A Survey on Blockchain-Based Telecommunication Services Marketplaces

Roman-Valentyn Tkachuk, Dragos Ilie, *Member, IEEE*, Kurt Tutschku, *Member, IEEE*, and Remi Robert

***Abstract*—Digital marketplaces were created recently to accelerate the delivery of applications and services to customers. Their appealing feature is to activate and dynamize the demand, supply, and development of digital goods, applications, or services. By being an intermediary between producer and consumer, the primary business model for a marketplace is to charge the producer with a commission on the amount paid by the consumer. However, most of the time, the commission is dictated by the marketplace facilitator itself and creates an imbalance in value distribution, where producer and consumer sides suffer monetarily. In order to eliminate the need for a centralized entity between the producer and consumer, a blockchain-based decentralized digital marketplace concept was introduced. It provides marketplace actors with the tools to perform business transactions in a trusted manner and without the need for an intermediary. In this work, we provide a survey on Telecommunication Services Marketplaces (TSMs) which employ blockchain technology as the main trust enabling entity in order to avoid any intermediaries. We provide an overview of scientific and industrial proposals on the blockchain-based online digital marketplaces at large, and TSMs in particular. We consider in this study the notion of *telecommunication services* as any service enabling the capability for information transfer and, increasingly, information processing provided to a group of users by a telecommunications system. We discuss the main standardization activities around the concepts of TSMs and provide particular use-cases for the TSM business transactions such as SLA settlement. Also, we provide insights into the main foundational services provided by the TSM, as well as a survey of the scientific and industrial proposals for such services. Finally, a prospect for future developments is given.**

***Index Terms*—Digital marketplace, telecommunication services marketplace, blockchain technology, communication service provider, distributed ledger technology.**

Acronyms

AM	Application Marketplace
CBAN	Communication Business Automation Network
CDR	Call Data Record
CSP	Communication Service Provider
CSM	Cloud Services Marketplace
DAG	Direct Acyclic Graph
DApp	Decentralized Application
DID	Decentralized Identifier
DLT	Distributed Ledger Technology
DPoS	Delegated Proof of Stake
GDPR	General Data Protection Regulation
IDS	Intrusion Detection System
IdM	Identity Management
IoT	Internet of Things
IPS	Intrusion Prevention System
IPFS	InterPlanetary File System
MNO	Mobile Network Operator
P2P	Peer-to-peer
PoW	Proof of Work
PoS	Proof of Stake
PBFT	Practical Byzantine Fault Tolerance
QoS	Quality of Service
SCP	Small Cell Provider
SFC	Service Function Chain
SLA	Service Level Agreement
SSO	Single Sign-On
SSI	Self-Sovereign Identity
TSM	Telecommunication Services Marketplace
VNF	Virtual Network Function.

Manuscript received May 3, 2021; revised September 17, 2021; accepted October 12, 2021. Date of publication October 28, 2021; date of current version March 11, 2022. The work was partly sponsored by the Swedish Knowledge Foundation through the project *Symphony - Supply-and-Demand-based Service Exposure using Robust Distributed Concepts.* The project partners in Symphony are Ericsson AB (Stockholm, Sweden) and Affärsverken Energi AB (Karlskrona, Sweden). The associate editor coordinating the review of this article and approving it for publication was B. Stiller. *(Corresponding author: Roman-Valentyn Tkachuk.)*

Roman-Valentyn Tkachuk, Dragos Ilie, and Kurt Tutschku are with the Department of Computer Science, Blekinge Institute of Technology, 374 35 Karlshamn, Sweden (e-mail: roman-valentyn.tkachuk@bth.se; dragos.ilie@bth.se; kurt.tutschku@bth.se).

Remi Robert is with Ericsson Research, 164 83 Stockholm, Sweden (e-mail: remi.robert@ericsson.com).

Digital Object Identifier 10.1109/TNSM.2021.3123680

I. Introduction

DIGITAL services and network computing constitute integral parts of today's and future telecommunication infrastructures [1], [2]. The services may range from operating high-performance hardware, dedicated computation for AI, Big Data services and extended to vertically integrated applications [3]. *Digital services marketplaces* were lately introduced as distribution platforms and permitted a booming economy on digital goods, e.g., Apple's gleaming *App Store*.[1]

Marketplaces are appealing mechanisms to deliver digital goods, incl. services. The developers (*producers*) can take advantage of bundling effects of a marketplace, e.g., indexing, cataloging, or storing goods, deploying software, or advertising on the marketplace. The platforms allow the developers to *supply* their digital products through a trusted intermediary (*marketplace*) without having to take care of legal implications of business transactions, e.g., billing. Customers, in turn, can

[1] https://www.apple.com/app-store/

express their *demand* and may take advantage of the amount of supply and of the simplicity to locate goods and services on a marketplace [4]. Marketplaces in telecommunication systems may also be winning for today's network operators, denoted here as *CSPs (Communication Service Providers)*. The platforms can bring additional revenues and innovations beyond simply accelerating the connectivity. The marketplace may expose services and engage developers to implement applications using these services [5], e.g., games or AI model training.

The major business model of marketplaces is to charge the producer a *commission* on the amount paid by a customer. This commission is eventually used to maintain and operate the marketplace and its infrastructure. Digital service marketplaces have often a centralized architecture and act as trust, assurance, and governance providers for the market participants and their transactions. This centralization allows for efficient cataloging or easy billing. In addition, it permits an uncomplicated implementation of the required trust mechanisms. The centralization, however, opens up negative effects. It permits the operators of marketplaces to combine the security requirements of the participants with their pricing ambitions, which in turn is likely to create asymmetry in value generation [6]. Moreover, centralized architectures suffer disproportionately when unauthorized access is gained. In such an architecture, an attacker, if gained unauthorized access, can compromise a large number of identities and eventually all identities. Hence, a *distributed marketplace architecture* is preferred when these platforms should have less controlled business models avoiding monopolies or when they should be more robust to attacks.

An appealing way to eliminate a centralized entity between the producer and consumer is to provide the marketplace actors with the set of tools to perform the business transaction in a distributed and trusted manner. Such a task may be achieved by the blockchain technology [7], which is an implementation of *Distributed Ledger Technology* (*DLT*). DLT provides system participants with distributed storage and brings benefits such as data provenance, accountability, and transparency to distributed systems. Moreover, DLT allows to reduce or completely eliminate the need for a trusted third-party [8], e.g., the marketplace, from the business transaction process, and bring balance to value distribution inside digital marketplaces. Although blockchain technology is still in its infancy, it has enabled a significant number of application scenarios in today's digital marketplaces, which we discuss in this work.

In addition, the process of business transaction execution, i.e., the business settlement, has gained importance as it enables to reach the final business agreement. Today's CSPs enjoy their independence and build their network infrastructures with the centralized operation and governance [9]. In order to execute inter-CSP business transactions, e.g., for allowing mobile customers to roam across different operators infrastructure and to pay for the usage, a *third-party* has to be involved, which acts as a *trust provider* towards non-trusting CSPs participating in business relations. Another use-case is the business transaction between customer and CSP. In this case, the signing of a Service Level Agreement (SLA) [10] may take place where the CSP commits to provide a customer with a certain level of quality of service (QoS) [11] for infrastructure and telecommunication services. Having a third-party in the middle results currently in parts of the process being executed manually which can be complex, expensive, and time-consuming [9]. The application of DLTs in inter-CSP and customer-CSP business transactions may allow the automation of transaction processes. In this way, the need for any manual human efforts can be eliminated almost totally as the DLT acts as a *trust-enabling* entity which under agreed rules, defined in smart contracts, does not need a trusted third-party to take care of parts of the transaction. In the case of SLA signing, the conditions on agreed QoS can be recorded on the distributed ledger [12], as well as intermediate measurements of service quality. In this way, the DLT as a trusted distributed storage enables all parties to agree on the recorded data and to settle in the case of SLA violation.

In this work, we describe, analyze and discuss the concept of a distributed *Telecommunication Services Marketplace* (*TSM*) which employs blockchain technology as the main trust enabling entity and which integrates multiple services offered by different CSPs. We outline the capabilities of distributed TSMs that provide a common set of processes that CSPs can trust and rely on. In addition, we provide a survey on scientific and industrial proposals on the blockchain-based digital marketplaces at large and blockchain-based TSMs in particular. We discuss major standardization activities around the concepts of blockchain-based TSMs and provide use-cases for TSM business transaction functions. Furthermore, we provide insights into the main services provided by blockchain-based TSM, as well as a survey of the scientific and industrial proposals for such services. Finally, a prospect for future developments is given.

The remainder of the paper is structured as follows. In Section II the methodology of this survey is described along with the discussion of related survey collections on digital marketplaces at large and proposals on TSMs in particular. Section III describes the technologies and background of blockchains and digital marketplaces. Furthermore, in this section, we discuss the *a*) scientific and industrial proposals for blockchain-based marketplaces, *b*) the benefits of using blockchains in digital marketplaces, and *c*) we describe a generic structure of blockchain-based TSMs. Section IV discusses the main services provided by blockchain-based TSMs and surveys on scientific and industrial proposals for them. Section V discussed the prospects for future work in an area of blockchain-based TSM. Finally, Section VI draws conclusions on the blockchain-based digital marketplaces at large and TSMs in particular.

II. Related Literature Overview

The overview of the related literature is an integral part of the survey since it outlines prior contributions on the topic of interest. As a consequence, a correct information retrieval methodology is required to ensure complete surveying and inclusiveness. The related literature and its retrieval methodology are discussed next.

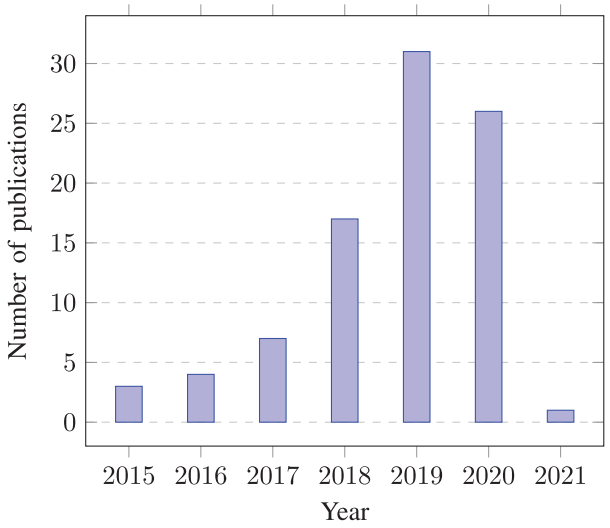

Fig. 1. Number of related publications per publication year.

A. Information Retrieval Methodology

We present a comprehensive survey on the work which has been done in the area of blockchain-enabled TSMs. This should clarify the view of the TSM as a concept and give an overview of the main building blocks that TSM's architecture comprise.

The survey information was retrieved using *database search* in combination with *snowballing* method [13]. The sources of information are bibliographic databases *Scopus*,[2] *Web of Science*,[3] IEEE *Xplore*,[4] *ACM Digital Library*,[5] and *Google Scholar*.[6] To create the search strings a number of keywords were used: *telecommunication, marketplace, blockchain, service, identity management, assurance, governance, business settlement*. Also, multiple variations of these words were constructed such as plural forms and different word combinations.

The search string that was used for TSM survey search in all bibliographic sources is: *blockchain AND telecommunication AND marketplace AND service AND survey*; (where certain parts of search string were excluded to increase the variety of search results). The main search criteria for related publications is the presence of discussion on blockchain technology and its applicability in the context of telecommunication services marketplaces. According to the search we conducted, there are no surveys at this point that target specifically TSMs based on blockchains. As a consequence, our search was extended to works that discuss the advantages and disadvantages of blockchain applicability in the context of digital marketplaces at large. In addition, the works which investigate digital marketplaces' core blockchain-based services were included as well. Fig. 1 presents a number of found related publications per publication year.

[2]https://www.scopus.com
[3]https://clarivate.com/Webofsciencegroup/solutions/Web-of-science
[4]https://ieeexplore.ieee.org
[5]https://dl.acm.org/
[6]https://scholar.google.com

B. Related Work

Despite no surveys that match the topics were found, a number of scientific proposals were found which discuss the idea of TSM. We highlight next the major contributions for decentralized marketplaces in the context of telecommunication services.

The work presented in [14] has shown a high degree of relevance for our own survey as its authors propose to use blockchain technology for the creation of a decentralized marketplace for telecommunication services. The proposed marketplace allows the entities collaborating within it to conduct business transactions without a need for a trusted third-party. Specifically, the authors describe the use-case of network infrastructure resource sharing, which nowadays involves trusted third-party and is a multi-step time-consuming process. Authors claim that blockchain technology can help to automate this process, enabling fast and efficient network resource sharing. Additionally, authors of [15] propose a blockchain-based system to manage SLAs between small cell providers (SCP) and mobile network operators (MNO). According to the authors, using blockchain smart contracts enhances the process of SCPs participation in the cellular market, as they can offer their capacity to MNOs in an automated and cost-efficient manner. These works have a high degree of relevance for this survey as they describe telecommunication network use-cases specifically and aim to enhance business settlement mechanisms between different CSPs.

C. Related Surveys

Considering that no surveys on specifically telecommunication marketplaces were found, we decided to incorporate surveys that explore the possibility of blockchain-based digital marketplaces at large.

The references provided next do not necessarily concentrate on a discussion of blockchain-based digital marketplaces. However, they provide some interesting insights on the concept of the marketplace and the advantages and disadvantages of blockchain incorporation. In [16] authors discuss the blockchain application in a context of Smart Cities [17], where different aspects of citizens' life can be improved with the decentralized nature of blockchain. In terms of marketplaces, the authors discuss an application of blockchain in the context of Smart Grids and peer-to-peer energy trading. They assert that blockchain technology can enhance users' independence in an energy trading market, and allows to reduce the need for a trusted third-party presence in today's trading process. Authors of [6], through a case-study approach, provide a comprehensive description of digital marketplaces at large and provide an insight into the benefits of blockchain technology incorporation. According to them, the decentralized nature of blockchain technology can enable new forms of collaboration in digital marketplaces, as well as transform the existing process of business settlement. In [18] authors survey the research proposals on blockchain incorporation in the area of Internet of Things (IoT) [19], exploring the idea of blockchain-based IoT data marketplaces. In such marketplaces, blockchain technology acts as an enabler of data assurance,

while IoT device's data is traded within a decentralized market in a trusted and secure manner. The author of [20] discusses the application of blockchain technology in the area of IoT data exchange in decentralized environments. In this work, the author explores the legal aspect of blockchain technology and its compliance with existing regulations in the area of information technology, and digital marketplaces in particular. In contrast to previous works, the author warns that the use of blockchain technology may harm the privacy of IoT device users, instead of enhancing it. In [21] authors conduct a comprehensive survey on the scientific and industrial proposals in network infrastructure resource sharing techniques. However, the authors provide very little insight into blockchain incorporation for the performance of resource sharing and the creation of market platforms.

Considering the information provided in the above surveys, the blockchain application in the area of digital marketplaces has gained traction and has been rather well defined. We aim to extend the application of blockchain technology to the TSM, by describing the needs of such a marketplace according to recent proposals and standardization activities. In addition, we describe a framework to enable CSPs to collaborate and conduct the business transaction execution.

III. Blockchains and Digital Marketplaces

It is important to provide an overview of technologies that are central to our survey. The discussion of the blockchain establishes a common understanding of this technology and helps to comprehend its features. In order to put blockchain into the context of telecommunication services, the applicability in the inter-communication service provider (inter-CSP) transactions is also discussed. Next, digital marketplaces are discussed at large, to establish a common understanding of this concept and the details behind it, with the survey of the proposals in blockchain-based digital marketplaces, to map the academic and industrial developments in this area. Finally, the definition of TSM and its core services is provided, to explain the concept and put it into the context of main application use-cases.

A. Blockchain Technology

Distributed Ledger Technology (DLT) has gained attention due to its decentralized nature and trust-enabling capabilities. DLT provides distributed data storage. It acts as a decentralized database where data is transmitted in a P2P network, thus, it does not have a central governing authority and all the security concerns that come with it, *c.f.,* [22]. Information in the ledger is replicated on every node in the P2P network, which prevents data loss. In addition, due to the immutable nature of the ledger, it is extremely difficult to alter transaction history. DLT provides a lot of benefits, such as provenance, accountability, and transparency for all the data which is stored on a distributed ledger [16]. Blockchain is one possible implementation of DLT. It bundles the pieces of data into blocks, where each block contains a reference to the previous one, thus, forming a chain of data blocks. Another structure that is used to implement DLT is Direct Acyclic Graph (DAG) [23]. In DAG-based DLTs, the newly added transaction can reference multiple previously added ones. IOTA [24] is the representative of DAG-based distributed ledger implementations. Further in this work, we survey proposals that utilize both blockchain-based and DAG-based DLTs in the context of digital marketplaces. However, in this section we discuss blockchain technology exclusively. The reasoning is that majority of academic proposals use the blockchain implementation of DLT, and only a few use DAG-based DLT.

The architecture of the blockchain depends on two things: 1) whether the access for reading the information stored on blockchain is public or private, and 2) whether the right to write to the ledger and participate in consensus protocol execution is permissioned or permissionless. There are three main blockchain architectures [16], [25]:

1) Public Permissionless Blockchain: In this architecture, everyone is allowed to become a part of the network and participate in the consensus process. Every node carries a copy of the shared ledger. The transactions are visible for all blockchain nodes, but participants retain a certain degree of anonymity, which may be subject to privacy issues [26]. The Bitcoin [7] is the first and well-known blockchain technology implementation that utilizes public permissionless architecture. It is also the first cryptocurrency and was launched in 2009 after being introduced by Satoshi Nakamoto in 2008. It is mainly used as a decentralized financial system, where token exchanges emulate banking transactions. Next, Ethereum [27] is another representative of public permissionless architecture. It is believed to be an evolutionary step of Bitcoin since it aimed to solve some of Bitcoin issues such as flexibility of on-chain code execution.

2) Private Permissioned Blockchain: Here it is the governing node (or set of nodes) that decides whether a new participant can enter the blockchain network. Moreover, after the new node has gained access to read the ledger, the governing node decides whether it is allowed to participate in consensus. The decision on the ability to participate in consensus for the existing members can also be reviewed by the governing node during the operation of the blockchain network. The main idea of private permissioned blockchain architecture is to fully control the access to different aspects of blockchain network operation. The governing node can be also represented by a *regulatory authority* which issues private blockchain participation licenses and helps to sign business agreements between participating stakeholders to carry out consensus process [28]. Hyperledger Fabric [29], which is developed by the Linux Foundation, is a representative of a private permissioned blockchain system. In Hyperledger Fabric, the nodes are divided into three types based on the task they are performing: endorsement, ordering, or validation. Endorsing nodes take a transaction proposal, execute it and return a transaction proposal response. Responses from multiple endorsers are then bundled together and then passed to the ordering nodes. These nodes take newly endorsed transactions and agree on the order in which these transactions are stored in the ledger. Finally, validation nodes receive the block that was newly added to the blockchain and check the validity of the transactions in that block. They check that each

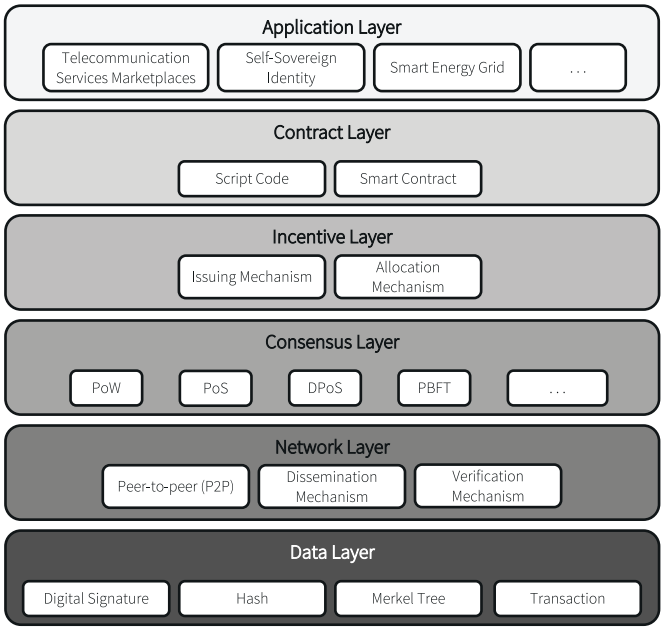

Fig. 2. Blockchain infrastructure model [16].

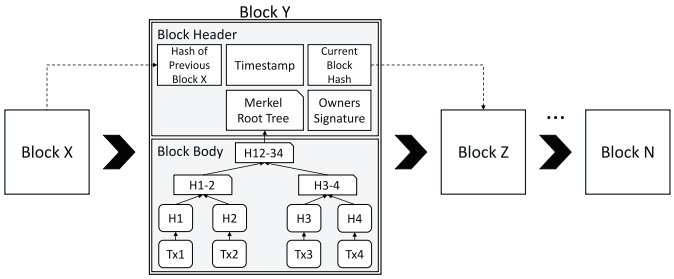

Fig. 3. Blockchain block structure [16].

transaction has received all the endorsements it needed based on the configured policy and that it is not conflicting with a previous transaction. Invalid transactions are kept in the blockchain but do not modify its state.

3) Public Permissioned Blockchain: This blockchain architecture allows initially non-trusting organizations to establish a trust bridge over a public yet permissioned system. In public permissioned blockchain architecture, everyone is allowed to join the blockchain network, thus obtaining the right to read and verify the state of the ledger, as well as propose new transactions. However, only authorized nodes have the possibility to participate in the consensus process. This type of architecture also presents a possibility for only a specific group of nodes to write new blocks to the ledger. It creates an opportunity for the creation of consortium-governed ledgers, where a number of companies share blockchain's governance, maintenance, and orchestration. This type of architecture was made popular by the Sovrin Foundation [30] in their blockchain-based identity management system implementation which is discussed in Section IV-A.

B. Blockchain Infrastructure Model

In order to provide a rather familiar structuring of blockchain infrastructure, we provide a model derived from [16]. The entire blockchain infrastructure is divided into six layers which are shown in Fig. 2. The layering approach is used as a way to divide the infrastructure into a set of blocks with the underlying components on the inside presented as technologies and processes used in blockchain operation. Here, we discuss each infrastructure layer and its components.

Data Layer: The first layer in the blockchain infrastructure model is the data layer. It presents a fundamental set of technologies that lay at the core of blockchain. The *blockchain* has received its name due to the resemblance of a chain, where instead of metal rings the blocks of structured data are interconnected in a sequence. This data is structured chronologically and is immutable, i.e., it is highly challenging to alter on-chain data. A blockchain with a detailed structure of a block [31] is shown in Fig. 3. The *block body* is used to store hashes of transactions that are verified and embedded in the block. These hashes are built as a Merkle Tree [32] and represented in the block header as a *Merkle Root Tree* component. The Merkle tree comprises a binary tree constructed of hashes of transactions that are stored in a block body and positioned at the beginning of the tree structure, e.g., Tx1. When the hash of the transaction is computed, e.g., H1, it is being added with the neighboring hash up until the moment when the top of the tree is reached. Since every computed hash is saved in a block, the Merkle tree can be later used for rapid and secure verification of the transactions included into the block [16]. The *block header* plays a key role in chain establishment since it contains the hash of the previous block in a sequence, which is called a *parent block*. The first block in a sequence is called *genesis block* and it does not have a parent block. The block header contains some additional metadata information such as the block owner's signature and timestamp of the block creation.

Network Layer: The network layer topology in permissionless blockchains is built and functions similarly to a P2P network [33]. The P2P network ensures no privileged participants partake in the life-cycle of blockchain events. The main events of the blockchain network are the dissemination, i.e., forwarding, and verification of the transactions according to the network layer protocols. A distinct feature of the blockchain network layer is that it ensures that only verified transactions are transmitted in the distributed network and stored in the local node's ledger. First, the dissemination mechanism utilizes the distributed nature of the P2P network and broadcasts transactions to neighboring nodes. Second, the verification mechanism ensures that only valid transactions continue to be forwarded by verifying transactions according to blockchain specifications. The verification itself is based on asymmetric cryptography where each node maintains a public and private key pair [34]. When a transaction is created, it is signed by the private key of the creator node, and then broadcasted to neighboring nodes. Meanwhile, neighbors use the public key of the creator node, to verify the transaction's signature [16]. If a transaction is valid, it is forwarded to other neighboring nodes. Otherwise, if the transaction is marked as invalid, forwarding is stopped, and the transaction is discarded.

In contrast, the blockchains with permissioned architecture are not necessarily a P2P network. Permissioned architecture frequently incorporates multiple interconnected blockchains and in some use-cases the peers from different organizations do not really communicate with each other. For instance, in Hyperledger Fabric the blocks distribution is reliant on the ordering node for providing blocks to the leader peer from each organization. The leader peer is then responsible for redistribution of the ordered blocks to the rest of the peers.

Consensus Layer: In centralized systems, the consensus is an inherent feature of the system, since all components are orchestrated by a centralized trust enabling entity. In contrast to centralized systems, where all the nodes are governed by the central silo which represents the root of trust, the blockchain network deliberately avoids centralized authorities, making the system decentralized. With this, a mechanism that allows establishing consensus between all nodes is needed to ensure secure and correct decentralized blockchain network operation.

At the present time, a number of consensus algorithms are used in blockchain systems. The Bitcoin blockchain uses Proof of Work (PoW) [7] consensus protocol where nodes in the blockchain network continuously execute hash calculations until the computed hash is less than a given target value. The first node to generate a correct hash obtains the ability to write the next block to the blockchain. The Proof of Stake (PoS) [35] consensus protocol was made popular by the Ethereum cryptocurrency and was developed as an alternative to PoW. In PoW, in order to generate a valid hash value, the entire network competes, thus, by design, consuming large amounts of electricity. PoS is designed to be energy efficient and gives the opportunity to add new blocks to the ledger to the nodes which hold the largest amounts of cryptocurrency. Moreover, for each block, the actual node is selected with a certain degree of randomness. A Delegated Proof of Stake (DPoS) [36] consensus protocol was designed as an evolution of PoS. DPoS makes the blockchain network more democratic and gives every node an opportunity to decide what is being written to the blockchain. The downside of DPoS is that still the votes of the nodes which have the most cryptocurrency, weigh the most. A Practical Byzantine Fault Tolerance (PBFT) [37], [38] consensus protocol is designed to tolerate Byzantine faults in a system where the data is being replicated. For a deeper discussion on consensus mechanisms in blockchain systems, the reader is referred to a survey on consensus protocols [39].

Incentive Layer: The incentive layer combines the mechanisms to issue and allocate portions of cryptocurrency to nodes that participate in the data verification process. The cryptocurrency, e.g., Bitcoin or Ether, works as an incentivizing factor for blockchain network participants, as far as when awarded, it can be spent in the network, or exchanged to fiat currencies. In Bitcoin cryptocurrency, which is built as permissionless blockchain, the incentive *issuing mechanism* is called "mining." Comparison to the mining process comes from the fact that in order to get some precious metal or stone it has to be "mined" from the earth. The process of mining involves the nodes in the blockchain network spending their computational power to verify the next hash in a sequence of blockchain to take part in the PoW consensus. The more computational power the node has, the bigger incentive is allocated. In Bitcoin cryptocurrency, miners can unite into *mining pools*, where large computational "farms" are used to mine large amounts of cryptocurrency. According to *allocation mechanism*, economic incentives are provided to the node which generated a new block. When computational efforts are registered by the blockchain network, the generator node gets a portion of cryptocurrency allocated to its crypto-wallet. The incentive layer represents the attractiveness of the blockchain network, as far as the more rewarding incentive is for the miners, the more nodes are attracted to join the network and contribute to the general pool. Also, diversification of the miners allows for a more secure blockchain, thus, reducing the possibility for a 51% attack [40], where more than 50% of the miners are malicious and can perform consensus faster than honest miners. This allows malicious miners to control the blockchain network and to double-spend the cryptocurrency.

Contract Layer: The contract layer of the blockchain infrastructure model introduces the way to embed executable code into the transaction. The primary way to execute on-chain code was introduced in Bitcoin cryptocurrency as a *script* which is embedded into a block. A script is stored on the immutable ledger in an individual block and is based on a limited programming language that states the conditions to validate a transaction, and acts as a termination guarantee in case of transaction conditions are not met. A script has a limitation, namely, it does not have the possibility to execute more complex transaction scenarios. A *smart contract* is considered to be an evolution of a script. It was first introduced in Ethereum blockchain as the way to make cryptocurrency transactions more flexible and complex. It is based on a programming language that is Turing complete and allows shifting from static transactions to the execution of code. A smart contract allows bringing a certain degree of programmability to the blockchain, thus, introducing the ability to describe cryptocurrency exchange scenarios of different complexity. In the context of business transactions, a smart contract is used to describe the conditions under which involved actors are collaborating. When all conditions of a business transaction are agreed upon, they are embedded into a smart contract and signed by collaborating actors. Next, the smart contract is verified by the blockchain network and written to the ledger [41]. Depending on the platform there might be an explicit signature by the involved parties. In some cases, the code of the smart contract is freely auditable, and just usage of the smart contract is equivalent to accepting the way it is written. When the conditions of the smart contract are met, it executes the code embedded inside of it, while acting as a guarantee of exactly what code is being executed as well as on what data it is operating. As a result of this, the smart contracts allow to automate complex business transaction scenarios, making them more error-resistant and time-efficient. Finally, as far as smart contracts can be executed by any member of the blockchain network to verify the validity of the data it is operating, this contributes to the transparency and trust establishment between smart contract actors. For a deeper discussion on smart contracts, the reader is referred to empirical studies of blockchain smart contracts at [41] and [42].

Application Layer: The top layer in the blockchain infrastructure model is the application layer. It aims to introduce different application scenarios for blockchain technology. The main application scenario discussed in this work is the Telecommunication Services Marketplaces, but there are multiple others such as Smart Energy Grid, IoT, Cloud Infrastructures, Self-Sovereign Identity, etc. [43]. The main aim of these applications is to enhance different aspects of business and social life such as enhancement of business settlement and augmentation of digital sovereignty. Nowadays, when the best application conditions of blockchain technology are yet to be found, we see that this topic is being researched by multiple academic communities as well as adopted by multiple companies in the industry sector. The sheer volume of academic works on blockchain technology generated in recent years gives an idea of the interest in the topic.

C. Reasoning for Blockchain Usage by CSPs

Existing operational frameworks of CSP are built on the premise that the entire telecommunication services chain belongs to one CSP. The *interoperability* of such operational frameworks is not always considered, as well as the system is centralized and governed by the owner company. Furthermore, existing operational frameworks are slow to adapt to the needs of next-generation Internet, as *integration* of new technologies with the legacy systems is challenging and time-consuming. Transaction execution between two or more CSPs involves manual operation processes which can be complex, expensive, and time-consuming. As these processes involve human intervention, they are a subject of multiple issues: manual errors, long payment cycles, and exposure to fraud. In this way, *accountability* and *trust* of the operational framework are jeopardized which may lead to consistent revenue losses [9].

With the creation of a unified framework to operate telecommunication service chains, the development of next-generation network services will be accelerated. This will also ensure the interoperability and integration ability of new services with legacy systems. Furthermore, an automated approach to handle inter-CSP transaction execution will enable real-time and trusted settlement between two or more CSPs [9].

The DLT is highly applicable to inter-CSP business settlement transactions. It allows automation of inter-CSPs processes, thus eliminating the need for any manual human efforts. In this case, the DLT acts as a *trust-enabling* entity which under agreed rules, defined in smart contracts, does not need a trusted *third-party* to take care of parts of the transaction. While all inter-CSP transactions are recorded in the DLT's storage (every CSP can verify transactions or smart contract data at any time) the data stored on DLT is immutable and the storage itself is distributed. Private permissioned blockchain architecture has the highest applicability in the use-case of CSP business settlement transactions. The ledger where trusted parties authenticate and are authorized to verify the business agreement recorded in a smart contract at any time, enables trusted, secure, and automated business settlement for two or more CSPs [44].

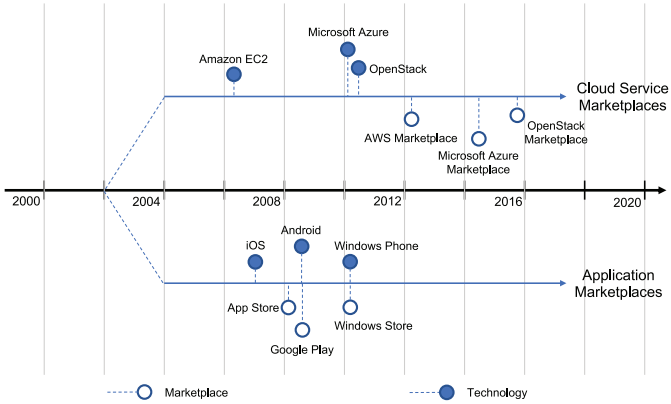

Fig. 4. Timeline of application and cloud marketplaces development [46].

Automation of inter-CSP business settlement processes benefits the business revenue growth, decreases the duration of transaction execution, and reduces the costs spent per business contract settlement [9], [44], [45].

A general risk from blockchain-based marketplaces for CSPs is that these platforms open the system for collaboration and may impact their functional integrity (incl. privacy violations) and business model. However, if trusted collaboration is enabled then the advantages of expanding a system by including additional stakeholders (developers) and new functionality leading to increased revenue, may outweigh the disadvantages of marketplace platforms, which are integrity checking and sharing revenues. Sharing revenue, however, may spark the discussion on how profits are taxed now in such a context. We believe that this discussion is important but would deviate too much the paper from its main objective to provide an understanding of the techniques to implement blockchain-based marketplaces.

D. Centralized Digital Marketplaces

Before we survey the blockchain-based digital marketplaces, we discuss centralized marketplaces that are being used nowadays. Today's marketplaces pose a number of challenges in terms operations and fairness towards users. These challenges are discussed next.

Digital marketplaces are a common and widely accepted concept for the formation of business opportunities. They are open platforms where IT companies or individual developers can offer their products for purchase. The timeline of application and cloud marketplace development initially described in [46] is depicted in Fig. 4. In general, digital marketplaces are defined to meet the requirements of the concepts of *supply and demand* [4]. The popularization of smartphones, for example, created a demand for apps, which led the main mobile phones vendors to deploy their marketplaces as a way to supply applications to end-users.

The marketplace allows products to be supplied to customers with increased speed and stimulates the popularity and expansion of the software. Having fulfilled the supply and demand capabilities of the marketplace, the business relations inside of the marketplace must be regulated. This is done through the *licensing approach* [47] when the relation of the

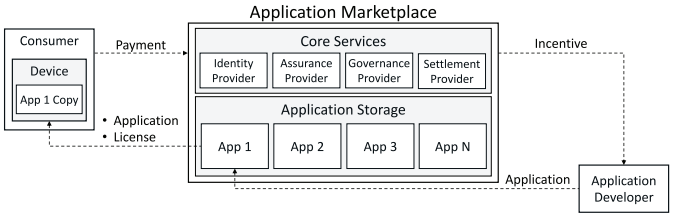

Fig. 5. Application marketplace with on-premise application delivery model.

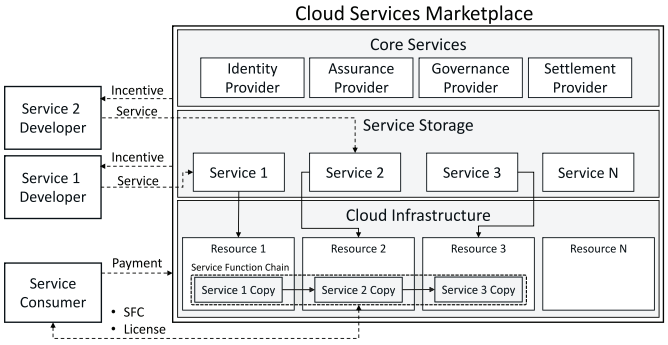

Fig. 6. Cloud service marketplace with in-cloud service delivery model.

consumer and supplier is defined in a document, i.e., license, which is signed by involved parties. The licensing approach enables the marketplace to execute business operations, make the process transparent and legally correct. The supply concept also provides a *payment* [48] for a software product, which is charged by the marketplace on behalf of the supplier. It acts as a foundation of the *business settlement*, i.e., business transaction execution, between the consumer and the supplier. In a marketplace with a centralized architecture, being the middleman in software distribution gives the ability to dictate the billing rules and payment distribution the majority of the time.

Digital marketplaces operate as a provider of specific foundation services to allow an optimal operation for their customers. Starting with the *identity management* system [49], a marketplace acts as a provider of digital identity which authenticates customers in a system and authorizes the execution of an allowed set of actions. Moreover, acting as an *assurance provider* [50] towards the customers, the marketplace provides a certain degree of confidence in the services and platforms which are provided by it. As a main distributing entity, it has to provide a certain degree of *trust* [51] to make customers feel confident about payment transactions. For a system to be properly operated the *governance* over the marketplace has to be maintained by one or a number of trusted parties.

Another major part of the marketplace concept is how the software products are delivered to the customers, i.e., executed, fulfilling their computational purpose. In today's marketplaces there are two main types of software delivery: 1) *On-premise*, when the software is executed on customers hardware infrastructure, and 2) *In-cloud*, when cloud hardware resources are used. These two software delivery models will be discussed next.

On-Premise Delivery Model: The widely known *Application Marketplaces* (AM) [52] such as *Apple App Store* and *Google Play* have gained their popularity by providing numerous applications for their respective *iOS* and *Android* operating systems (OS) [53]. These OSs are installed on a wide variety of personal devices, which nowadays carry a substantial amount of computing power. The AMs define rather strict distribution rules for the applications they provide. The applications for some of the operating systems can officially be provided only through the respective marketplace. Moreover, the application itself is allowed to be executed only within a certain operating system. This limits the developers of the applications in terms of the number of different marketplaces where they can distribute their products. Also, developers are limited in the tools that they can use to develop their applications since every operating system acts as an execution environment for a certain runtime. On the other side, when the marketplace is bound to a specific OS, it also can act as an *assurance provider*, who guarantees the proper execution of the application. For example, applications on the Apple App Store go through a multi-step verification process before becoming available for the customers. Also, the AMs are built around a centralized server which acts as a *trust provider* between the customers and application developers. Being in the middle, the marketplace has the opportunity to dictate the rules on billing, e.g., taking a percentage of the profits as the main distributor.

The *on-premise* delivery model is intrinsic for AMs due to their *consumer-oriented* approach. The structure of this delivery model is shown in Fig. 5. In the on-premise model, the applications are delivered as software packages with the aim to perform a range of tasks. The specifics are in the behavior of software that is being distributed - it works as a standalone program, and not as a part of a Service Function Chain (SFC) [54], which can be defined as a sequence of software components that build the service chain and interact with each other to reach a common goal. Therefore, AMs are aimed to fulfill the demands of a single consumer, and the software distributed by it is not intentionally designed to be a part of SFC. Although the end-devices with mobile operating systems can become a part of SFC, it is not the aim of the products which are mainly distributed by the AM.

In-Cloud Delivery Model: The major public cloud infrastructure providers, such as *Amazon Web Services* and *Microsoft Azure*, have recently introduced a new type of digital marketplaces: *Cloud Services Marketplaces* (CSM) [55], [56]. The cloud services are not bounded to specific software requirements, on a contrary, they are designed to be software- and OS-agnostic. The only limitation is that the cloud service has to be executed within the hardware infrastructure of the cloud provider. Much like the AM, the CSM is also built with a centralized server representing the trust provider. Also, while all services are executed inside of the cloud infrastructure, the CSM provider acts as an assurance provider towards the customers. Unlike the AM, CSM is designed to distribute services that can become a part of the SFC. SFCs can be executed simultaneously - forming a grid of services, or in a sequence - forming a service pipeline.

The *in-cloud* delivery model is intrinsic for the CSMs due to their service-oriented approach. The structure of this delivery model is shown in Fig. 6. In the case of CSMs, the

services play a key role in forming the SFC. Within SFC, it is important to fulfill minimum hardware requirements for some specific service, e.g., Trusted Platform Module (TPM) or specific CPU architecture, which cloud infrastructure can provide. SFCs can be used in application development as an execution environment for application builds generation in version control systems. Also, SFCs can execute so-called *Artificial Intelligence (AI) pipelines* which are used in a collaborative form of AI engineering [57]. An important feature of the in-cloud delivery model is that it introduces the ability for multiple stakeholders to interconnect their services deployed within the same cloud infrastructure provider. This opens the opportunity for a new type of collaboration when a business settlement is performed between multiple stakeholders. However, these stakeholders still need to rely on a trusted third-party, i.e., cloud provider, which acts as a trust provider towards the business settlement execution.

Today's cloud providers are limited in providing business settlement interfaces for inter-cloud multi-stakeholder operations due to a number of reasons. To begin with, cloud infrastructure providers do not use a unified API standard for the provisioning of different cloud service models such as IaaS, PaaS, and SaaS. Next, identity management systems are built with a centralized model which makes multi-cloud provisioning challenging, as every cloud infrastructure uses a separate identity. The interoperability of services provided in CSM is not considered outside of the boundaries of a specific cloud provider. In addition, the assurance provided by CSM is centralized within one cloud provider, which makes it challenging for every CSM involved in SFC construction to guarantee reliability and stability of its execution. Lastly, the existing monitoring frameworks are mostly designed to work with a specific cloud provider which makes the multi-cloud system maintenance costly and time-consuming. The authors of [58] provide an insight on this issue and propose a way to enable a multi-cloud provisioning system.

E. Blockchain-Based Digital Marketplaces

In recent years, to address the disadvantages of centralized marketplaces, the concept of a decentralized marketplace has been introduced. Coupled with the widespread application of blockchain technology, it resulted in a number of scientific proposals exploring blockchain-based digital marketplaces. These proposals are listed in chronological order in Table I along with their *application area* and are discussed in more detail in the remainder of this paper. Additionally, a number of industrial proposals on blockchain-based marketplaces are presented in Table II.

1) Smart Energy Grid: The application of blockchain in the area of Smart Grid [84] and peer-to-peer (P2P) energy trading has gained traction in recent years. Blockchain technology reduces distributed energy prosumers' dependence on the energy supplier during trading process and enables P2P energy trading using smart contracts as a tool for trade settlement. In [59], authors investigate a possibility of blockchain-based marketplace creation for P2P energy trading to bring flexibility and transparency to all actors involved in the energy market. In the proposed model, a blockchain holds the amount of electricity produced and allows regulating the electricity prices based on the prosumer generation rate. Authors of [60] propose a decentralized blockchain-based platform for energy trading. With blockchain technology, authors are able to reduce the need for a trusted intermediary in a trading process. The main aims of the platform are to make the usage of the energy generated by households more efficient and reduce electricity bills.

Both aforementioned proposals can be summarized in two main reasons to apply blockchain in the context of P2P energy trading. First, it is the reduction of the need for a third party, e.g., a marketplace, in an electricity trading process. Eventually, the third party cannot be eliminated entirely since the electricity prices are regulated by the government, which in turn places a restriction on the maximum price that energy can be sold for [85]. However, blockchain technology enables P2P trading between marketplace customers, where different trading concepts can be applied and enhanced, e.g., auction bidding or fixed price selling. Second, the ledger as a data storage provides statistical information which helps marketplace maintainers to dynamically adjust electricity prices during the day. This enables making trading more efficient in relation to energy consumption and production rates and possibly allows to reduce electricity bills for households.

2) Internet of Things (IoT): In the area of IoT, blockchain technology enables new opportunities in the creation of decentralized data marketplaces. The IoT devices generate and exchange large amounts of data, which poses challenges in terms of privacy, data assurance, and scalability. However, the ability to trade the IoT data in a decentralized and democratic way creates an opportunity for IoT device owners to monetize their data and opens new business opportunities for IoT device manufacturers. In [61] authors explore the benefits of the blockchain technology incorporation into decentralized IoT data marketplaces. They present a test implementation of such a decentralized blockchain-based marketplace, where IoT data can be posted for further purchase. As result, the authors present such challenges for decentralized marketplace advancement as compliance with regulatory documents, e.g., General Data Protection Regulation (GDPR) [86], identity management and trust establishment. Authors of [62] discuss the issue of central point of failure in centralized IoT marketplaces where devices rely on the availability of the marketplace to use remote services and storage. To address this issue authors propose the concept of the distributed blockchain-based marketplace. This enables the distribution of servers and storage resources, increasing the marketplace's availability and robustness. In addition, authors evaluate their test implementation in an experimental testbed which shows the transparency and operational ability of distributed marketplace, without the need for a trusted centralized entity. In [63], authors present a framework for decentralized blockchain-based IoT data marketplace. According to the authors, the novelty of their framework is the ability to consider such factors as data's location and supplier availability, which gives the buyer better data context. This opens the opportunities for the data collection tasks ordering, where suppliers fulfill the locational and contextual needs of data buyers. Authors

TABLE I
ACADEMIC PROPOSALS TAXONOMY ON BLOCKCHAIN-BASED MARKETPLACES

Reference	Application Area	Platform	Architecture	Description
N. Afraz et al. [14]	Telecommunication Services	Hyperledger Fabric [29]	Private Permissioned	A network infrastructure resource sharing in a blockchain-based decentralized marketplace.
E. D. Pascale et al. [15]	Telecommunication Services	Ethereum [27]	Public Permissionless	A decentralized system to manage SLAs between SCP and MNO with blockchain smart contracts.
C. Pop et al. [59]	Smart Energy Grid	Ethereum	Public Permissionless	A decentralized marketplace for P2P energy trading with blockchain smart contracts addressing enerfy flexibility.
S. Saxena et al. [60]	Smart Energy Grid	Hyperledger Fabric	Private Permissioned	A decentralized blockchain-based platform for energy trading with increased efficiency.
G. S. Ramachandran et al. [61]	IoT	Ethereum	Public Permissionless	A test implementation and discussion of main challenges for decentralized IoT marketplaces advancement.
L. Mikkelsen et al. [62]	IoT	Ethereum	Public Permissionless	A concept of blockchain-based marketplace which distributes services and storage resources for IoT.
D.-D. Nguyen et al. [63]	IoT	Not Applicable[1]	Public Permissionless	A decentralized blockchain-based IoT data marketplace with the ability to consider data's location and supplier availability.
H. T. T. Truong et al. [64]	IoT	Hyperledger Fabric	Private Permissioned	A framework for a decentralized IoT data marketplace that stores access control policies and makes access controlling decisions.
S. Bajoudah [65]	IoT	Ethereum	Public Permissionless	A model for a blockchain-based decentralized IoT data trading marketplace that provides a trade-off between transaction costs and data loss risks.
K. R. Ozyilmaz et al. [66]	IoT, Sensors Data	Ethereum	Public Permissionless	A blockchain-based decentralized marketplace where for IoT data trading where developers of ML solutions can collaborate.
P. Tzianos et al. [67]	IoT, Sensors Data	IOTA [24], Blockchain agnostic[2]	DAG-based	A blockchain-based marketplace for IoT sensor data trading with the blockchain agnostic architecture.
S. Musso et al. [68]	IoT, Sensors Data	IOTA	DAG-based	A decentralized DLT-based marketplace designed to trade streaming data in a context of smart cities.
K. Nguyen et al. [69]	IoT, Sensors Data	Ethereum	Public Permissionless	A blockchain-based marketplace to search and trade IoT data based on the geographical location of the device.
A. Seitz et al. [70]	IoT, Applications	Ethereum	Public Permissionless	A blockchain-based marketplace with the ability to trace application installation on edge IoT devices.
D. Miehle et al. [71]	IoT, Supply Chain	Hyperledger Fabric	Private Permissioned	A blockchain-based marketplace model where machines perform full chains of tasks to supply manufacturers with needed details.
V. P. Ranganthan et al. [72]	E-commerce	Ethereum	Public Permissionless	A decentralized e-commerce marketplace based where merchants fully control transaction process.
Z. Wang [73]	E-commerce	Ethereum	Public Permissionless	A blockchain-based marketplace for art trading that allows to trace the art assets owner and location history.
J. Martins [74]	E-commerce	Ethereum	Public Permissionless	A model of blockchain-based e-marketplace where suppliers compete with each other to fulfill the customer order.
N. Baranwal Somy et al. [75]	Cloud Services, Data Trading	Hyperledger Fabric	Private Permissioned	A blockchain-based decentralized marketplace where different actors can collaborate in AI engineering process.
J. Li et al. [76]	Cloud Services, Data Trading	Bitcoin[3][7]	Public Permissionless	A model for blockchain-based decentralized marketplace for online content trading with indexing of content names.
P. Banerjee et al. [77]	Cloud Services, Data Trading	Hyperledger Fabric	Private Permissioned	A decentralized blockchain-based marketplace for online content trading which provides a searching and trading mechanisms.
M. F. Franco et al. [78]	Cloud Services, VNF	Ethereum	Public Permissionless	A blockchain-based marketplace model for VNFs hosting where infrastructure providers compete to host VNF.
B. Nour et al. [79]	Cloud Services, VNF	Custom PoW-based blockchain	Public Permissionless	A blockchain-based brokering mechanism used to allocate and manage network slicing in 5G network.
E. Scheid et al. [80]	Cloud Services, VNF	Ethereum	Public Permissionless	A blockchain-based VNF package repository where package integrity is verified without the involvement of a third party.
M. Franco et al. [81]	Cloud Services, VNF	Ethereum	Public Permissionless	A blockchain-based catalog where vendors of distributed denial of service protection software can post and sell their products.
V. Arya et al. [82]	Cloud Services, API	Ethereum or Hyperledger fabric[4]	Multiple Architectures	A blockchain-based marketplace model for Artificial Intelligence APIs access trading.
M. Pincheira et al. [83]	Cloud Services	Ethereum	Public Permissionless	A decentralized blockchain-based marketplace for Fog/Edge computing resources trading.

[1] No implementation available.
[2] IOTA DLT is used for data storage. Overall system is not designed to work with any specific DLT in mind and aims to be blockchain agnostic.
[3] Proposed blockchain is based on the Bitcoin blockchain, with significant modifications.
[4] No implementation available, however authors plan to base future implementation either on Ethereum or Hyperledger Fabric.

of [64] propose a framework for a decentralized IoT data marketplace. According to the authors, the novelty of their proposal is that in addition to storing access control policy on the blockchain, it also makes access control decisions. This contributes to auditability of the marketplace and brings transparency to the marketplace participants. In addition, the

TABLE II
INDUSTRIAL PROPOSALS TAXONOMY ON BLOCKCHAIN-BASED MARKETPLACES

Reference	Application Area	Platform	Architecture	Description
Ericsson [90]	Cloud Services	Hyperledger Fabric	Private Permissioned	A decentralized blockchain-based marketplace prototype and list of key requirements for decentralized digital marketplaces.
Wibson marketplace [91]	Cloud Services, Data Trading	Ethereum	Public Permissionless	A decentralized blockchain-based marketplace for fair, transparent and secure data trading.
Project XBR [92]	Cloud Services, Data Trading	Ethereum	Public Permissionless	An infrastructure for decentralized blockchain-based data marketplaces on-demand provisioning, where users can trade data assets.
IOTA marketplace [24]	IoT, Data Trading	Tangle	DAG-based	A decentralized blockchain-based marketplace based on a new type of distributed ledger based on DAG for IoT data trading.
Databroker DAO [93]	IoT, Data Trading	Ethereum	Public Permissionless	A decentralized blockchain-based marketplace designed to provide a transparent and secure way to buy and sell IoT sensors data.
Datum [94]	IoT, Data Trading	Ethereum	Public Permissionless	A blockchain-based decentralized network, that allows to store and trade data assets with enforcement of data usage rules.
Weeve [95]	IoT, Data Trading	IOTA, Ethereum, Hyperledger Fabric	Multiple Architectures	A blockchain-based decentralized platform to enable IoT data trading and establishment of Economy of Things.

authors also provide a possibility to settle the financial transactions on the blockchain by utilizing its on-chain currency. In [65] authors present a model for a blockchain-based decentralized IoT data trading marketplace. In their marketplace, authors enable the users to perform the full chain of trading operations, from the initial advertisement of the data to the final business settlement with payments delivered and legal contract signed. Authors claim, that usage of the blockchain smart-contracts enables initially non-trusted parties to conduct business settlements without third-party involvement providing a trade-off between transaction costs and data loss risks. Authors of [66] propose a blockchain-based decentralized marketplace for IoT data trading. In addition, the developers of Machine Learning (ML) solutions can collaborate within such a marketplace while using the IoT data for ML model training. According to the authors, usage of blockchain increases transparency and regulates access to the data traded within the marketplace. In [67] authors describe a DLT-based marketplace for IoT sensor data trading. The interesting part of the proposal is that authors use IOTA [24] distributed ledger as a data storage solution, while the overall marketplace is designed to be blockchain agnostic. Authors of [68] present a decentralized DLT-based marketplace designed to operate in the context of smart cities. According to the authors, their marketplace enables IoT devices data stream trading without the need of a trusted intermediary. Authors claim that IOTA's distributed ledger is IoT-tailored with emphasis on system's scalability and trust. In [69] authors propose a blockchain-based marketplace for IoT data trading. This particular model of the marketplace allows to search and trade IoT data based on the geographical location of the device. According to the authors, with blockchain technology, they are able to mitigate such issues as accountability and correctness of geographical data and provide a platform that allows buyers to create more location targeted IoT data searches. Authors of [70] propose a blockchain-based marketplace with the ability to trace application installation on edge IoT devices. According to authors, the blockchain technology brings transparency and accountability into application trading and installation processes. In addition, authors also employ Augmented Reality (AR) [87], in order to enhance user experience during the application installation. In [71] authors propose a blockchain-based marketplace model where machines perform full chains of tasks to supply manufacturers with needed parts. While all trading decisions are recorded on the ledger, machines execute selection and ordering of the parts with a final trading settlement recorded in smart contracts.

All aforementioned IoT data marketplaces proposals share a number of common goals that they pursue when applying blockchain technology. First, data privacy has to be preserved according to legal regulations. For example, European GDPR poses rather strict regulations on the rights of users to rectify or remove the data from the storage of specific service, e.g., marketplace. Thus, due to the immutability of the blockchain, any confidential data has to be stored off-chain with ledger storing only hashed references to real data locations. Second, due to the trust-enabling capabilities of the blockchain, it allows to eliminate the need for a trusted third-party and makes the data trading process more transparent and fair. The trade agreement conditions can be embedded into the smart contract and the contract itself can be executed automatically. It contributes to the value distribution balance since there is a possibility to reduce the price of smart contract execution in comparison to the involvement of third-party. Third, blockchain allows to securely store data access control policies which can be automatically enforced during and after trade settlement. Finally, the on-chain currency, i.e., token or cryptocurrency, enables automated payment release to the seller according to contract conditions.

3) E-Commerce: Blockchain technology has found an application in the area of e-commerce [88], [89] as well. It allows making marketplaces more democratic while acting as an instrument for distributed control over the users and merchants operating within the e-commerce platform. In [72] authors lay the foundation for e-commerce marketplaces based on Ethereum blockchain [27]. The common problems of today's marketplaces are in the lack of distributed instruments within the marketplace to make the trading process

transparent and efficient. Today's marketplaces, being centralized systems, may block merchants at will, being the only entity to decide on such action, and fully control the process of the financial settlement between the customer and merchant while taking a portion of the payment to itself. According to authors, the blockchain technology helps to mitigate these issues by making the marketplace decentralized, thus, removing a middleman in the financial settlement process, providing an ability for merchants to fully control the transaction process and conduct an audit of the data on an immutable ledger making the process transparent and secure. Authors of [73] present a blockchain-based marketplace for art trading. According to the authors, along with bringing such benefits of blockchain technology as transparency and data assurance of financial transactions, this platform also allows tracing the art assets owner and location history. Authors claim that their marketplace model is the first to address the task of art assets trading. In [74] authors approach the model of e-marketplace from the direction of the customer. They propose a blockchain-based e-commerce marketplace where customers make their orders and submit them to the platform. In turn, the suppliers make their bids on the order and compete with each other to fulfill it. The auction takes place on the blockchain which brings transparency and trust into the bidding process.

The e-commerce blockchain application contains a lot of similar goals which were described in the context of Smart Grids and IoT. However, the distinct feature of e-commerce blockchain-based marketplaces is the ability to provide fairness towards customers and merchants who operate within it. Since the data stored on a permissionless blockchain is open, all dispute resolution can be done in a transparent and fair way. Moreover, this distributes the merchants' or customers' blocking decision-making process, thus, removing authoritative control present in centralized e-commerce marketplaces. Also, the distributed blockchain storage permits indexation of products catalog, which makes search requests execution rapid and fair. Finally, the usage of blockchain in the bidding process makes it more transparent and tamper-proof.

4) Cloud Services: Blockchain technology is incorporated into Cloud Services [55] deployment as well. The blockchain allows to establish trust between different actors within the cloud infrastructure, thus, enabling trusted collaboration in multi-step computation tasks, e.g., ML pipelines execution training [57]. In addition, blockchain technology helps to bring transparency into the processes of cloud storage accounting and data assurance within a cloud infrastructure. In [75] authors present a blockchain-based decentralized marketplace where different actors can collaborate in the AI engineering process. The main asset that drives the AI applications development is the data on which the ML model is trained. With blockchain, authors make sure that data owners retain the ownership and privacy of the data while providing developers the means to access data for model training. The training algorithms are executed in the cloud infrastructure, where usage of permissioned blockchain allows to preserve the ownership and privacy of the data on the distributed computing resources. Authors of [76] present a model for a blockchain-based decentralized marketplace for online content. This model provides a tool-set to conduct data management and trading within the marketplace, without a need for a trusted intermediary. According to the authors, the novelty of the presented model is in a new content naming approach, which allows global indexing, thus, providing a mechanism for fast and transparent content search. In [77] authors present a decentralized blockchain-based marketplace for online content. The platform acts as an indexer, storing content listings and providing a mechanism to search and trade the content. In addition, the marketplace allows automatic payment to creators in case the content is bought. Blockchain technology allows performing the trading settlement without a trusted third party and enables transparent and fair content distribution within the marketplace. Authors of [78] present a blockchain-based marketplace model for Virtual Network Functions (VNFs) [96] hosting. The owners of VNFs do not necessarily have sufficient resources to host their function. Thus, it creates a demand for the platform where these resources could be found. The proposed marketplace allows VNF owners to submit their order, indicating what are the requirements towards the resources that are needed to run VNF. Infrastructure owners in turn, compete to fulfill the order by placing their bids, indicating the cost of VNF hosting. According to the authors, blockchain technology allows making such a marketplace easy to audit and eliminates the need for a trusted third-party. Also, such a marketplace brings together VNF developers and infrastructure providers, thus promoting the development and usage of VNFs. In [79] authors propose a blockchain-based brokering mechanism that is used to allocate and manage network slicing in a 5G network. Authors introduce a *slice broker* as a new entity to help construct network slices from the resources supplied by different network providers. According to the authors, blockchain technology brings enhanced security and privacy features without a negative impact on the performance of the slice broker. Authors of [80] describe a Blockchain-based trUsted VNF packagE Repository (BUNKER). According to the authors, a blockchain-based BUNKER allows verifying VNF package integrity without the involvement of a trusted third party. Moreover, the rights and obligations of VNF package acquisition can be described in the Ethereum Smart Contract, which eliminates the need for a trusted third party and allows to automate the final settlement process. In addition, blockchain technology incorporation makes the VNF repository tamper-proof, and brings such benefits as transparency, data provenance, and accountability. In [81] authors describe a blockchain-based catalog *ProtectDDoS*, where vendors of distributed denial of service (DDoS) protection software can post and sell their products. Moreover, the users of ProtectDDoS can receive recommendations on the type of protection according to their requirements. Authors also use Ethereum smart contracts in order to maintain the integrity of the data about available DDoS protections. Finally, the authors implement their concept and demonstrate that confidentiality and integrity features are maintained for all parties collaborating within the ProtectDDoS system. In [82] authors propose a blockchain-based marketplace model for AI API access selling. The proposed marketplace, allows data owners to expose their cloud-hosted APIs in a secure way, allowing AI

engineers to use ML models through the respective API. The novelty of this approach is that ML model exposure though API is distributed over several cloud infrastructures to secure the data from both cloud infrastructure providers and AI developers. Blockchain technology allows the distribution of API over multiple providers removing the need for a trusted centralized entity and making the system transparent and easy to audit. Authors of [83] present a model of a decentralized blockchain-based marketplace for Fog/Edge computing resources trading. Authors claim, that existing blockchain marketplaces while having decentralized components still partly rely on a number of centralized services. With their proposal, the authors show that the use solely of blockchain technology allows building a fully decentralized system while proving necessary functionality for marketplace operation.

In the context of cloud services, the application of blockchain technology has a number of common goals with the area of IoT such as data privacy and ownership preservation. However, within blockchain-based cloud services marketplaces, it is the infrastructure that is being the object of trade with the aim to host cloud-based services in it. Blockchain technology allows distributing the execution of the cloud-based service over several infrastructures, thus, protecting the data and services privacy and ownership. It can be also traced as a pattern, that the main goal of blockchain technology in all aforementioned application areas is the elimination of trusted third-party in the trading settlement process. In cloud services, blockchain smart contracts allow trading cloud infrastructure resources, as well as cloud-hosted data and services without an intermediary, allowing automation of settlement process and making it more transparent, time-efficient, and error-proof.

5) Industrial Proposals: There has been a number of industrial proposals and initiatives to apply blockchain technology to digital marketplaces. The majority of the proposals aim to implement a solution that will become a foundation for blockchain-based marketplaces mainly in areas of cloud services and IoT. In [90] author details the implementation of a prototype of decentralized marketplace using Hyperledger Fabric [29]. According to the author, smart contracts, while being the important technology for a marketplace implementation, are only a fraction of the functionality needed to build a functioning decentralized marketplace. The author claims that in private permissioned blockchain, in order for the participants to trust marketplace's operations each participant has to maintain at least one blockchain network node which hosts the ledger and smart contracts. Otherwise, there is no possibility to verify the validity of data operated by the smart contract, and trusted relationship on the blockchain can not be established. In addition, the author details requirements for decentralized marketplace implementation along with argumentation towards the design decisions made. Authors of [91] describe a decentralized marketplace called *Wibson*. The marketplace acts as a stage where the data is exchanged for tokens. The distinct feature of Wibson marketplace is that it uses an additional entity, called a notary, in the transaction settlement process. The notary is the data authenticity verification authority and acts as an intermediary in the transaction process. When the notary verifies the data, an encrypted copy of it is sent to the buyer. Further, after the funds are released to the seller, the data decryption key is sent back to the buyer. According to the authors, usage of blockchain technology and the introduction of the notary makes the data trading process fair, transparent, and secure. In [92] the author describes a decentralized marketplace infrastructure provider, called *XBR*. The main author's argument is that nowadays the data is collected and stored in a centralized manner, which limits the opportunities for potential buyers, i.e., developers, to find and purchase the necessary data. Thus, the main aim of XRB is to develop the infrastructure which allows rapid, secure, and on-demand decentralized marketplace deployment. According to the author, deployed marketplaces are designed to perform trading operations with the help of blockchain smart contracts and provide a needed level of data privacy and security in a given data context. The author of [24] describes the main principles of new distributed ledger called *IOTA*. It uses a new data structure based on DAG called *Tangle*. In IOTA, transactions do not have fees, thus, eliminating the need for the mining process. The DAG itself is structured in a manner different to the blockchain, thus, there no blocks or resulting blockchain. According to the author, IOTA solves such challenges of the public blockchain networks as scalability and privacy. Thus, as the main application area for the IOTA ledger is IoT, it enables high throughput of transactions as well as preserving data privacy within the IoT data marketplace. In [93] the authors introduce decentralized marketplace called *DataBroker DAO*. The main aim of the marketplace, according to the authors, is two-fold. Firstly, it aims to provide a transparent and secure way for IoT data owners to sell their data. Secondly, it aims to implement a decentralized marketplace where data consumers can easily find and buy required IoT data. According to the authors, such a marketplace enables new data usage scenarios and business opportunities such as smart city initiatives and governmental services enhancement. Authors of [94] describe a blockchain-based decentralized network called *Datum*. Datum allows secure storage of the data on the blockchain. For the purpose of data monetization, the DAT smart token is used as a currency in trading operations. The distinct feature of the Datum network is that it records data sharing rules established by the owner in a smart contract, and automatically enforces them during the trade process. Data sharing rules determine groups of entities, with whom data can be traded and access shared. In [95] authors present blockchain-based decentralized marketplace platform called *Weeve*. The main aim of the platform is to enable the deployment of transparent, secure, and scalable marketplaces for IoT data trading. The distinct feature of Weeve platform is that all IoT data is testified, i.e., before being traded, data properties and validity are verified by the marketplace. According to the authors, with their platform they want to transform IoT data trading into Economy of Things, where data is traded transparently, fairly, and with reasonable pricing.

As can be seen from both academic and industrial proposals, there is a number of common goals that all aforementioned areas share in the context of blockchain-based marketplaces. However, each application area requires some specific service, e.g., dynamic energy price regulation, or system characteristic,

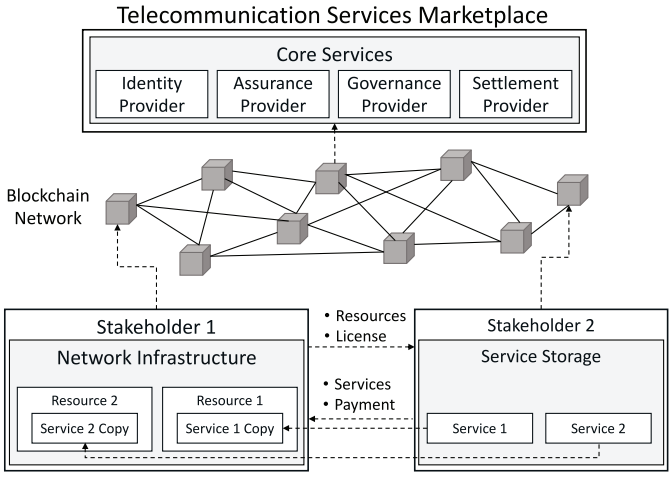

Fig. 7. Telecommunication Service Marketplace.

e.g., GDPR compliance, which poses additional requirements to the blockchain system in terms of architecture, privacy-preserving capabilities, and trust.

F. Telecommunication Service Marketplaces

The applications and services in centralized AM and CSM typically do not span over several different governing entities. Thus, they do not introduce issues to build trust and automate business processes, since they are controlled in a centralized manner by one entity that acts as a trusted intermediary. However, in decentralized systems, where multiple non-trusting actors collaborate, a trust-enabling mechanism is needed for business settlement automation. The blockchain-based marketplace proposals discussed in Section III-E describe multiple application possibilities for blockchain technology, allowing us to reduce or completely eliminate the need for a trusted intermediary. In this work, we aim to extend the blockchain-based marketplace concept to *Telecommunication Services Marketplace* (*TSM*) that integrates multiple services offered by different CSPs. A structure of TSM is shown in Fig. 7. The idea behind the TSM is to make sure that there is a common set of processes that all actors who collaborate within the marketplace can rely on to establish their business relationship, without the need of a trusted third-party. In order to provide these processes, the following core services of the TSM must be established: *Identity Management, Assurance, Governance* and *Business Settlement* [97]. The core services provide fundamental functionality for TSM operation and give users the ability to conduct business transactions in an automated manner. Due to telecommunication services being governed by different CSP it is essential to establish trust between CSPs within TSM to make automation of business transactions possible. In this case, automation and trust are achieved with the incorporation of the DLT into the core services of the TSM. With the distributed and immutable storage of DLT, every TSM participant can hold a synchronized copy of the ledger, and execute business transactions with blockchain smart contracts. With all core services established, a range of telecommunication services chains, *i.e., wholesale voice settlement, data on demand* or *mobile roaming*, can be decomposed into separate services, and provided within the TSM for CSPs. In turn, TSM is built to provide interoperability of core services with existing systems, e.g., blockchain-based self-sovereign identity management systems. In this way, we can maximize the inclusiveness of the TSM and conduct standardization activities to provide a unified way for companies to connect to TSM. For demonstration purposes we describe the next use-cases where such business settlement is involved.

SLA Settlement Use-Case Scenario: You are an innovative Virtual Reality (VR) [98] service developer. You have developed a new VR service that allows the users of your service to perform conference calls where they can see their conversation partners in full height and the figures of people can have premodeled face of a real person visible in VR [3], [99]. As a demonstration of the capabilities of your VR service, you have organized an event with 40 participants that takes place in two different physical locations. The participants will be brought together in a VR where they will have a possibility to break the barrier of distance by appearing near each other in the digital world. The VR services, especially on such a large scale, transfer multiple gigabytes of data per second since different types of information are transmitted live: video, audio, location in a digital meeting, rendered face mimics, etc. For your event, you need an underlying network infrastructure that supports the communication requirements of the event. From a financial standpoint, you have no reason to buy all the network hardware, hence, you need to find an alternative. Such network infrastructure is owned by the local network provider, i.e., CSP, which has the capacity to arrange the transmission of such high volumes of data per second, but none of the conventional billing plans covers the necessary network capacity. Ordinarily, you would need to go to the CSP and arrange the allocation of the network infrastructure beforehand. In such a case, the business settlement of the transaction would require the signing of an SLA involving a trusted third party, and possible additional costs and preparation time for the CSP if this is the first time that such a business transaction takes place. In contrast to manually executed, expensive and time-consuming [9] business settlement, i.e., signing of SLA, described above, TSM allows you, as a VR developer, to find and rent the needed network infrastructure via the marketplace. The CSP is a supplier of infrastructure registered in the marketplace. The rental procedure of the required network infrastructure would be settled without involving a trusted third party, but via smart contract execution on the underlying blockchain P2P network. A ledger provides a distributed root of trust which is a key component of the automated business settlement. The governance of the system is distributed over the decentralized network of blockchain nodes who participate in the marketplace's maintenance. The assurance of QoS of the supplied services or the infrastructure is recorded in the smart contracts as an SLA and works as an obligation of the supplier towards the consumer [14].

Inter-CSP Settlement Use-Case Scenario: You are a small cell provider (SCP) that has entered a cellular market. As you just begin to establish yourself on the market, you have a

TABLE III
SUMMARY OF STANDARDIZATION ACTIVITIES IN THE AREA OF TSM

Name	Area	Leader	Goals
Communication Business Automation Network [9]	Communication Service Provides	ITW Global Leaders Forum	An introduction of a standardized framework to make the process of business settlement automated, real-time, and trusted between two or more CSPs.
ETSI ISG PDL [100]	Permissioned Distributed Ledger	The European Telecommunications Standards Institute	A summary of standardization activities and research proposals on activities that have been done in the area of Permissioned Distributed Ledger.
Global System for Mobile Communications [45]	Mobile Operators	GSM Association	An analysis of the opportunities for the blockchain smart contracts to be used to record the agreements between operators, while using cryptocurrencies for business settlement.
TM Forum Catalyst [44]	Communication Service Provides	TeleManagement Forum	Construction of a federated CSPs marketplace where network infrastructure can be shared flexibly and securely in an automated way.

limited network infrastructure as your customer base is still growing and revenue has not been generated yet. For your brand to grow, the coverage area and data plans have to be attractive for the customers to be competitive in the market. Since your investments are limited, the resources of your own network infrastructure may not be sufficient to meet the standards set by your competitors. Thus, you need to reach out to a large MNO, which has extended cellular network coverage, to rent additional network infrastructure on a long- or short-term basis. In this way, you can obtain the ability to grow as a cellular network brand by expanding over the areas of interest of your potential customers and generate new revenue by the increased customer base [15]. According to the current process of business settlement, you as an SCP need to contact every MNO available in your area and conduct negotiations on the terms and conditions of the agreement. The current process of such an inter-CSP transaction contains a portion of manually executed parts, which can be expensive and time-consuming. Also, the need for human intervention in the process may lead to manual errors and exposure to fraud. The TSM would enable you to review the network infrastructure options proposed by all the MNOs that are available in the area in a rich Web and application interface, with the blockchain technology allowing you to automate the final settlement. The terms and conditions can be recorded in a smart contract providing legal context, with the blockchain bringing data assurance and trust into the business settlement process without a need for third-party involvement.

The described use-cases are aimed to demonstrate the telecommunication industry blockchain applicability in situations where a trust-enabling technology is needed to enable process automation. With it, the creation of TSM would provide a platform for such processes to execute, in addition to the definition of the place where interested customers and CSPs can meet to enable new business opportunities.

G. Standardization Activities

Recently, a number of standardization activities have been conducted in the area of TSMs. These activities are aimed to present a set of well defined interfaces and processes which will help relevant parties in the industry to enable new business opportunities and collaboration models. Table III provides a summary of standardization activities included in this paper.

CBAN: Communication Business Automation Network (CBAN)[7] was launched by the ITW Global Leaders Forum ("GLF") and it is targeted to develop a platform which provides a set of core services to accelerate business settlement between different CSPs. The main premise to start this standardization activity is that nowadays business settlement process involves a mix of automated and manual activities. Manual activities are the results of involvement of a trusted third-party which acts as a trust anchor on behalf of participants of business settlement process. As far as manual activities involve human intervention, they are a subject of multiple issues: manual errors, long payment cycles, and exposure to fraud. The introduction of standardized framework for business settlement will make this process automated, real-time and trusted between two or more CSPs. The development of new telecommunication services will be also accelerated making them interoperable, while increasing integration ability of new services with legacy systems [9].

In order to achieve settlement automation, CBAN employs the DLT. By standardizing DLT technologies which are used for core services CBAN makes the platform inclusive and interoperable. Also, due to DLT's distributed nature, it enables the possibility to avoid trusted third-party, thus, opening an opportunities to a full automation of business settlement process. Additionally, CBAN defines a TSM reference architecture [97], where minimum functionality and core services for the TSM are described.

CBAN initiative plays a number of roles in development of new unified approach to business settlement. First, CBAN governs the adoption of technological standards in order to guarantee interoperability between all participants of CBAN network. Second, CBAN governs the network of participants by maintaining participants registry. Lastly, CBAN coordinates all developments of new architectures and services within the CBAN network.

ETSI ISG PDL: The European Telecommunications Standards Institute (ETSI)[8] is an independent organization

[7]https://www.cban.net/
[8]https://www.etsi.org/

TABLE IV
ADVANTAGES OF DECENTRALIZED BLOCKCHAIN-BASED MARKETPLACES VS. FEATURES OF CENTRALIZED MARKETPLACES

Core Service	Features of Centralized Marketplace	Advantages by Decentralized Blockchain-based Marketplace
Identity Management	• A centralized authority manages a single identity database setup. • Centralized authority represents a single point of failure. • Restricts interoperability and reusability of digital identity.	• A decentralized network of nodes managing identity information, which protects from a single point of failure. • Enables reusability and interoperability of identity. • Enables users full control over the identity information.
Assurance	• Data assurance is provided by the centralized authority. • Inability to inspect the marketplace by external parties, *e. g.*, producers and consumers. • Possibility of violations by the marketplace, *e. g.*, unfair commission on consumer payments.	• Data assurance is provided by the immutability and transparency of the decentralized blockchain. • Blockchain's immutability ensures that the data smart contract operates on is valid. • Transparency of operations for collaborating parties.
Governance	• Governance is performed solely by the marketplace operator. • All decisions are made within the centralized authority.	• Decentralization of governance within the system actors. • Increased automation, democratization, and time-efficiency of the governance activities.
Business Settlement	• Business settlement is executed and controlled by a central authority, which acts as a trusted third party. • May result in value distribution imbalance, as the marketplace may dictate billing rules and payments distribution.	• Smart contracts eliminate the need for a trusted third party. • Ability to verify the validity of the smart contract data. • Fair value distribution due to trusted, transparent, and automated business settlement.

which performs standardization activities in the area of communications. In their recent document [100], exploring the global trend, ETSI have made a taxonomy of activities which have been done in the area of Permissioned Distributed Ledger (PDL). The document contains both standardization activities and research proposals. The main aim of the document is to identify applicable solutions, and provide enhancements and recommendations on the way forward.

GSMA: Global System for Mobile Communications (GSMA or GSM Association)[9] is an organization which represents mobile operators on a worldwide arena. In their report [45], they have analyzed the opportunities which may be enabled by the blockchain technology in the area of business settlement for Mobile Operators. In this scenario, according to GSMA, smart contracts can be used to record the agreements between operators, while using cryptocurrencies for business settlement. The governance over a blockchain network is achieved by managing the network and smart contracts definition together, with the requirement that all parties agree on the contract revision. Also, since call data records (CDRs) are digital, they can be recorded on the ledger. Due to ledger's distributed nature, different operators connected to blockchain network can verify all CDRs in a trustworthy manner.

TM Forum: TeleManagement (TM) Forum is an association for CSPs in the telecommunication industry sector. With the recent initiative called *TM Forum Catalyst* their aim is to build a federated CSPs marketplace. The main premise of the initiative is that CSPs nowadays need a mechanism to share their network infrastructure flexibly and securely in an automated way [44]. With the rise of 5G and an increasing number of IoT devices, such a mechanism can enable new ways for revenue generation and stimulate business growth. Thus, TM Forum employs DLT to define such a federated CSPs marketplace. DLT acts as a main trust-enabling technology, which enables transaction execution and value exchange between different actors within the marketplace. The business settlement agreement can be recorded in the smart contract and the settlement process itself can be automated and executed in real-time. In addition, DLT provides an audit infrastructure in the form of distributed immutable data storage providing a transparent way for all involved parties to verify any data operated by the smart contracts. Consequentially, the number of disputes can be reduced, due to the transparency and trustfulness of such a blockchain-based marketplace [101].

In [44], TM Forum specifies the high level architecture design as well as roles which are needed for minimum viable ecosystem establishment. Also, they define the value distribution mechanisms along with assurance and governance services description. Further, they describe APIs required for marketplace operation. Finally, they identify a number of challenges in federated CSPs marketplace implementation that TM Forum Catalyst initiative will explore in future.

IV. BLOCKCHAIN IN TELECOMMUNICATION SERVICES MARKETPLACES

Having introduced the concept of the TSMs in Section III-F, here we survey and elaborate the concepts and core services that comprise TSM. A basic set of necessary functionality for the TSM was outlined by CBAN [97]. It comprises the four core service *Identity Management, Assurance, Governance* and *Business Settlement*. We focus on this group of functions since it represents an agreed amount of functionality by the current telecommunication industry (operators and manufacturers). In addition, Table IV provides a condensed view of the advantages of using TSM core services in the context of a decentralized blockchain-based marketplace as compared to their use in a centralized marketplace. The emphasis is on characteristics that lead to more democratic and robust services. The aim of the table is to provide an underlying basis such that the details of core services can be quickly understood. These core services are discussed in detail next.

A. Identity Management Service

The discussion on the identity management (IdM) service models is built in a way that shows the development and evolution of IdM systems derived from [26]. The evolution of

[9]https://www.gsma.com/

TABLE V
PROPOSALS TAXONOMY ON BLOCKCHAIN-BASED IDENTITY MANAGEMENT SERVICES

Reference	Application Area	Platform	Architecture	Description
T. Zhou et al. [105]	Self-Sovereign IdM	Ethereum	Public Permissionless	An IdM which uses smart contracts and is capable of merging different user identities under one unique identifier.
Y. Liu et al. [106]	Self-Sovereign IdM	Parity [107]	Public Permissioned	An IdM system architecture with guidelines for efficient usage of design patterns for data security and system scalability improvement.
H. Gulati et al. [108]	Self-Sovereign IdM	Not Applicable[1]	Not Applicable	An IdM scheme for a dynamic digital identity with the usage of blockchain technology.
Z. Cui et al. [109]	Self-Sovereign IdM	Hybrid blockchain model[2]	Multiple Architectures	A mutual authentication scheme for IoT nodes in Wireless Sensor Networks (WSN).
R. Soltani et al. [110]	Self-Sovereign IdM	Hyperledger Indy [111]	Private Permissioned	An IdM framework where authors aim to address the privacy requirements described in GDPR [86].
A. Othman et al. [112]	Self-Sovereign IdM	Not applicable[3]	Not Applicable	A novelty decentralized authentication method based on blockchain technology and SSI principles with the usage of DIDs.
R. Soltani et al. [113]	Self-Sovereign IdM	Hyperledger Indy	Private Permissioned	A key recovery solution that is based on SSI concepts and blockchain technology.
S. K. Gebresilassie et al. [114]	Self-Sovereign IdM	Tangle	DAG-based	A novel approach for IoT devices IdM based on DIDs, IOTA's Tangle DLT, and SSI principles.
M. P. Bhattacharya et al. [115]	Self-Sovereign IdM	Hyperledger Indy	Private Permissioned	An evaluation of blockchain-based IdM system's security against sensitive data leaks and man-in-the-middle attacks.
uPort [116]	Self-Sovereign IdM	Ethereum	Public Permissionless	An implementation of an IdM system that provides self-sovereign identity to users and organizations.
Sovrin [30]	Self-Sovereign IdM	Hyperledger Indy	Private Permissioned	An implementation of an IdM system which transitions the responsibility for identity information from traditional centralized identity to the identity holder.
Z. Zhao et al. [117]	User-centric IdM	Ethereum	Public Permissionless	A user-centric blockchain-based IdM model which allows users to control their identity information.

[1] No implementation available.
[2] The model assumes usage of hybrid public and private blockchains, but no implementation is available.
[3] No implementation available.

IdM models in the history of computing systems and services development helps to realize the problems that each new IdM model solved or introduced. Also, it helps to avoid identified problems in newly designed IdM models. Finally, a number of scientific and industrial proposals on blockchain-based IdM models are discussed, *c.f.* Table V.

IdM service combines all needed operations which are required to create and use a digital identity within a computing system. Digital identity is a requirement for any system where the target is to exchange data in a secure and accountable way. Traditionally, with the developments of network services architectures, the first IdM models were designed around the concept of centralized systems. In such a system, one centralized trust authority is set up to provide identity services for all users within a single service domain [102]. Since there is only one entity that provides identity services, it is usually protected by perimeter-based defenses, e.g., firewalls, IDS, and IPS. However, this implies that there is a central point of failure in the centralized IdM model with only one target to penetrate which frequently results in breaches and digital identity theft. In addition, the disadvantage of the centralized IdM model is that while identity can be used within a single domain, it cannot be reused in the context of another centralized IdM system. The further development of IdM to federated models enables the use of cross-domain identity. The IdMs which implement a federated model are called Single Sign-On (SSO) systems [103]. In the SSO model, the users are not bound to a single domain anymore, thus, the IdM system provides the ability to use the same identity to log-in to different services. The disadvantage of the federated model is that in a process of authentication, the user is still redirected to a home identity provider [26].

As an evolution of federated IdM, user-centric IdM systems allow users to use their identity across different domains without being bound to a home identity provider. In this case, a user takes control over personal identity data, and the home identity provider asks permission to release identity data to different IdM services for authentication. A Stork IdM initiative [104] applied this IdM model in the context of the European Union (EU) where users can authenticate in governmental services of different countries with the same identity. Although user-centric IdM is an advancement towards more flexible and usable identity management, it still has a number of disadvantages. Despite user-centric identity being used across different domains, it is still stored on a server-side, i.e., in centralized storage, and performs server-side authentication [26].

In contrast to previously described approaches, IdM systems based on a Self-Sovereign Identity (SSI) [118]

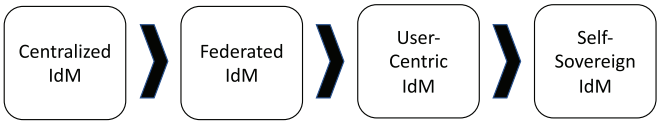

Fig. 8. Identity management models development.

are aimed to enable users' full control of their identity data. During online authentication, users can determine the amount of identity data released to authorizing party without a need for a centralized entity that stores identity data and which is placed in the middle between the user and the service. Users transitioning from the role of data subject to the data controller and manage their identity data directly determining ways in which data is being processed. The detailed path towards the Self-Sovereign Identity Management model was described by Allen in [119], where ten core principles of SSI are defined: Existence, Control, Access, Transparency, Persistence, Portability, Interoperability, Consent, Minimalization, and Protection. The progression of the IdM models from centralized to SSI is depicted in Fig. 8.

Nowadays, SSI is moving from a conceptual model to implementation in industrial solutions with the help of blockchain technology. In [120], the author describes the main advantages and disadvantages of blockchain incorporation in the implementation of the SSI. Additionally, the author provides a description of the SSI model where blockchain is used as a central technology. According to the author, the novelty of the paper is in bringing multiple opinions on the advantages and disadvantages of the SSI model from both academic and industrial representatives, where a road ahead is defined in the development of SSI. Authors of [105] propose an SSI framework based on the Ethereum blockchain, named EverSSDI. It uses smart contracts saved on the ledger, which merge different user identities under one unique identifier. With it, authors try to solve the identity information fragmentation problem by integrating into the proposed framework the Hierarchical Deterministic protocol [121]. This protocol allows the creation of cryptographical keys in a hierarchical structure, i.e., to derive child keys from a parent key. According to the authors, the implementation solution allowed to demonstrate that the system allows the users to become single owners of their identity. In [106] authors identify and discuss critical components of the SSI system such as keys, identifiers, and credentials. Also, the authors provide an SSI-centred system view and guidelines for efficient usage of design patterns for data security and system scalability improvement. Finally, the authors present their platform's architecture and evaluate their proposal denoted as design pattern as a service (DPaaS). In [108] authors propose a scheme for a dynamic digital identity maintained with the help of blockchain technology. The proposed scheme makes use of biometric information in combination with other identity information that is being recorded on the blockchain with the consideration that it may evolve over time, i.e., being dynamic. According to the authors, building a chain of dynamic identities recorded on the blockchain allows verifying previous identity operations up to the initial identity, i.e., the origin. In [109] authors propose a mutual authentication scheme for IoT nodes in Wireless Sensor Networks (WSN). Authors propose the usage of a hybrid blockchain network where cluster head nodes authenticate themselves on a global public blockchain and lower level IoT nodes are authenticated on a local private blockchain. According to the authors, the advantage of such a system is the control of local areas in the IoT network by enforcing private blockchain participation restrictions. In [110] authors employ a Hyperledger Indy [111] to their proposed identity management framework based on principles of SSI. With their proposal authors aim to address the privacy requirements described in the GDPR. In [112] authors employ the blockchain technology and SSI principles to propose a novel decentralized authentication method called *Horcrux*. According to the authors, the advantage of their protocol is in relying on the Decentralized identifiers (DIDs) [122], [123], which enable a decentralized identity implementation and remove the single point of compromise in the identity verification. In [113] authors provide a key recovery solution that is based on SSI concepts and blockchain technology. According to the authors, the solution can recover decentralized keys and uses Shamir's secret sharing scheme and Hyperledger Indy as a blockchain solution. In [114] authors employ DIDs, IOTA's Tangle DLT, and SSI principles to introduce a novel approach for IoT devices IdM. According to the authors, having analyzed the scalability and performance of blockchain-based DLTs, they came to the conclusion that it is not the best option to choose in the context of IoT IdM. With these considerations, authors employed IOTA's Tangle DLT which is DAG-based and fundamentally focuses on IoT, and, according to authors, shows better scalability and performance. In [115] authors discuss Hyperledger Indy based IdM system which employs SSI principles. In their study authors evaluate the IdM system's security against such security risks as sensitive data leaks and man-in-the-middle (MITM) [124] attack. Based on the evaluation, the authors propose to mitigate MITM attacks by encryption of DIDs before sending them to a verifier, to ensure the confidentiality of the data. Also, in terms of sensitive data leaks, the authors propose a sensitivity score model based on DID's attributes to evaluate the risks of sharing a particular portion of personal data.

From the industry side, a number of solutions have been presented in recent years. *uPort* [116] is an industrial open-source IdM system that targets both individual users and organizations to provide them with a blockchain-based self-sovereign identity. Identity itself is implemented as an Ethereum smart contract that serves as a digital identifier. An interesting characteristic of the uPort IdM systems is the ability to perform the identity operations both on- and off-chain. Authors of [125] provide an assessment of the advantages and limitations of uPort's efficiency and architecture. Also, the authors implement a Decentralized Application (DApp) [126], [127] based on the uPort IdM system to evaluate its operational capabilities, scalability, and efficiency. Lastly, the authors discuss the advantages and disadvantages of the uPort IdM based on the evaluation. uPort was compared to another emerging industrial IdM system called *Sovrin* [30]. The Sovrin was introduced by Sovrin Foundation as an IdM system that transitions the responsibility for identity information from traditional

centralized identity to the identity holder and allows individuals to make decisions on how their personal data is processed and disclosed. According to the Sovrin Foundation, this transforms the interaction between identity holder and verifier, enhancing the user's control over the use of their personal information. For a more detailed read on blockchain-based IdM systems that employ SSI principles, the reader is referred to [128].

Blockchain technology is not only applied to IdM systems that follow the SSI model. In [117] authors build a user-centric decentralized IdM which is based on smart contract technology. According to the authors, such IdM allows users to take full control over their identity and make decisions on which third-parties can obtain access to their identity information. In order to preserve identity anonymity authors support an attribute-based authentication scheme, additionally supporting an attribute reputation model, which, according to authors, preserves the user's identity trustworthiness in a decentralized system. For a more detailed read on blockchain-based identity systems, the reader is referred to [49].

Lessons Learned: Blockchain technology opens opportunities for IdM systems enhancement. It allows the conceptual model of SSI to be implemented with help of DLT and blockchain smart contracts. Blockchain-based SSI systems enhance user sovereignty and allow making the identity management process decentralized and secure. Further, blockchain-based SSI allows combining different types of identities, e.g., biometrics, identity attributes, and DIDs, allowing users to not be bounded to a single authentication technique. Also, distributed ledger allows making the user identity dynamic, enabling it to evolve over time while still having access to older identities which preserves identity operations accountability. Moreover, these IdM systems allow to completely eliminate the use of centralized storages of identity information, thus, protecting from a single point of failure, breaches, and identity theft, associated with centralized approaches, and allowing user's full control over personal information.

In the context of TSMs, blockchain-based SSI enables the inclusiveness of the marketplace, giving the ability for willing CSPs to seamlessly connect to TSMs' infrastructure and conduct business settlement within it. Digital identity can be applicable over different blockchain networks which would allow seamless and fast integration of blockchain-based IdM systems of an interested CSP into a TSM. However, it is important that blockchain-based IdM systems, whether they follow SSI principles or not, are implemented according to a unified standard which would make IdM systems interoperable and easy to integrate.

B. Assurance Service

The *assurance service*, i.e., data assurance, in any computational system, especially where financial operations take place, is essential to establish a trusted relationship between multiple parties. Data provenance is one of the key factors in data assurance, which is defined as information about data's origin, modifications, and storage. In centralized systems, trusted storage of information is present, which acts as an assurance guarantee towards collaborating parties. All operations take place on a centralized server where the data is processed, verified, saved, and accounted for. Thus, the system has the ability to assure the data provenance, under the condition that collaborating parties trust a central authority. With the introduction of decentralized environments and cloud-native service development methodology [129], it has become possible to distribute the processing of the data over several microservices, each performing a certain type of data manipulation, e.g., encryption, anonymization, and storage. In the case of the entire system being managed by one operator, the assurance level still can be maintained since one governing authority is used. However, when the data assurance has to be ensured among several initially non-trusted parties, a number of challenges emerge in ensuring the data provenance and validity in today's decentralized environments [130].

Blockchain technology with its distributed immutable storage may help to solve the issue of providing data assurance in decentralized systems. The immutability of the distributed ledger serves as an assurance that stored data has not been changed and has the original ancestry. The transaction validation and consensus protocols prevent anybody on the blockchain network from flooding the ledger with unverified information, which ensures data validity and provenance. Furthermore, on-premise data auditing is possible for all collaborating parties, due to the ledger's distributed nature, i.e., each party holds a copy of the entire history of blockchain. With the introduction of private blockchain architectures, stakeholders can control who enters the blockchain network, thus, preventing outside adversaries from tampering with the blockchain. Finally, having data assurance established, opens new opportunities for digital assets management in a trusted decentralized blockchain-based environment [3].

Several research efforts have investigated the ability of blockchain technology to enhance data assurance in distributed systems. The question of data provenance becomes more and more important for customers, amplified by the use of supply chains that make it increasingly more challenging to know the exact source from where the product came from. In [131] authors present a blockchain-based framework that increases products' provenance knowledge. In their work, authors conclude that with the blockchain incorporation overall system data assurance is increased with a reduction of the risks of failing to obtain original products provenance. In [132] authors propose a framework that collects the information about the interaction of supply chain participants and shares it among them. According to the authors, their system helps to monitor the product provenance and bring transparency to supply chain participants and end customers.

The issue of data assurance is present as well in every field where any kind of personal data is flowing. In [133] authors discuss data assurance related to Big Data [134] and Healthcare [135]. Data assurance and security are discussed in general, and how the incorporation of blockchain technology can improve the system characteristics in both areas. In the discussion, the authors claim that Big Data users can benefit from the immutability of the blockchain as it puts the power to ensure data provenance into users' hands. Also,

smart contracts can be the provenance guarantee of the data resources present on the blockchain. In Healthcare, the storage of the patients' medical data has to meet strict confidentiality requirements. In [133], authors discuss another proposal from [136], where storing of patients' data on the blockchain is described. According to the authors, this would benefit data assurance in comparison to the usage of cloud infrastructure for the same task. However, direct storage of personal data on the blockchain brings a number of challenges due to ledger immutability and GDPR restrictions. With these considerations, authors of [137] develop a framework for personal and confidential data sharing with respect to GDPR regulations. In the GDPR, the roles and responsibilities of the data controller and data processor are strictly defined and any violations may be subject to punishment. While blockchain immutability brings benefits to the data provenance, GDPR requires the system to give users the possibility to modify or remove personal data. This is why the authors propose to record the data access actions of the data controller in the smart contracts on the blockchain, while the data itself is stored and processed off-chain. In this way, the data processing contracts are recorded on the blockchain along with the location of the data itself. This enables data access withdrawal from the controller in case of any violations and makes data removal possible, while the provenance of the contracts is guaranteed by the immutable ledger.

In the area of cloud infrastructures, data assurance is being enhanced with blockchain technology as well. In [138] authors propose a hybrid system whereby a cloud server along with the blockchain is used for the assurance of data provenance in drone communication. The direct communication channel is established between the drone and the cloud server, where for each record stored in the cloud a blockchain receipt is generated for communication data assurance and enhanced auditing. The authors of [139] propose to use a dedicated blockchain to store the provenance data of the objects stored in the cloud. The system called *ProvChain* collects and verifies the provenance data and securely stores it on the blockchain. According to the authors, usage of a dedicated blockchain makes the provenance data tamper-proof, reliable, and enhances data accountability. In [140] authors propose a similar system, where they employ cloud storage, InterPlanetary File System (IPFS) [141] and Ethereum blockchain. While the data is being saved in cloud storage, the data provenance assuring records are saved in the IPFS. While being saved in IPFS, a hash is being generated from every provenance record and saved on the Ethereum blockchain. With the implementation of the system, the authors also show the performance and scalability analysis results, along with the simulation of a provenance data modification attempt. The authors of [142] went a step further and proposed a system that automatically compensates the party whose rights were violated. In case of any SLA disagreement from the side of the cloud infrastructure provider, the Ethereum-based system automatically repays the agreed amount of compensation.

Lessons Learned: Data assurance is of high importance in decentralized computing systems where non-trusting parties collaborate with each other. In particular, data provenance and validity are the main assurance characteristics that define the overall level of trust in the *assurance service* of the system. Current centralized systems provide data assurance as a central silo of trust, but still are vulnerable due to being a single point of failure. In decentralized systems, we can benefit from blockchain incorporation by exploiting its immutable storage as well as smart contracts programmability and flexibility. However, we need to take into consideration private data regulations if personal data is being processed in the system. For example, the immutability of the blockchain, while being beneficial for accounting, collides with GDPR's requirements for the user to have the right to remove or modify the personal data, stored in the system. As can be seen from the surveyed proposals, it is manageable with hybrid solutions, where blockchain stores only a hashed reference to real data.

From a TSM perspective, a blockchain-based assurance service allows formerly non-trusting parties to meet on the TSM's platform and conduct business settlement in a trusted manner. In this way, the data assurance, i.e., provenance, and validity are ensured by the distributed immutable ledger. Moreover, new opportunities are opened for TSM participants in business operations accounting and computational assets management.

C. Governance Service

Without an established *governance service*, the system's stability and operational ability may be compromised. The governance service denotes an entity or a consortium, i.e., number of entities, which performs an orchestration of the system, i.e., makes decisions on how the system is operated and maintained. In addition, the governor of the system makes the decisions on system architectural and functional changes, performs standardization activities, and decides which existing industry standards should be adopted [9].

In centralized systems, governance is concentrated within one entity. All decisions are made within the central entity's boundaries, and any discussions with the system's users have a recommendatory character, as the final decision is up to central authority [143]. While the centralized governance allows the taking of fast decisions, as no multi-stakeholder discussions have to be held, it may be inefficient in the adoption of new technologies, be slow in the transformation of its internal systems to meet requirements of next-generation Internet, and become a platform for the creation of a monopoly. With the shift towards decentralized systems, the governance becomes distributed over several entities with equal decision-making power. From a business perspective, every party presents its own interests which may collide with the interests of other governing bodies. Ultimately, it leads to the decision-making process becoming more time-consuming since all governing bodies have to come to a verbal and legal consensus, but contributes to the system's democratization and trust enhancement, and may be beneficial for the information technology industry's positive transformations. Blockchain technology incorporation has introduced new opportunities in decentralized systems governance development.

From a technical perspective, depending on the architecture of the blockchain, a pool of governing entities may be open or

restricted. The Bitcoin cryptocurrency, which has public permissionless architecture, originally was designed to be an open system with unprecedented democracy where the blockchain is governed by all nodes participating in the transaction verification, i.e., mining, process [7]. In practice, due to PoW consensus protocol, the governance of the system is performed by less than 10 nodes which maintain the majority of the hash rate produced in the network [144]. Considering such a consequence of PoW protocol operation, this started a number of initiatives that resulted in private blockchain architectures. The Hyperledger Fabric is designed as a permissioned system and enforces so-called private governance, which restricts the number of consensus participating nodes, thus, leaving the governance power within this group. The private blockchain governance is suitable for organizational deployment since it has better privacy-preserving characteristics and is better suited to address business needs [145].

From a legal perspective, the governance over blockchain-based decentralized systems depends on the architecture of the blockchain as well. In a permissioned blockchain, it is done by the consortium of organizations that operate and maintain the computational system, whereas in the permissionless blockchain it is all or a certain portion of the mining community. In [146] authors propose a theoretical framework to describe governance in the blockchain networks. The framework consists of six governance dimensions and three governance layers. They divide the whole governance process into the actions which happen on-chain and off-chain, thus, splitting technical and legal perspectives. The introduced governance dimensions are aimed to describe different aspects of blockchain operation and how they should be dealt with on different governance layers. Authors of [147] examine the history of decisions made by governing entities in Bitcoin and Dash [148] cryptocurrencies from both legal and technical points of view. In Bitcoin, the implemented governance mechanism is called *Bitcoin Improvement Process (BIP)* [149]. It requires 95% of the nodes to agree on the change before it is applied. In order to address the rapidly growing Bitcoin network, the *Bitcoin Core* team proposed to increase the block size [150], to future-proof the cryptocurrency. This proposal resulted in a clash of interests between the miners and the Core team. Miners, being mostly interested in the amount of cryptocurrency they are generating, didn't want to reduce the amount of incentive they are receiving with increased block size. In conclusion, it took three years of negotiations to make the final decision and resolve pending issues. In contrast, Dash cryptocurrency uses *Decentralized Governance By Blockchain* (*DGBB*) [151] mechanism which defines a certain group of nodes called *Masternodes* which perform governance of the system. The proposal submitted by Evan Duffield to increase the Dash block size to 2MB [152] was accepted by the majority of the Masternodes in 24 hours. Authors of [153] propose a new governance model for the prevention of high-level governance issues. The model is based on a combination of PoW and PoS consensus protocols and targets to secure the governance of blockchain systems from the authoritative control and re-centralization of decision power. In addition, according to authors, their model enhances the environment of Decentralized Autonomous Organizations (DAO) [154] creation by transitioning part of governance power into the creators' hands. The DAO is the new type of organization, which has the governance rules specified on the blockchain network.

Having discussed the governance of the blockchain networks themselves, research proposals where blockchain technology is used to enhance decentralized systems governance are discussed next. Authors of [155] propose a blockchain-based technical solution that enables governance of decentralized micro-clouds. According to the authors, the main reasoning behind this proposal is the lack of the governance layer in the decentralized micro-cloud environments. With the incorporation of the blockchain system, authors were able to build a trusted and decentralized governance layer. In [156] authors propose a governance framework to enhance transparency and trust in software delivery where the software is developed by multiple distributed teams. The framework allows to control and enforce the Software Development Life Cycle (SDLC) [157] process compliance with decentralized governance of development steps in SDLC. Authors of [158] present a blockchain-based academic governance system with increased transparency and trust towards the process of verification of student records. According to the authors, for current academic systems, it takes up to 30 days to handle the verification of the student records, since a large portion of process execution is performed manually. Blockchain incorporation allowed automating some manually executed parts, resulting in less time needed for record verification.

In the area of Big Data, a number of proposals suggested the usage of blockchain to improve data governance in decentralized systems, thus, putting control in the hands of the data owners to decide how and by whom it is being processed. In the [159], authors, along with highlighting the limitations of centralized systems governance, discuss the benefits of blockchain technology usage to enhance the distribution of data governance in a decentralized system. According to authors, the blockchain technology enables the distribution of the governance towards the data owners and enables them to decide on the full life-cycle of the data processing, starting from storage and ending with the precise entities who retrieve access to process it. For a further read on the blockchain application for data governance in decentralized systems, the reader is referred to [160].

In the area of Smart Cities governance, authors of [161] propose a new system called *blockchain-based employee assessment system* (*BEMPAS*). The system is designed to address the issues of centralized governance such as lack of trust and accountability. Authors take the use-case of employee performance assessment and build a decentralized blockchain-based system which, according to authors, achieves transparency and trust of the governance between governmental workers in a Smart City context.

Lessons Learned: Without an efficient and secure governance service, the blockchain network may be compromised and even go out of operation. Although the very idea of blockchain technology is to establish digital democracy and self-sovereignty, the example of the Bitcoin governance model showed that when

too many unverified nodes are included in the decision-making process, it may become cumbersome and time-consuming. The idea of Masternodes introduction solves the issue of unverified nodes. However, it also introduces the possibility of authoritative control and re-centralization of decision power in case a certain amount of Masternodes become malicious. With the introduction of the permissioned blockchain architecture, private governance became possible leaving the decision-making power within a certain group of nodes. This type of governance is said to have good privacy-preserving characteristics and is better suited to address business needs.

Blockchain technology incorporation can enhance the governance service of decentralized systems. Blockchain technology allows the distribution of governance within the respective system and enables increased automation and time-efficiency of the processes. Also, in the case of multi-step processes such as SDLC, it allows distributing governance over to developing parties, thus, making the process transparent and trusted.

From the perspective of the TSM, blockchain-based governance service enables the distribution of decision-making power over a number of consortium nodes, as well as preserving the possibility for a close circle of trusted decision-makers with private blockchain architecture. However, according to CBAN [9], the consortium which governs the TSM should be inclusive but secure, providing TSM's participants with a sufficient level of assurance that the TSM is future-proof, robust, and trusted.

D. Business Settlement Service

The *business settlement* is a key service for the companies enabling their business opportunities. The settlement process comprises a number of steps which include the negotiation of the license, and legal license signing, i.e., settlement. The process of business settlement is essential in revenue generation for the companies, and such characteristics as fault-tolerance, automation, and time consumption may be decisive in the implementation of the business opportunity. Nowadays, when systems are mostly being built with a centralized architecture, the business settlement does not pose any challenges as long as it is concealed within one system. However, at the moment when two or more non-trusted parties require settlement execution, human intervention is required. The parts of the process which are manually executed may be subject to fraud and simple human errors. The outcome of the manually executed part is the assembling of a contract, e.g., license, which reflects the right and obligations of involved parties. Another major part of the settlement process is the establishment of trust between initially non-trusted parties. Nowadays, in the context of two or more centralized systems, a third-party is often needed to be involved in the settlement process with two aims: 1) to act as a trust-enabling entity between non-trusted parties, and 2) to sign an assembled contract. The involvement of a third-party, while allowing to establish trust, makes the settlement process time-consuming and expensive, since reaching a third-party manually takes time and its services have to be paid.

Naturally, the idea of third-party elimination from the process sets the prospect towards enhanced business settlement and enables positive developments, such as automation and cost reduction. Therefore, the main obstacle is the trust enabling technology that substitutes third-party, can be automated, and does not require or reduces the incentive for the job done. The DLT technology appears to have a set of characteristics that contribute towards the solution of the problems present in a settlement process. The ledger helps to establish a root of trust by providing immutable storage of information in the form of a blockchain. When collaborating parties are a part of a blockchain network, they write to the ledger only the information which was verified by the consensus protocol, thus agreeing on the information's correctness, i.e., provenance, and validity. Further, the settlement agreement can be recorded in executable smart contracts where participants' rights and obligations are specified. Finally, when all parts of the system in place, the entire business settlement execution process can be automated by orchestration technology.

In recent years, a number of research articles have been published in the area of blockchain-based business settlement. With blockchain, researchers aim to make the on-chain settlement process trusted and efficient, and automated. In [162] the author explores the idea of blockchain technology application in the energy market, i.e., Smart Energy Grid. The author claims that blockchain technology can help with the accounting of metered energy flows. The author claims that the smart contract technology applied to the settlement process makes it more efficient, thus allowing to remove a trusted third-party. In addition, blockchain technology allows the ability to fully automate the business settlement process. Authors of [163] present a blockchain-based decentralized market solution for P2P energy trading. The main argument of the paper is that current centralized market solutions cannot provide enough scalability and flexibility for a rapidly growing number of distributed prosumers of electrical energy. Thus, the energy market has to be decentralized, to be able to handle consumer and prosumer needs. Authors base the market's energy trading settlement process on blockchain smart contracts, where transaction details are recorded. The blockchain also enhances the market's ability to analyze electricity consumption and production rates through the immutable ledger. The trading data analysis helps to regulate electricity trading prices, thus increasing the efficiency of prosumer-generated electricity. In [164] authors provide a detailed analysis of blockchain-based settlement mechanisms called Global Balancing Settlement (GBS) and Splitting Settlement (SS). These settlement mechanisms are implemented as smart contracts stored on the blockchain. The authors provide a reference to current centralized settlement efficiency and how blockchain-based mechanisms perform in comparison to it. The distinct feature of this study is that the implemented system was applied in real-life conditions in a small residential community. The results are provided in a form of an electricity price increase for the seller, and an electricity price decrease for a buyer throughout the day. The results have shown, that although GBS gives a larger price efficiency boost for both sellers and buyers compared to SS, both blockchain-based settlement methods outperform traditional centralized settlement.

In the area of e-commerce, the authors of [165] propose a blockchain-based system with autonomous transaction settlement called NormaChain. Since all transaction settlement is handled via cryptocurrency transition from one user wallet to another, authors derive their own coin called NorMaCoin (NMC) to decrease fiat currency inclusion in a system, thus increasing scalability and efficiency with native blockchain currency. The settlement terms are recorded in a blockchain smart contract where all information on buyer, seller, product, and amounts of currency is available. According to the authors, they are able to demonstrate that the settlement approach can be fully automated, and at the same time it can be executed in a trusted, transparent and efficient manner.

There has also been a number of industry initiatives to enhance and standardize the business settlement process in TSM. While academic proposals mostly discuss new ways of settlement execution on a newly designed blockchain-based marketplace, industrial proposals aim to help current CSPs to transform their operational frameworks in a way they are interoperable with TSM's core services. Since TSM is by design a decentralized marketplace, the participants are becoming a part of the distributed infrastructure, which exposes their telecommunication services and infrastructure to be rented within a marketplace. The CBAN [9] is an initiative that aims to define a *tool-set* for the TSM by standardizing the technologies and development practices with which the core services of the marketplace are implemented. With this, according to CBAN, it will become possible to fully automate business settlement process routines that are executed in a trusted and transparent manner. Authors of [44] describe the new initiative called *TM Forum Catalyst*, which aims to create a federated CSPs Marketplace. The authors emphasize the obsolescence of current approaches towards CSPs' network infrastructure rental settlement process. The settlement process has to be transformed in a way that allows CSPs to implement a more agile and on-demand rental which enables new business opportunities for telecommunication market participants.

Lessons Learned: The business settlement process is of high importance in the context of digital marketplaces. It is the main service-enabler of new business opportunities for companies. In general, business settlement starts with the assembling of a contract. The next step, signing of the contract, in today's business conditions often requires the presence of a trusted third-party, i.e., intermediary, which acts as a trust enabling entity and concludes business settlement. Such settlement process flow involves a number of manual steps, which require human intervention and represent the bottleneck in an execution. The aim of eliminating the trusted third-party requirement is pursued by both academia and industry and appears to be solved with the employment of DLT as the main trust-enabling technology. DLT and the blockchain as an implementation of it appear to be able to enable trusted and transparent business settlement while providing acceptable data assurance and security.

In the context of TSMs, the settlement process that is used nowadays complicates the implementation of new business opportunities. Blockchain technology enables the process of telecommunication services and network infrastructure renting to be executed without the involvement of a trusted third-party, thus allowing full automation. In addition, full automation allows making the rental settlement process more agile and on-demand, opening a new set of opportunities towards the implementation of new business scenarios.

V. Future Research Directions

Today's blockchain-enabled services still face a number of challenges that need to be solved in order for blockchain to be applied in the context of digital marketplaces at large and in TSMs in particular. Although in this paper we provide an overview of the TSM's architecture and core services that constitute the foundation of such a marketplace, next, we describe the challenges that are out of the scope of this survey and should be addressed in the future. Future challenges are chosen with the consideration of TSM's core services and the possibility to make them more *democratic* while *robust*.

First, the assurance and governance services are enabled by the inherent characteristics of blockchain technology. Thus, the improvements and new developments in this technology itself may trigger improvements in these core services. The openness of blockchain technology makes the overall system more democratic while its distributed nature makes it more robust.

Further, the Blockchain-based IdM service may benefit from incorporating physical identity, making it more *robust* in terms of available options to authenticate oneself in a system. The business settlement service may benefit from an established way to transition financial assets to a blockchain and use them as a cryptocurrency, making them more *democratic*. Finally, the interoperability of blockchain-based services is the main aim of the majority of standardization activities. Interoperable blockchain-based services would maximize the inclusiveness of digital marketplaces, and open a new set of business opportunities. These future research directions are discussed next in detail.

A. Physical Identity Management on a Blockchain

As discussed in Section IV-A, blockchain-based IdM systems are mostly based on the SSI principles and are well described by both academia and industry. Blockchain and SSI principles make the IdM process more democratic and decentralized, thus, eliminating the need for a centralized identity server. Research efforts and interest in blockchain-based SSI model resulted in such industrial implementations as uPort and Sovrin. Both implementations show that SSI is possible to apply in digital systems and it helps to solve such issues of previous IdM models as a central point of failure and data breaches. However, these systems do not consider the connection between the physical and digital identity within the IdM system.

Physical identity is represented most of the time by a card that is issued to the identity holder and provided to an identification entity as identity proof [166]. On a national level, it is for example the passport of a person, which is used for identification in governmental and private institutions within a particular country. However, there should be a mechanism

of physical identity usage in the context of a digital system. At this point, to the best of our knowledge, the systems which enable the digital representation of physical identity are mainly designed as SSO [167], and they are built on a user-centric IdM model which uses centralized silos of identity information. We think that it is worth exploring the possibility of physical identity representation in the blockchain-based SSI model. In this case, the digitized physical identity is stored on the user premise which enables full control over it and makes the overall IdM system more democratic and robust, in contrast to SSO.

B. The Transition of Financial Assets to a Blockchain

In the physical world, it is the fiat currencies, e.g., a national currency or precious metals, that allow us to pay for items and services that we want to acquire. These currencies can be digitized in a form of banking accounts, where one's assets are accessible through the respective card number and password, as well as some ownership verification mechanisms, e.g., text message or SSO. While a banking system is convenient to use within a particular bank, the transition of assets between different banks may require paying a high fee and pose possible complications on the transaction process, e.g., additional reference number of a receiver bank. Thus, the employment of blockchain technology in financial systems opens an opportunity to implement trustworthy and agile money transferring systems in an inter-bank and cross-country context [168], [169]. In addition, on-chain currencies can be used in the digital marketplace context to make payments during transactions as was described in Section IV-D. However, we face a number of challenges in the case of fiat currencies transitioning to blockchain-enabled systems. First, there should be an entity that regulates an exchange ratio of fiat currency into an on-chain token. The regulatory body should be present to make the price of on-chain tokens stable and protected from illegal financial operations. Second, all transactions have to meet legal requirements for such financial transitions to take place. The governments of countries tend to regulate all financial transactions as it is a vital part of a country's economy [170].

Nowadays the cryptocurrencies such as Bitcoin and Ethereum have shown that financial assets in a form of fiat currencies can be transitioned to blockchain in a form of on-chain tokens and used as a new form of digital currency. While this makes the transactions more democratic, in certain countries such on-chain financial operations are banned due to the government's inability to track transaction participants and control the overall payment process [170]. Thus, we think that it is worth exploring the mechanisms to enable legal and secure fiat currencies transitioning into on-chain tokens.

C. Interoperability of Blockchain-Enabled Services

Blockchain technology brings a number of advantages to the services that employ it as was shown in Section IV. DLT acts as a trust enabling entity and provides an immutable distributed storage that prevents data loss and makes it highly challenging to alter transactions embedded into it. However, while there are a number of initiatives to build blockchain-based services and systems, the majority of times initial system design is not based on a common standard. While this is not an issue for a sole system's operation, it limits its interoperability and restricts the ability to interconnect different blockchain-based systems [171].

There is a number of standardization activities conducted on blockchain technology application in an area of TSM as described in Section III-G. However, the core services which potentially can be used within TSM, even at this point are being developed with different blockchain architectures, e.g., uPort and Sovrin. Thus, we think that it is worth investigating the interoperability of blockchain-based services overall. In addition, we would like to explore the possibility to propose unified guidelines to build interoperable blockchain-based services.

VI. Summary and Outlook

This work provides a survey on the academic and industrial proposals in the area of digital marketplaces at large and TSMs in particular. We discuss the current state of the digital marketplaces and the advantages and disadvantages of the centralized marketplace architecture. As our discussion showed, a centralized architecture poses a number of challenges in terms of transparency and democracy for the entities operating within the marketplace. In addition, it is necessary for the trusted intermediary to be present in a centralized system's business settlement process. The transition towards a *decentralized marketplace architecture allows addressing these challenges*. Proposals of such marketplaces and adoption of blockchain technology resulted in a number of scientific and industrial solutions for architectural components needed by blockchain-enabled digital marketplaces. These solutions demonstrated that blockchain technology reduces or eliminates the need for a trusted intermediary in business settlement process while providing data assurance, transparency, and making the overall marketplace system more democratic. In addition, blockchain technology provides a foundation for identity management, governance, and business settlement services implementation.

We describe the challenges that current CSP face while conducting the business settlement and provide the use-cases for the TSM where the business settlement can be automated in a decentralized marketplace while giving service developers and CSPs a "central" place, e.g., marketplace's user interface, to look for telecommunication services or network infrastructure renting. Also, we discuss the main standardization activities on the TSMs and provide the discussion on the set of core services that establish TSM's platform and give marketplace's collaborators the common set of processes that they can rely on to establish their business relationships and enable new business opportunities.

The surveyed literature shows evidence that blockchain can provide advantages in the four core services in TSMs: *identity management, assurance, governance,* and *business settlement*. As shown in Section IV, there are multiple proposals on how to implement these four core services. The common denominator for these proposals is that they are all based on blockchain technologies, but otherwise they each emphasize

various aspects and characteristics for the service they define. Whereas each proposal has its own benefits and drawbacks, it is not yet clear what combination is the optimal one when architecting a TSM. More work is required in this direction, which also explains the existence of several ongoing standardization activities, described in Section III-G. Similarly, there are multiple competing blockchain technologies that can support the implementation of these proposals. It is important to understand the tradeoffs between these technologies in terms of performance (e.g., transactions per time unit, energy consumption, consensus algorithm) as well as security, privacy, and last but not least compliance with existing (national and international) laws and regulations. These are fundamental research issues that require additional studies. We also see a need for a more comprehensive quantitative evaluation of existing solutions in realistic environments.

REFERENCES

[1] F. Fitzek, F. Granelli, and S. Patrick, Eds., *Computing in Communication Networks*. London, U.K.: Academic, 2020.

[2] A. Sefidcon, W. John, M. Opsenica, and B. Skubic, *The Network Compute Fabric*, Ericsson Technol. Rev., Stockholm, Sweden, Jul. 2021.

[3] S. Yrjola *et al.*, "White paper on business of 6G," 2020, *arXiv:2005.06400*.

[4] A. S. Prasad, M. Arumaithurai, D. Koll, and X. Fu, "DMC: A differential marketplace for cloud resources," in *Proc. 19th IEEE/ACM Int. Symp. Cluster Cloud Grid Comput. (CCGRID)*, May 2019, pp. 198–209.

[5] J. Friman, M. Ek, P. Chen, J. Manocha, and J. Soares, *Service Exposure—A Critical Capability in a 5G World*, Ericsson Technol. Rev., May 2019.

[6] T. Kollmann, S. Hensellek, K. de Cruppe, and A. Sirges, "Toward a renaissance of cooperatives fostered by Blockchain on electronic marketplaces: A theory-driven case study approach," *Electron. Markets*, vol. 30, no. 2, pp. 273–284, Jun. 2020.

[7] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Rep., 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[8] J. Singh and J. D. Michels, "Blockchain as a service (BaaS): Providers and trust," in *Proc. IEEE Eur. Symp. Security Privacy Workshops (EuroS&PW)*, Apr. 2018, pp. 67–74.

[9] "Communications Business Automation Network Whitepaper Version 1.0." CBAN. [Online]. Available: https://www.cban.net/resources (Accessed: Oct. 12, 2021).

[10] Y. Diao, L. Lam, L. Shwartz, and D. Northcutt, "Modeling the impact of service level agreements during service engagement," *IEEE Trans. Netw. Service Manag.*, vol. 11, no. 4, pp. 431–440, Dec. 2014.

[11] W. Chen and I. Paik, "Toward better quality of service composition based on a global social service network," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 5, pp. 1466–1476, May 2015.

[12] R. B. Uriarte, R. de Nicola, and K. Kritikos, "Towards distributed SLA management with smart contracts and blockchain," in *Proc. IEEE Int. Conf. Cloud Comput. Technol. Sci. (CloudCom)*, vol. 2018, Dec. 2018, pp. 266–271.

[13] S. Jalali and C. Wohlin, "Systematic literature studies: Database searches vs. backward snowballing," in *Proc. ACM-IEEE Int. Symp. Empir. Softw. Eng. Measur.*, 2012, pp. 29–38.

[14] N. Afraz and M. Ruffini, "A distributed bilateral resource market mechanism for future telecommunications networks," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, 2019, pp. 1–6.

[15] E. D. Pascale, H. Ahmadi, L. Doyle, and I. Macaluso, "Toward scalable user-deployed ultra-dense networks: Blockchain-enabled small cells as a service," *IEEE Commun. Mag.*, vol. 58, no. 8, pp. 82–88, Aug. 2020.

[16] J. Xie *et al.*, "A survey of blockchain technology applied to smart cities: Research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2794–2830, Jul. 2019.

[17] V. Fernandez-Anez, *Stakeholders Approach to Smart Cities: A Survey on Smart City Definitions* (LNCS 9704). Cham, Switzerland: Springer-Verlag, 2016, pp. 157–167.

[18] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and IoT integration: A systematic survey," *Sensors*, vol. 18, no. 8, p. 2575, Aug. 2018.

[19] S. Singh and N. Singh, "Internet of Things (IoT): Security challenges, business opportunities & reference architecture for E-commerce," in *Proc. Int. Conf. Green Comput. Internet Things (ICGCIoT)*, Oct. 2015, pp. 1577–1581.

[20] G. Ishmaev, "The ethical limits of blockchain-enabled markets for private IoT data," *Philos. Technol.*, vol. 33, no. 3, pp. 411–432, Sep. 2020.

[21] N. Slamnik-Krijestorac, H. Kremo, M. Ruffini, and J. M. Marquez-Barja, "Sharing distributed and heterogeneous resources toward end-to-end 5G networks: A comprehensive survey and a taxonomy," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1592–1628, 3rd Quart., 2020.

[22] T. Gabriel, A. Cornel-Cristian, M. Arhip-Calin, and A. Zamfirescu, "Cloud storage. A comparison between centralized solutions versus decentralized cloud storage solutions using Blockchain technology," in *Proc. 54th Int. Univ. Power Eng. Conf. (UPEC)*, Sep. 2019, pp. 1–6.

[23] Y. Lewenberg, Y. Sompolinsky, and A. Zohar, *Inclusive Block Chain Protocols* (Lecture Notes in Computer Science, 8975). Berlin, Germany: Springer, 2015, pp. 528–547.

[24] S. Popov. "The Tangle." 2018. [Online]. Available: https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf

[25] T. Ali Syed, A. Alzahrani, S. Jan, M. S. Siddiqui, A. Nadeem, and T. Alghamdi, "A comparative analysis of blockchain architecture and its applications: problems and recommendations," *IEEE Access*, vol. 7, pp. 176838–176869, 2019.

[26] J. B. Bernabe, J. L. Canovas, J. L. Hernandez-Ramos, R. Torres Moreno, and A. Skarmeta, "Privacy-preserving solutions for blockchain: Review and challenges," *IEEE Access*, vol. 7, pp. 164908–164940, 2019.

[27] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum Project, Zug, Switzerland, Yellow Paper, 2014, pp. 1–32. [Online]. Available: https://gavwood.com/paper.pdf

[28] R. Yang *et al.*, "Public and private blockchain in construction business process and information integration," *Autom. Construct.*, vol. 118, Oct. 2020, Art. no. 103276.

[29] E. Androulaki *et al.*, "Hyperledger fabric," in *Proc. 13th EuroSys Conf.*, Apr. 2018, pp. 1–15.

[30] A. Tobin and D. Reed, "The inevitable rise of self-sovereign identity," Provo, UT, USA, Sovrin Found., White Paper, Sep. 2017, p. 24. [Online]. Available: https://sovrin.org/wp-content/uploads/2018/03/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf

[31] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Commun. Surveys Tuts.*, vol. 18, pp. 2084–2123, 3rd Quart., 2016.

[32] R. C. Merkle, "Protocols for public key cryptosystems," in *Proc. IEEE Symp. Security Privacy*, 1980, pp. 122–134.

[33] T. Neudecker and H. Hartenstein, "Network layer aspects of permissionless blockchains," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 838–857, 1st Quart., 2019.

[34] O. Pal, B. Alam, V. Thakur, and S. Singh, "Key management for blockchain technology," *ICT Exp.*, vol. 7, no. 1, pp. 76–80, Mar. 2021.

[35] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, D. Niyato, H. T. Nguyen, and E. Dutkiewicz, "Proof-of-stake consensus mechanisms for future blockchain networks: Fundamentals, applications and opportunities," *IEEE Access*, vol. 7, pp. 85727–85745, 2019.

[36] F. Yang, W. Zhou, Q. Wu, R. Long, N. N. Xiong, and M. Zhou, "Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism," *IEEE Access*, vol. 7, pp. 118541–118555, 2019.

[37] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proc. 3rd Symp. Oper. Syst. Design Implement.*, 1999, pp. 173–186.

[38] M. Castro and B. Liskov, "Practical Byzantine fault tolerance and proactive recovery," *ACM Trans. Comput. Syst.*, vol. 20, no. 4, pp. 398–461, Nov. 2002.

[39] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1432–1465, 2nd Quart., 2020.

[40] C. Ye, G. Li, H. Cai, Y. Gu, and A. Fukuda, "Analysis of security in blockchain: Case study in 51%-attack detecting," in *Proc. 5th Int. Conf. Depend. Syst. Their Appl. (DSA)*, Sep. 2018, pp. 15–24.

[41] M. Bartoletti and L. Pompianu, "An empirical analysis of smart contracts: Platforms, applications, and design patterns," in *Proc. Int. Conf. Financ. Cryptography Data Security*, vol. 10323, 2017, pp. 494–509.

[42] R. M. Parizi, Amritraj, and A. Dehghantanha, *Smart Contract Programming Languages on Blockchains: An Empirical Evaluation of Usability and Security* (Lecture Notes in Computer Science (Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)), Jun. 2018, vol. 10974, pp. 75–91.

[43] M. Pournader, Y. Shi, S. Seuring, and S. L. Koh, "Blockchain applications in supply chains, transport and logistics: a systematic review of the literature," *Int. J. Prod. Res.*, vol. 58, no. 7, pp. 2063–2081, Apr. 2020.

[44] M. Nati *et al.*, *Federated CSPs Marketplace*, TMForum, 2020, pp. 1–19. [Online]. Available: https://arxiv.org/abs/1407.3561#

[45] "Blockchain–Operator Opportunities Version 1.0." GSMA. [Online]. Available: https://www.gsma.com/newsroom/resources/ig-03-blockchain-operator-opportunities-v1-0/ (Accessed: Oct. 12, 2021).

[46] L. Bondan *et al.*, "FENDE: Marketplace-based distribution, execution, and life cycle management of VNFs," *IEEE Commun. Mag.*, vol. 57, no. 1, pp. 13–19, Jan. 2019.

[47] Y. V. Maksimov, S. A. Fricker, and K. Tutschku, "Artifact compatibility for enabling collaboration in the artificial intelligence ecosystem," in *Proc. Lecture Notes Bus. Inf. Process.*, vol. 336, Jun. 2018, pp. 56–71.

[48] J. D. Harris and B. Waggoner, "Decentralized and collaborative AI on blockchain," in *Proc. 2nd IEEE Int. Conf. Blockchain*, no. 2, Jul. 2019, pp. 368–375.

[49] Y. Liu, D. He, M. S. Obaidat, N. Kumar, M. K. Khan, and K. K. R. Choo, "Blockchain-based identity management systems: A review," *J. Netw. Comput. Appl.*, vol. 166, Apr. 2020, Art. no. 102731.

[50] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A state of the art survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 858–880, 1st Quart., 2019.

[51] B. Shala, U. Trick, A. Lehmann, B. Ghita, and S. Shiaeles, "Blockchain and trust for secure, end-user-based and decentralized IoT service provision," *IEEE Access*, vol. 8, pp. 119961–119979, 2020.

[52] S.-F. Chang, "Application marketplace as a service—A reference architecture for application marketplace service," in *Proc. Int. Conf. P2P Parallel Grid Cloud Internet Comput.*, Nov. 2010, pp. 186–192.

[53] D. Tilson, C. Sorensen, and K. Lyytinen, "Change and control paradoxes in mobile infrastructure innovation: The android and iOS mobile operating systems cases," in *Proc. 45th Hawaii Int. Conf. Syst. Sci.*, Jan. 2012, pp. 1324–1333.

[54] A. OI, M. Nakajima, Y. Soejima, and M. Tahara, "Reliable design method for service function chaining," in *Proc. 20th Asia–Pacific Netw. Oper. Manag. Symp. (APNOMS)*, Sep. 2019, pp. 1–4.

[55] Y. Jiang *et al.*, "CSM: A cloud service marketplace for complex service acquisition," *ACM Trans. Intell. Syst. Technol.*, vol. 8, no. 1, pp. 1–25, 2016.

[56] D. Pudasaini and C. Ding, "Service selection in a cloud marketplace: A multi-perspective solution," in *Proc. IEEE 10th Int. Conf. Cloud Comput. (CLOUD)*, Jun. 2017, pp. 576–583.

[57] R.-V. Tkachuk, D. Ilie, and K. Tutschku, "Towards a secure proxy-based architecture for collaborative AI engineering," in *Proc. 8th Int. Symp. Comput. Netw. Workshops (CANDARW)*, 2020, pp. 373–379.

[58] B. Karim, Q. Tan, J. R. Villar, and E. de la Cal, "Resource brokerage ontology for vendor-independent cloud service management," in *Proc. IEEE 2nd Int. Conf. Cloud Comput. Big Data Anal. (ICCCBDA)*, Apr. 2017, pp. 466–472.

[59] C. Pop, T. Cioara, M. Antal, I. Anghel, I. Salomie, and M. Bertoncini, "Blockchain based decentralized management of demand response programs in smart energy grids," *Sensors*, vol. 18, no. 2, p. 162, Jan. 2018.

[60] S. Saxena, H. Farag, A. Brookson, H. Turesson, and H. Kim, "Design and field implementation of blockchain based renewable energy trading in residential communities," in *Proc. 2nd Int. Conf. Smart Grid Renew. Energy (SGRE)*, Nov. 2019, pp. 1–6.

[61] G. S. Ramachandran, R. Radhakrishnan, and B. Krishnamachari, "Towards a decentralized data marketplace for smart cities," in *Proc. IEEE Int. Smart Cities Conf. (ISC2)*, Sep. 2018, pp. 1–8.

[62] L. Mikkelsen, K. Mortensen, H. Rasmussen, H.-P. Schwefel, and T. Madsen, "Realization and evaluation of marketplace functionalities using ethereum blockchain," in *Proc. Int. Conf. Internet Things Embedded Syst. Commun. (IINTEC)*, Dec. 2018, pp. 47–52.

[63] D.-D. Nguyen and M. I. Ali, "Enabling on-demand decentralized IoT collectability marketplace using blockchain and crowdsensing," in *Proc. Global IoT Summit (GIoTS)*, Jun. 2019, pp. 1–6.

[64] H. T. T. Truong, M. Almeida, G. Karame, and C. Soriente, "Towards secure and decentralized sharing of IoT data," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Jul. 2019, pp. 176–183.

[65] S. Bajoudah, C. Dong, and P. Missier, "Toward a decentralized, trustless marketplace for brokered IoT data trading using blockchain," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Jul. 2019, pp. 339–346.

[66] K. R. Ozyilmaz, M. Dogan, and A. Yurdakul, "IDMoB: IoT data marketplace on blockchain," in *Proc. Crypto Valley Conf. Blockchain Technol. (CVCBT)*, Jun. 2018, pp. 11–19.

[67] P. Tzianos, G. Pipelidis, and N. Tsiamitros, "Hermes: An open and transparent marketplace for IoT sensor data over distributed ledgers," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, May 2019, pp. 167–170.

[68] S. Musso, G. Perboli, M. Rosano, and A. Manfredi, "A decentralized marketplace for M2M economy for smart cities," in *Proc. IEEE 28th Int. Conf. Enabling Technol. Infrastruct. Collaborat. Enterprises (WETICE)*, Jun. 2019, pp. 27–30.

[69] K. Nguyen, G. Ghinita, M. Naveed, and C. Shahabi, "A privacy-preserving, accountable and spam-resilient geo-marketplace," in *Proc. 27th ACM SIGSPATIAL Int. Conf. Adv. Geograph. Inf. Syst.*, Nov. 2019, pp. 299–308.

[70] A. Seitz, D. Henze, D. Miehle, B. Bruegge, J. Nickles, and M. Sauer, "Fog computing as enabler for blockchain-based IIoT app marketplaces—A case study," in *Proc. 5th Int. Conf. Internet Things Syst. Manag. Security*, Oct. 2018, pp. 182–188.

[71] D. Miehle, M. M. Meyer, A. Luckow, B. Bruegge, and M. Essig, "Toward a decentralized marketplace for self-maintaining machines," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Jul. 2019, pp. 431–438.

[72] V. P. Ranganthan, R. Dantu, A. Paul, P. Mears, and K. Morozov, "A decentralized marketplace application on the ethereum blockchain," in *Proc. IEEE 4th Int. Conf. Collaborat. Internet Comput. (CIC)*, Oct. 2018, pp. 90–97.

[73] Z. Wang, L. Yang, Q. Wang, D. Liu, Z. Xu, and S. Liu, "ArtChain: Blockchain-enabled platform for art marketplace," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Jul. 2019, pp. 447–454.

[74] J. Martins *et al.*, "Fostering customer bargaining and E-procurement through a decentralised marketplace on the blockchain," *IEEE Trans. Eng. Manag.*, early access, Sep. 21, 2020. doi: 10.1109/TEM.2020.3021242.

[75] N. B. Somy *et al.*, "Ownership preserving AI market places using blockchain," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Jul. 2019, pp. 156–165.

[76] J. Li, A. Grintsvayg, J. Kauffman, and C. Fleming, "LBRY: A blockchain-based decentralized digital content marketplace," in *Proc. IEEE Int. Conf. Decentralized Appl. Infrastruct. (DAPPS)*, Aug. 2020, pp. 42–51.

[77] P. Banerjee, C. Govindarajan, P. Jayachandran, and S. Ruj, "Reliable, fair and decentralized marketplace for content sharing using blockchain," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Nov. 2020, pp. 365–370.

[78] M. F. Franco, E. J. Scheid, L. Z. Granville, and B. Stiller, "Brain: Blockchain-based reverse auction for infrastructure supply in virtual network functions-as-a-service," in *Proc. IFIP Netw. Conf.*, May 2019, pp. 1–9.

[79] B. Nour, A. Ksentini, N. Herbaut, P. A. Frangoudis, and H. Moungla, "A blockchain-based network slice broker for 5G services," *IEEE Netw. Lett.*, vol. 1, no. 3, pp. 99–102, Sep. 2019.

[80] E. J. Scheid, M. Keller, M. F. Franco, and B. Stiller, *BUNKER: A Blockchain-Based Trusted VNF Package Repository* (Lecture Notes in Computer Science (Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, 11819)). Cham, Switzerland: Springer Int., 2019, pp. 188–196.

[81] M. Franco, E. Sula, B. Rodrigues, E. Scheid, and B. Stiller, *ProtectDDoS: A Platform for Trustworthy Offering and Recommendation of Protections* (Lecture Notes in Computer Science (Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, 12441)). Cham, Switzerland: Springer Int., 2020, pp. 28–40.

[82] V. Arya, S. Sen, and P. Kodeswaran, "Blockchain enabled trustless API marketplace," in *Proc. Int. Conf. Commun. Syst. Networks (COMSNETS)*, Jan. 2020, pp. 731–735.

[83] M. Pincheira, M. Vecchio, and R. Giaffreda, "Rationale and practical assessment of a fully distributed blockchain-based marketplace of fog/edge computing resources," in *Proc. 7th Int. Conf. Softw. Defined Syst. (SDS)*, Apr. 2020, pp. 165–170.

[84] R. Bayindir, E. Hossain, and S. Vadi, "The path of the smart grid -the new and improved power grid," in *Proc. Int. Smart Grid Workshop Certificate Program (ISGWCP)*, Mar. 2016, pp. 1–8.

[85] P. D. Suzzoni, "Are regulated prices against the market?" *Eur. Rev.*, vol. 3, no. 3, pp. 1–31, 2009.

[86] General Data Protection Regulation (GDPR)—Official Legal Text." GDPR. 2016. [Online]. Available: https://gdpr-info.eu/

[87] M. Matteucci, D. Raponi, M. Mengoni, and M. Peruzzini, "Tangible augmented reality model to support manual assembly," in *Proc. 13th ASME/IEEE Int. Conf. Mechatronic Embedded Syst. Appl.*, vol. 9, Aug. 2017, pp. 1–9.

[88] Y. Zou, Q. Zhang, and X. Zhao, "Improving the usability of E-commerce applications using business processes," *IEEE Trans. Softw. Eng.*, vol. 33, no. 12, pp. 837–855, Dec. 2007.

[89] Y. Huang, Y. Chai, Y. Liu, and J. Shen, "Architecture of next-generation e-commerce platform," *Tsinghua Sci. Technol.*, vol. 24, no. 1, pp. 18–29, Feb. 2019.

[90] R. Robert. "A Decentralized Marketplace With Hyperledger Fabric." 2020. [Online]. Available: https://www.ericsson.com/en/blog/2020/5/a-decentralized-marketplace-with-hyperledger-fabric

[91] A. Futoransky, C. Sarraute, D. Fernandez, M. Travizano, and A. Waissbein, "Fair and Decentralized Exchange of Digital Goods," Feb. 2020, *arXiv:2002.09689*

[92] *Open Data Markets Infrastructure*, XBR, Astoria, NY, USA, 2019, pp. 1–57. [Online]. Available: https://xbr.network/static/docs/xbr_whitepaper_v1.pdf

[93] M. Van Niekerk and R. Veer. "Global Market for Local Data." 2018. [Online]. Available: https://www.allcryptowhitepapers.com/wp-content/uploads/2018/11/Databroker-DAO.pdf

[94] R. Haenni. "Datum Network: The Decentralized Data Marketplace." 2017. [Online]. Available: https://datum.org/

[95] M. Davidsen, S. Gajek, M. Kruse, and S. Thomsen. "Empowering the Economy of Things." 2017. [Online]. Available: https://weeve.network/weeve_whitepaper.pdf

[96] R. Riggio, A. Bradai, D. Harutyunyan, T. Rasheed, and T. Ahmed, "Scheduling wireless virtual networks functions," *IEEE Trans. Netw. Service Manag.*, vol. 13, no. 2, pp. 240–252, Jun. 2016.

[97] CBAN, "Working draft CBAN reference architecture," Rep., 2020. [Online]. Available: https://www.cban.net/resources

[98] P. Häfner, V. Häfner, and J. Ovtcharova, "Teaching methodology for virtual reality practical course in engineering education," *Procedia Comput. Sci.*, vol. 25, pp. 251–260, Jan. 2013.

[99] U. C. Pendit, M. B. Mahzan, M. D. F. Bin Mohd Basir, M. Bin Mahadzir, and S. N. B. Musa, "Virtual reality escape room: The last breakout," in *Proc. 2nd Int. Conf. Inf. Technol. (INCIT)*, Nov. 2017, pp. 1–4.

[100] "Permissioned distributed ledger (PDL); landscape of standards and technologies," ETSI, Sophia Antipolis, France, Rep. ETSI GR PDL 001, pp. 1–25, 2020.

[101] "Blockchain-Based Telecom Infrastructure Marketplace." TM Forum. 2019. [Online]. Available: https://www.tmforum.org/blockchain-based-telecom-infrastructure-marketplace/

[102] P. Seltsikas and H. van der Heijden, "A taxonomy of government approaches towards online identity management," in *Proc. 43rd Hawaii Int. Conf. Syst. Sci.*, 2010, pp. 1–8.

[103] A. G. Revar and M. D. Bhavsar, "Securing user authentication using single sign-on in Cloud Computing," in *Proc. Nirma Univ. Int. Conf. Eng.*, Dec. 2011, pp. 1–4.

[104] C. Ribeiro, H. Leitold, S. Esposito, and D. Mitzam, "STORK: A real, heterogeneous, large-scale eID management system," *Int. J. Inf. Security*, vol. 17, no. 5, pp. 569–585, Oct. 2018.

[105] T. Zhou, X. Li, and H. Zhao, "EverSSDI: Blockchain-based framework for verification, authorisation and recovery of self-sovereign identity using smart contracts," *Int. J. Comput. Appl. Technol.*, vol. 60, no. 3, pp. 281–295, 2019.

[106] Y. Liu, Q. Lu, H.-Y. Paik, X. Xu, S. Chen, and L. Zhu, "Design pattern as a service for blockchain-based self-sovereign identity," *IEEE Softw.*, vol. 37, no. 5, pp. 30–36, Sep. 2020.

[107] G. Wood. "Polkadot: Vision for a Heterogeneous Multi-Chain Framework." 2017. [Online]. Available: https://polkadot.network/PolkaDotPaper.pdf

[108] H. Gulati and C.-T. Huang, "Self-sovereign dynamic digital identities based on blockchain technology," in *Proc. SoutheastCon*, vol. 2019, pp. 1–6, Apr. 2019.

[109] Z. Cui *et al.*, "A hybrid blockchain-based identity authentication scheme for multi-WSN," *IEEE Trans. Services Comput.*, vol. 13, no. 2, pp. 241–251, Mar./Apr. 2020.

[110] R. Soltani, U. T. Nguyen, and A. An, "A new approach to client onboarding using self-sovereign identity and distributed ledger," in *Proc. IEEE iThings GreenCom IEEE CPSCom IEEE SmartData*, Jul. 2018, pp. 1129–1136.

[111] D. Li, W. E. Wong, and J. Guo, "A survey on blockchain for enterprise using hyperledger fabric and composer," in *Proc. 6th Int. Conf. Depend. Syst. Appl. (DSA)*, Jan. 2020, pp. 71–80.

[112] A. Othman and J. Callahan, "The horcrux protocol: A method for decentralized biometric-based self-sovereign identity," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, Jul. 2018, pp. 1–7.

[113] R. Soltani, U. T. Nguyen, and A. An, "Practical key recovery model for self-sovereign identity based digital wallets," in *Proc. IEEE Int. Conf. Depend. Auton. Secure Comput. (DASC)*, Aug. 2019, pp. 320–325.

[114] S. K. Gebresilassie, J. Rafferty, P. Morrow, L. Chen, M. Abu-Tair, and Z. Cui, "Distributed, secure, self-sovereign identity for IoT devices," in *Proc. IEEE 6th World Forum Internet Things (WF-IoT)*, Jun. 2020, pp. 1–6.

[115] M. P. Bhattacharya, P. Zavarsky, and S. Butakov, "Enhancing the security and privacy of self-sovereign identities on hyperledger indy blockchain," in *Proc. Int. Symp. Netw. Comput. Commun. (ISNCC)*, Oct. 2020, pp. 1–7.

[116] C. Lundkvist, R. Heck, J. Torstensson, Z. Mitton, and M. Sena. "Uport: A Platform for Self-Sovereign Identity 2016-09-16." 2016. [Online]. Available: http://blockchainlab.com/pdf/uPort_whitepaper_DRAFT20161020.pdf

[117] Z. Zhao and Y. Liu, "A blockchain based identity management system considering reputation," in *Proc. 2nd Int. Conf. Inf. Syst. Comput. Aided Educ. (ICISCAE)*, Sep. 2019, pp. 32–36.

[118] P. C. Bartolomeu, E. Vieira, S. M. Hosseini, and J. Ferreira, "Self-sovereign identity: Use-cases, technologies, and challenges for industrial IoT," in *Proc. 24th IEEE Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, vol. 2019, Sep. 2019, pp. 1173–1180.

[119] C. Allen, "The path to self-sovereign identity," CA, USA, Rep., 2016. [Online]. Available: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

[120] A. Abraham, *A Position Paper on Blockchain Enabled Identity and the Road Ahead*, Berlin, Germany, Blockchain Bundesverband, Oct. 2017, pp. 1–39.

[121] P. Wuille. "BIP-0032—Hierarchical Deterministic Wallets." 2012. [Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki

[122] *Decentralized Identifiers (DIDs) V1.0*, W3C, Cambridge, MA, USA, 2021. [Online]. Available: https://w3c.github.io/did-core/

[123] R. Ansey, J. Kempf, O. Berzin, C. Xi, and I. Sheikh, "Gnomon: Decentralized identifiers for securing 5G IoT device registration and software update," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2019, pp. 1–6.

[124] P. Ekparinya, V. Gramoli, and G. Jourjon, "Impact of man-in-the-middle attacks on ethereum," in *Proc. IEEE 37th Symp. Rel. Distrib. Syst. (SRDS)*, vol. 2019, Oct. 2018, pp. 11–20.

[125] N. Naik and P. Jenkins, "uPort open-source identity management system: An assessment of self-sovereign identity and user-centric data platform built on blockchain," in *Proc. IEEE Int. Symp. Syst. Eng. (ISSE)*, Oct. 2020, pp. 1–7.

[126] F. Wessling, C. Ehmke, M. Hesenius, and V. Gruhn, "How much blockchain do you need?" in *Proc. 1st Int. Workshop Emerg. Trends Softw. Eng. Blockchain*, May 2018, pp. 44–47.

[127] R. A. Mishra, A. Kalla, N. A. Singh, and M. Liyanage, "Implementation and analysis of blockchain based DAPP for secure sharing of students' credentials," in *Proc. IEEE 17th Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2020, pp. 1–2.

[128] B. Houtan, A. S. Hafid, and D. Makrakis, "A survey on blockchain-based self-sovereign patient identity in healthcare," *IEEE Access*, vol. 8, pp. 90478–90494, 2020.

[129] B. Dab, I. Fajjari, M. Rohon, C. Auboin, and A. Diquelou, "An efficient traffic steering for cloud-native service function chaining," in *Proc. 23rd Conf. Innov. Clouds Internet Netw. Workshops (ICIN)*, Feb. 2020, pp. 71–78.

[130] B. Lee, A. Awad, and M. Awad, "Towards secure provenance in the cloud: A survey," in *Proc. IEEE/ACM 8th Int. Conf. Utility Cloud Comput. (UCC)*, pp. 577–582, 2015.

[131] M. Montecchi, K. Plangger, and M. Etter, "It's real, trust me! Establishing supply chain provenance using blockchain," *Bus. Horizons*, vol. 62, no. 3, pp. 283–293, May 2019.

[132] M. Demir, O. Turetken, and A. Ferwom, "Blockchain and IoT for delivery assurance on supply chain (BIDAS)," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2019, pp. 5213–5222.

[133] C. A. Alexander and L. Wang, "Cybersecurity, information assurance, and big data based on blockchain," in *Proc. SoutheastCon*, vol. 2019, Apr. 2019, pp. 1–7.

[134] S. Wibowo and T. Sandikapura, "Improving data security, interoperability, and veracity using blockchain for one data governance, case study of local tax big data," in *Proc. Int. Conf. ICT Smart Soc. (ICISS)*, Nov. 2019, pp. 1–6.

[135] F. Alam Khan, M. Asif, A. Ahmad, M. Alharbi, and H. Aljuaid, "Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development," *Sustain. Cities Soc.*, vol. 55, Apr. 2020, Art. no. 102018.

[136] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K.-K. R. Choo, "Blockchain: A panacea for healthcare cloud-based data security and privacy?" *IEEE Cloud Comput.*, vol. 5, no. 1, pp. 31–37, Jan. 2018.

[137] R. Neisse, G. Steri, and I. Nai-Fovino, "A blockchain-based approach for data accountability and provenance tracking," in *Proc. 12th Int. Conf. Avail. Rel. Security*, Aug. 2017, pp. 1–10.

[138] X. Liang, J. Zhao, S. Shetty, and D. Li, "Towards data assurance and resilience in IoT using blockchain," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, vol. 2017, Oct. 2017, pp. 261–266.

[139] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, "ProvChain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability," in *Proc. 17th IEEE/ACM Int. Symp. Clust. Cloud Grid Comput. (CCGRID)*, May 2017, pp. 468–477.

[140] A. Patil, A. Jha, M. M. Mulla, D. G. Narayan, and S. Kengond, "Data provenance assurance for cloud storage using blockchain," in *Proc. Int. Conf. Adv. Comput. Commun. Mater. (ICACCM)*, Aug. 2020, pp. 443–448.

[141] J. Benet, *IPFS—Content Addressed, Versioned, P2P File System*, Jul. 2014.

[142] A. Taha, A. Zakaria, D. Kim, and N. Suri, "Decentralized Runtime Monitoring Approach Relying on the Ethereum Blockchain Infrastructure," in *Proc. IEEE Int. Conf. Cloud Eng. (IC2E)*, Apr. 2020, pp. 134–143.

[143] R. Angarita, A. Dejous, and P. Blake, "From centralized to decentralized blockchain-based product registration systems: The use case of lighting and appliances," in *Proc. IEEE Conf. Comput. Commun. Workshops (IEEE INFOCOM) (INFOCOM WKSHPS)*, Apr. 2019, pp. 650–655.

[144] "Bitcoin is Not Ruled by Miners." 2017. [Online]. Available: https://en.bitcoin.it/wiki/Bitcoin_is_not_ruled_by_miners

[145] M. Liu, K. Wu, and J. J. Xu, "How will blockchain technology impact auditing and accounting: Permissionless versus permissioned blockchain," *Current Issues Audit.*, vol. 13, no. 2, pp. A19–A29, Sep. 2019.

[146] R. van Pelt, S. Jansen, D. Baars, and S. Overbeek, "Defining blockchain governance: A framework for analysis and comparison," *Inf. Syst. Manag.*, vol. 38, no. 1, pp. 21–41, Jan. 2021.

[147] S. DiRose and M. Mansouri, "Comparison and analysis of governance mechanisms employed by blockchain-based distributed autonomous organizations," in *Proc. 13th Annu. Conf. Syst. Syst. Eng. (SoSE)*, Jun. 2018, pp. 195–202.

[148] E. Duffield and D. Diaz. "Dash: A Payments-Focused Cryptocurrency." 2018. [Online]. Available: https://github.com/dashpay/dash/wiki/Whitepaper

[149] S. Khatwani. "What is a BIP (Bitcoin Improvement Proposal)? Why do You Need to Know About it?" 2017. [Online]. Available: https://coinsutra.com/bip-bitcoin-improvement-proposa/

[150] G. Andresen. "Bitcoin Improvement Process 101." 2015. [Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0101.mediawiki

[151] "Governance–Dash Documentation." 2016. [Online]. Available: https://docs.dash.org/en/stable/governance/

[152] E. Duffield. "Block Size Limitation Increase." 2016. [Online]. Available: https://www.dashcentral.org/p/2mb-blocksize

[153] M. Baudlet, D. Fall, Y. Taenaka, and Y. Kadobayashi, "The best of both worlds: A new composite framework leveraging PoS and PoW for blockchain security and governance," in *Proc. 2nd Conf. Blockchain Res. Appl. Innov. Netw. Services (BRAINS)*, Sep. 2020, pp. 17–24.

[154] S. Wang, W. Ding, J. Li, Y. Yuan, L. Ouyang, and F.-Y. Wang, "Decentralized autonomous organizations: Concept, model, and applications," *IEEE Trans. Comput. Soc. Syst.*, vol. 6, no. 5, pp. 870–878, Oct. 2019.

[155] F. Freitag, "On the collaborative governance of decentralized edge microclouds with blockchain-based distributed ledgers," in *Proc. IEEE/WIC/ACM Int. Conf. Web Intell. (WI)*, Dec. 2018, pp. 709–712.

[156] K. Singi, V. Kaulgud, R. P. J. C. Bose, and S. Podder, "CAG: Compliance adherence and governance in software delivery using blockchain," in *Proc. IEEE/ACM 2nd Int. Workshop Emerg. Trends Softw. Eng. Blockchain (WETSEB)*, May 2019, pp. 32–39.

[157] R. Lekh and Pooja, "Exhaustive study of SDLC phases and their best praxctices to create CDP model for process improvement," in *Proc. Int. Conf. Adv. Comput. Eng. Appl.*, Mar. 2015, pp. 997–1003.

[158] M. Bhagwat, J. C. Shah, A. Bilimoria, P. Parkar, and D. Patel, "Blockchain to improve Academic Governance," in *Proc. IEEE Int. Conf. Electron. Comput. Commun. Technol. (CONECCT)*, Jul. 2020, pp. 1–5.

[159] X. Liu, X. Sun, and G. Huang, "Decentralized services computing paradigm for blockchain-based data governance: Programmability, interoperability, and intelligence," *IEEE Trans. Services Comput.*, vol. 13, no. 2, pp. 343–355, Mar./Apr. 2019.

[160] H.-Y. Paik, X. Xu, H. M. N. D. Bandara, S. U. Lee, and S. K. Lo, "Analysis of data management in blockchain-based systems: From architecture to governance," *IEEE Access*, vol. 7, pp. 186091–186107, 2019.

[161] E. B. Sifah, H. Xia, C. N. A. Cobblah, Q. Xia, J. Gao, and X. Du, "BEMPAS: A decentralized employee performance assessment system based on blockchain for smart city governance," *IEEE Access*, vol. 8, pp. 99528–99539, 2020.

[162] H. Cheng, "Research on the distributed photovoltaic trading and settlement model based on the energy blockchain," in *Proc. IEEE Int. Conf. Power Data Sci. (ICPDS)*, Nov. 2019, pp. 59–62.

[163] K. Nakayama, R. Moslemi, and R. Sharma, "Transactive energy management with blockchain smart contracts for P2P multi-settlement markets," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Feb. 2019, pp. 1–5.

[164] S.-V. Oprea, A. Bara, and A. I. Andreescu, "Two novel blockchain-based market settlement mechanisms embedded into smart contracts for securely trading renewable energy," *IEEE Access*, vol. 8, pp. 212548–212556, 2020.

[165] C. Liu, Y. Xiao, V. Javangula, Q. Hu, S. Wang, and X. Cheng, "NormaChain: A blockchain-based normalized autonomous transaction settlement system for IoT-based E-commerce," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4680–4693, Jun. 2019.

[166] S. Dangalla, C. Lakmal, C. Wickramarathna, C. Herath, G. Dias, and S. Fernando, "Measuring the correlation of personal identity documents in structured format," in *Proc. IEEE/ACIS 17th Int. Conf. Comput. Inf. Sci. (ICIS)*, Jun. 2018, pp. 240–245.

[167] Z. Saquib, S. Dwivedi, and A. Dubey, "Electronic authentication for e-Government services—A survey," in *Proc. 10th IET Syst. Safety Cyber Security Conf.*, vol. 2015, 2015, pp. 1–9.

[168] X. Wang, X. Xu, L. Feagan, S. Huang, L. Jiao, and W. Zhao, "Inter-bank payment system on enterprise blockchain platform," in *Proc. IEEE Int. Conf. Cloud Comput. (CLOUD)*, vol. 2018, 2018, pp. 614–621.

[169] M. Zouina and B. Outtai, "Towards a distributed token based payment system using blockchain technology," in *Proc. Int. Conf. Adv. Commun. Technol. Netw. (CommNet)*, Apr. 2019, pp. 1–10.

[170] "Regulation of Cryptocurrency Around the World." Jun. 2018. [Online]. Available: https://www.loc.gov/law/help/cryptocurrency/world-survey.php#compsum

[171] Monika and R. Bhatia, "Interoperability solutions for blockchain," in *Proc. Int. Conf. Smart Technol. Comput. Elect. Electron. (ICSTCEE)*, Oct. 2020, pp. 381–385.