high rate of transactions per second and pipelined transaction flow [9]. Consequently, violation transactions are completed relatively quickly within a transaction flow pipeline. For both depicted scenarios in Figure 22, the specified time ranges are fixed within certain thresholds and cannot be significantly altered in a positive or negative direction. This is due to the enclaved chaincodes utilized in the solution being submitted to the immutable transaction ledger while being invoked from triggers that originate from the blockchain network leveraging the irreversibility property of the chain. This way the smart contract code immutability is validated ensuring stability and consistency in the solution's performance timing. Finally, in terms of scalability, the system's workflow scales for both SLA violation scenarios (Figure 22) as it aligns with the scalability features of the underlying Hyperledger Fabric network [87]. The chosen blockchain platform scales in

terms of network entities and transactional workflow, providing robust support to thousands of transactions per second [88]. The execution of the private smart contract structures follows the scaling attributes of the underlying blockchain infrastructure as well by utilizing the corresponding performance capabilities.

The presented solution has been thoroughly discussed throughout the related involvement with the Open Source Community of Hyperledger Foundation – The Linux Foundation. Notably, the research work examination led to the formulation of a Hyperledger White Paper that describes the applicability of the system in terms of SLA self-assessment in the Telecom industry [89].

6

Conclusions and Future Improvement

Following the analysis of the industrial architectures presented in the previous chapters, the main vision of the doctoral dissertation constitutes the examination of privacy-oriented approaches on blockchains and distributed ledgers. As already depicted in the introductory chapter's Figure 1, the contribution of the dissertation is the extracted blockchain privacy stack that envisions the usability and applicability of privacy for blockchain-based solutions. The examination and understanding of further use cases would trigger more details on the stack, however, the presented architectures already cover significant centralization and blockchain privacy challenges, offering the following key benefits to application owners and ecosystem administrators that build their blockchain use case or dApp on the next generation Internet infrastructure of Web3.0:

- Decentralized network security.
- Enterprise blockchain network activity.
- Sensitive information protection with private function execution and secret transacting.
- Secure data calculations and enclaved computations with isolated smart

contracts.

With respect to each individually proposed architecture, the corresponding conclusions that target specifically their research domain and future works are presented as follows.

6.1 KYC User Identification Systems

Addressing privacy and security concerns on blockchains is crucial across various industry-focused applications, particularly for instances involving data sharing over media channels, like social media, personal preferences, or user interactions. Although blockchains are primarily intended for distributed data storage and sharing, their inherent immutability and transparency might initially render them unsuitable for privacy-sensitive data. Such sensitive data may reveal physical identities, consumer habits, or privacy-related details, and even disclose proofs of location. Due to the irreversibility of blockchain-stored data, specific blockchain designs are essential for securing user privacy. One viable approach involves using blockchains solely as timestamping mechanisms for specific workflow information linked to external data repositories. This approach not only aids scalability when dealing with substantial data volumes but also allows for additional data encryption prior to insertion into the blockchain. However, encrypting data creates its own challenges, particularly if decryption keys are ever compromised, leading to unauthorized access. Despite of the chosen

approach, all blockchain implementations—public or private—must adhere to privacy by design principles when incorporating transaction data into their ledgers. Future transactions over blockchains will increasingly rely on robust, efficient and simple KYC processes. The presented architecture demonstrated how easily managed and modular industrial frameworks can be established on top of permissioned blockchains like Quorum, equipped with open public blockchains and Solidity-based smart contracts. The showcased integration paves the way for implementing KYC processes suitable for a wide array of decentralized applications.

In terms of expanding the system's capabilities, future efforts are focusing on enabling the integration of additional data sources into the presented architecture and facilitate more complex procedures for collecting diverse information about specific entities. The latter includes enhancing the seamless connections between verified machines and the deployed blockchain smart contracts, allowing for efficient data provision and retrieval from the KYC system.

Moreover, machine learning strategies and artificial intelligence tools have been proposed to enhance fraud detection and automate the KYC process by handling enormous amounts of data. For instance, such tools can analyze uploaded images and assess document authenticity in very short time. Investigating the interaction between such tools and the proposed KYC system creates interesting future research directions, aiming to elevate the overall procedure's accuracy. The KYC process can also involve complex procedures

regarding the examination of multiple external sources and the request of additional documents to verify an individual's identity. Furthermore, evolving regulatory requirements demand a KYC system's adaptability to new legal rules. Consequently, the research roadmap extends the study of smart contracts in order to handle multidisciplinary processes, aiming at a holistic KYC solution.

6.2 Copyrights Governance

Regarding the musical copyright governance, the corresponding individual outcomes and future work follow in this section. In principle, the study introduces a comprehensive and efficient application for managing copyrights, leveraging Quorum permissioned blockchain technology. In the music industry, where a diverse array of roles and entities must collaborate to identify and manage music asset rights and address conflicts, blockchain emerges as a viable solution. Blockchains offer an immutable ledger of claims, eliminating the need for intermediaries. The proposed implementation brings together diverse business sectors within music industry organizations and non-profit blockchain associations. The presented dApp successfully merges blockchain and smart contracts with rights management in order to establish a novel decentralized framework that addresses important challenges faced by music industry stakeholders, especially CMOs. Leveraging core blockchain principles like transparency, trust, traceability, and decentralization, the

solution offers an effective approach to resolving common issues confronted by CMOs in the music industry landscape. Particularly, the utilized public-permissioned blockchain of Alastria offers strong security and required privacy for the use case. Furthermore, the interactions with dedicated APIs, tools, components, and conventional databases create a unified system that is founded on a decentralized architecture. The corresponding capabilities of the deployed smart contracts model and resolve rights conflicts in the music sphere under dedicated privacy principles.

Moreover, the system's potential extensions could be the enabling of automated rights resolution. This would involve exploring the feasibility of a decentralized approach based on IPFS for storing rights management and claims conflicts data. Smart contracts would then read rights from IPFS during new claim submissions, while blockchain would determine the legitimacy of the conflicting claims. Additional enhancements could be implemented such as adjusting copyrights in alignment with the underlying blockchain technology and deploying more robust communication mechanisms for end users. This would enable users to better trace the individual stages of conflict resolution. Furthermore, future research aims to enrich smart contracts with features that optimize interaction with external data sources containing media assets and relevant metadata. Algorithms for music asset identification could also be explored, aiming to create a holistic solution for monitoring the usage of specific music items across various distribution channels and geographical regions. These efforts target the expansion of these tools capabilities for the

higher benefit of CMOs.

6.3 Blockchain SLA Assessment

The showcased SLA evaluation system introduces a novel approach to achieving consensus on SLA terms adherence within the domain of public cloud infrastructure. The core concept revolves around distributed ledger software that accommodates TEEs possessing isolating and computational capabilities. The privacy-enhancing attributes of this arrangement are advantageous throughout the entirety of the SLA assessment process, as each SLA agreement is thoroughly evaluated from the standpoint of both the IaaS provider and their customers. All of these activities unfold within a permissioned blockchain, while the specialized SLA intelligence is isolated and executed within the utilized TEE. The outcome comprises of a reliable system that benefits both the IaaS provider and their clientele in terms of accuracy and fair calculations and computational processes.

Regarding the exhibited experimental results, the proposed approach is capable of scaling for enterprise-oriented scenarios, offering profitability and efficiently implemented interest in alignment with the inherent scalability features of the underlying blockchain technology. Regarding future potential enhancements of the system setup, the current directions primarily center on expanding support for more actions in case of violations, which may

encompass aspects such as managing the reputation of involved parties and establishing a scoring mechanism for SLA products within the context of SLA violation workflows. Furthermore, as far as the discussions and the involvement with the Open Source Community is concerned, there exists keen interest in expanding the presented system in terms of technological tools employed. In particular, the introduction of zero-knowledge proofs has been proposed since it would add an extra layer of data privacy and validation regarding the dedicated details contained in the transactional flows.

Glossary

AWS	Amazon Web Services
CID	Content identifier
CMO	Collective Management Organization
CPU	Central Processing Unit
CRUD	Create, Read, Update, Delete
dApp	Decentralized Application
DLT	Distributed Ledger Technology
DRM	Digital Rights Management
FPC	Fabric Private Chaincode
IaaS	Infrastructure as a Service
ID	Identity
I/O	Input/output
IoT	Internet of Things
IPFS	InterPlanetary File System
IBFT	Istanbul Byzantine Fault Tolerance
ISRC	International Standard Recording Code
ISWC	International Standard Musical Work Code
JWT	JSON Web Token
KPI	Key Performance Indicator
KYC	Know Your Customer
P2p	Peer-to-peer
PBFT	Practical Byzantine Fault Tolerance
PoS	Proof of Stake
PoW	Proof of Work
RAM	Random Access Memory
QoS	Quality of Service

SLA	Service Level Agreement
TEE	Trusted Execution Environment
UI	User Interface
Web3.0	3rd iteration of World Wide Web

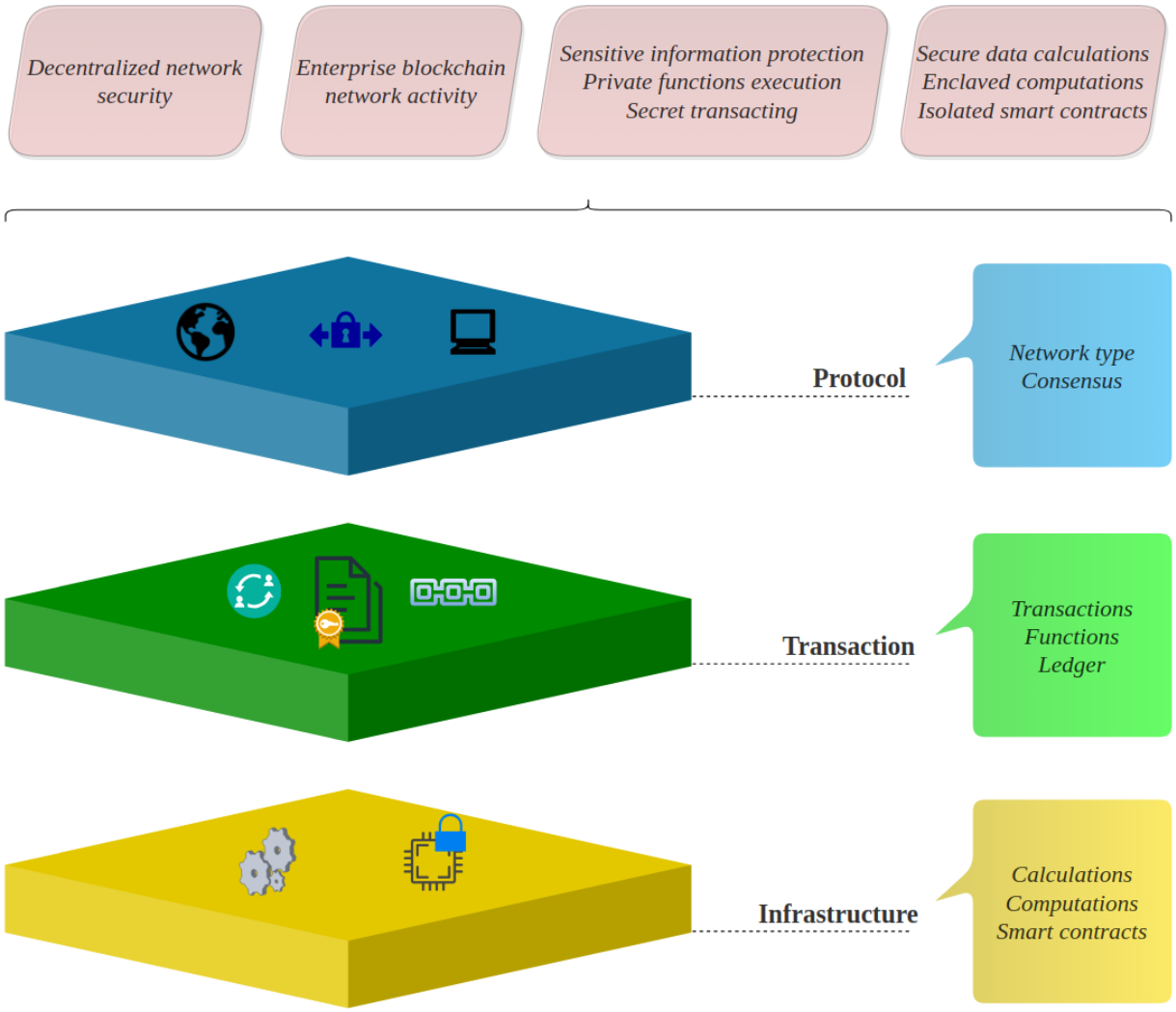
Εκτεταμένη Περίληψη

Εισαγωγή

Τα κεντρικοποιημένα συστήματα αποτελούν το βασικότερο θεμέλιο του Διαδικτύου Web2.0 παρέχοντας έναν πρωτοπόρο τρόπο διανομής των πληροφοριών και συμμετοχής των χρηστών σε σχέση με την πρώτη γενιά Διαδικτύου (Web1.0). Ωστόσο, η παγκόσμια υιοθέτηση της τεχνολογίας και η αυξανόμενη και απεριόριστη χρήση της έχει δημιουργήσει πολλά θέματα και προβλήματα ιδιωτικότητας και ασφαλείας από την οπτική γωνία των δεδομένων και των συμμετεχόντων. Οι αλυσίδες-κορμού και οι τεχνολογίες κατανεμημένης λογιστικής προσφέρουν σημαντικές λύσεις σε αυτά, επί το πλείστον μέσω των κατανεμημένων αλγορίθμων συναίνεσης που εκτελούνται από ένα ευρύ δίκτυο κόμβων. Ειδικότερα, η διακυβέρνηση και ο έλεγχος δεδομένων που κατανέμονται σε ένα δίκτυο κόμβων μετριάζουν μια μεγάλη πληθώρα των κινδύνων κεντρικοποίησης, εφόσον τα μέλη του δικτύου σε πλειοψηφία συμφωνούν σε μια κοινή έκδοση των δεδομένων χωρίς κανένα μεμονωμένο σημείο αποτυχίας.

Στην παρούσα διδακτορική διατριβή, τρεις (3) βιομηχανικές αρχιτεκτονικές που είναι προσανατολισμένες στην ιδιωτικότητα αλυσιδών-κορμού, έχουν διερευνηθεί, σχεδιαστεί και υλοποιηθεί. Η πρώτη περίπτωση αναφέρεται σε αρχιτεκτονική διατήρησης ιδιωτικότητας Know Your Customer (KYC) η οποία χρησιμοποιεί έξυπνα συμβόλαια αλυσίδας-κορμού προκειμένου

να προστατέψε τα ιδιωτικά και απόρρητα δεδομένα χρηστών [12]. Η δεύτερη περίπτωση υλοποίησης εισάγει μια προηγμένη αποκεντρωμένη εφαρμογή σε ένα περιβάλλον αλυσίδας-κορμού με επίτρεψη, ειδικά προσαρμοσμένη για το σκοπό της διαχείρισης δικαιωμάτων μουσικής μέσω της χρήσης έξυπνων συμβολαίων [13].



Σχήμα 23: Όραμα διατριβής: Στοίβα Ιδιωτικότητας Αλυσιδών-κορμού

Η τρίτη υλοποίηση που διερευνήθηκε εξετάζει τις διαδικασίες αξιολόγησης

Συμφωνιών Επιπέδου Υπηρεσίας Υπολογιστικού Νέφους (SLA) [14], ενώ έχει συζητηθεί και συνεισφέρει στην Κοινότητα Ανοιχτού Κώδικα Hyperledger του Linux Foundation [15].

Συνολικά, η παρούσα διατριβή οραματίζεται την τυποποίηση επιπέδων ιδιωτικοποίησης για αλυσίδες-κορμού όπως εξηγείται παρακάτω. Τα διάφορα επίπεδα έχουν να προσφέρουν σημαντικό πλεονέκτημα σε διαχειριστές οικοσυστημάτων ή τους σχεδιαστές και τους κατασκευαστές αποκεντρωμένων εφαρμογών που στοχεύουν στην εφαρμοσιμότητα ιδιωτικοποίησης στην εκάστοτε αλυσίδα-κορμού ή αποκεντρωμένη εφαρμογή τους. Πιο συγκεκριμένα, η διδακτορική διατριβή οραματίζεται την τυποποίηση μιας στοίβας ιδιωτικότητας αλυσιδών-κορμού (Σχήμα 23) η οποία πηγάζει εκ των ερευνητικών περιπτώσεων που εξετάζονται.

Στην προτεινόμενη στοίβα ιδιωτικότητας αλυσιδών-κορμού για το Διαδίκτυο επόμενης γενιάς (Web3.0), τα αντίστοιχα επίπεδα παρουσιάζουν τα παρακάτω σημαντικά προτερήματα:

- Ασφάλεια αποκεντρωμένου δικτύου.
- Δραστηριότητα δικτύου αλυσίδας-κορμού για επιχειρήσεις.
- Προστασία ευαίσθητων δεδομένων με εκτέλεση ιδιωτικών λειτουργιών και μυστικές συναλλαγές.
- Ασφαλείς μαθηματικοί υπολογισμούς δεδομένων και περίκλειστοι λογικοί υπολογισμοί με απομόνωση έξυπνων συμβολαίων.

Βιβλιογραφική Ανασκόπηση Σχετικών Αρχιτεκτονικών Υλοποιήσεων

Αρχικά η τεχνολογία αλυσίδας-κορμού εισήχθη ως το υποκείμενο πλαίσιο για την δημιουργία κρυπτονομισμάτων καθώς εμφανίστηκε στον τομέα της πληροφορικής μέσω της δημιουργίας του Bitcoin το 2009 [1]. Το Bitcoin παρουσίασε ένα καινοτόμο σύστημα ηλεκτρονικών μετρητών peer-to-peer (p2p) που επικεντρώνεται στη δημιουργία ενός ασφαλούς και αποκεντρωμένου ευρετηρίου (καθολικού) για την καταγραφή και την επικύρωση ψηφιακών συναλλαγών. Μια πληθώρα κατανεμημένων εφαρμογών (dApps) έχουν προταθεί στο πλαίσιο της ακαδημαϊκής έρευνας, που εκτείνονται σε τομείς όπως η κυβέρνηση [20,21], οι μηχανισμοί χρηματοδότησης [22] και άλλοι. Η σύγκλιση της τεχνολογίας με το Διαδίκτυο των Πραγμάτων (IoT) έχει παρουσιάσει διάφορες επιτυχημένες περιπτώσεις εφαρμογών [23].

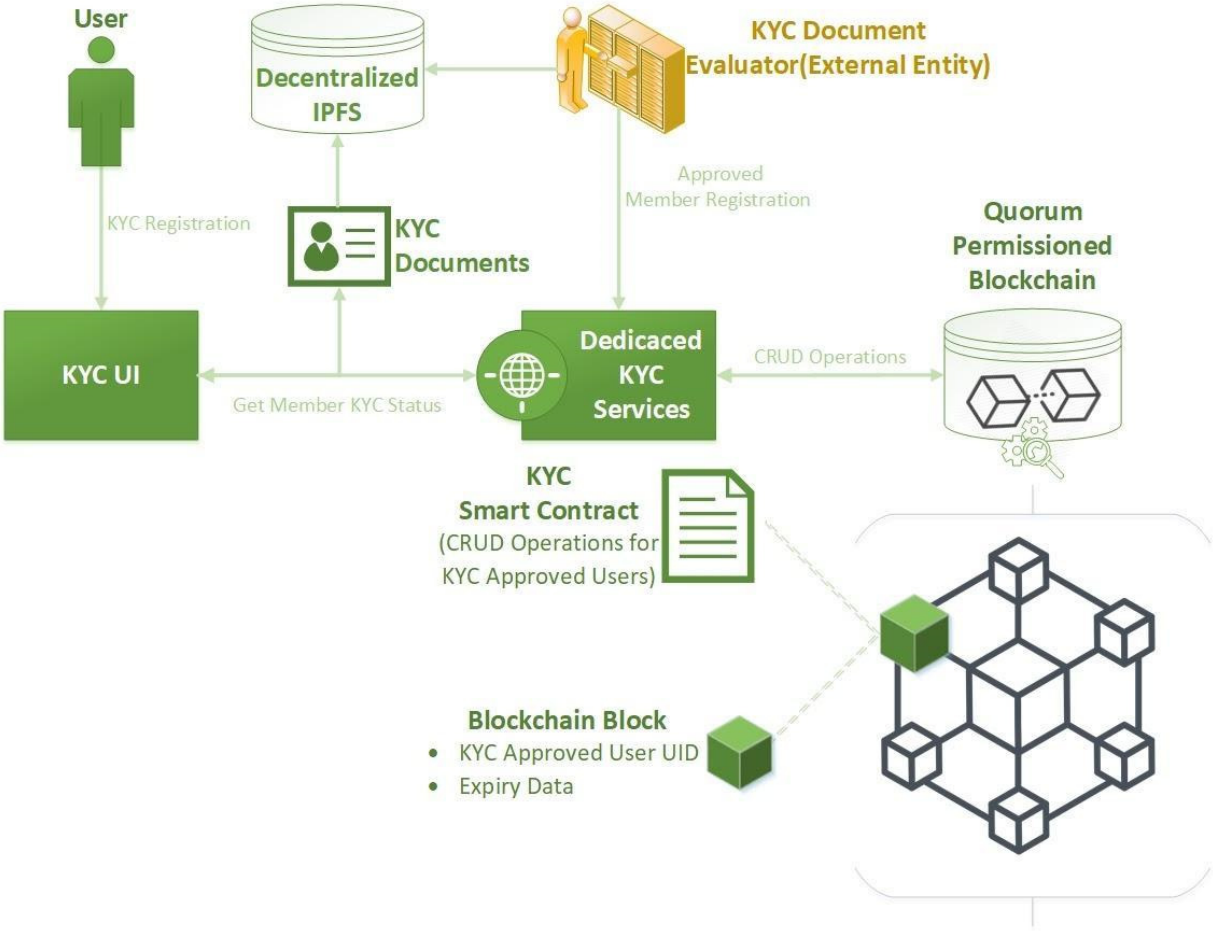
Όσον αφορά σχετική επιστημονική έρευνα, οι συγγραφείς στην [30] προτείνουν ένα τεχνολογικό πλαίσιο ελέγχου ταυτότητας και εξουσιοδότησης προσανατολισμένο σε τεχνολογία αλυσίδας-κορμού που ελέγχει την πρόσβαση πόρων για συσκευές IoT. Ταυτόχρονα, η έρευνα των Mudliar και συνεργατών [31] συνδυάζει την τεχνολογία της αλυσίδας-κορμού για την ανάπτυξη μιας εφαρμογής με εθνικές ταυτότητες. Άλλα έργα σχετικά με συστήματα αναγνώρισης ταυτότητας χρηστών σε αλυσίδες-κορμού μπορούν να βρεθούν στις αναφορές [32-38].

Όσον αφορά τη διαχείριση πνευματικών δικαιωμάτων, οι Xu και

συνεργάτες εισήγαγαν ένα σύστημα που χρησιμοποιεί και αναπτύσσει μηχανισμούς συναίνεσης, έξυπνα συμβόλαια, ψηφιακές υπογραφές και αλυσίδες κατακερματισμού τη διασφάλιση επικύρωση και επαλήθευσης πνευματικών δικαιωμάτων σε πραγματικό χρόνο [41]. Για την αντιμετώπιση ζητημάτων ανεξέλεγκτης διάδοσης και μη εξουσιοδοτημένης μετάδοσης δεδομένων, οι Ma και συνεργάτες πρότειναν ένα σχετικό σύστημα πνευματικών δικαιωμάτων βασισμένο σε αλυσίδες-κορμού που αντιστοιχίζει το κατάλληλο περιεχόμενο με σχετικούς χρήστες, διασφαλίζοντας παράλληλα ιχνηλασιμότητα συναλλαγών υπό όρους και εμπιστοσύνη [42]. Τα σχετικά έργα με αλυσίδες-κορμού για πνευματικά δικαιώματα φαίνονται στις [39-50]. Τέλος, αναφορικά με το υπολογιστικό νέφος, οι Nguyen και συνεργάτες [51] πρότεινε μια αρχιτεκτονική σχετική με τα SLAs για την αξιολόγηση και την επίβλεψη συμφωνιών τουρισμού χρησιμοποιώντας λογισμικό κατανεμημένης λογιστικής. Η μέθοδος που παρουσιάστηκε από τους συγγραφείς περιστρέφεται γύρω από τη διατήρηση της ακεραιότητας της διαδικασίας αξιολόγησης SLA μέσω της εγγενούς αμεταβλητότητας δεδομένων της τεχνολογίας. Στην προσέγγισή τους, μια αυτοματοποιημένη διαδικασία παρακολούθησης και υπολογισμού SLA λαμβάνει χώρα εξασφαλίζοντας επιτυχή αξιολόγηση SLA με αντίστοιχη πληροφόριση των τελικών χρηστών. Περισσότερα σχετικά έργα βρίσκονται στις [52-58].

Δημόσια και Ιδιωτικά Έξυπνα Συμβόλαια για Συστήματα Αναγνώρισης Ταυτότητας Χρηστών

Στις επόμενες παραγράφους περιγράφεται εν συντομία η σχετική KYC υλοποίηση αναγνώρισης ταυτότητας χρηστών. Στο Σχήμα 2 απεικονίζεται η αντίστοιχη εφαρμοσμένη αρχιτεκτονική και περιγράφονται οι επιμέρους διεργασίες.



Σχήμα 24: Αρχιτεκτονική ανάπτυξη και επεξεργασία διαδικασιών

Η συνολική αρχιτεκτονική προσέγγιση του συστήματος βασίζεται στον συνδυασμό απλών διαδικασιών και αλληλεπιδράσεων, ενώ δίνεται περιγραφική

έμφαση στην λειτουργικότητα της τεχνολογίας αλυσίδας-κορμού. Τα στοιχεία και οι λειτουργίες των δομικών στοιχείων του συστήματος εξηγούνται μέσω της λογικής ροής της διαδικασίας KYC. Αρχικά, ο χρήστης, ως υποψήφιος πελάτης του συστήματος, εμπλέκεται στο «KYC Registration» υποβάλλοντας τα αντίστοιχα έγγραφα μέσω της φιλικής προς το χρήστη διεπαφής «KYC UI» (Σχήμα 24). Συγκεκριμένα, οι χρήστες καθίστανται υπεύθυνοι από την πλευρά τους για την παροχή των απαιτούμενων πληροφοριών με ακρίβεια, ενώ ο αντίστοιχος μηχανισμός σάρωσης έχει σχεδιαστεί για να εντοπίζει πιθανές ανάρμοστες συμπεριφορές στο δίκτυο και να αποκλείει αμέσως τέτοιους χρήστες από τη διαδικασία, όπως εξηγείται παρακάτω.

Μετά την επιτυχή υποβολή των εγγράφων, η αποθήκευσή τους ακολουθεί στο αποκεντρωμένο, peer-to-peer, διαπλανητικό σύστημα αρχείων (IPFS) [38]. Πιο συγκεκριμένα, το πρωτόκολλο IPFS δημιουργεί ένα ανθεκτικό σύστημα αποθήκευσης αρχείων εντός ενός αποκεντρωμένου peer-to-peer δικτύου. Ωστόσο, το IPFS χρησιμοποιεί ειδικά μέτρα ασφαλείας για τα αποθηκευμένα δεδομένα, βασιζόμενα σε τεχνικές και μηχανισμούς κρυπτογραφικού κατακερματισμού. Κάθε κομμάτι δεδομένων που είναι αποθηκευμένο στο IPFS λαμβάνει μια ξεχωριστή διεύθυνση που προέρχεται από μια εξειδικευμένη διαδικασία κατακερματισμού δεδομένων. Μια μονόδρομη συνάρτηση μετατρέπει τα δεδομένα εισόδου σε ένα ενιαίο αλφαριθμητικό μέσω κατακερματισμού, χωρίς τη δυνατότητα αντιστροφής αυτής της διαδικασίας. Ομοίως, η διεύθυνση περιεχομένου IPFS εκχωρεί ένα μόνο αλφαριθμητικό, το οποίο χρησιμεύει ως διαδρομή προς τα δεδομένα

περιεχομένου. Με αυτόν τον τρόπο, η πρόσβαση στα δεδομένα περιεχομένου απαιτεί γνώση της αντίστοιχης διεύθυνσης περιεγχομένου, Content Identifier (CID).

Έπειτα από την ασφαλή αποθήκευση και επικύρωση των δεδομένων KYC, ξεκινά μια διαδικασία αποθήκευσης πληροφοριών εντός της αλυσίδας. Αυτές οι πληροφορίες περιλαμβάνουν τις βασικές λεπτομέρειες που απαιτούνται για την ταυτοποίηση του εγκεκριμένου χρήστη, περιλαμβάνοντας σε αυτές και την περίοδο ισχύος της ταυτοποίησης που προτείνεται από το υποψήφιο μέλος. Κατά συνέπεια, ευαίσθητες πληροφορίες δεν αποθηκεύονται στην αλυσίδα διασφαλίζοντας με αυτόν τον τρόπο ότι τα μέλη του δικτύου δεν μπορούν να έχουν πρόσβαση στα ευαίσθητα δεδομένα του χρήστη (νέο μέλος), παρά μόνο στην εγκυρότητα ή μη αυτών. Έπειτα, η διαδικασία συνεχίζεται με την αποθήκευση των μη ευαίσθητων δεδομένων στο δίκτυο της αλυσίδας. Η αλληλεπίδραση αυτή απαιτεί συγκεκριμένες βιβλιοθήκες κώδικα που δημιουργούν συνδέσεις και διευκολύνουν την ανταλλαγή πληροφοριών μεταξύ των εμπλεκόμενων στοιχείων. Για παράδειγμα, το "Dedicated KYC Services" παρέχει το απαραίτητο λογισμικό και προγράμματα οδήγησης για τη δημιουργία σύνδεσης και αλληλεπίδρασης με την αλυσίδα, καθώς και τα σχετικά έξυπνα συμβόλαια.

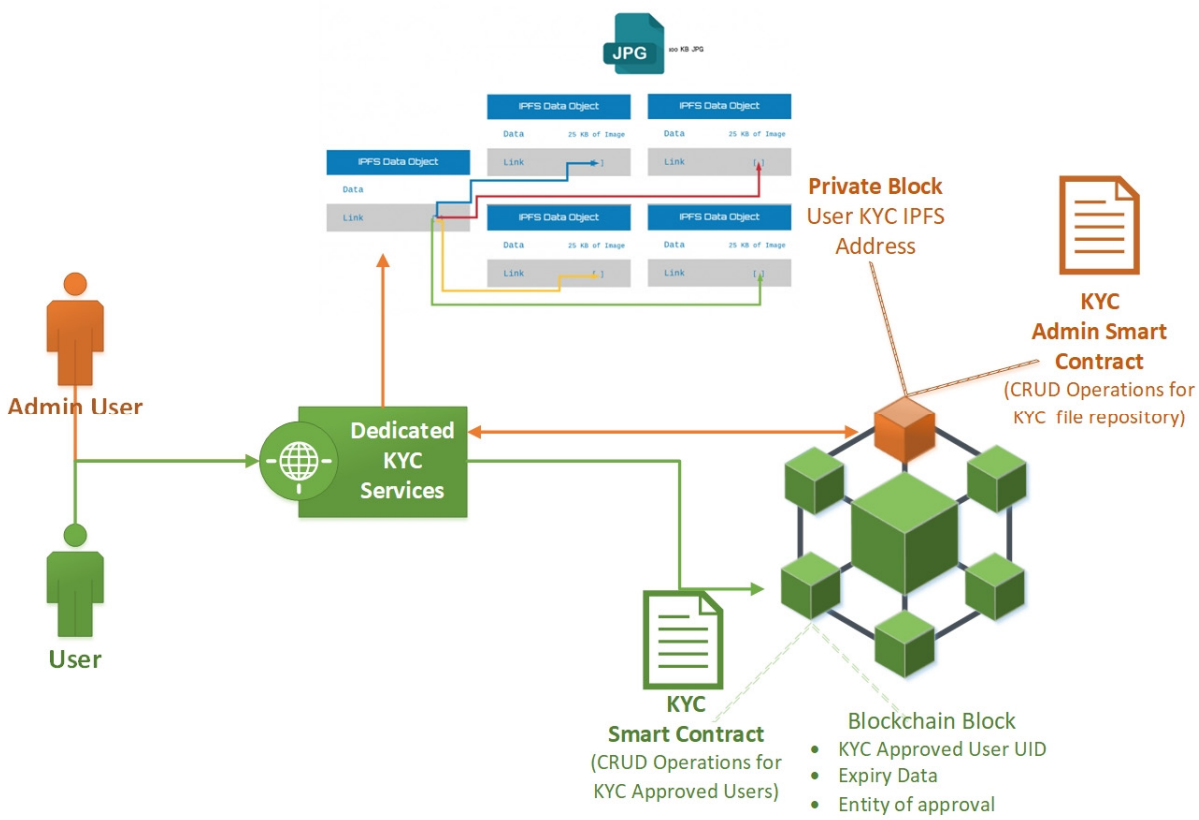
Όσον αφορά το δίκτυο της αλυσίδας, το υλοποιημένο σύστημα χρησιμοποιεί Quorum λόγω διαφόρων παραγόντων και κυρίως την αλληλοσυσχέτισής του με το Ethereum [59]. Η ικανότητα του Quorum να αναπτύσει και να εκτελεί έξυπνα συμβόλαια που χρησιμοποιούν τη γλώσσα

προγραμματισμού Solidity [61,62] και σε συνδυασμό με τα εγγενή χαρακτηριστικά ασφαλείας οδήγησαν ευκολότερα στην υιοθέτησή του. Όπως αναφέρθηκε προηγουμένως, τα δεδομένα που αποθηκεύονται στην αλυσίδα, ιδιαίτερα στο πλαίσιο έξυπνων συμβολαίων, έχουν επιλεχθεί ώστε να είναι επαρκώς λειτουργικά για την αναγνώριση ταυτότητας του χρήστη, διατηρώντας παράλληλα την ανωνυμία αυτού. Η ανάπτυξη ιδιωτικών έξυπνων συμβολαίων απαιτεί συγκεκριμένες διαχειριστικές λειτουργίες να είναι προσβάσιμες από τα "Dedicated KYC Services" που επιβεβαιώνουν την έγκριτη συμμετοχή ενός συγκεκριμένου νέου χρήστη στο σύστημα.

Τόσο το IPFS όσο και το Quorum στοχεύουν στη δημιουργία ενός αποκεντρωμένου συστήματος που όχι μόνο προστατεύει αλλά και ενισχύει την ιδιωτικότητα και την ασφάλεια των προσωπικών πληροφοριών. Όπως αναλύθηκε, το IPFS φιλοξενεί τα ευαίσθητα δεδομένω των μελών του συστήματος. Όπως αντικατοπτρίζεται στα σχήματα 25 και 26, το πρωτόκολλο IPFS διαιρεί τα ανεβασμένα αρχεία σε επιμέρους τμήματα, δημιουργώντας ένα τελικό σημείο (endpoint) που συνδέει τα διάφορα τμήματα KYC αρχείων ενός χρήστη.

Προκειμένου να υπάρχει πρόσβαση στα δεδομένα που περιέχονται στο IPFS, η αντίστοιχη διεύθυνση του endpoint πρέπει να είναι γνωστή. Η ενοποιημένη αλυσίδα-κορμού Quorum διευκολύνει τη δημιουργία ιδιωτικών ή επιτρεπόμενων μπλοκ δεδομένων που γίνονται προσβάσιμα αποκλειστικά από συγκεκριμένους χρήστες, ενώ ταυτόχρονα μεταδίδει μόνο τον κρυπτογραφικό κατακερματισμό αυτών στο υπόλοιπο δίκτυο. Με αυτόν τον τρόπο

επικυρώνεται η ακεραιότητα των μπλοκ σε ολόκληρη την αλυσίδα ενώ ταυτόχρονα προστατεύονται τα ιδιωτικά δεδομένα των μελών.



Σχήμα 25: Δημόσια (χρήστης) και ιδιωτικά (διαχειριστής) έξυπνα συμβόλαια KYC

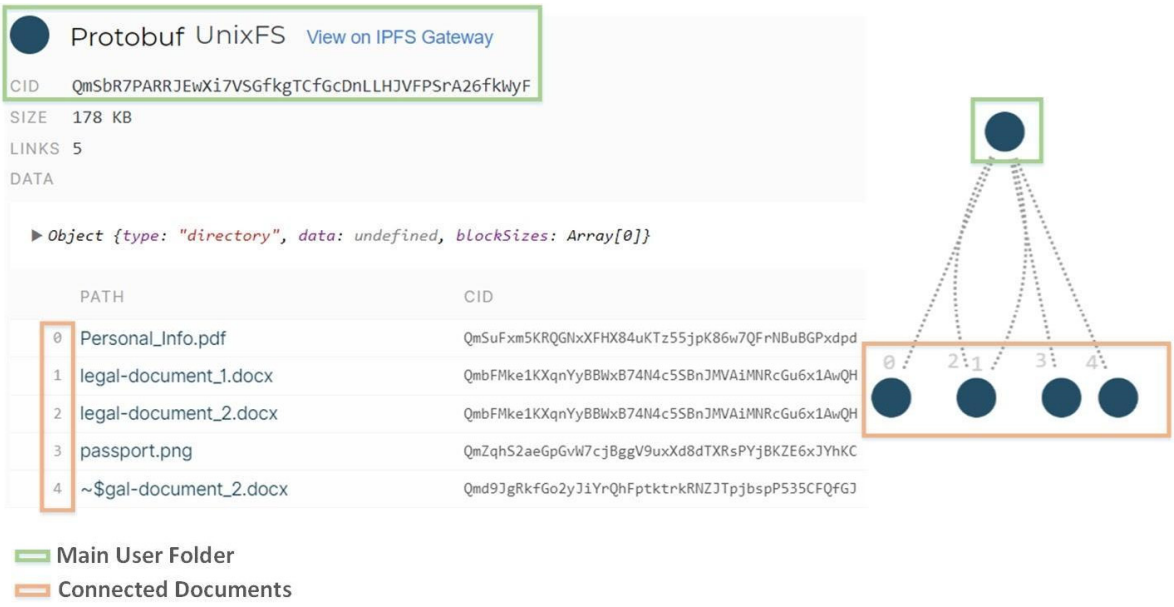
Όπως απεικονίζεται στο Σχήμα 25, η ανάπτυξη του δικτύου blockchain Quorum φιλοξενεί τόσο ιδιωτικά όσο και δημόσια έξυπνα συμβόλαια, καθένα από τα οποία παρέχει διαφορετικά επίπεδα πρόσβασης στις πληροφορίες.

Στον Πίνακα 3, αναλύονται οι επιμέρους λειτουργίες του δημόσιου KYC έξυπνου συμβολαίου οι οποίες διευκολύνουν τις αντίστοιχες CRUD λειτουργίες πληροφοριών των χρηστών.

Ομοίως, η ασφάλεια των διευθύνσεων περιεγχομένου είναι εγγυημένη

στο πλαίσιο του ιδιωτικού KYC έξυπνου συμβολαίου, καθώς είναι προσβάσιμα αποκλειστικά από εξουσιοδοτημένα μέλη ρόλου διαχειριστή. Αυτά τα μέλη διαθέτουν εξουσιοδότηση να επικαλούνται μεθόδους έξυπνων συμβολαίων επιστρέφοντας διευθύνσεις περιεγχομένου χρηστών, παρέχοντας έτσι πρόσβαση στα αντίστοιχα αρχεία τους. Στον Πίνακα 4, περιγράφονται οι συναρτήσεις που μπορούν να κληθούν μόνο από συγκεκριμένους ρόλους με δικαιώματα διαχειριστή.

Όταν τα μέλη διαχειριστή που επιθυμούν να ελέγξουν την ταυτότητα ενός μέλους ή να επαληθεύσουν την ημερομηνία λήξης συμμετοχής, επικαλούνται την μέθοδο του δημοσίου KYC έξυπνου συμβολαίου "GetKYCMemberApproval()", λαμβάνοντας μόνο τις απαραίτητες πληροφορίες ως απάντηση από τον αποκεντρωμένο χώρο αποθήκευσης IPFS, συμπεριλαμβανομένου του ονόματος της εξωτερικής οντότητας που ενέκρινε το μέλος.



Σχήμα 26: Σύστημα αρχείων με διεύθυνση περιεχομένου IPFS.

Πίνακας 3: Περιγραφές μεθόδων δημοσίου συμβολαίου.

Όνομα μεθόδου	Περιγραφή	Είσοδος	Απάντηση
GetKYCMemberApproval()	Αυτή η μέθοδος είναι υπεύθυνη για την παροχή βασικών πληροφοριών KYC κατόπιν αιτήματος. Όλα τα δεδομένα που επιστρέφονται από αυτήν την μέθοδο δεν περιέχουν ευαίσθητες πληροφορίες για τον χρήστη, παρά μόνο τον ελάχιστο όγκο πληροφοριών για την αναγνώριση του χρήστη και τη χρονική περίοδο για την οποία έχει εγκριθεί.	**Address:** Διεύθυνση λογαριασμού χρήστη	**Date:** Ημερομηνία λήξης KYC. **String:** Οντότητα που ενέκρινε το μέλος
UpdateKYCMember()	Η έγκριση ενός λογαριασμού KYC πρέπει να ενημερωθεί όταν παρέλθει η εγκεκριμένη περίοδος, ενώ υπάρχουν επίσης περιπτώσεις στις οποίες ένα εγκεκριμένο μέλος πρέπει να αποκλειστεί λόγω κακόβουλων δραστηριοτήτων.	**Address:** Διεύθυνση λογαριασμού χρήστη **Date:** Ανανεωμένη ημερομηνία λήξης. **String:** Οντότητα που ενέκρινε το μέλος	Μήνυμα επιτυχίας
CreateKYCMember()	Αυτή η μέθοδος είναι υπεύθυνη για την ενημέρωση των πληροφοριών KYC που είναι αποθηκευμένες στην αλυσίδα. Όταν ένα νέο μέλος εγκριθεί	**String:** Ιδιωτικό κλειδί λογαριασμού διαχειριστή **Address:**	Μήνυμα

	από το σύστημα, οι πληροφορίες KYC πρέπει να αποθηκεύονται σε μια δομή μέσα στο έξυπνο συμβόλαιο. Αυτή η μέθοδος είναι υπεύθυνη για τη δημιουργία μιας νέας εγγραφής με τις πληροφορίες KYC ενός νέου μέλους.	Διεύθυνση λογαριασμού χρήστη **Date:** Ανανεωμένη ημερομηνία λήξης **String:** Οντότητα που ενέκρινε το μέλος **Bytes32:** Ιδιωτικό κλειδί λογαριασμού διαχειριστή	επιτυχίας

Αυτά τα δεδομένα δεν εμπεριέχουν ευαίσθητες πληροφορίες χρήστη, όπως οικογενειακή κατάσταση ή οικονομικά στοιχεία, ενώ αποθηκεύονται μέσα στο έξυπνο συμβόλαιο, όπως απεικονίζεται στο Σχήμα 27.

```
struct registeredMember {
    address memberAddr;
    uint256 time;
    string approveEntity;
}
```

Σχήμα 27: Μη ευαίσθητες πληροφορίες μελών στην αλυσίδα-κορμού (on-chain).

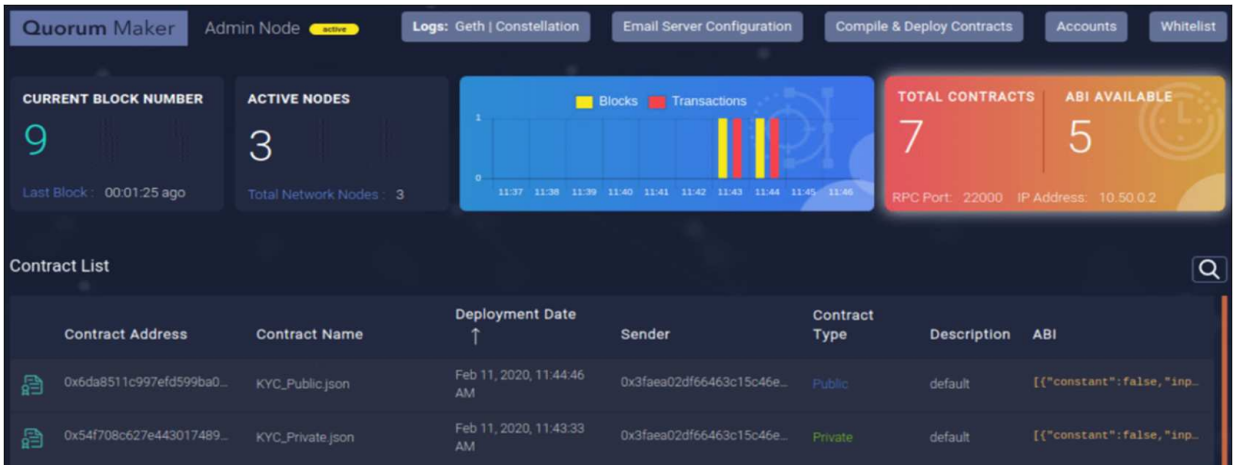
Οι ευαίσθητες πληροφορίες αποθηκεύονται στο σύστημα αρχείων IPFS με διεύθυνση περιεχομένου όπου έχουν πρόσβαση μόνο εξουσιοδοτημένα μέλη ρόλου διαχειριστή.

Το δημόσιο "KYC Smart Contract" και το ιδιωτικό "KYC Admin Smart Contract" αναπτύσσονται στο δίκτυο Alastria μέσω του Quorum Maker Utility [63] για την παρακολούθηση έξυπνων συμβολαίων και άλλων δραστηριοτήτων

και στατιστικών στοιχείων δραστηριοτήτων της αλυσίδας.

Πίνακας 4: Περιγραφές μεθόδων ιδιωτικού συμβολαίου.

Όνομα μεθόδου	Περιγραφή	Είσοδος	Απάντηση
GetUserCID()	Αυτή η μέθοδος είναι υπεύθυνη για την επιστροφή της διεύθυνσης περιεγχομένου (CID) του φακέλου που περιέχει τα έγγραφα KYC ενός χρήστη. Είναι σημαντικό να αναφέρουμε ότι για να αποκτηθεί πρόσβαση από τον χρήστη στη λειτουργικότητα αυτής της μεθόδου, το έξυπνο συμβόλαιο ελέγχει τον χρήστη εάν την άδεια ασφαλούς πρόσβασης, δηλαδή εάν έχει ρόλο διαχειριστή. Επιπλέον, η μέθοδος απαιτεί το κατακερματισμένο ιδιωτικό κλειδί του χρήστη για λόγους προσπέλασης.	**String:** Αναγνωριστικό λογαριασμού χρήστη **String:** Κατακερματισμένο ιδιωτικό κλειδί διαχειριστή	**String:** Αντίστοιχη διεύθυνση περιεγχομένου
CreateUserCID()	Όταν τα έγγραφα KYC αποθηκευτούν επιτυχώς στο IPFS, αυτή η μέθοδος καλείται να αποθηκεύσει τη διεύθυνση περιεγχομένου KYC προκειμένου να καταστήσει τα αρχεία ανιχνεύσιμα και προσβάσιμα από διαχειριστές μέσω του ιδιωτικού έξυπνου συμβολαίου.	**String:** Αναγνωριστικό λογαριασμού χρήστη **String:** Διεύθυνση περιεγχομένου φακέλου **String:** Κατακερματισμένο ιδιωτικό κλειδί διαχειριστή	Μήνυμα επιτυχίας

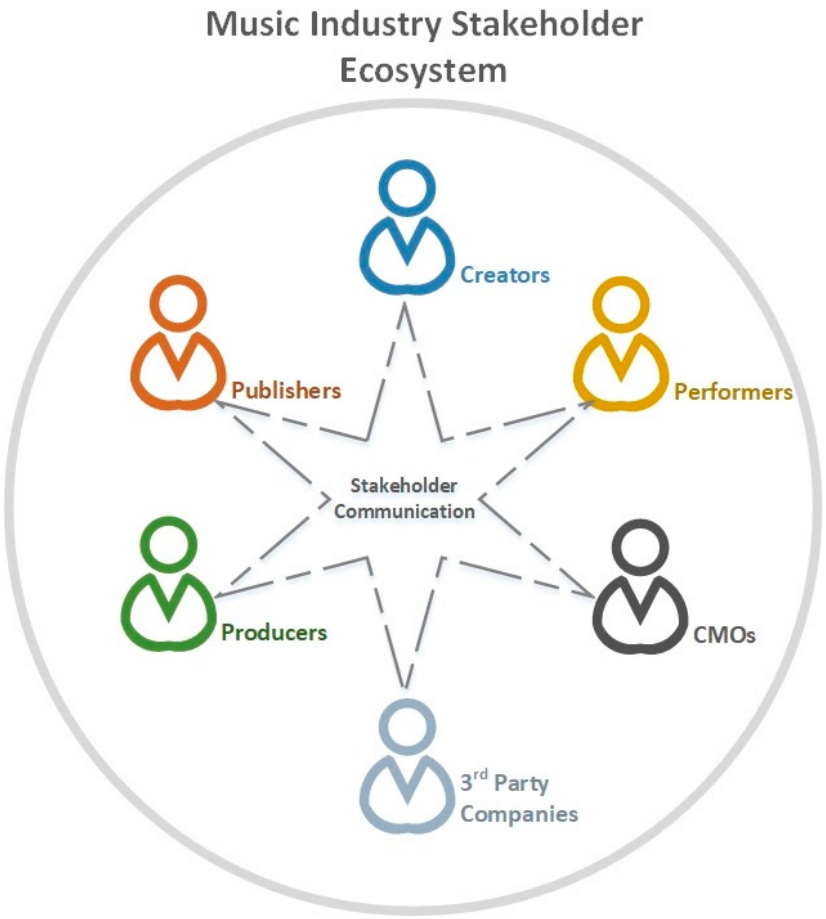


Σχήμα 28: Έξυπνα συμβόλαια στο Quorum Maker.

Το Σχήμα 28 παρουσιάζει το δημόσιο KYC έξυπνο συμβόλαιο καθώς και το έξυπνο συμβόλαιο διαχειριστή από την οπτική γωνία της παρακολούθησης εφαρμογών.

Διακυβέρνηση Πνευματικών Δικαιωμάτων με Έξυπνα Συμβόλαια Κοινοπραξίας

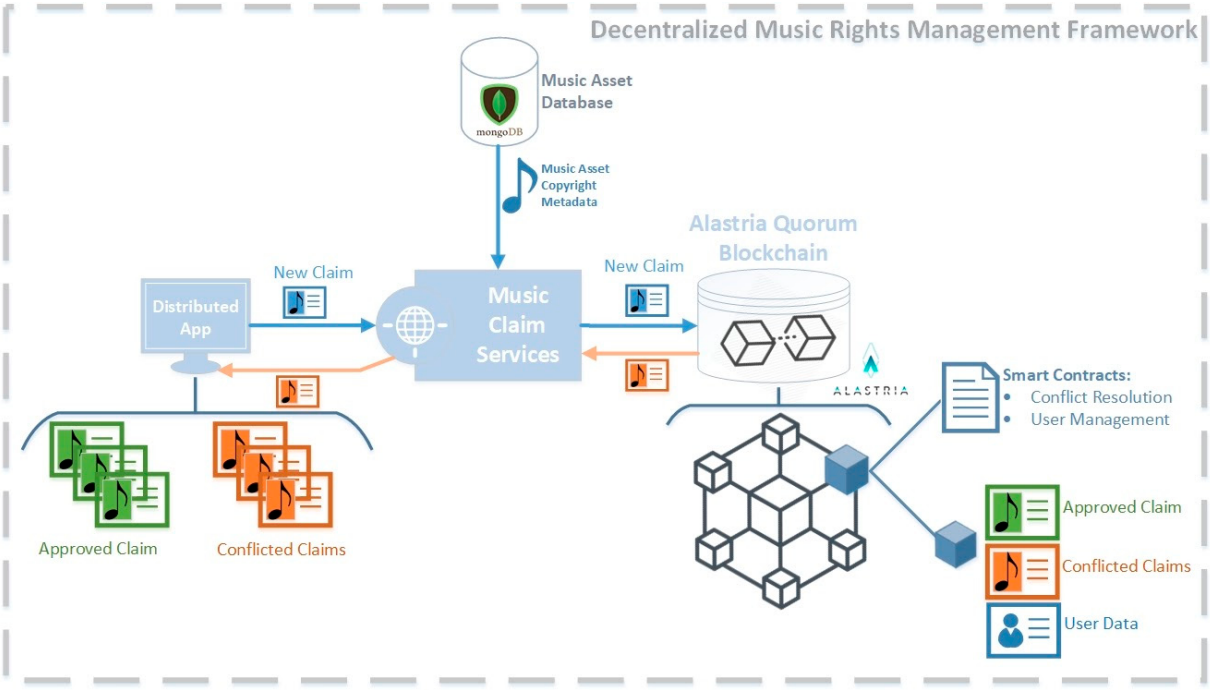
Σχετικά με την υλοποίηση εφαρμογής πνευματικών δικαιωμάτων σε αλυσίδες-κορμού, το Σχήμα 29 περιγράφει τις σχέσεις μεταξύ των εμπλεκόμενων φορέων του κλάδου. Μέσω αυτών των σχέσεων καθίστανται ποικίλες διανομές πνευματικών δικαιωμάτων και σχετικών εγγράφων, καταλήγοντας σε μια διαδικασία παρακολούθησης και επαλήθευσης ακρίβειας δεδομένων πνευματικών δικαιωμάτων για Οργανισμούς Συλλογικής Διαχείρισης (CMO).



Σχήμα 29: Οικοσύστημα ενδιαφερόμενων μελών μουσικής βιομηχανίας.

Η παρούσα προσέγγιση στοχεύει στη δημιουργία ενός πραγματικά αποκεντρωμένου συστήματος που είναι προσβάσιμο από διαφορετικούς φορείς και εφαρμογές αυτών, με αποτέλεσμα ένα ενιαίο πλαίσιο όπου διευκολύνεται το περίπλοκο τοπίο διαχείρισης μουσικών δικαιωμάτων. Όπως απεικονίζεται στο Σχήμα 29, η υλοποιημένη αποκεντρωμένη εφαρμογή συνδέεται με την αλυσίδα-κορμού και εμφανίζει τις κατάλληλες πληροφορίες πνευματικών δικαιωμάτων επιτρέποντας στους ενδιαφερόμενους να τις διαχειρίζονται. Οι υπηρεσίες Musical Claim Services ενσωματώνουν τόσο τη λογική της

αποκέντρωσης όσο και του δικτύου βάσης δεδομένων μουσικών έργων.



Σχήμα 30: Πλαίσιο αποκεντρωμένης διαχείρισης μουσικών δικαιωμάτων.

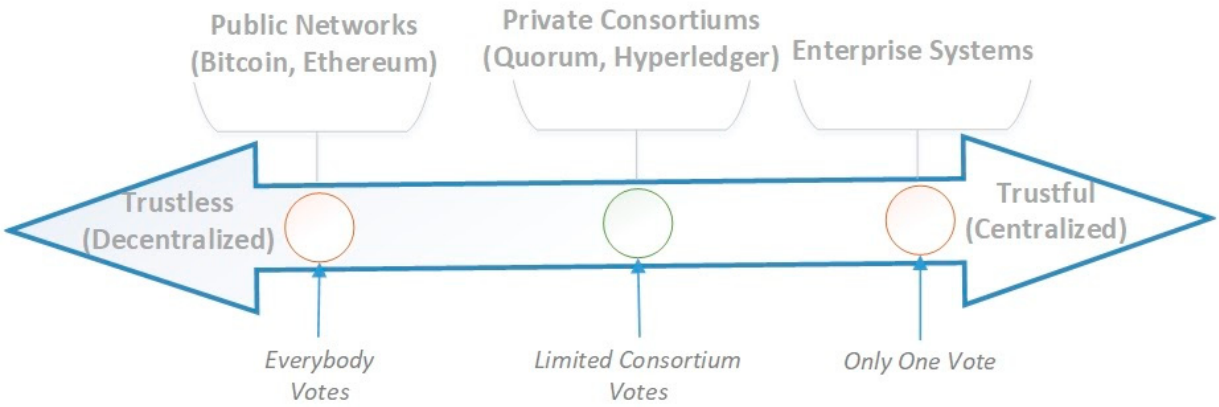
Η αποκεντρωμένη εφαρμογή και όλο το πλαίσιο αποκεντρωμένης διαχείρισης μουσικών δικαιωμάτων χαρακτηρίζονται από τις έννοιες:

- Διαφάνεια: Κάθε ενδιαφερόμενος μπορεί να συμμετάσχει και να επαληθεύσει την κατάσταση των δικαιωμάτων του.
- Εμπιστοσύνη: Κανείς δεν μπορεί να χειραγωγήσει ισχυρισμούς δικαιωμάτων.
- Ιχνηλασιμότητα: Δυνατότητα παρακολούθησης των ισχυρισμών δικαιωμάτων που έχει λάβει ένα περιουσιακό στοιχείο με την πάροδο του χρόνου.
- Αποκέντρωση: Η βάση δεδομένων δεν ελέγχεται από μία μόνο οντότητα.

Οι συνεισφορές προέρχονται από μια κατανεμημένη ομάδα μελών.

- Επίλυση συγκρούσεων: Η ενοποίηση των δικαιωμάτων σε μια ολική προβολή εντοπίζει τις συγκρούσεις σε αρχικά στάδια.
- Αποδοτικότητα: Απλοποίηση μέσω μιας διαλειτουργικής λύσης που μοιράζεται πληροφορίες μεταξύ των ενδιαφερόμενων μελών και ενσωματώνεται στα συστήματά τους.

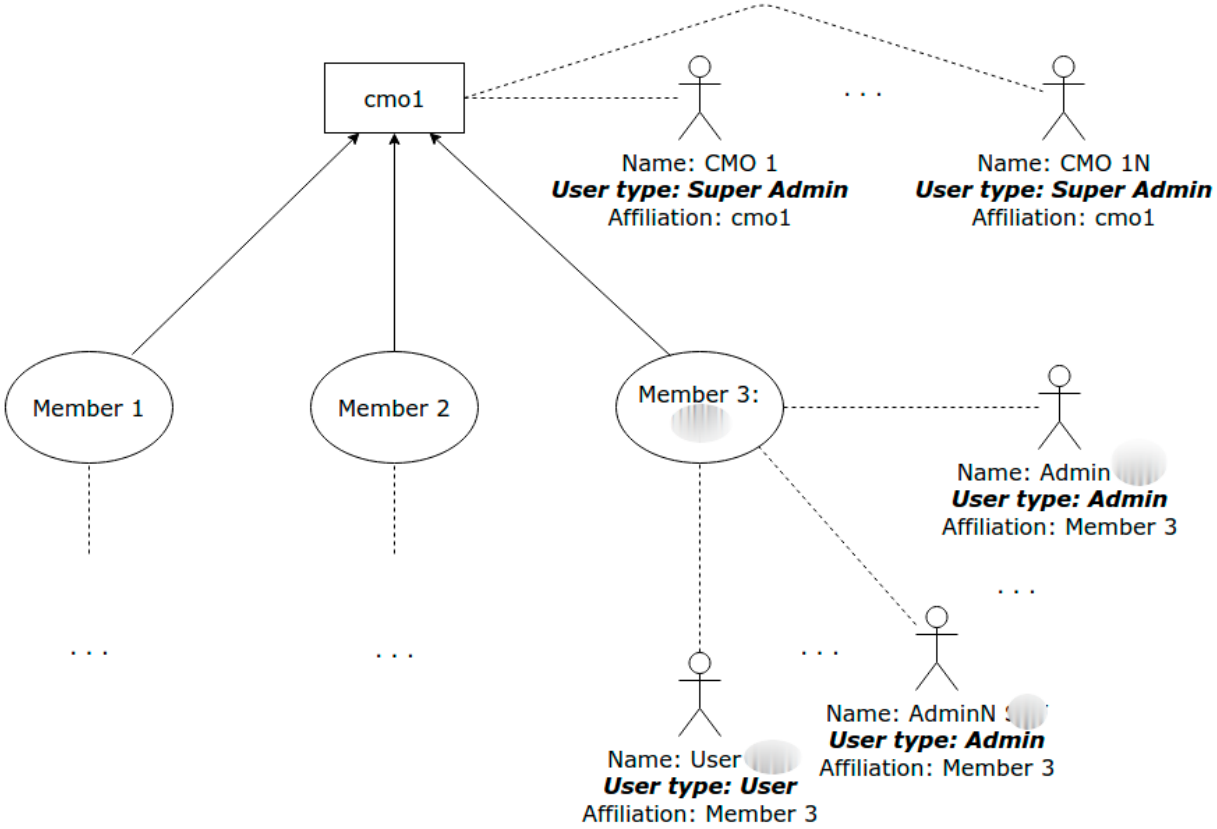
Στο Σχήμα 31 απεικονίζεται το δίκτυο της αλυσίδας που χρησιμοποιείται στο προτεινόμενο πλαίσιο βασίζεται σε μια αλυσίδα blockchain Quorum που αναπτύσσεται στο δίκτυο Alastria T [60]. Το Quorum blockchain είναι ουσιαστικά ένα δίκτυο Ethereum ενισχυμένο με ένα πρόσθετο επίπεδο ασφαλείας [59].



Σχήμα 31: Το φάσμα εμπιστοσύνης σε δίκτυα τελευταίας τεχνολογίας.

Η τρέχουσα εφαρμογή του Alastria Quorum χρησιμοποιεί τον συναινετικό αλγόριθμο Istanbul Βυζαντινής Ανοχής Σφαλμάτων (IBFT), μια παραλλαγή της Πρακτικής Βυζαντινής Ανοχής Σφαλμάτων (PBFT) [69].

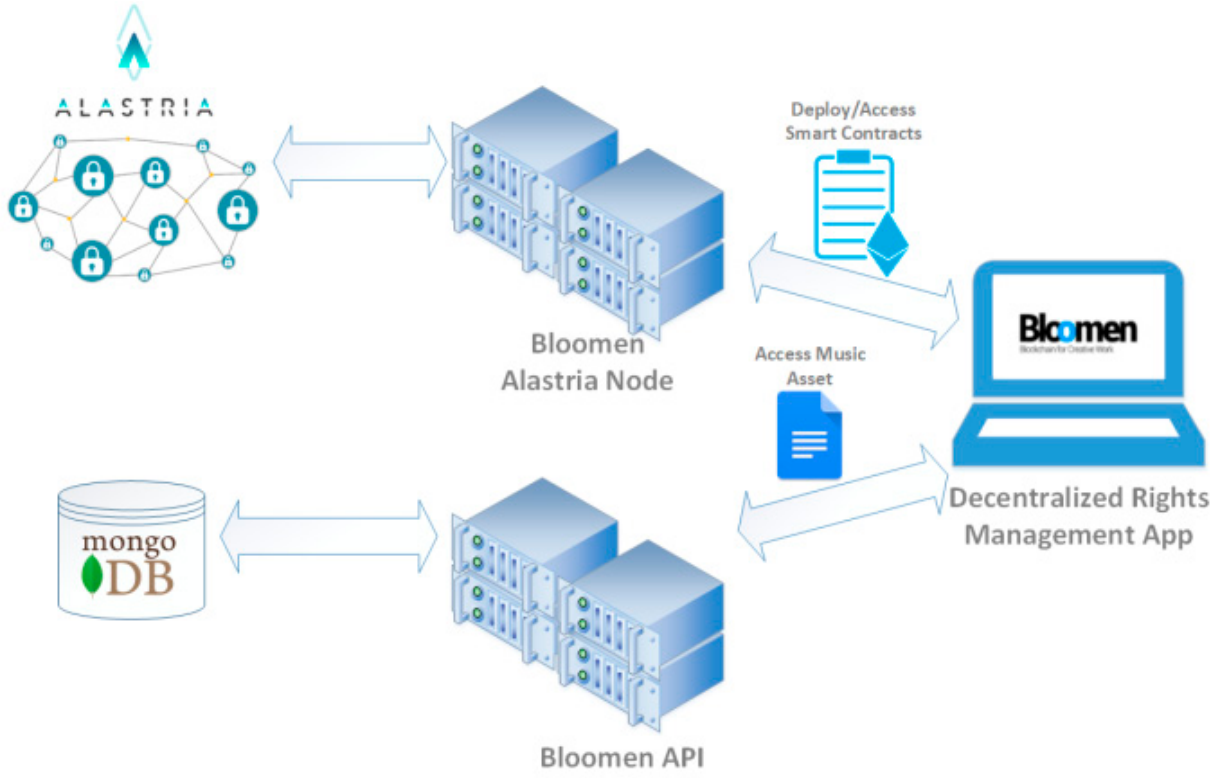
Σε αυτήν την αποκεντρωμένη εφαρμογή, υπάρχουν τρεις (3) κατηγορίες χρηστών: Super Admins, Admins και Users. Οι Super Admins αντιπροσωπεύουν τους συμμετέχοντες CMOs, ενώ οι Διαχειριστές και οι Χρήστες συνδέονται με τα Μέλη που σχετίζονται με τους CMOs. Στο Σχήμα 32, παρουσιάζεται μια σαφής εικόνα σε σχέση με την ιεραρχία χρήστη εντός της εφαρμογής.



Σχήμα 32: Ιεραρχία χρηστών και επιχειρηματικοί ρόλοι.

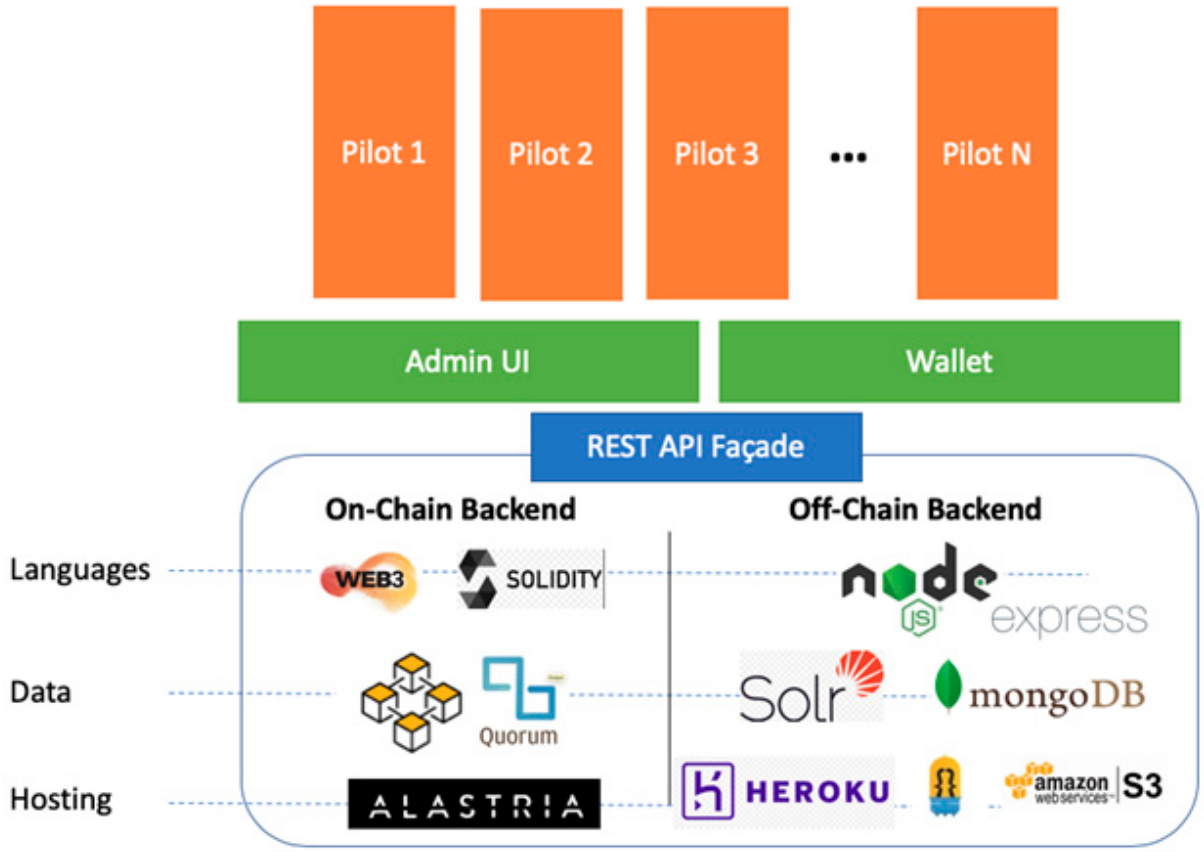
Στο Σχήμα 33, η βασική εφαρμογή, γνωστή ως Εφαρμογή Αποκεντρωμένης Διαχείρισης Δικαιωμάτων, απεικονίζεται μαζί με τα

διαδραστικά της στοιχεία. Ο Alastria κόμβος επιτρέπει την άμεση και αποτελεσματική επικοινωνία μεταξύ της εφαρμογής και των έξυπνων συμβολαίων που εγκθίστανται και εκτελούνται στο Alastria δίκτυο.



Σχήμα 33: Τεχνική αρχιτεκτονική άποψη του συστήματος.

Επιπλέον, το Σχήμα 34 εμφανίζει τη στοίβα τεχνολογίας και την αρχιτεκτονική ολόκληρης της πλατφόρμας. Το backend χωρίζεται σε δύο μέρη: τα εξαρτήματα εντός και εκτός της αλυσίδας. Ένα επιπλέον λογικό επίπεδο συγχρονίζει τις κλήσεις μεταξύ των διαφόρων τμημάτων εκτός της αλυσίδας και του backend εκθέτοντας ένα RESTful API για την εφαρμογή διαχείρισης των δικαιωμάτων, ενώ άλλα είδη εφαρμογών θα μπορούσαν να αναπτυχθούν και να ενσωματωθούν σε ολόκληρη την πλατφόρμα.



Σχήμα 34: Τεχνολογική στοίβα από το REST API.

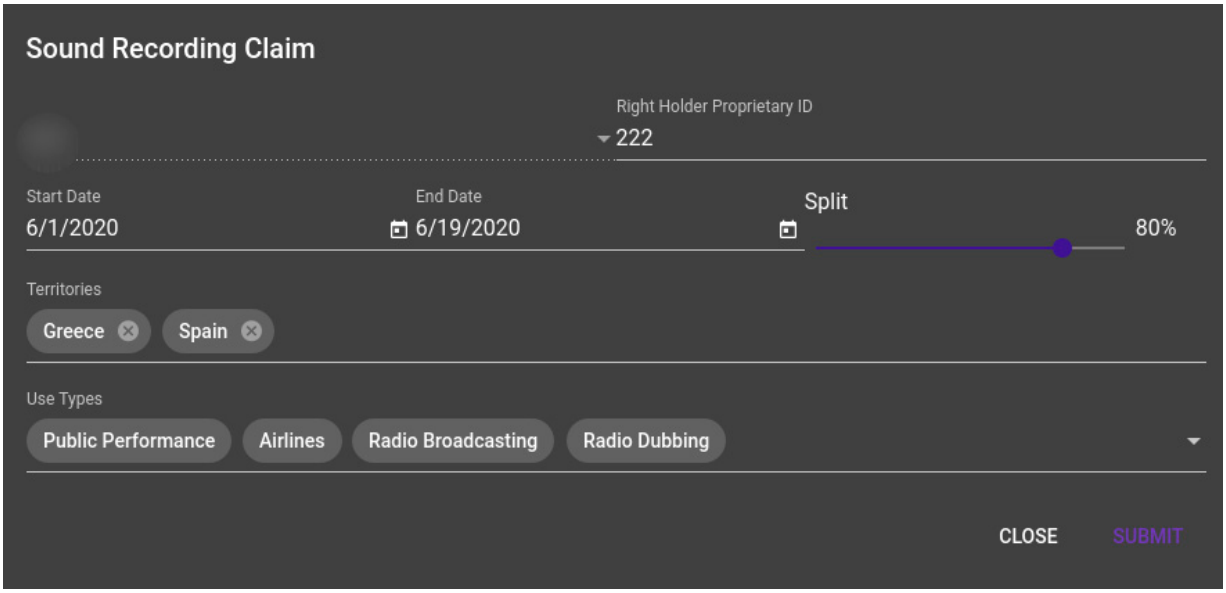
Η λύση της Εφαρμογής Αποκεντρωμένης Διαχείρισης Δικαιωμάτων εισάγει μια μοναδική και καινοτόμο προσέγγιση. Το όνομα του έξυπνου συμβολαίου "Claims" αντιπροσωπεύει κάθε ισχυρισμό μουσικού δικαιώματος χρησιμοποιώντας μια αντίστοιχη δομή Solidity που ονομάζεται "struct Claim". Η δομή αποτελείται από διακριτά χαρακτηριστικά, όπως φαίνεται στο Σχήμα 35. Η "struct Claim" περιλαμβάνει έναν δείκτη κατάστασης για τον ισχυρισμό που μπορεί είτε να αντιπροσωπεύει ένα διεκδικούμενο δικαίωμα, σε περίπτωση που δεν υπάρχει διαφωνία στη δήλωση δικαιωμάτων σε σύγκριση με άλλες απαιτήσεις που έχουν υποβληθεί στην αλυσίδα για το ίδιο δικαίωμα, είτε μία

σύγκρουση δικαιωμάτων, σε περίπτωση αλληλοεπικαλυπτόμενων δικαιωμάτων.

```
struct Claim {
  uint256 creationDate;
  uint256 claimId;
  NameValue[] claimData;
  bool claimType;
  uint256 memberOwner;
  bool status;
  uint256 lastChange;
  uint16 maxSplit;
}
```

Σχήμα 35: Δομή έξυπνου συμβολαίου σε Solidity για ισχυρισμούς.

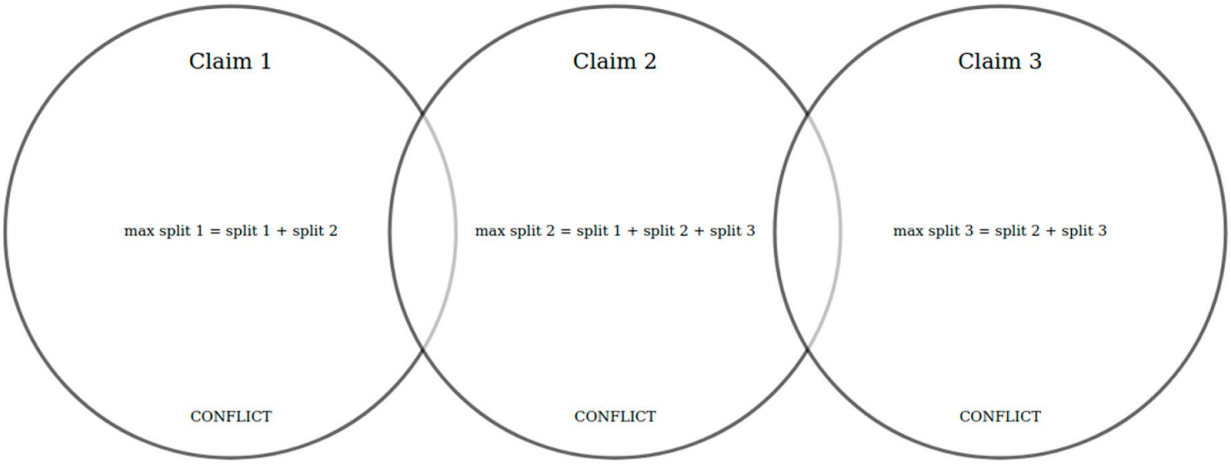
Η δομή ισχυρισμού "struct Claim" περιλαμβάνει επίσης το ποσοστό κατανομής δικαιωμάτων, τις ημερομηνίες έναρξης και λήξης των δικαιωμάτων, τις περιοχές ισχύος και τον τύπο τους, όπως απεικονίζεται για έναν ισχυρισμό ηχογράφηση στο Σχήμα 36.



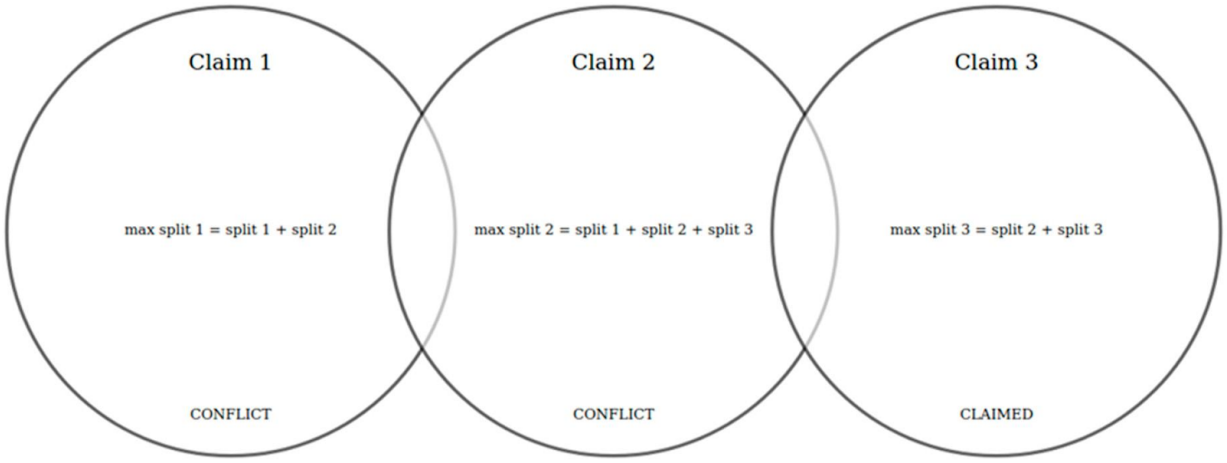
Σχήμα 36: Επισκόπηση ισχυρισμού με τα δεδομένα του εν μέσω ανανέωσής του.

Ένα σημαντικό μέρος του συστήματος για τη διακυβέρνηση αντικρουόμενων πνευματικών δικαιωμάτων διατηρώντας την ιδιωτικότητα των δεδομένων αποτελεί η μέθοδος "checkClaimStatus()" εντός του ιδιωτικού έξυπνου συμβολαίου "Claims". Η μέθοδος checkClaimStatus() έχει πρόσβαση στην ιδιωτική αντιστοίχιση ισχυρισμών εντός του έξυπνου συμβολαίου. Εφόσον η μελέτη σύγκρουσης γίνεται διατηρώντας την ιδιωτικότητα, το σύστημα υπολογίζει με ασφάλεια αντικρουόμενους ισχυρισμούς.

Μέγιστος διαχωρισμός ισχυρισμού ορίζεται το ποσοστό που έχει δηλωθεί ο ισχυρισμός για συγκεκριμένο συνδυασμό των ίδιων πεδίων της δομής έξυπνου συμβολαίου στο Σχήμα 35. Εάν ο μέγιστος διαχωρισμός ενός ισχυρισμού υπερβαίνει το 100, επισημαίνεται ως σύγκρουση (conflict) όπως φαίνεται στο σχήμα 37, διαφορετικά, επισημαίνεται ως ισχύων (claimed, Σχήμα 38). Όταν εντοπίζονται δύο επικαλυπτόμενοι ισχυρισμοί, οι μέγιστες τιμές διαχωρισμού τους υπολογίζονται εκ νέου στην αλυσίδα και οι κατάστασή τους ενημερώνονται ανάλογα.



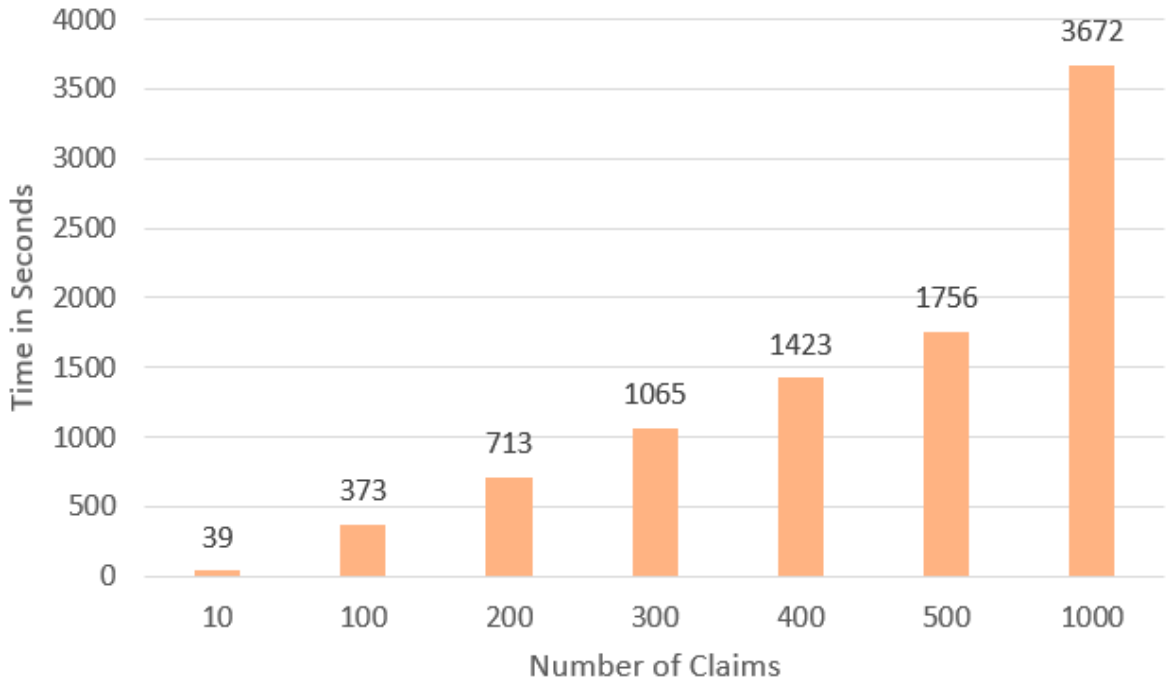
Σχήμα 37: Αντικρουόμενοι ισχυρισμοί. Σύγκρουση.



Σχήμα 38: Αντικρουόμενοι ισχυρισμοί. Σύγκρουση και Ισχύων.

Επίσης, αναπτύχθηκε ένας μηχανισμός νομισματικών κινήτρων. Όταν ένας χρήστης επιχειρεί να υποβάλει μια νέα συναλλαγή και έχει επαρκές υπόλοιπο, η συναλλαγή υποβάλλεται και το νομισματικό του υπόλοιπο μειώνεται κατά την αξία της συναλλαγής. Αρχικά, καθορίζεται ένα συγκεκριμένο κόστος συναλλαγής που σχετίζεται με οποιαδήποτε συναλλαγή ισχυρισμού για δημιουργία, ενημέρωση ή διαγραφή.

Τέλος, σχετικά με την αξιολόγηση του συστήματος στοχεύθηκε η προσομοίωσή του σε πραγματικές συνθήκες. Συγκεκριμένα, αξιολογήθηκε η απόκριση του συστήματος κάτω από απαιτητικά φορτία τα οποία δημιουργήθηκαν με ομαδικά αρχεία μορφής CSV. Καθένα από αυτά περιείχε μια σειρά ισχυρισμών που έπρεπε να υποβληθούν για επεξεργασία από το σύστημα και στη συνέχεια να αποθηκευτούν στην αλυσίδα. Τα αρχεία διέφεραν σε μέγεθος, από 100 έως 10.000 ισχυρισμούς, μετρώντας με αυτόν τον τρόπο την ανταπόκριση του συστήματος σε διαφορετικά ποσοστά δημιουργίας ισχυρισμών. Η αξιολόγηση παρουσιάζεται σε δύο (2) γραφήματα.

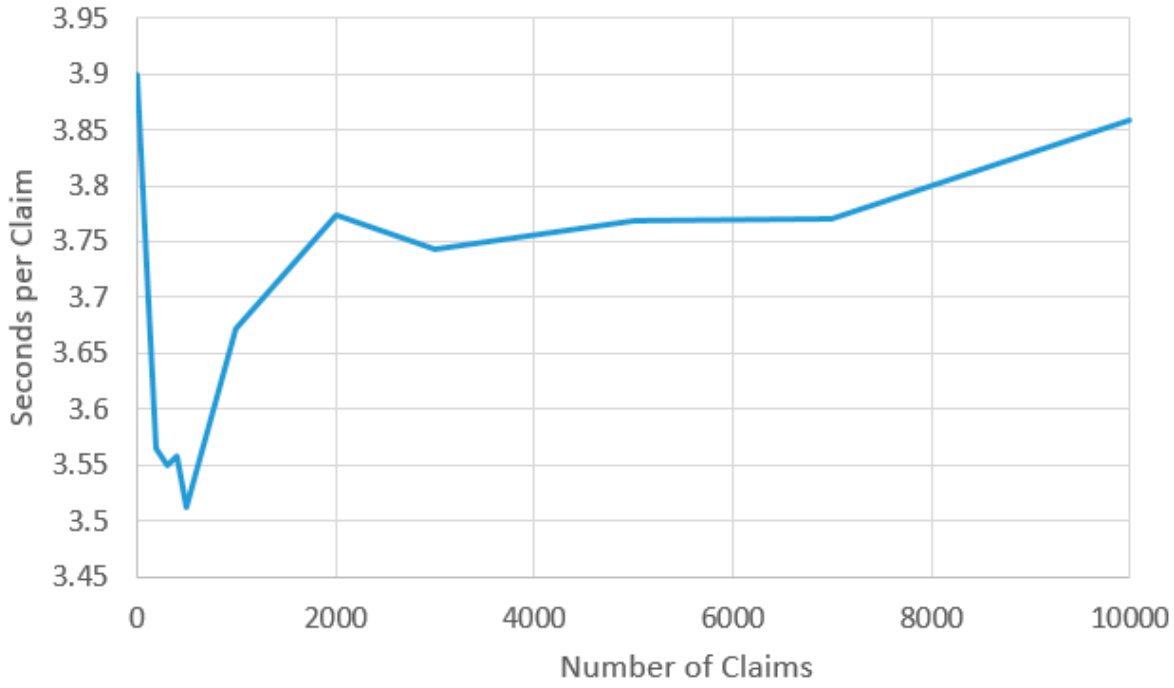


Σχήμα 39: Χρόνος επεξεργασίας διαφορετικών αρχείων ομαδικά.

Στο πρώτο γράφημα (Σχήμα 39) απεικονίζεται ο χρόνος που απαιτείται για την ομαδική επεξεργασία αρχείων διαφόρων μεγεθών, ενώ το δεύτερο γράφημα (Σχήμα 40) δείχνει τον μέσο χρόνο που χρειάζεται το σύστημα για την επεξεργασία μεμονωμένων ισχυρισμών.

Δεδομένων των περιορισμών στη δημιουργία μπλοκ που περιέχουν συναλλαγές μαζί με τη διαδοχική επεξεργασία των αξιώσεων, ο συνολικός χρόνος παρτίδας είναι σχετικά αποδοτικός. Αν και η επεξεργασία 10.000 αξιώσεων διαρκεί περίπου 10 ώρες, ένας συνηθισμένος φόρτος εργασίας στη μουσική βιομηχανία, το σύστημα είναι σε θέση να εντοπίσει συγκρούσεις σε λιγότερο από μία ημέρα, κάτι που αντιπροσωπεύει σημαντική βελτίωση σε αυτό το

σενάριο. Σε περιβάλλον παραγωγής, οι ισχυρισμοί μπορούν να αποθηκεύονται κατά ομάδες από το σύστημα αντί να υποβάλλονται σε επεξεργασία γραμμικά.



Σχήμα 40: Μέσος χρόνος επεξεργασίας ισχυρισμών.

Αυτή η προσέγγιση χρησιμοποιείται συχνά σε αλυσίδες παραγωγής όπως το Bitcoin και το Ethereum που φιλοξενούν εκατομμύρια συναλλαγές καθημερινά. Συγκεκριμένα, ο μέσος χρόνος που απαιτείται για την επεξεργασία μιας αξίωσης παρέμεινε σταθερός (περίπου 3,7 δευτερόλεπτα) σε διαφορετικούς φόρτους εργασίας (ποσότητες ισχυρισμών). Αυτή η σταθερότητα υποδηλώνει ένα στιβαρό σύστημα χωρίς σημαντικά σημεία συμφόρησης. Στο γράφημα του Σχήματος 40, η αντίστοιχη ακίδα είναι εμφανής για μικρότερες ομάδες αρχείων (3,9 δευτερόλεπτα) και προκαλείται από αρχική κατάσταση κατά την προετοιμασία της επικοινωνίας με την αλυσίδα.

Αυτή η καθυστέρηση μειώνεται καθώς ο αριθμός των ισχυρισμών αυξάνεται.

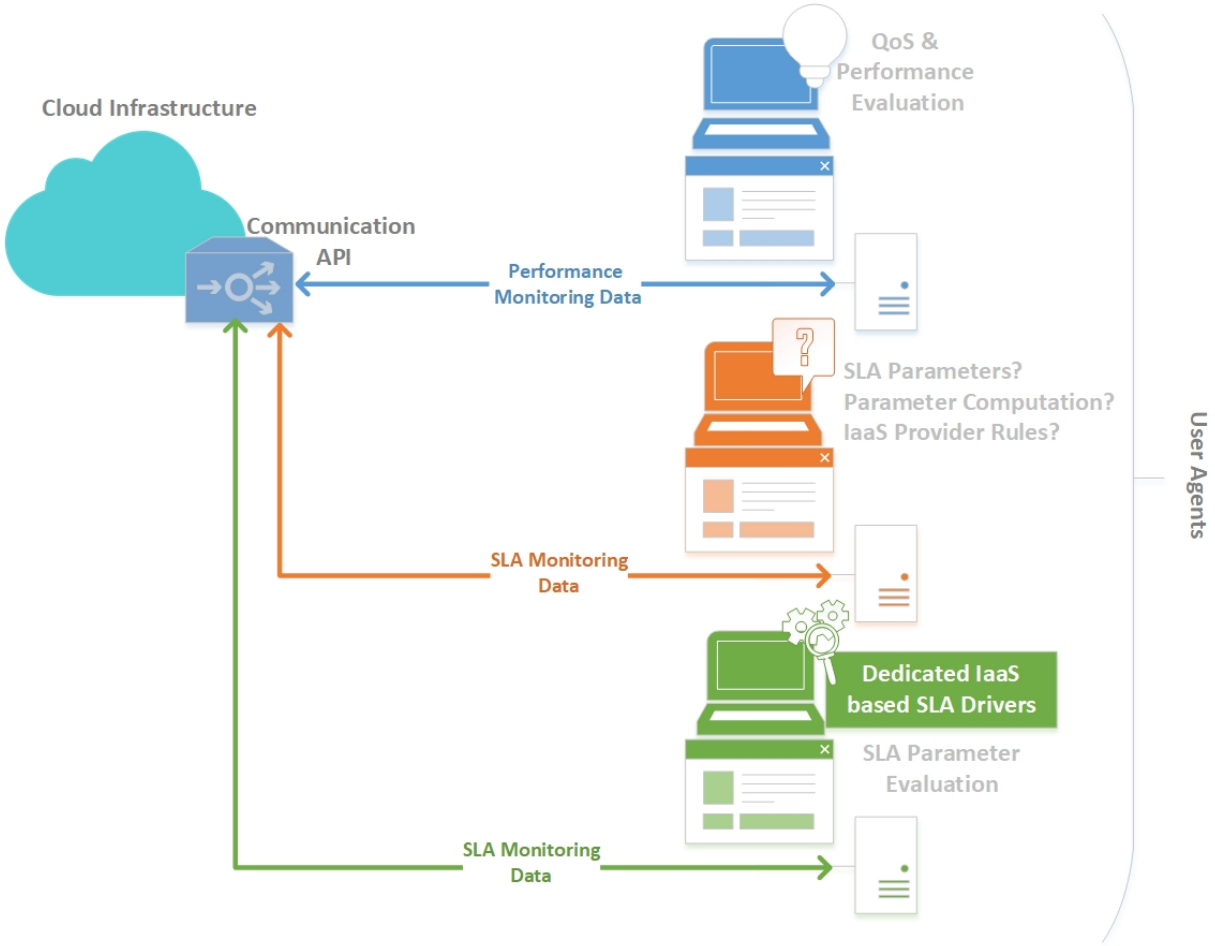
Αυτοαξιολόγηση Συμφωνιών Επιπέδου Υπηρεσίας Υπολογιστικού Νέφους μέσω Απομόνωσης Έξυπνων Συμβολαίων

Οι Συμφωνίες Επιπέδου Υπηρεσίας (SLAs) έχουν αποκτήσει κεντρικό ρόλο στη δημιουργία εμπιστοσύνης μεταξύ των παρόχων Cloud και του πελατολογίου τους. Στις ιδιωτικές λύσεις Cloud, οι πάροχοι αξιολογούν εσωτερικά τα SLA και κοινοποιούν τα αποτελέσματα των μετρήσεων στους πελάτες. Αντίθετα, πολλοί δημόσιοι πάροχοι Cloud, συμπεριλαμβανομένων μεγάλων εταιρειών όπως η Amazon, δεν παρακολουθούν ενεργά τις προεπιλεγμένες παραμέτρους SLA, όπως η διαθεσιμότητα, κάτι που είναι λογικό δεδομένης της τεράστιας βάσης χρηστών και της φήμης των IaaS παρόχων. Ωστόσο, η αποτυχία αντιμετώπισης παραβιάσεων συμφωνιών μπορεί να οδηγήσει σε σημαντικές οικονομικές απώλειες [72].

Πληθώρα εργαλείων λογισμικού είναι διαθέσιμα για την παρακολούθηση, την αξιολόγηση και την αντιμετώπιση ζητημάτων απόδοσης και Ποιότητας Υπηρεσίας (QoS) που σχετίζονται με πόρους cloud. Συγκεκριμένα, δημόσιοι πάροχοι όπως η Amazon, η Microsoft και η Google έχουν αναπτύξει τα δικά τους εργαλεία και περιβάλλοντα [73-75] για την

αξιολόγηση και την ενορχήστρωση των δικών τους, αλλά ακόμη και άλλων υπηρεσιών Cloud. Η διαδικασία παρακολούθησης SLA περιλαμβάνει την αντιμετώπιση συγκεκριμένων ερωτήσεων, όπως απεικονίζεται στο Σχήμα 41.

1. Ποιες παράμετροι συμφωνίας περιέχονται στο SLA;
2. Πώς υπολογίζονται αυτές οι παράμετροι;
3. Είναι ο υπολογισμός των παραμέτρων σύμφωνος με τον ορισμό του IaaS;



Σχήμα 41: Τυπική διαδικασία παρακολούθησης SLA.

Για παράδειγμα, όσον αφορά τη διαθεσιμότητα υπηρεσίας, μια παράμετρος SLA ορίζεται εύκολα, αλλά ο καθορισμός της τιμής παραμέτρου που δηλώνει πότε μια υπηρεσία Cloud είναι ή δεν είναι διαθέσιμη και πώς υπολογίζεται αυτή η τιμή είναι κρίσιμα σημεία που καθορίζουν την εγκυρότητα μιας διαδικασίας παρακολούθησης SLA. Επιπλέον, παράγοντες όπως ο ρυθμός δειγματοληψίας, η περίοδος αξιολόγησης και ο τύπος που χρησιμοποιείται για τον υπολογισμό των παραμέτρων παίζουν ζωτικό ρόλο στον υπολογισμό των μετρικών.

Η παρούσα υλοποίηση εισάγει μια νέα προσέγγιση για την αντιμετώπιση τέτοιων αβεβαιοτήτων στην αξιολόγηση SLA. Με βάση την έννοια της αυτοαξιολόγησης SLA, το παρόν σύστημα δημιουργεί ένα ασφαλές και απομονωμένο υπολογιστικό περιβάλλον μέσα σε ένα αμετάβλητο αποκεντρωμένο οικοσύστημα. Προκειμένου να διασφαλιστούν διαφανείς και ιδιωτικές υπολογιστικές ροές εντός του περιβάλλοντος αλυσίδας-κορμού με επίτρεψη, ο προτεινόμενος μηχανισμός συναίνεσης SLA ενσωματώνει τις δυνατότητες TEE [76]. Με αυτόν τον τρόπο, ο IaaS εμπλέκει την πελατεία του σε ένα ασφαλές σύστημα που διασφαλίζει διαφάνεια των λειτουργιών και ιδιωτικότητα των υπολογισμών. Η διαφάνεια προέρχεται κυρίως από τη συναίνεση των μερών SLA σχετικά με το αλγοριθμικό πρόγραμμα οδήγησης που υποβάλεται στην αλυσίδα (ορισμός παρακάτω) και είναι υπεύθυνο για την παρακολούθηση των αρχείων καταγραφής μετρικών του SLA, ενώ η ιδιωτικότητα υπολογισμών εδραιώνεται μέσω των ιδιοτήτων και των δυνατοτήτων του TEE.

Από την άλλη πλευρά, οι πελάτες επωφελούνται από μια ασφαλή πλατφόρμα όπου εφαρμόζεται μια αξιόπιστη διαδικασία συναίνεσης SLA. Ειδικότερα, οι πελάτες εμπιστεύονται ότι οι παρεχόμενοι υπολογισμοί SLA ακολουθούν ένα συμφωνημένο σχήμα υπολογισμού που είναι κοινά αναγνωρισμένο με τον πάροχο υποδομής πριν από την υπογραφή της συμφωνίας.

Η όλη διαδικασία της αξιόπιστης παρακολούθησης SLA λαμβάνει χώρα μέσα σε ένα εξουσιοδοτημένο δίκτυο αλυσίδας-κορμού το οποίο χρησιμοποιεί χαρακτηριστικά Κατανεμημένης Τεχνολογίας Ledger (DLT) μαζί με TEE εντός της αλυσίδας. Συγκεκριμένα, η λύση βασίζεται στο λογισμικό κατανεμημένης λογιστικής Hyperledger Fabric [77], το οποίο ενσωματώνει δυνατότητες TEE εντός αλυσίδας μέσω ενός αποκλειστικού συνδετικού προγράμματος, δηλαδή του Fabric Private Chaincode (FPC) [78]. Το τελευταίο επεκτείνει το πλαίσιο εντός της αλυσίδας, επιτρέποντας την ανάπτυξη έξυπνων συμβολαίων που εκτελούνται σε προστατευμένα απομονωμένα περιβάλλοντα.

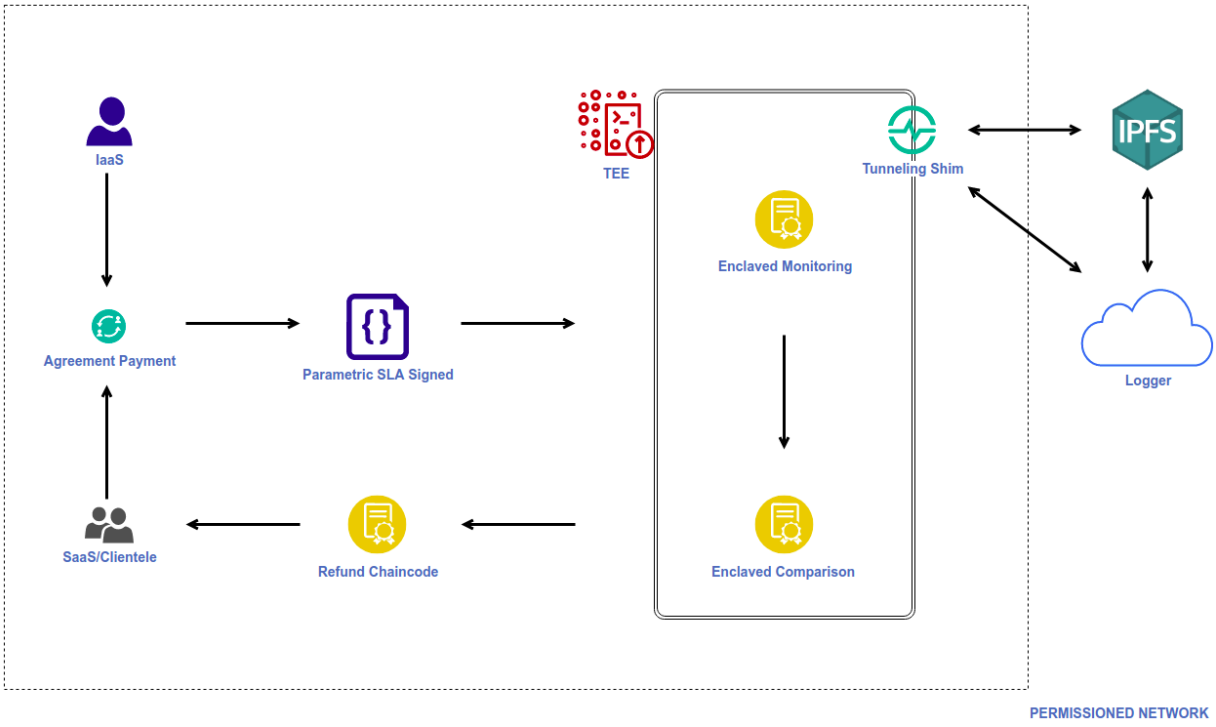
Επιπλέον, το Σχήμα 42 παρέχει μια ολοκληρωμένη επισκόπηση της αρχιτεκτονικής του οικοσυστήματος η οποία αναλύεται αργότερα, απεικονίζοντας τη διαδικασία συναίνεσης SLA με έμφαση στη λειτουργική διαφάνεια και την ιδιωτικότητα των υπολογισμών. Τόσο οι πάροχοι IaaS όσο και η πελάτες τους πλοηγούνται στην τυποποιημένη ροή εργασίας του οικοσυστήματος, η οποία περιλαμβάνει κυρίως το σύστημα εντός της αλυσίδας με σαφείς αλληλεπιδράσεις εκτός αλυσίδας.

Για την σύναψη μιας συμφωνίας εντός της αλυσίδας, γίνεται χρήση ενός

παραμετροποιήσιμου αρχείου, Parametric SLA. Για να λειτουργήσει σωστά, πρέπει να περιλαμβάνονται όλες οι απαραίτητες πληροφορίες από το έγγραφο SLA όπως ορίζεται στη συμφωνία με τον πάροχο IaaS. Αυτές οι πληροφορίες θα πρέπει να ακολουθούν μια τυποποιημένη μορφή σχήματος δεδομένων, ενώ αυτή η περίπτωση χρήσης συμμορφώνεται με το πρότυπο ISO 19086-2 SLA [79].

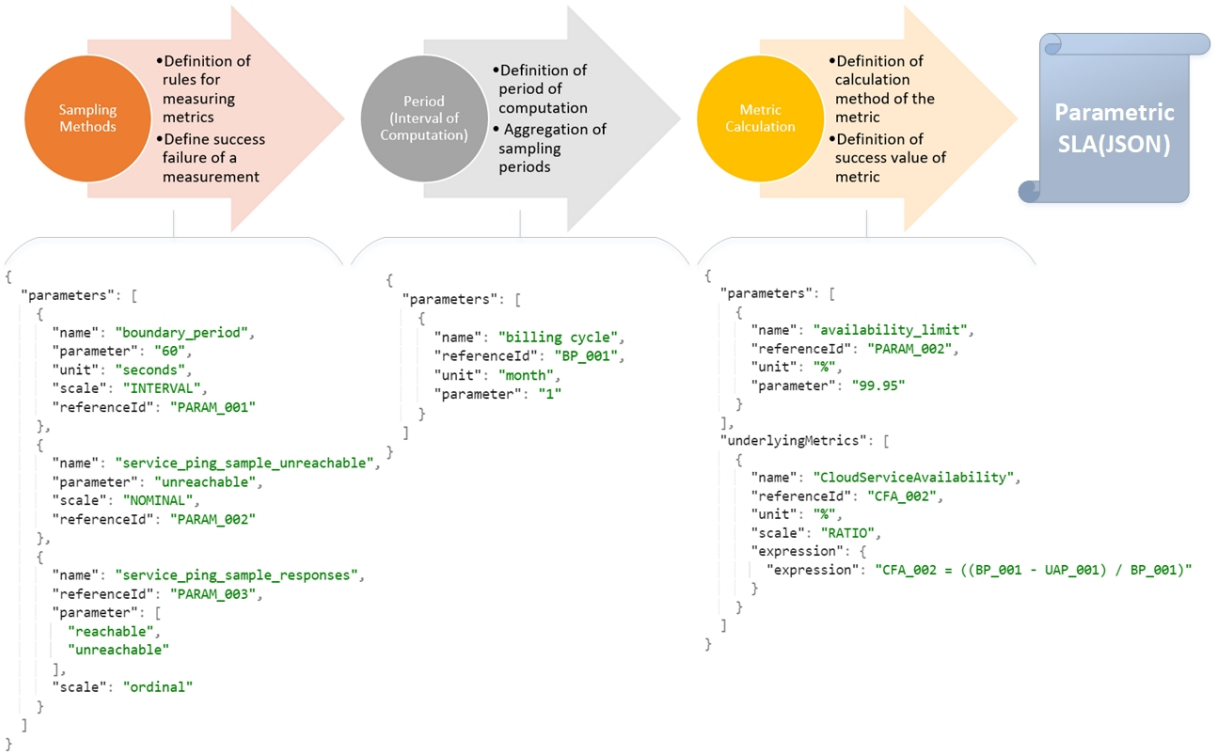
- Μετρικές: Αυτή η κλάση ενσωματώνει όλους τους στόχους που σχετίζονται με τις εγγυήσεις SLA. Για παράδειγμα, η διαθεσιμότητα είναι μια δημοφιλής μέτρηση που χρησιμοποιείται σε SLA. Επιπλέον, αυτή η κλάση περιλαμβάνει βασικές πληροφορίες που σχετίζονται με τις μετρήσεις και στοχεύουν κυρίως στη διευκόλυνση της παρακολούθησης και της μέτρησης μιας δεδομένων συμφωνιών.
- Παράμετροι: Αυτή η κλάση περιγράφει κάθε μεμονωμένη μέτρηση, προσφέροντας αναλυτικές λεπτομέρειες σχετικά με τις αντίστοιχες παραμέτρους της μέτρησης. Επιπλέον, περιλαμβάνει τους τύπους μεταβλητών που εκφράζουν μια μέτρηση και τους τρόπους μέτρησης αυτών.
- Κανόνες: Στις συμφωνίες SLA, υπάρχουν συγκεκριμένοι κανόνες που διέπουν όχι μόνο τις καθορισμένες εγγυήσεις αλλά και τους κανόνες που υπαγορεύουν την διαδικασία μέτρησης. Τέτοιοι κανόνες καθορίζουν πώς πρέπει να ερμηνεύονται οι μετρήσεις. Ένα τυπικό σενάριο κανόνα περιλαμβάνει τον καθορισμό του τι σημαίνει αποτυχία ή επιτυχία για μια συγκεκριμένη μέτρηση. Για παράδειγμα, όσον αφορά τη διαθεσιμότητα,

το Amazon Web Services (AWS) SLA [80] θεωρεί ότι μια υπηρεσία δεν είναι διαθέσιμη όταν δεν γίνεται δυνατή η πρόσβαση σε αυτή σε δύο (2) ζώνες διαθεσιμότητας.



Σχήμα 42: Αρχιτεκτονική συναίνεσης συμφωνιών SLA αλυσίδας-κορμού.

Το επίπεδο των μεθόδων δειγματοληψίας (Sampling Methods), όπως απεικονίζεται στο Σχήμα 43, αναλαμβάνει την ευθύνη για το σχεδιασμό μεθόδων που συλλέγουν και αξιολογούν την εγκυρότητα των δεδομένων του δείγματος που είναι ζωτικής σημασίας για τον υπολογισμό μετρικών. Οι περιορισμοί που προκύπτουν από τέτοιους κανόνες εκδηλώνονται με υπαγορεύουν εάν ένα συγκεκριμένο δείγμα διατηρείται για μετρικούς υπολογισμούς ή απορρίπτεται λόγω μη συμμόρφωσης με περιορισμούς μέτρησης (Boolean μορφή).



Σχήμα 43: Διαμόρφωση σε επίπεδα αλγοριθμικού προγράμματος οδήγησης.

Το επίπεδο διαστήματος υπολογισμού (Interval of Computation) διέπει τη συχνότητα με την οποία γίνεται δειγματοληψία δεδομένων για μετρικούς υπολογισμούς. Καθορίζει επίσης τα διαστήματα στα οποία υπολογίζονται και αξιολογούνται οι μετρήσεις SLA. Μια σύμβαση SLA συνήθως περιλαμβάνει λεπτομέρειες σχετικά με τον κύκλο χρέωσης και, κατά συνέπεια, τον κύκλο αξιολόγησης SLA. Υπάρχουν υπηρεσίες που υπολογίζουν τις παραμέτρους SLA τους σε μηνιαία βάση ή άλλες, όπως ανά διετία.

Το επίπεδο υπολογισμού μετρήσεων (Metric Calculation) στοχεύει στον πραγματικό υπολογισμό των μετρήσεων μέσα σε ένα δεδομένο χρονικό

διάστημα. Καθορισμένες συναρτήσεις, οι οποίες λαμβάνουν υπόψη τους ορισμούς μετρήσεων και τους σχετικούς κανόνες, επεξεργάζονται τα δεδομένα του δείγματος και δημιουργούν τις αριθμητικές τιμές για τις μετρήσεις SLA.

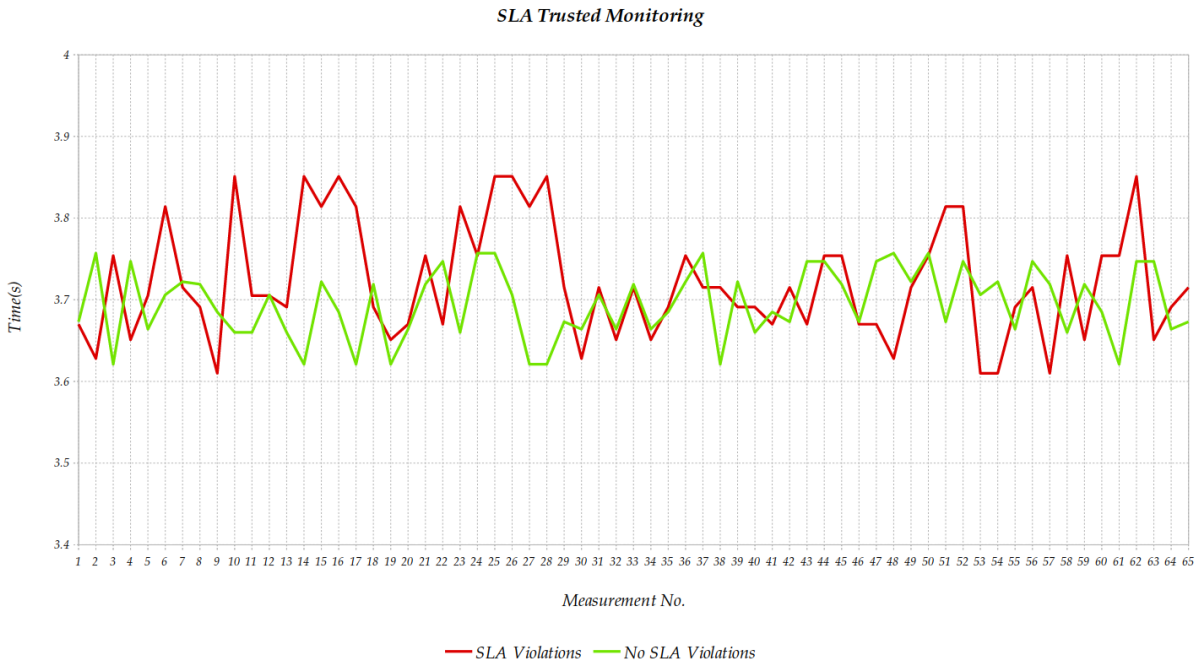
Για την σύναψη συμφωνίας SLA, οι εμπλεκόμενοι συμπληρώνουν τη παραμετροποιημένη συμφωνία και υπογράφουν σε μία συναλλαγή (Agreement Payment, Σχήμα 42) τη συμμετοχή τους στο SLA. Με την ανακοίνωση του υπογεγραμμένου SLA στο σύστημα, το TEE της αλυσίδας ξεκινά τη διαδικασία αξιόπιστης παρακολούθησης για τη νέα συμφωνία. Η λειτουργία περίκλειστης παρακολούθησης (Enclaved Monitoring) με τη σειρά της ενσωματώνει τη νέα συμφωνία στη λίστα της ανακτώντας τα πιο πρόσφατα αρχεία καταγραφής SLA και υποβάλλοντάς τα σε επεξεργασία εντός του TEE. Είναι σημαντικό να αναφέρουμε ότι το FPC διασφαλίζει ισχυρή ιδιωτικότητα για τις λειτουργίες που εκτελούνται από φιλοξενούμενα στοιχεία, ονομαστικά, οι λειτουργίες έξυπνων συμβολαίων περίκλειστης παρακολούθησης και περίκλειστης σύγκρισης (Enclaved Comparison). Συγκεκριμένα, το FPC εκμεταλλεύεται τις εγγενείς δυνατότητες των TEE απομονώνοντας μαθηματικούς και λογικούς υπολογισμούς έξυπνων συμβολαίων σε επίπεδο υλικού. Έτσι, οι δραστηριότητες που λαμβάνουν χώρα εντός του FPC απομονώνονται και προστατεύονται από άλλες οντότητες που συμμετέχουν στο δίκτυο και έχουν πρόσβαση στην αλυσίδα.

Η λειτουργία περίκλειστης σύγκρισης αποτελείται κυρίως από λειτουργίες έξυπνων συμβολαίων, οι οποίες αναγνωρίζουν τη συμφωνία που υπογράφηκε πρόσφατα και ανακτούν τα πιο πρόσφατα αντίστοιχα αρχεία καταγραφής

συμφωνιών από το δίκτυο IPFS μέσω της βοήθειας του Tunneling Shim που ενσωματώνει τέτοιου είδους αλληλεπιδράσεις στον κώδικά του. Ολόκληρη η ροή εργασίας εκτελείται στο πλαίσιο ενός περίκλειστου έξυπνου συμβολαίου που κληρονομεί τις προαναφερθείσες δυνατότητες ιδιωτικότητας.

Επιπλέον, σε όλη τη διάρκεια του κύκλου ζωής της ροής εργασίας, η λειτουργική μονάδα Logger μοιράζεται με το δίκτυο IPFS νέα αρχεία καταγραφής που σχετίζονται με τη συμφωνία. Τελικά, η επιστρεφόμενη διεύθυνση περιεγχομένου IPFS χρησιμοποιείται από το Tunneling Shim για την ανάκτηση αρχείων καταγραφής συμφωνιών εντός της αλυσίδας-κορμού. Σε περίπτωση παραβίασης SLA, η λειτουργία περίκλειστης σύγκρισης ενεργοποιεί την εκτέλεση του έξυπνου συμβολαίου αποζημίωσης (Refund Chaincode, Σχήμα 42). Όταν συμβαίνει παραβίαση SLA, η πελατεία του παρόχου λαμβάνει μια εντολή επιστροφής χρημάτων ως αποζημίωση για την παραβίαση της συμφωνίας, ενώ ο IaaS χρεώνεται ίδιο ποσό για την παράβαση αντίστοιχα. Το έξυπνο συμβόλαιο αποζημίωσης χρησιμοποιείται ως το τελευταίο στοιχείο του κύκλου ζωής της παρούσας λύσης συναίνεσης SLA κατά τη ροή εργασιών της διαδικασίας παραβίασης.

Σε γενικές γραμμές, ο χρόνος που απαιτείται για την επίλυση και την υποβολή συναλλαγών ιδιωτικού περίκλειστων έξυπνων συμβολαίων ποικίλλει ανάλογα με την ύπαρξη ή όχι παραβίαση. Όπως φαίνεται στα πειραματικά αποτελέσματα (Σχήμα 44), και στα δύο σενάρια η απόδοση χρονισμού της λύσης εμπίπτει σε ένα συγκεκριμένο εύρος, ενώ παρατηρείται λίγο μεγαλύτερο χρονικό εύρος στην περίπτωση που εντοπιστεί παραβίαση.



Σχήμα 44: Μετατόπιση της χρονικής απόδοσης παραβάσεων SLA.

Ειδικότερα, όταν δεν υπάρχει παραβίαση, το σύστημα βγάζει αποτελέσματα πιο γρήγορα από ό,τι όταν υπάρχει. Αξίζει να σημειωθεί ότι κατά τη διάρκεια παραβίασης απαιτούνται πρόσθετοι υπολογισμοί ιδιωτικών περίκλειστων συμβολαίων οδηγώντας σε αυξημένο χρόνο εκτέλεσης. Όσον αφορά την κλιμάκωση, η ροή εργασιών του συστήματος κλιμακώνεται και για τα δύο σενάρια (παραβίασης ή μη, Εικόνα 44) καθώς κληρονομεί τα χαρακτηριστικά κλιμάκωσης του υποκείμενου δικτύου Hyperledger Fabric [87]. Η ερευνητική εργασία οδήγησε στη διατύπωση ενός Hyperledger White Paper που περιγράφει τη δυνατότητα εφαρμογής του συστήματος από την άποψη της αυτοαξιολόγησης SLA στον κλάδο των τηλεπικοινωνιών [89].

Συμπεράσματα και Μελλοντικές Κατευθύνσεις

Όπως έχει ήδη απεικονιστεί στο Σχήμα 23, η συμβολή και καινοτομία της διδακτορικής διατριβής αποτελεί την εξαγόμενη στοίβα ιδιωτικότητας αλυσιδών-κορμού που προβλέπει και προσδίδει την κατάλληλη χρηστικότητα και εφαρμοσιμότητα της ιδιωτικότητας στην τεχνολογία. Η εξέταση και η κατανόηση περαιτέρω περιπτώσεων χρήσης θα ενεργοποιούσε περισσότερες λεπτομέρειες σχετικά με τη στοίβα, ωστόσο, οι αρχιτεκτονικές που παρουσιάζονται καλύπτουν ήδη σημαντικές προκλήσεις κεντρικοποιημένων συστημάτων και ιδιωτικότητας αλυσιδών-κορμού, προσφέροντας τα ακόλουθα σημαντικά οφέλη σε ιδιοκτήτες εφαρμογών και διαχειριστές οικοσυστημάτων που κατασκευάζουν αλυσίδες ή αποκεντρωμένες εφαρμογές στην υποδομή του Διαδικτύου επόμενης γενιάς (Web3.0):

- Ασφάλεια αποκεντρωμένου δικτύου.
- Δραστηριότητα δικτύου αλυσίδας-κορμού για επιχειρήσεις.
- Προστασία ευαίσθητων δεδομένων με εκτέλεση ιδιωτικών λειτουργιών και μυστικές συναλλαγών.
- Ασφαλείς υπολογισμούς δεδομένων και έγκλειστους υπολογισμούς με απομονωμένα έξυπνα συμβόλαια.

Σχετικά με τις επιμέρους υλοποιήσεις στα πλαίσια της διατριβής, φαίνονται τα ακόλουθα συμπεράσματα και μελλοντικές επεκτάσεις. Αν και οι

αλυσίδες-κορμού προορίζονται κυρίως για κατανεμημένη αποθήκευση και κοινή χρήση δεδομένων, η εγγενής αμεταβλητότητα και διαφάνειά τους μπορεί αρχικά να τα καταστήσει ακατάλληλα για δεδομένα ευαίσθητα στην ιδιωτικότητα. Τέτοια ευαίσθητα δεδομένα ενδέχεται να αποκαλύπτουν φυσικές ταυτότητες, συνήθειες καταναλωτών ή λεπτομέρειες που σχετίζονται με το απόρρητο, ακόμη και να αποκαλύπτουν αποδείξεις τοποθεσίας. Οι μελλοντικές συναλλαγές μέσω αλυσιδών-κορμού θα βασίζονται όλο και περισσότερο σε απλές, αποτελεσματικές και ισχυρές διαδικασίες KYC. Η αρχιτεκτονική που παρουσιάστηκε απέδειξε πόσο εύκολα διαχειριζόμενα και αρθρωτά βιομηχανικά περιβάλλοντα μπορούν να δημιουργηθούν πάνω από αλυσίδες-κορμού όπως το Quorum, εξοπλισμένες με έξυπνα συμβόλαια που προγραμματίζονται σε Solidity. Η ενσωμάτωση που παρουσιάζεται ανοίγει το δρόμο για την εφαρμογή διαδικασιών KYC κατάλληλων για ένα ευρύ φάσμα αποκεντρωμένων εφαρμογών. Επιπλέον, οι εξελισσόμενες ρυθμιστικές απαιτήσεις οδηγούν την προσαρμοστικότητα συστημάτων KYC σε νέους νομικούς κανόνες. Κατά συνέπεια, η έρευνα επεκτείνεται γύρω από τη μελέτη έξυπνων συμβολαίων με σκοπό το χειρισμό διεπιστημονικών διαδικασιών και με στόχο μια ολοκληρωμένη λύση KYC.

Στη μουσική βιομηχανία, όπου μια ποικιλία ρόλων και οντοτήτων πρέπει να συνεργαστεί για τον εντοπισμό και τη διαχείριση των δικαιωμάτων μουσικών περιουσιακών στοιχείων και την αντιμετώπιση συγκρούσεων, οι αλυσίδες-κορμού αναδύεται ως μια βιώσιμη λύση με τις κατάλληλες ιδιότητες αποκέντρωσης και ιδιωτικοποίησης. Οι αλυσίδες προσφέρουν ένα αμετάβλητο

περιβάλλον εγγραφών εξαλείφοντας την ανάγκη για μεσάζοντες. Η προτεινόμενη εφαρμογή συγκεντρώνει διάφορους επιχειρηματικούς τομείς εντός οργανισμών της μουσικής βιομηχανίας και μη κερδοσκοπικών ενώσεων αλυσιδών-κορμού. Αξιοποιώντας βασικές αρχές αλυσιδών-κορμού όπως η διαφάνεια, η εμπιστοσύνη, η ιχνηλασιμότητα και η αποκέντρωση, η παρούσα λύση προσφέρει μια αποτελεσματική προσέγγιση για την αντιμετώπιση κοινών ζητημάτων πνευματικών δικαιωμάτων που αντιμετωπίζουν οι CMO στη μουσική βιομηχανία. Επίσης, η χρησιμοποιούμενη αλυσίδα Quorum Alastria προσφέρει ισχυρή ασφάλεια και προστατευμένη ιδιωτικότητα στην υλοποίηση λόγω εγγενών ιδιοτήτων αρχιτεκτονικής. Τέλος, σχετικά με την αναγνώριση μουσικών στοιχείων θα μπορούσαν να διερευνηθούν μελλοντικά αντίστοιχοι αλγόριθμοι με στόχο τη δημιουργία μιας γενικής λύσης που συμβάλει στην παρακολούθηση χρήσης συγκεκριμένων μουσικών στοιχείων σε διάφορα κανάλια διανομής ή γεωγραφικές περιοχές.

Όσον αφορά την υλοποίηση σχετικά με τις συμφωνίες επιπέδου υπηρεσίας, η βασική ιδέα περιστρέφεται γύρω από το λογισμικό κατανεμημένης λογιστικής το οποίο φιλοξενεί TEEs με απομονωτικές και υπολογιστικές ιδιότητες. Τα χαρακτηριστικά που ενισχύουν την ιδιωτικότητα αυτής της συμφωνίας αποτελούν πλεονεκτήματα σε όλη τη διάρκεια της διαδικασίας αξιολόγησης SLA, καθώς κάθε συμφωνία SLA αξιολογείται διεξοδικά από τη σκοπιά τόσο του παρόχου IaaS όσο και των πελατών του. Το συνταχθέν αποτέλεσμα καταλήγει σε ένα αξιόπιστο σύστημα που ωφελεί τόσο τον πάροχο IaaS όσο και την πελατεία του όσον αφορά την ακρίβεια και τους

δίκαιους υπολογισμούς και τις υπολογιστικές διαδικασίες. Σχετικά με τα πειραματικά αποτελέσματα που παρουσιάζονται, η προτεινόμενη προσέγγιση είναι ικανή να κλιμακωθεί για διάφορα σενάρια και κυρίως τα προσανατολισμένα στις επιχειρήσεις, προσφέροντας κερδοφορία και ενδιαφέρον για προσαρμογή με τα εγγενή χαρακτηριστικά κλιμάκωσης της υποκείμενης αλυσίδας. Επιπλέον, όσον αφορά τις συζητήσεις και την συμμετοχή στην Κοινότητα Ανοιχτού Κώδικα, υπάρχει έντονο ενδιαφέρον για την επέκταση του παρουσιαζόμενου συστήματος ως προς τα τεχνολογικά εργαλεία που χρησιμοποιούνται. Ειδικότερα, έχει προταθεί η εισαγωγή αποδείξεων μηδενικής γνώσης προσθέτοντας ένα επιπλέον επίπεδο ιδιωτικότητας και επικύρωσης δεδομένων σχετικά με τις λεπτομέρειες που περιέχονται στις ροές συναλλαγών.

Πίνακας 5: Γλωσσάριο Αντιστοίχισης Αγγλικών-Ελληνικών Όρων

3rd iteration of World Wide Web	3η έκδοση του Διαδικτύου
Algorithmic Driver	Αλγοριθμικό Πρόγραμμα Οδήγησης
Amazon Web Services	Υπηρεσίες Ιστού της Amazon
Blockchain	Αλυσίδα-κορμού
Content identifier	Αναγνωριστικό Περιεγχομένου
Collective Management Organization	Οργανισμός Συλλογικής Διαχείρισης
Central Processing Unit	Κεντρική Μονάδα Επεξεργασίας
Decentralized Application	Αποκεντρωμένη Εφαρμογή
Distributed Ledger Technology	Τεχνολογία Κατανεμημένης Λογιστικής
Digital Rights Management	Διαχείριση Ψηφιακών Δικαιωμάτων

Enclaved	Περίκλειστος
Endpoint	Τελικό σημείο
Fabric Private Chaincode	Ιδιωτικό Έξυπνο Συμβόλαιο της Fabric
Infrastructure as a Service	Υποδομή ως Υπηρεσία
Identity	Ταυτότητα
Input/output	Είσοδος-Έξοδος
Internet of Things	Διαδίκτυο των Πραγμάτων
InterPlanetary File System	Διαπλανητικό Σύστημα Αρχείων
Istanbul Byzantine Fault Tolerance	Istanbul Ανοχή Βυζαντινών Σφαλμάτων
International Standard Recording Code	Διεθνές Σύστημα Αναγνώρισης Ηχογραφημάτων
International Standard Musical Work Code	Διεθνές Σύστημα Αναγνώρισης Μουσικής Εργασίας
Key Performance Indicator	Βασικός Δείκτης Απόδοσης
Know Your Customer	Γνωρίστε τον Πελάτη σας
Lifecycle	Κύκλος ζωής
Monitoring	Παρακολούθηση
Open Source Community	Κοινότητα Ανοιχτού Κώδικα
Practical Byzantine Fault Tolerance	Πρακτική Ανοχή Βυζαντινών Σφαλμάτων
Privacy	Ιδιωτικότητα
Proof of Stake	Απόδειξη Μεριδίου
Proof of Work	Απόδειξη Εργασίας
Random Access Memory	Μνήμη Τυχαίας Προσπέλασης
Quality of Service	Ποιότητα Υπηρεσίας
Service Level Agreement	Συμφωνία Επιπέδου Υπηρεσίας
Smart Contract	Έξυπνο Συμβόλαιο
Transaction	Συναλλαγή
Trusted Execution Environment	Περιβάλλον Αξιόπιστης Εκτέλεσης
User Interface	Διεπαφή Χρήστη

Bibliography

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”.

[2] “Litecoin - Open Source P2P Digital Currency.” Accessed September 28, 2023. https://litecoin.org/.

[3] N. v. Saberhagen, “CryptoNote v 2.0”.

[4] “Peercoin — The Pioneer of Proof-of-Stake.” Accessed September 28, 2023. https://www.peercoin.net/read/papers/peercoin-paper.pdf.

[5] Chase, B.; MacBrough, E. Analysis of the XRP Ledger Consensus Protocol. *arXiv* February 20, **2018**. https://doi.org/10.48550/arXiv.1802.07242.

[6] D. G. Wood, “Ethereum: A Secure Decentralised Generalised Transaction Ledger”.

[7] Yakovenko, A. Solana: A New Architecture for a High Performance Blockchain.

[8] Wood, D. G. Polkadot: Vision For A Heterogeneous Multi-Chain Framework.

[9] Androulaki, E.; Barger, A.; Bortnikov, V.; Cachin, C.; Christidis, K.; De Caro, A.; Enyeart, D.; Ferris, C.; Laventman, G.; Manevich, Y.; Muralidharan, S.; Murthy, C.; Nguyen, B.; Sethi, M.; Singh, G.; Smith, K.; Sorniotti, A.; Stathakopoulou, C.; Vukolić, M.; Cocco, S. W.; Yellick, J. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. *In Proceedings of the Thirteenth EuroSys Conference*; **2018**; pp 1–15. https://doi.org/10.1145/3190508.3190538.

[10] R3. “Corda Technical Whitepaper,” December 16, 2019. https://r3.com/blog/corda-technical-whitepaper/.

[11] GDPR.eu. “General Data Protection Regulation (GDPR) Compliance Guide-

lines.” Accessed September 29, 2023. https://gdpr.eu/.

[12] Kapsoulis, Nikolaos, Alexandros Psychas, Georgios Palaiokrassas, Achilleas Marinakis, Antonios Litke, and Theodora Varvarigou. “Know Your Customer (KYC) Implementation with Smart Contracts on a Privacy-Oriented Decentralized Architecture.” *Future Internet* 12, no. 2 (**February 2020**): 41. https://doi.org/10.3390/fi12020041.

[13] Kapsoulis, Nikolaos, Alexandros Psychas, Georgios Palaiokrassas, Achilleas Marinakis, Antonios Litke, Theodora Varvarigou, Charalampos Bouchlis, Amaryllis Raouzaiou, Gonçal Calvo, and Jordi Escudero Subirana. “Consortium Blockchain Smart Contracts for Musical Rights Governance in a Collective Management Organizations (CMOs) Use Case.” *Future Internet* 12, no. 8 (**August 2020**): 134. https://doi.org/10.3390/fi12080134.

[14] Kapsoulis, Nikolaos, Alexandros Psychas, Antonios Litke, and Theodora Varvarigou. “Reinforcing SLA Consensus on Blockchain.” *Computers* 10, no. 12 (**December 2021**): 159. https://doi.org/10.3390/computers10120159.

[15] “Hyperledger - The Open Global Ecosystem for Enterprise Blockchain.” Accessed September 29, 2023. https://www.hyperledger.org.

[16] Tschorsch, Florian, and Björn Scheuermann. “Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies.” *IEEE Communications Surveys & Tutorials* 18, no. 3 (**2016**): 2084–2123. https://doi.org/10.1109/COMST.2016.2535718.

[17] Tian, F. An Agri-Food Supply Chain Traceability System for China Based on RFID & Blockchain Technology. In 2016 *13th International Conference on Service Systems and Service Management* (ICSSSM); **2016**; pp 1–6. https://doi.org/10.1109/ICSSSM.2016.7538424.

[18] Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. MedRec: Using Blockchain for Medical Data Access and Permission Management. In 2016 *2nd International Conference on Open and Big Data (OBD)*; **2016**; pp 25–30. https://doi.org/10.1109/OBD.2016.11.

[19] Wilson, Duane, and Giuseppe Ateniese. "From Pretty Good to Great: Enhancing PGP Using Bitcoin and the Blockchain." In Network and System Security, edited by Meikang Qiu, Shouhuai Xu, Moti Yung, and Haibo Zhang, 368–75. Lecture Notes in Computer Science. *Cham: Springer International Publishing*, **2015**. https://doi.org/10.1007/978-3-319-25645-0_25.

[20] Hou, Heng. "The Application of Blockchain Technology in E-Government in China." In 2017 *26th International Conference on Computer Communication and Networks (ICCCN)*, 1–4, **2017**. https://doi.org/10.1109/ICCCN.2017.8038519.

[21] Alketbi, Ahmed, Qassim Nasir, and Manar Abu Talib. "Blockchain for Government Services — Use Cases, Security Benefits and Challenges." In 2018 *15th Learning and Technology Conference (L&T)*, 112–19, **2018**. https://doi.org/10.1109/LT.2018.8368494.

[22] Noyen, K.; Volland, D.; Wörner, D.; Fleisch, E. When Money Learns to Fly: Towards Sensing as a Service Applications Using Bitcoin. *ArXiv* **2014**, ArXiv:1409.5841.

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

[24] Musso, S.; Perboli, G.; Rosano, M.; Manfredi, A. A Decentralized Marketplace for M2M Economy for Smart Cities. *In Proceedings of the 2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for*

Collaborative Enterprises (WETICE), Napoli, Italy, **12–14 June 2019**; pp. 27–30.

[25] Papadodimas, G.; Palaiokrasas, G.; Litke, A.; Varvarigou, T. Implementation of smart contracts for blockchain based IoT applications. *In Proceedings of the 2018 9th International Conference on the Network of the Future (NOF)*, Poznan, Poland, **19–21 November 2018**; pp. 60–67.

[26] Palaiokrassas, G.; Litke, A.; Fragkos, G.; Papaefthymiou, V.; Varvarigou, T. Deploying Blockchains for a New Paradigm of Media Experience. *In Proceedings of the International Conference on the Economics of Grids, Clouds, Systems, and Services*, Pisa, Italy, **18–20 September 2018**; pp. 234–242.

[27] Dunphy, P.; Petitcolas, F. A first look at identity management schemes on the blockchain. *IEEE Secur. Priv.* **2018**, 16, 20–29.

[28] Lim, S.Y.; Fotsing, P.T.; Almasri, A.; Musa, O.; Kiah, M.L.M.; Ang, T.F.; Ismail, R. Blockchain technology the identity management and authentication service disruptor: A survey. *Int. J. Adv. Sci. Eng. Inf. Tech.* **2018**, 8, 1735.

[29] Mikula, T.; Jacobsen, R. Identity and access management with blockchain in electronic healthcare records. *In Proceedings of the 2018 21st Euromicro Conference on Digital System Design (DSD)*, Prague, Czech Republic, **29 August 2018**; pp. 699–706.

[30] Widick, L.; Ranasinghe, I.; Dantu, R.; Jonnada, S. Blockchain Based Authentication and Authorization Framework for Remote Collaboration Systems. *In Proceedings of the 2019 IEEE 20th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)*, Washington, DC, USA, **10 June 2019**.

[31] Mudliar, K.; Parekh, H.; Bhavathankar, P. A comprehensive integration of na-

tional identity with blockchain technology. *In Proceedings of the 2018 International Conference on Communication information and Computing Technology (ICCICT)*, Mumbai, India, **2–3 February 2018**; pp. 1–6.

[32] Shbair, W.; Steichen, M.; François, J. Blockchain orchestration and experimentation framework: A case study of KYC. *In Proceedings of the First IEEE/IFIP International Workshop on Managing and Managed by Blockchain (Man2Block)* colocated with IEEE/IFIP NOMS 2018, Jeju Island, Korea, **23–25 August 2018**.

[33] Norvill, R.; Steichen, M.; Shbair, W.M.; State, R. Blockchain for the Simplification and Automation of KYC Result Sharing. *In Proceedings of the 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, Seoul, Korea, 18–21 **November 2019**; pp. 9–10.

[34] Zhang, X.; Yin, Y. Research on Digital Copyright Management System Based on Blockchain Technology. *In Proceedings of the 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, Chengdu, China, **15–17 March 2019**.

[35] Kwon, Jae. “Tendermint: Consensus without Mining,”.

[36] Bhaskaran, K.; Ilfrich, P.; Liffman, D.; Vecchiola, C.; Jayachandran, P.; Kumar, A.; Lim, F.; Nandakumar, K.; Qin, Z.; Ramakrishna, V.; et al. Double-blind consent-driven data sharing on blockchain. *In Proceedings of the 2018 IEEE International Conference on Cloud Engineering (IC2E)*, Orlando, FL, USA, **17–20 April 2018**; pp. 385–391.

[37] Vishwa, A.; Hussain, F.K. A Blockchain based approach for multimedia privacy protection and provenance. *In Proceedings of the 2018 IEEE Symposium Series on Computational Intelligence (SSCI)*, Bangalore, India, **18–21 Novem-**

ber 2018; pp. 1941–1945.

[38] “IPFS Powers the Distributed Web.” Accessed September 29, 2023. https://ipfs.tech/.

[39] Zhang, Z.; Zhao, L. A design of digital rights management mechanism based on blockchain technology. *In International Conference on Blockchain*; Springer: Cham, Germany, **2018**.

[40] Ding, Y.; Yang, L.; Shi, W.; Duan, X. The Digital Copyright Management System Based on Blockchain. *In Proceedings of the 2019 IEEE 2nd International Conference on Computer and Communication Engineering Technology (CCET)*, Beijing, China, **16–18 August 2019**; pp. 63–68.

[41] Xu, R.; Zhang, L.; Zhao, H.; Peng, Y. Design of Network Media’s Digital Rights Management Scheme Based on Blockchain Technology. *In Proceedings of the 13th International Symposium on Autonomous Decentralized System (ISADS)*, Bangkok, Thailand, **22–24 March 2017**; pp. 128–133.

[42] Ma, Z.; Jiang, M.; Gao, H.; Wang, Z. Blockchain for digital rights management. *Future Gener. Comput. Syst.* **2018**, 89, 746–764.

[43] Fujimura, S.; Watanabe, H.; Nakadaira, A.; Yamada, T.; Akutsu, A.; Kishigami, J.J. BRIGHT: A concept for a decentralized rights management system based on blockchain. *In Proceedings of the 5th International Conference on Consumer Electronics—Berlin (ICCE-Berlin)*, Berlin, Germany, **2–5 September 2015**; pp. 345–346.

[44] Savelyev, A. Copyright in the blockchain era: Promises and challenges. *Comput. Law Sec. Rev.* **2018**, 34, 550–561.

[45] O’Dair, V.; Beaven, Z. The networked record industry: How blockchain technology could transform the record industry. *Strategic Change* **2017**, 26, 471–

480.

[46] Zhao, S.; O'Mahony, D. Bmcprotector: A blockchain and smart contract based application for music copyright protection. *In Proceedings of the International Conference on Blockchain Technology and Application*, Xi'an, China, **10–12 December 2018**; pp. 1–5.

[47] Gomaa, Ahmed. "A DRM Solution for Online Content Using Blockchain - A Music Perspective." *SSRN* Scholarly Paper. Rochester, NY, **December 27, 2018**. https://doi.org/10.2139/ssrn.3351542.

[48] Chen, L.M.; Guan, S.P.; Du, R.R. Study on copyright protection path of music from the perspective of blockchain technology. *In Proceedings of the 6th International Conference on Management Science and Management Innovation (MSMI 2019)*, Changsha, China, **17–18 May 2019**.

[49] Ouyang, Y.; Zheng, X.; Lu, X.; Xiaowei, L.; Zhang, S. Copyright Protection Application Based on Blockchain Technology. *In Proceedings of the Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom)*, Xiamen, China, **16–18 December 2019**; pp. 1271–1274.

[50] Ito, K.; O'Dair, M. A Critical Examination of the Application of Blockchain Technology to Intellectual Property Management. *In Business Transformation Through Blockchain*; Palgrave Macmillan: Cham, Germany, **2019**; pp. 317–335.

[51] Nguyen, T.-V.; Lê, T.-V.; Dao, B.; Nguyen-An, K. Leveraging Blockchain in Monitoring SLA-Oriented Tourism Service Provisioning. *In Proceedings of the International Conference on Advanced Computing and Applications (ACOMP)*, Nha Trang, Vietnam, **26–28 November 2019**; pp. 42–50.

[52] Ranchal, R.; Choudhury, O. SLAM: A Framework for SLA Management in Multicloud ecosystem using Blockchain. *In Proceedings of the IEEE Cloud Summit*, Harrisburg, PA, USA, **21–22 October 2020**; pp. 33–38.

[53] Alowayed, Y.; Canini, M.; Marcos, P.; Chiesa, M.; Barcellos, M. Picking a Partner: A Fair Blockchain Based Scoring Protocol for Autonomous Systems. *Proc. Appl. Netw. Res. Workshop* **2018**, 33–39.

[54] Uriarte, R.B.; Zhou, H.; Kritikos, K.; Shi, Z.; Zhao, Z.; De Nicola, R. Distributed service-level agreement management with smart contracts and blockchain. *Concurr. Comput. Pract. Exper* **2021**, 33, e5800.

[55] Alzubaidi, A.; Mitra, K.; Patel, P.; Solaiman, E. A Blockchain-based Approach for Assessing Compliance with SLA-guaranteed IoT Services. *In Proceedings of the IEEE International Conference on Smart Internet of Things (SmartIoT)*, Beijing, China, **14–16 August 2020**; pp. 213–220.

[56] Alzubaidi, A.; Solaiman, E.; Patel, P.; Mitra, K. Blockchain-Based SLA Management in the Context of IoT. *IT Prof.* **2019**, 21, 33–40.

[57] D'Angelo, G.; Ferretti, S.; Marzolla, M. A Blockchain-based Flight Data Recorder for Cloud Accountability. *In Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, Munich, Germany, **15 June 2018**; pp. 93–98.

[58] Tan, W.; Zhu, H.; Tan, J.; Zhao, Y.; Xu, L.D.; Guo, K. A novel service level agreement model using blockchain and smart contract for cloud manufacturing in industry 4.0. *Enterp. Inf. Syst.* **2021**, 1–26.

[59] Consensys. "Consensys Quorum." Accessed September 24, 2023. https://consensys.net/quorum/.

[60] Alastria. "Alastria - Where Blockchain Happens." Accessed September 29,

2023. https://alastria.io/en/home/.

[61] ethereum.org. “Home.” Accessed September 28, 2023. https://ethereum.org.

[62] Solidity Programming Language. “Home.” Accessed September 28, 2023. https://soliditylang.org/.

[63] Inc, Synechron. “Quorum Maker V2.6.5.” Shell, September 14, 2023. https://github.com/synechron-finlabs/quorum-maker.

[64] “GRD’s Failure – Music Business Journal.” Accessed September 29, 2023. http://www.thembj.org/2015/08/grds-failure/.

[65] Rogers, J.; Sparviero, S. Same tune, different words: The creative destruction of the music industry. *Obs. (OBS*)* J. **2011**, 5, 1–30.

[66] Carretta, Silvia A, and Marianne Levin. “Blockchain Challenges To Copyright”.

[67] Saraf, C.; Siddharth, S. Blockchain platforms: A compendium. *In Proceedings of the IEEE International Conference on Innovative Research and Development (ICIRD)*, Bangkok, Thailand, **11–12 May 2018**.

[68] GitHub. “Alastria-Core-Technical-Platform.Md” Accessed September 16, 2023. https://github.com/alastria/alastria-platform-TO_BE_UPDATED/blob/master/en/Alastria-Core-Technical-Platform.md.

[69] Miguel Castro and Barbara Liskov. 1999. Practical Byzantine fault tolerance. *In Proceedings of the Third Symposium on Operating Systems Design and Implementation (OSDI ’99)*, USENIX Association, New Orleans, LA, USA, **22–25 February 1999**; pp. 173–186.

[70] “Web3.Js — Javascript Ethereum API.” Accessed September 30, 2023. https://web3js.org/.

[71] ethereum.org. “Recursive-Length Prefix (RLP) Serialization.” September 17,

2023. https://ethereum.org.

[72] Columbus, Louis. “Roundup Of Cloud Computing Forecasts And Market Estimates, **2016**.” *Forbes*. Accessed September 16, 2023. https://www.forbes.com/sites/louiscolumbus/2016/03/13/roundup-of-cloud-computing-forecasts-and-market-estimates-2016/.

[73] “Application and Infrastructure Monitoring – Amazon CloudWatch – Amazon Web Services.” Accessed September 16, 2023. https://aws.amazon.com/cloudwatch/.

[74] “Azure Monitor - Modern Observability Tools | Microsoft Azure.” Accessed September 16, 2023. https://azure.microsoft.com/en-us/products/monitor.

[75] “Cloud Monitoring | Google Cloud.” Accessed September 16, 2023. https://cloud.google.com/monitoring/.

[76] Sabt, M.; Achemlal, M.; Bouabdallah, A. Trusted Execution Environment: What It is, and What It is Not. *In Proceedings of the 2015 IEEE Trustcom/BigDataSE/ISPA*, Helsinki, Finland, **20–22 August 2015**; pp. 57–64.

[77] “Hyperledger Fabric.” Accessed September 16, 2023. https://www.hyperledger.org/projects/fabric.

[78] “Hyperledger Fabric Private Chaincode.” Go. **2018**. Reprint, *Hyperledger*, September 16, 2023. https://github.com/hyperledger/fabric-private-chaincode.

[79] “ISO/IEC 19086-2:2018.” ISO. Accessed September 16, 2023. https://www.iso.org/standard/67546.html.

[80] Amazon Web Services, Inc. “Amazon Compute Service Level Agreement.” Accessed September 16, 2023. https://aws.amazon.com/compute/sla/.

[81] SLALOM “SLA Specification and Reference Model”. Accessed September 16, 2023. https://ec.europa.eu/research/participants/documents/downloadPublic?

documentIds=080166e5aa6eccf3&appId=PPGMS

[82] Diego, O.; John, O. In search of an understandable consensus algorithm. *In Proceedings of the 2014 USENIX Conference on USENIX Annual Technical Conference (USENIX ATC'14)*, Philadelphia, PA, USA, **19–20 June 2014**; pp. 305–320.

[83] "Compute – Amazon EC2 Instance Types – AWS." Accessed September 16, 2023. https://aws.amazon.com/ec2/instance-types/.

[84] "Contractapi Package - Github.Com/Hyperledger/Fabric-Contract-Api-Go/Contractapi - Go Packages." Accessed September 16, 2023. https://pkg.go.dev/github.com/hyperledger/fabric-contract-api-go/contractapi.

[85] Fujisaki, E.; Okamoto, T.; Pointcheval, D.; Stern, J. RSA-OAEP Is Secure under the RSA Assumption. *Adv. Cryptol.* **2018**, 2139, 260–274.

[86] Brown, Daniel R L. "SEC 2: Recommended Elliptic Curve Domain Parameters,".

[87] Nguyen, M.; Loghin, D.; Dinh, T.T. Understanding the Scalability of Hyperledger Fabric. *arXiv* **2021**, arXiv:2107.09886.

[88] Dreyer, J.; Fischer, M.; Tönjes, R. Performance analysis of hyperledger fabric 2.0 blockchain platform. *In Proceedings of the Workshop on Cloud Continuum Services for Smart IoT Systems (CCIoT '20)*; Association for Computing Machinery: New York, NY, USA, **2020**; pp. 32–38.

[89] "[Hyperledger] Research." Accessed September 16, 2023. https://www.hyperledger.org/research.