The Seybold Report
ISSN 1533-9211

ANALYZE OF USING BLOCKCHAIN TECHNOLOGY IN CLOUD, FOG, AND IoT

RAWAD SALAH HADI [1], SEYED EBRAHIM DASHTI [2]*,

HALAH MAHDI HUSSEIN [3] and QUSAY ABDULRAZZAQ HASHIM [4]

[1, 3, 4] Department of Computer Engineering, Shiraz Branch, Islamic Azad University, Iran.
[2] Department of Computer Engineering, Jahrom Branch, Islamic Azad University, Iran. *Corresponding Author

Abstract

It has been determined that blockchain technology is the best option for improving current computing systems in many ways. Integrating blockchain into cloud, fog and IoT offers significant potential to boost both performance and security. How blockchain technology integrates with already-live computing technologies and makes possible computing re-engineering is an open subject. This article delves into current initiatives that aim to merge blockchain technology with cloud and fog computing to solve this problem. This work roughly addresses three technological dimensions. In this work, we first consider the service model and review an emerging cloud-relevant blockchain service model, Blockchain-as-a-Service (BaaS); then, we evaluate the performance of computing that supports or participates in blockchain from a hardware and software perspective; and finally, we consider security to be a key technical dimension and evaluate both access control and searchable encryption schemes. The article concludes that using blockchain in cloud, fog and IoT increases security and improves data management without decreasing the tangible efficiency of the system.

Keywords: Analyze, Blockchain, Cloud computing, Cloud fog, IoT, Security.

I. INTRODUCTION

Blockchain is a relatively new technical concept, but it is already being seen as a viable option for creating a trustworthy platform because of features like its capacity to track and record changes to data without being altered. Many people think that blockchain technology's potential applications go beyond financial services (like Bitcoin) [1] [2]. A smart contract's capacity to add automatic control [3] is a fundamental motivating factor in blockchain-enabled applications. Through the use of smart contracts, blockchain creates a trustworthy environment that is intrinsically linked to procedures and operations. An anticipated technical path for bolstering cloud datacenters is the implementation of blockchain-enabled technologies. Our research shows that many current studies are looking for ways to leverage blockchain technologies to enhance preexisting infrastructure. One of the most prominent trends toward establishing trustworthiness and dependability in the aforementioned interconnected networking environment is the reengineering of cloud datacenters via a blockchain-enabled approach [4] [5]. It is generally agreed that blockchain's tamper resistance [6], [7], transparent governance [8], decentralization-powered security [9] [10], and unique business models [11] [12] are all significant advantages.

Our research revealed that despite the many benefits of blockchain technology, two major problems persist with existing blockchain-enabled cloud solutions. The first kind of problem is that using blockchain in cloud applications is notoriously difficult. Most problems arise as a

The Seybold Report
ISSN 1533-9211

result of the technical features of blockchain, some of which are also seen as benefits. For instance, in a purely decentralized setting (such as a public blockchain), autonomous operation is prioritized, but the lack of centralized oversight is seen as a drawback in many real-world contexts. Many factors, including legal constraints and government responsibilities, make it impossible to completely abandon centralized forms of governance. Our new research [13] indicates that data saved in blocks are publicly accessible, which poses a privacy risk to the consortium's blockchain-based autonomous trading system based on a real-world situation. When it comes to the cloud datacenter, tamper-resistance is a barrier to developing controllable/scalable cloud systems [14] [15], even though consortium/private blockchain mitigates the impact of decentralization.

The other widespread difficulty is in the area of blockchain service model development and implementation. Although blockchain technology was first developed as a distributed ledger-based storage system a few years before Bitcoin's birth, the term "blockchain" was commonly used as a synonym for "Bitcoin" when the cryptocurrency was initially exposed to the public. While blockchain's early success in the cryptocurrency market has sparked a wave of similar digital currencies and financial services built on the technology, this model has yet to catch on in other sectors [14] [16]. Although several attempts have been made over the years [17] [19], the lack of suitable service models is a significant factor that inhibits blockchain implementations. Blockchain technology also faces challenges when applied to the cloud datacenter environment. Our study [15] also contends that many current management methods, which have traditionally relied on a centralized administration, are incompatible with a computing system with 100% decentralization. Our findings have implications for both public and private sectors as a result of our investigation.

In reality, overcoming the aforementioned obstacles and other problems associated with technical fusion is more difficult than it may initially appear. Inflexibility arises from a number of factors, including system compatibility, the blockchain-cloud interface, the need for governability, and the necessity of deploying the necessary infrastructure. Understanding the interdependencies between blockchain and cloud infrastructure is a cornerstone for maximizing the potential of this hybrid system. Three questions are posed below that correspond with at least three aspects of the importance of completing an article in this area.

There is a pressing need to facilitate the use of blockchain technology in real-world applications Figure 1 (Show Illustration of how blockchain technology might be used in several fields graphically).

Considering its widespread use, cloud computing is an appropriate end goal for implementing blockchain technologies. But how to make blockchain work in the cloud is still an open subject. For instance, the concentration of computation that cloud services rely on runs counter to the decentralized nature of a blockchain.

While the novel service models made possible by blockchain such as the incorporation of trustworthy values seem to be congruent with cloud service models, the provision of blockchain services is more involved than that of traditional cloud services. The answers to many open

ISSN 1533-9211

questions still await discovery. When numerous blockchain networks are combined, blockchain technology has trouble exchanging/sharing data, in contrast to infrastructure or software that fits in an On-demand Pay (ODP) way. The need for a reliable service model that works with cloud computing and blockchain is at an all-time high.

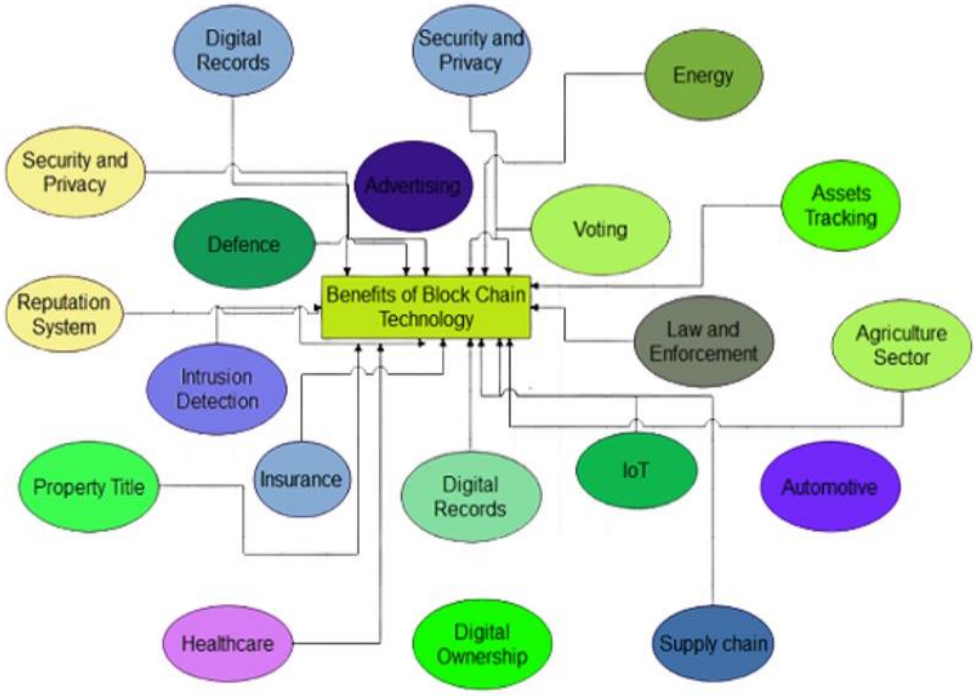

Figure 1: Illustration of How Blockchain Technology Might Be Used In Several Fields Graphically

While cloud computing's ability to provide technical support for blockchain may seem straightforward at first glance, a great deal of research is still needed in this area to determine whether or not it is, in fact, the best option for a variety of use cases, including blockchain. There is a significant need to learn about recent developments in cloud services designed for use with blockchain technology.

Even though some recent studies have surveyed blockchain techniques from different per-perspectives, such as digital currencies [20] [22], security [23] [24], privacy [21] [25], edge-integration [26], IoT [27], and smart city [29], we notice that fusing these two approaches has rarely been addressed by prior survey studies. This article, then, looks specifically at how blockchain and cloud computing may work together technically. This article provides a synthesis of recent research on the relevant topic. Data provenance, access control, searchable encryption, data deduplication, automatic control and resource allocation, hardware upgrade, and data storage are only a few of the topics covered in this assessment from the perspective of cloud products and functionality.

The Seybold Report
ISSN 1533-9211

The goal of this article is to identify contemporary blockchain research that can be used to strengthen blockchain systems in the cloud, as well as unique mechanisms that leverage cloud-based ways to do so. Each technical aspect of blockchain is covered, including its throughput capacity, compatibility with other systems, energy consumption, platform availability, and security.

There are two main takeaways from this study.

To begin, this article gives an in-depth look at how blockchain applications are reengineering cloud computing. This work presents clear research/practical guidance for scholars/practitioners by comparing similar technical dimensions. Second, this poll provides a quick primer on how to combine blockchain with cloud computing. The organization of this work is based on a set of technical characteristics that are useful for helping academic and industrial researchers construct a foundation of knowledge in the field.

To create blockchain-based cloud or on-premises server infrastructure.

This work is structured in the same order as the graphically depicted organizational structure.

In Section II, we introduce a novel business model focused on blockchain technology, coined "Blockchain as a Service" (BaaS). In Section III and Section IV, we examine blockchain-enabled data provenance and access control approaches from the standpoint of data governance. In addition, we provide a synthesis of research in Sections V and VI about blockchain-based applications in data deduplication and searchable encryption methods made possible by the blockchain. Section VII then details a handful of recent research articles that all deal with the same topic: using smart contracts to allocate cloud resources. Section VIII also discusses blockchain's offloading mechanism. Recent hardware performance improvements are highlighted in Section IX, while pertinent work in the area of blockchain-related storage is showcased in Section X. Section XII also includes comments and primary findings. Section XIII is a wrap-up and finalization of the project.

II. BLOCKCHAIN AS A SERVICE

BaaS Ideology

The BaaS model is one flavor of blockchain service that takes inspiration from the cloud computing paradigm. As a computing resource that can be utilized to back up cloud systems and other applications, blockchain systems or components are treated as such in this service model [30]. Using BaaS, customers can avoid getting bogged down in the nitty-gritty of blockchain technology so they can concentrate on running their businesses.

A blockchain service provided under a cloud service model is metaphorically described as "Cloud over Blockchain" in work [5]. It's common knowledge that the proliferation of cloud services is a direct result of the industry's ever-increasing demand. Emerging cloud services, such Backend-as-a-Service, Process-as-a-Service, and Security-as-a-Service, transmit even partial processing components or processes in a transferable manner for service demanders. Service interoperability in the Internet of Things (IoT) was also considered in [31], which stated

The Seybold Report
ISSN 1533-9211

that trusted environments and smart contract executions may be utilized to improve interoperability.

Due to the malleability of the cloud service architecture, the content of the service might be anything from a system to a controllable network. The service offering in a BaaS may also be blockchain infrastructure or backend. To elaborate, BaaS is a service that lets clients use the cloud to access blockchain-related resources. Take Alibaba Cloud as an example. Offering users access to blockchain infrastructure, BaaS delivers a wide range of services including transaction tracking database, smart contract, and consortium governance. The value of BaaS varies between service providers. Security, monetary savings, system integration, and control optimization are just a few of the most often sought-after outcomes.

We focus primarily on the process of using blockchain technologies as a means of bolstering cloud services in this article. BaaS is predicated on the premise that the blockchain network/application may be viewed as a service offering, with customers having the freedom to tailor some aspects of it to their needs. The service provider provides the necessary infrastructural support for launching a blockchain network, and some blockchain source code is open source. Recent research has addressed the question of how to construct unique BaaS, with papers like FSBaaS [32], uBaaS [33], and NutBaaS [34] providing examples. We see that the potential of unified BaaS is still being investigated and that most previous initiatives are still in the system design phase. Problems with technological aspects such as communication, consensus, and data synchronization remain a challenge. Because of technical limitations, unified BaaS is not yet widely used in the real world.

For a more thorough explanation, we'll focus on two unique aspects of the BaaS idea in addition to the standard cloud computing features.

- Cloud Service Providers (CSPs) manage/govern all necessary blockchain computing resources (such as infras- tructure or operations) and provide customers with an agile service offering, allowing customers to obtain bespoke acquisitions to host their blockchain applications or partial blockchain functions (such as smart contracts).
- The complexity of the blockchain implementation is filtered out by BaaS. The breadth and depth of the services provided by an ODP approach, from initial setup and configuration to ongoing management and upkeep, are flexible and extensible. In most cases, rapid adoptions can be achieved with the help of plug-in architecture.

Furthermore, it is theorized that implementing blockchain techniques provides a method for resolving issues and adding value to cloud services. In the case of an integrated cloud data management system, for instance, multiple CSPs may be involved, leading to frequent occurrences of data sharing/transferring operations [35] [36]. When several people are involved in a data-sharing operation, it might be difficult to monitor where the information goes. Deploying a data-tracing system based on the blockchain is the answer to the problem.

The Seybold Report
ISSN 1533-9211

Construction and maintenance of the blockchain platform are under the purview of BaaS CSPs. This includes measures to boost performance (such as source scheduling and API design) and safeguard against potential threats (such as security protection) [37]. The advent of BaaS allows users to keep constant connectivity to blockchain networks [38].

BaaS in the Workplace

BaaS products of today are conceptually similar to BPaaS (Business Process as a Service) in that they emphasize the links between logical business processes and actual service delivery. CSPs' attention has been piqued by the emerging blockchain movement. Many established cloud providers, including Microsoft, IBM, and Amazon, offer BaaS. Oracle BaaS is rapidly eroding IBM's lead in the market for logistics and payment services [40], while IBM BaaS is making an effort to provide services for automotive systems [39]. This section provides a comparison of several BaaS options.

Microsoft Azure [41] is a cloud platform that allows for rapid blockchain deployment and configuration, and it is compatible with Ethereum, Corda, and Hyperledger Fabric. The user of Azure just needs to configure a few settings rather than the underlying mechanics. Furthermore, Microsoft's technology can perform automatic off-chain cloud storage backups of the on-chain data. While the implementation of a consortium blockchain is being investigated, the current version of Azure primarily supports the single-node setup in Fabric.

Next, another widely utilized cloud service, Amazon Web Services (AWS) [42], has offered BaaS in their established, widely adopted cloud environment since 2016. BaaS on AWS works with Ethereum and Hyperledger, giving customers a choice of blockchain platforms and service providers.

The IBM Blockchain Platform allowed customers to deploy their blockchains to a public cloud. The biggest drawback of the IBM Blockchain Platform compared to other BaaS is that it only supports the solution template provided by the Hyperledger Fabric, not the widely used Ethereum. When it comes to user blockchains, however, other BaaS providers have fallen short. IBM's data life-cycle management services can give customers peace of mind when outsourcing their data management needs. IBM's BaaS also made use of encrypted containers. It also helps customers set up Blockchain in on-premises or private cloud environments. With these features, IBM BaaS provides a trustworthy and safe cloud service.

The blockchain system's limitations mean that most existing BaaS are attached to a single cloud ecosystem, despite the many benefits of BaaS. Since the multi-chain technique has not yet been fully explored, additional study is required before it can be implemented in a multi-cloud scenario.

Exploration of BaaS

The majority of BaaS offerings strive to provide a blockchain service that is both reliable and safe to use. Obtaining a hosting service from the cloud opens up new possibilities for customization and adaptability. BaaS system performance differences between cloud and fog deployments were studied and analyzed by Samaniego et al. [30] [44]. Based on the findings,

The Seybold Report
ISSN 1533-9211

a BaaS system deployed in the cloud may offer superior computational power and storage resources to fog computing, but at the expense of higher latency. According to the research conducted by Samaniego et al. [44], a fog-based BaaS system outperformed a cloud-based one by reducing communication costs between the BaaS server and IoT devices for a variety of client counts and network conditions.

Most existing blockchain systems operate under the assumption that the need for a trustworthy third party is diminished in a decentralized environment. It was considered that all communications between stakeholders were safe, regardless of who was involved. New research suggests that this assumption may not hold after BaaS is put into place. The introduction of new service providers into the blockchain system has the potential to lead to recentralizations, as noted by Singh et al. [38]. There was a potential trust issue with the blockchain offering because the service provider was or may be a stakeholder. As the blockchain system was outsourced to a third party, there was a high probability that the majority of voters were hostile. Signing a service agreement to limit the CSP's behavior was one option.

Service providers' mistrust of their customers has also slowed the development of BaaS [45] [38]. In the past, service providers needed to demonstrate their data security prowess by providing transparent distributed ledger activities. The four proposed solutions by Singh et al. [38] are (i) increasing user controllability in a PaaS-like setting; (ii) reducing recentralization by establishing CSP federations; (iii) developing an authenticated trustful environment (like ARM's trust zone); and (iv) bolstering access controls.

Many additional BaaS model perspectives have been investigated. The Dynamic Reliability Block Diagrams (DRBDs) used to build the hyper ledger "master" and "slave" were evaluated for their reliability and availability by Melo et al. [46]. The study found that the BaaS system's availability and reliability improved as a direct result of the cloud backend offering. A similar effort was made by Lee et al. [47] to apply BaaS to IAM services. To do away with the need for a vetted third party in identity management, a Blockchain-based ID as a Service (BIDaaS) was proposed. This method published virtual ID- and ID-signature-related transactions as a service to anyone interested in registering a virtual ID. A mutual authentication linking to the BaaS ledger was used to verify identities when users accessed the BIDaaS service. Data auditing's practicability was looked into by Xu et al. [48] using BaaS.

There had also been enhancements based on preexisting BaaS models. To extend the BaaS to the server-less architecture, Chen et al. [49] suggested a Functional BaaS (FBaaS) model. The Big Data Open Architecture (BDOA) served as the inspiration for this development; the resulting model has four distinct layers (infrastructure, component, service, and business logic). BaaS-based development help toolkits were proposed by Lu et al. [50] to enable blockchain design pattern services, which included data management and smart contract designs.

Additionally, smart contract-oriented service is an avenue of study in the area of BaaS. A smart contract-based secure charging strategy for ride-hailing services was attempted by Zhang et al. [51]. Although the research did not provide a path of X-as-a-service, it did reveal a potential blue map of smart contract-as-a-service because the rule established by smart contracts might

The Seybold Report
ISSN 1533-9211

be implanted into other systems. A smart contract has the potential to catalyze the development of new services. Smart contracts enable trustworthy transactions, which can be used to implement services like Mobility as a Service (MaaS), as demonstrated in [52].

Finally, eglitar- ianism found consensus to be an essential aspect of blockchain. In [53], Marandi et al. considered a possible consensus-as-a-service technique for an SLA. To achieve the desired throughput and fault-tolerance, the approach integrated agreement and consensus. Optimizing cloud and fog computing resources may be possible using a PoW consensus strategy. To save time and resources, Kumar et al. [54] looked into the viability of employing maximization-factorization statistics with a PoW consensus. This statistical approach might obtain accurate probability in a very short amount of time. The Vehicle-to-Grid (V2G) scenario was considered by Zhou et al. [55], who employed a consortium blockchain trading mechanism to provide a low-cost demand-supply matching approach. This paper tackled the problem of information asymmetry by employing a contract-based control technique and a consensus.

Summary: Both the business and academic applications of BaaS were covered in this section. With the help of BaaS services, customers are free to focus on the features and usability of their blockchain-based applications rather than on learning how to set up a blockchain network. Easy configuration and outsourcing of maintenance contribute to BaaS's low total cost of ownership. Several large IT companies have been busy creating new BaaS service models as a subset of their cloud offerings. Our analysis showed that while the business world made some bold endeavors to delve into BaaS, very modest research accomplishments were uncovered. Trust management, data security, and recentralization’s were all issues that needed to be addressed by the more widespread use of BaaS.

III. PROVENANCE OF CLOUD-STORED DATA AS ENABLED BY THE BLOCKCHAIN

Questions of Data Origin

By 2025, the amount of information in the world is expected to grow to 175 Zettabytes explain in Figure 2, according to a prediction by the International Data Corporation (IDC) [56]. When it comes to the efficient and trustworthy administration of such massive amounts of data, data provenance is a must. Provenance is a type of metadata that tracks and explains information about an operation. When a competent provenance is implemented, CSPs are expected to provide trustworthy cloud-data management, as this information is revealed by the when, where, and how of data storage, access, modification, and deletion in the cloud datacenter.

Both cloud service providers and their customers can benefit from using provenance. Provenance meta-data could be used for debugging [66] to find potential security flaws, which would help meet providers' needs. Data provenance was introduced by Titian [67] to facilitate debugging in Data-Intensive Scalable Computing (DISC) systems. When provenance is not used, aberrant processes in clouds, such as unexpectedly running applications that continuously consume resources, may go undetected, but a provenance system can help CSPs find them [68]. The primary service provided by provenance is automated data life-cycle management. To

ISSN 1533-9211

track both product delivery and components used in production, Westerkamp et al. [57] advocated using blockchain technology. Tokens were employed to establish a connection between blocks and their respective items or parts.

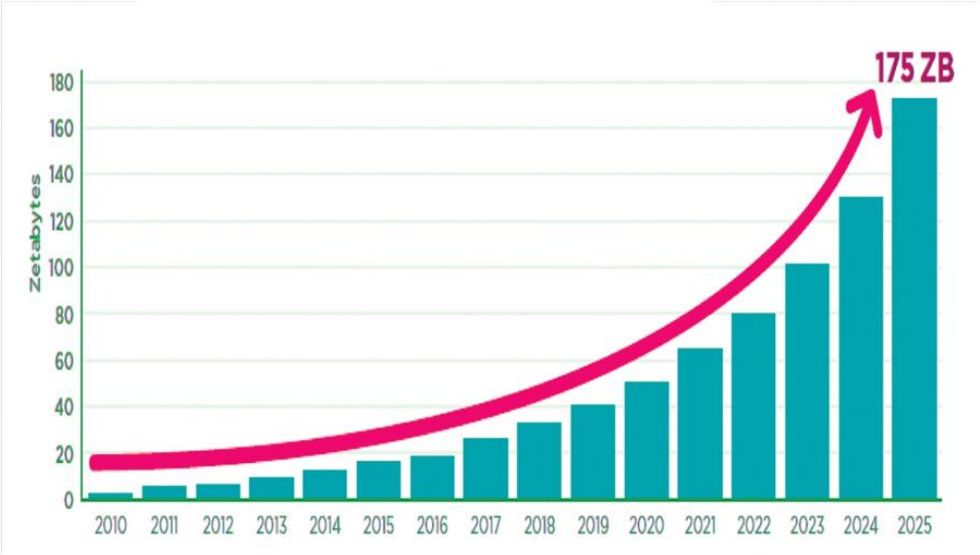

Figure 2: Information Overload In 2025

Alternatively, from the user's vantage point, provenance helps safeguard user data from the risk of malicious insiders [69], such as adversarial data mining. Provenance is a system that keeps track of both legitimate and malevolent actions. Provenance information limits the time over which SLA compliance can be tracked [70]. The potential for provenance to be employed as a recovery tool in the event of false positive detection was also demonstrated in a recent study [71].

The aforementioned provenance benefits assume that metadata is trustworthy and safe. However, the threat agent might still tamper with provenance records by disabling or misusing the provenance system [72]. An inadvertent shutdown and malicious assaults on provenance services are mentioned in [58]. To realize trustworthy provenance collections, it was suggested that a storage and analysis mechanism be implemented.

The provenance of Cloud Data via Blockchain

Blockchain's properties as a distributed, immutable ledger make it a promising tool for protecting provenance information. To record all changes made to data on blocks, blockchain-based data provenance relies on this technology's defining characteristic of immutability. Figure 3 overarching design principles for distributed ledger technology (Blockchain) in the cloud. Data provenance is improved thanks to the immutable, deterministic, and public nature of blockchain technology, as underlined by Saquib et al. [73]. Whether data are stored on-chain or off-chain, smart contracts play a crucial role in striking a balance between data provenance, functionality, and a trustworthy environment.

The Seybold Report
ISSN 1533-9211

To gather, store, and validate provenance data in the cloud, ProvChain [58] was a private chain. Programs called "hooks" in this blockchain-based provenance architecture tracked changes to the cloud infrastructure and stored the resulting data. Additionally, provenance data were delicate and prone to data misuse [74]. To ensure users' anonymity, ProvChain displays their identities in a hashed format. The hashed value could only be linked to the user's actual identity by the service provider. Some private information, however, was still recorded in the blockchain's unencrypted plaintext form.

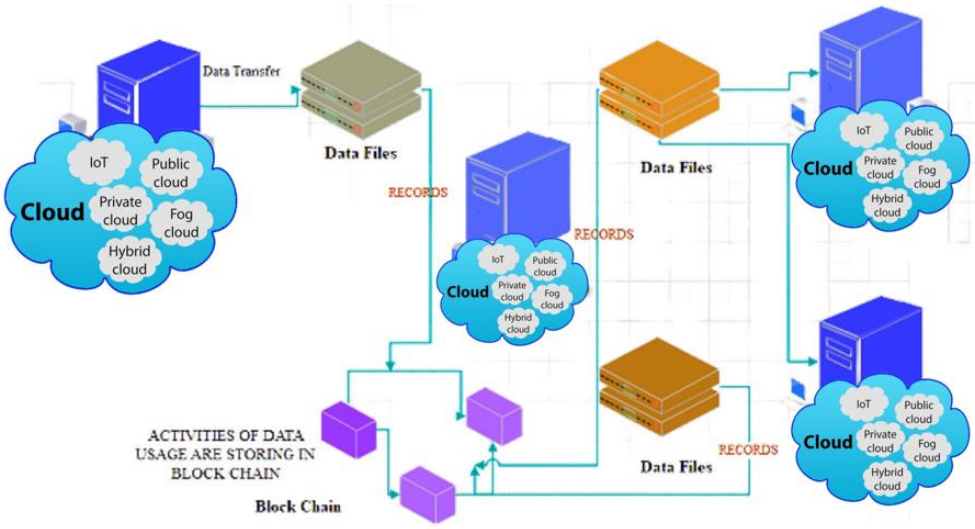

Figure 3: Overarching Design Principles for Distributed Ledger Technology (Blockchain) In the Cloud

Automatic verification of the data provenance process was first presented by the Smart Provenance [59] system. Smart Provenance uses a voting method to construct a decentralized peer-to-peer verification scheme, unlike ProvChain's reliance on auditors for verification. This eliminates the need for a trusted auditor. Smart contracts were used for both provenance collection and verification, making the system automated. To protect users' anonymity, Smart Provenance kept just hash values on the blockchain and kept all other data off-chain. Blockchain technology was also utilized by Grid Monitoring [61] to provide an immutable record of the origin of cloud-hosted information about electricity consumption. Therefore, with the help of a smart contract, which offered transparency and a non- credible data record, discrepancies in actual power usage between consumers and power providers could be addressed.

Due to the layered architecture of the cloud, federated service providers will need to be included in the service delivery process [5]. Offloading of resources and work was commonplace among CSPs. Because of their one-provider focus, ProvChain and Smart Provenance weren't a good fit for federated clouds. The absence of compatibility made it difficult to apply [58] [59], and [61] in a federated cloud setting.

The Seybold Report
ISSN 1533-9211

Xia's [60] group launched MeD- Share to accomplish data provenance and auditing in the federated cloud setting, which was a significant problem. To combat malicious assaults that could cause financial and reputational harm, a provenance function was developed for use in secure data sharing across service providers that cannot be trusted. Because of the access control-oriented smart contract and the tamper-resistant provenance system, data owners hosted full control of data provenance [75]. CSPs were expected to implement automatic access control to revoke access to harmful or abnormal entities when violations or misbehaviors were found during the provenance phase. Under the terms outlined in the paper, medical institutions were able to share patient data without jeopardizing the privacy of their patients.

Nessie et al. [62] also built a blockchain-based data provenance tracking system to meet the privacy standards of the European Union (EU). Similar to MedShare [60] [62] used a smart contract to keep track of provenance data and access policies. Three distinct forms of smart contracts worked in this system to back detailed provenance records from the viewpoints of the controller and the subset of data in question. With complete metadata records from both the controller's and the data's points of view, CSPs were able to confidently engage in data-sharing manipulations. The research [76] took into account the block-based organization of data and applied differential privacy methods to the screening of raw data. Differential privacy in blocks was investigated as a potential strategy for protecting against data mining-based attacks.

From a safety standpoint, the blockchain-based prove- nance method was identified as a means of protecting manufacturing operations' data-handling procedures. A secure data operation architecture was proposed by Maw et al. [65], which took into account both immutability and redundancy. Integrity verification and auditable data replication mechanisms were both built using the blockchain system. One way to characterize this approach is as a blockchain-backed storage service. The distributed nature of the network architecture also helped boost the data's inherent defenses [77].

Blockchain was a technological option for integrating data as well. The blockchain technique was shown by Chen et al. [78] to provide improved data integrity protection compared to conventional techniques. A stochastic blockchain technique was implemented, limiting the number of cooperative nodes and making use of IoT edge devices for offloading.

Instead of providing massive amounts of storage on a pay-as-you-go basis, some cloud services attempted to provide High-Performance Computing (HPC). Thus, these cloud data centers shared the remote storage and did not use any disks. The substantial I/O overhead of the aforementioned blockchain provenance designs makes them unsuitable for use in an HPC environment. To achieve reliable and effective provenance in HPC systems, Al-Mamun et al. [63] developed an in-memory blockchain. Distributed ledgers are at the heart of this new framework.

Were kept in temporary memory and communicated using fast and persistent protocols to cut down on I/O latency. To provide reliable provenance data validation and replication in an uncertain setting, a novel consensus protocol called Proof-of-Reproducibility (PoR) has integrated the concepts of Proof-of-Work (PoW) and Proof-of-Stake (PoS). The experimental

The Seybold Report
ISSN 1533-9211

findings showed that the proposed solution has a lower latency overhead compared to the conventional database and file provenance system.

Consensus methods in blockchain-based cloud provenance systems were also the topic of BlockCloud [64]. De-anonymization, 51% attack, blockchain fork, consensus latency, and selfish mining are the five security issues addressed in this method for PoW provenance systems. BlockCloud was built with PoS in mind to solve the aforementioned issues and provide trustworthy data provenance. BlockCloud's provenance procedure was very similar to ProveChain's [58]. The limitations of a cloud provenance system based on PoS were also explored.

The data lifetime was managed and recorded in detail thanks to data provenance technologies. Data provenance methods of the past were typically centralized, complex, and lacked adequate safeguards and validation. Existing works that utilize blockchain technology to address contemporary issues are outlined below. Data provenance privacy and interoperability were also considered. Future efforts to solve cloud data provenance using blockchain technology should center on a smart contract-based system that rewards good conduct and penalizes bad.

IV. BLOCKCHAIN-BASED CLOUD ACCESS MANAGEMENT

Security and Privacy in the Cloud

To prevent unauthorized users from gaining access to sensitive information stored in the cloud, access control was a crucial measure. Because of the inaccuracy of the access control technique, other features, including authentication, authorization, and data auditing, were compromised. The difficulties of using conventional approaches to controlling access in cloud computing were explored in Figure 4 (A framework for the organization of data privacy and security in cloud computing).

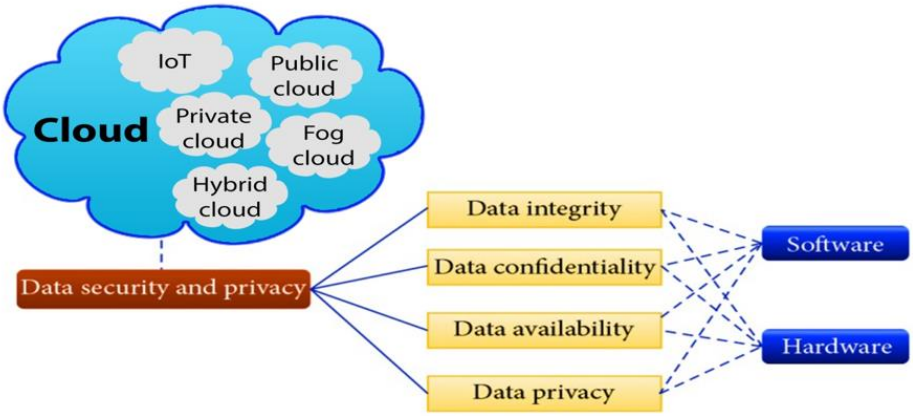

Figure 4: Cloud Computing Data Security and Privacy Organization

When it comes to clouds, the standard technique of access control has always relied on preexisting policies. Existing conventional rules have been broken down into four classes:

The Seybold Report
ISSN 1533-9211

Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role-Based Access Control (RBAC), and Attribute-Based Access Control (ABAC). DAC required the legitimate user (e.g., service provider) to control how unauthorized users (e.g., cloud users) accessed things [79]. Since no hard and fast rule is necessary for DAC, this approach allowed for a versatile kind of access control for cloud users. In contrast to DAC, MAC relied on a static trust policy that had already been established. The model emphasized confidence over integrity [24], as the system administrator was in charge of access controls rather than objects.

Instead of basing permissions on users' names, the RBAC model takes into account users' roles and responsibilities inside the system [24]. The problem with RBAC is inherent in the system, as it does not take into account various facets of a subject. Additionally, ABAC was proposed to address these concerns. Attribute analysis of objects and subjects was used to set up the access rule [80]. The all-encompassing nature of ABAC's examination during authentication was a major gain. While the ABAC authentication procedure took some time, the amount of computational resources it consumed was minimal in a cloud setting.

Each access control approach, as we've seen, has its advantages and disadvantages. Traditional access control techniques sometimes have the drawback of being overly dependent on a centralized setting, which makes them less than ideal in terms of lack of transparency, traceability, tamper- resistant, and multi-party governance. The trade-off between security and efficiency occurs and is difficult to solve in nature when the specific application environment is taken into account.

Controlled Access to the Cloud Using Blockchain

There are a few advantages to using Blockchain-based Access Control (BAC) instead of more conventional techniques of access control. Our research reveals two major benefits. To start, BAC makes it possible for all relevant parties to reach an agreement on how access control should be implemented. From a decentralization standpoint, security is enhanced because reaching a consensus typically requires the agreement of all participating voters or decision-makers. Second, the audit trail provided by blockchain makes it possible to have immutable, auditable controls on who has entry. Because of this, enemies will be more challenging to take on. Here, we take a look back at some of the more notable recent contributions to BAC. Access control in clouds primarily served two purposes due to the layered nature of cloud architecture. The first was the cloud service role, whose responsibility was to regulate how cloud users accessed the cloud's resources. Recent research by the name of BlockSLaaS [81] suggests using blockchain technology to facilitate the provision of Logging-as-a-Service (LaaS). The proposed mechanism dealt with cloud forensics, which served as a representative example of how blockchain and access control may be combined. However, it was visible enough that control was required over Virtual Machine (VM) access to actual machines to protect against side-channel analysis concerns [82]. The potential for data misuse and single points of failure can be mitigated using blockchain-powered decentralized access control systems. Using blockchain technology, data owners would have total and granular control over who has access to their data [83]. The ability to share data in an untrusted environment was recently demonstrated by a study [84]. Risks posed by untrustworthy actors could be sidestepped in a

The Seybold Report
ISSN 1533-9211

decentralized system [85]. Nugyen et al. [86] looked at the performance of BAC in a scenario where medical records are shared. According to the results, BAC has the potential to provide reliable access controls for a wide range of healthcare organizations.

Because blockchain transactions are immutable and transparent, they have been used in some methods to direct the cloud's access control process. A decentralized personal data controlling system for off-chain mobile data storage was created by Zyskind et al. [87]. There are two kinds of deals in this blockchain system. The original transaction format, Taccess, was created specifically for the administration of security clearances. Tdata transactions, on the other hand, were in charge of archiving information. By establishing a new policy set in the Taccess transaction, data owners can alter the authentications used to gain access to their data. To further regulate read/write activities, Tdata works together with the check policy protocol. In this blockchain-enhanced DAC paradigm, malicious invasions (from unauthorized users) could be prohibited because users have complete control over their data thanks to digitally-signed transactions. Specifically, four protocols compound key generation, permission check, access control, and data on/off-chain protocols were built to create a dynamic and fine-grained access control protocol for the protocol-based transaction.

Extensions of blockchain were also discussed by the authors of [87]. Since the initial phase of the extension's implementation relied on off-chain data processing efficiency, it was necessary to ensure the confidentiality of off-chain information while it was being processed. Analysis employing a secure multi-party computation model to partition data into shares was presented as a solution to this problem [87]. The second part of the upgrade was a confidence index for the blockchain infrastructure. One alternative method of gauging trust proposes using the sigmoid function defined by the ratio of "good" to "bad" deeds. The evaluation findings demonstrated that the blockchain system might be protected from sybil assaults thanks to this trust metric.

Engima [88] is another study that presented a decentralized computing system that protects user privacy. It was built to be the most efficient system possible for conducting secure multi-party computations. The various components of this system were purpose-built to perform specific computing and privacy-protection duties. The scalability problem was solved by implementing this architecture, which avoided redundant computations and storage. To implement Prove- nance Based Access Control (PBAC), as specified by Nguyen [89] in 2012, ProvChain [58] gathered immutable on-chain provenance data.

When implementing transaction-based access control, we also noticed that scalability was an issue. To address this problem, BBDS [90] presented a lightweight block structure to boost the system's efficiency and scalability. This concept was used to safeguard private health records kept in the cloud. This private blockchain network's scalability was made possible by its innovative block structure design. Furthermore, access control was implemented by a coordinated effort between identity-based authentication, cryptographic methods, and transaction verification. However, BBDS was not built on any public blockchain project, hence it lacked the maturity and substantial experimental verification of more established blockchain projects.

The Seybold Report
ISSN 1533-9211

Smart contracts were another commonly utilized alternative that could be used to fortify access control as we entered the blockchain 2.0 era. Some researchers developed an access management system for private health and medical data in a telemedicine setting using smart contracts.

A blockchain-based therapeutic management approach was developed by Rahman et al. [91]. The access policy of off-chain data was built into smart contracts while users' medical records were stored in off-chain clouds. The reliance on trusted third parties like physiotherapy facilities, caregivers, and therapists was the approach's biggest flaw. The MedShare [60] solution implemented access control through a combination of several types of smart contracts and cloud-provenance data. Some contracts were in charge of making decisions about whether or not to take action based on provenance data, while others were tasked with carrying out the decisions. In addition, malevolent cloud users had their access privileges revoked as a kind of punishment. Unfortunately, the only action MedShare could do in access control was to revoke authentication privileges.

Smart contract-based access controls were also applicable in the context of decentralized cloud infrastructure. Under the aegis of the Organization Based Access Control (OrBAC) concept, FairAccess [92] deployed an access control mechanism based on smart contracts. Different access tokens from transactions could be used to grant, read, delegate, and cancel permissions in this system. Fine-grained and context-aware access control policies were given through a smart contract embedded into the transaction. This system was built using a Raspberry PI to demonstrate its viability. Similar to how Novo et al. [93] centralized access policy management via a smart contract architecture. A variety of edge devices in this work could connect to the blockchain infrastructure through centralized nodes. Additionally, all edge devices had their access policies updated in real-time by the central administration hub. To accomplish both access management and punishment for wrongdoing, Zhang et al. [82] used a three-part smart contract architecture consisting of an access-control contract, a judge contract, and a registered contract.

Wang et al. [94] combined ABAC with the blockchain framework to create a DSS with fine-grained access control based on attributes rather than just permissions. Historically, Public Key Generator (PKG) has been used for attribute-based encryption. If the PKG were compromised, the entire system would crash and important data may be stolen. Instead of relying on a trusted PKG, the blockchain was in charge of key management in Wang et al.'s [94] architecture. Users had complete control over their data thanks to blockchain's immutable and traceable key management system, which rendered the technique immune to the leakage and misuse typical of systems with only a single point of failure.

However, the aforementioned studies (except MedShare, which just performs a revoke operation) were developed for a single CSP scenario and hence did not take into account cloud federation. Therefore, these architectures can only guarantee the privacy of data within a single cloud, not a federation of clouds. In 2016, FaaS [97] offered a centralized authorization framework for federated cloud infrastructure. The authors of this study introduced a PEP and a PDP, two components of a policy-based access control architecture. User requests were

The Seybold Report
ISSN 1533-9211

collected by PEP, while access permissions were handled by PDP. From the success of the FaaS framework, a few further attempts were undertaken. For instance, DRAMS [95] was built using the FaaS infrastructure. For authentication and threat detection, this system made use of smart contracts to gather, compare, and check user logs. DRAMS was impervious to changes in policy and choices made by access control systems. Problems with this strategy included delays and potentially insecure off-chain system components. Alansari et al. [96] developed an attribute-based fine-grained access control technique with similar goals to DRAMS. The Oblivious Commitment-Based Envelope (OCBE) protocol was used across the decentralized federation to protect user anonymity. In this application, blockchain ensured the consistency of attributes and policies [43].

In conclusion, access control was crucial in preventing hackers from gaining access to sensitive user information. Problems with signal point failure, unreliable trusted third parties, and a lack of user control plague conventional approaches to access control. Users would have complete control over their data without worrying about a central point of failure if blockchain technology were implemented. Smart contracts also enabled automated access management, behavior monitoring, and enforcement of appropriate sanctions. All of these approaches of access control were used to implement safe cloud-based data storage. But cloud virtual machines also required access control mechanisms to prevent side-channel assaults. We found little research on the use of blockchain for managing virtual machine access. Soon, blockchain-based cloud virtual machine security will emerge as a hot topic of study.

V. SEARCHABLE CLOUD ENCRYPTION BASED ON BLOCKCHAINS

Questions and Concerns about Searchable Encryption

Users who are worried about giving up control of their data can take precautions like encrypting files before uploading them to the cloud. This precaution will ensure that the service provider is unable to access and analyze private information. Depending on the level of security implemented, this may result in a decrease in service availability. One of the most typical issues was the difficulty in searching the encrypted outsourced data. Searchable encryption was proposed to solve this problem by allowing users to access search results without having to decrypt all of their cloud-stored encrypted data. Searchable symmetric encryption (SSE) and searchable public key encryption (PKE) are two types of existing searchable encryption methods. As a representative technique of the first generation of search encryption, Song et al. [98] developed a searchable encryption scheme based on symmetric encryption as a two-layered form. Public key-based asymmetric searchable encryption was proposed by Boneh et al. [99], building on the foundational work of Song et al. To perform a multi-keyword search, the authors of [100] proposed using a conjunctive keyword search technique. All the aforementioned strategies for decreasing availability performance relied, however, on exact matching. To further address this concern, Li et al. [101] substituted the fuzzy keyword search with exact matching, which provided the most relevant result Figure 5 explains the system model for the verifiable search encryption scheme based on blockchain in the cloud environment. The above works were built on the premise that CSPs adhere to an honest-but-

The Seybold Report
ISSN 1533-9211

curious model [102]. However, several insider threats rendered this premise untenable in the real world. Due to concerns over energy efficiency and redundancy, dishonest servers may intentionally return inaccurate data. This meant that in a searchable encryption scheme, a verification mechanism would be desirable. Although various efforts [103–105] attempted to ensure the accuracy of returned values, no penalties could be enforced in the absence of a reliable third party. Also, there was a lack of thorough investigation into the verifications, both on the server end and against rogue users.

Searchable Encryption Facilitated by Blockchain

Recent efforts have centered on improving upon preexisting blockchain-based mechanisms. A study on improving encrypted keyword search with blockchain was completed by Cai et al. [106]. The research uncovered a problem with integrating encryption with a keyword search using a distributed hash table protocol: malevolent nodes could corrupt search results. Most nodes operate on their own accord, therefore the suggested approach can identify and eliminate any bad apples. Zhang et al. [107] proposed a PKE supported by the blockchain and referred to as a SEPSE to protect against KGAs. Several approaches, including screening key encryption, periodic key renewal, and key request monitoring, were recommended in this work to lessen the likelihood of successful KGA. To combat the problem of key leakage, the authors of the study [108] devised a searchable encryption system based on key aggregation to be used in opposition to CPA.

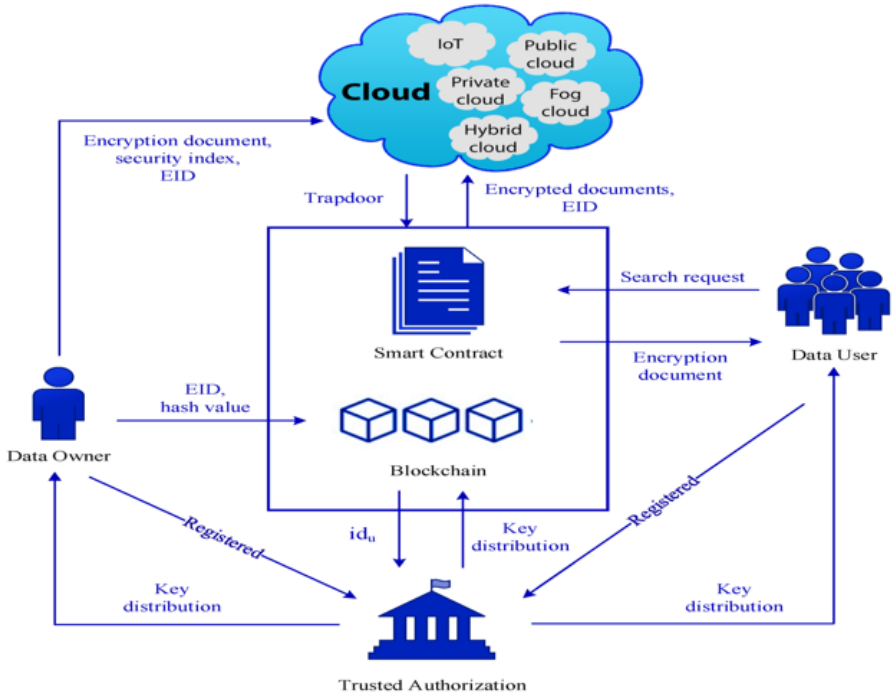

Figure 5: The Cloud-Based Blockchain-Based Verifiable Search Encryption System Model

The Seybold Report
ISSN 1533-9211

In other methods, broadcasted transactions helped verify the search result. One such technique is Searchchain [109], which uses the Obvious Keyword Search with Authentication (OKSA) mechanism to offer public key encryption without compromising privacy. Keyword search authorization is a revolutionary OKSA mechanism that was developed to overcome the limitations of conventional Oblivious Keyword Search (OKS). It was proposed that CSPs validate user access authentication with a search term as a means of further protecting user privacy. Without acknowledging any keyword information, data retrieval instructions were stored on the block and transmitted to all nodes for verifications via consensus.

A blockchain-based time commitment approach with many transaction types was proposed by Bpay et al. [110]. In this scenario, the dishonest party would be financially penalized in bitcoins without the need for a TTP. Two-way verification in a searchable encryption system was initially proposed by TKSE [111], a follow-up study. It's possible to punish both the malicious service provider and the malicious data owner. The authors built a Merkle tree out of ciphertext leaves and checked the results by looking at the root. Payment fairness [116] was founded on the same principle as Bpay, namely the concept of time investment.

In [112], the value of the returned keyword and the token used to search were both saved on the search transaction. Data integrity checks were executed using multi-set hashing, an incremental hashing algorithm. There were two categories of people taking part in this scenario. To begin, Clint Peers acted as the data owner, while Storage Peers provided the underlying storage infrastructure. The other group, Client Peers, asked Storage Peers to look for ciphertext that could be verified. Additionally, this approach offered improved storage efficiency and real-time modifications. Instead of relying on a time commitment, as was done in [110][111], this approach relied on transparent metadata as its method for fairness.

Even while there are measures in place to ensure transactions are legitimate, miners can still choose to ignore them in favor of more lucrative endeavors. They coined the term "Verifier's Dilemma" to describe the situation [117]. In [113], the authors investigate the use of smart contracts to provide safe keyword searches without requiring extensive validation procedures on the part of data owners. That is to say, if the Ethereum blockchain was secure, then the results would be guaranteed to be sound. By including the search algorithm in the smart contract, only upon the successful execution of the contract on the blockchain would accurate results be guaranteed. No longer was it necessary to manually verify the accuracy of the found information. Additionally, the author used encrypted indexes in the dictionary to lessen the burden on the computer. Gas was also saved through efficient packing.

In addition, this method uses smart contracts to ensure that all parties are fairly compensated. Implementing payment fairness measures may encourage the honest and punish the dishonest. In both a single-user and a multi-user environment, time commitment was employed to guarantee equality. To promote integrity throughout the SSE procedure, for instance, Zhang et al. [110] [111] implemented a fair payment system.

Users' file indices were kept in the blockchain, while actual file storage was handled by third-party cloud providers. Smart contracts also gave time commitment, which is a type of fairness

The Seybold Report
ISSN 1533-9211

[116]. When testing for fairness, we took into account both a single-user and a multi-user environment. Subsequent work by Chen et al. [106] extended Hu's work [113] into a scenario of exchanging electronic health records in response to queries from various health agents. Unlike Hu's work, the EHR index was not manually compiled but rather generated using complicated logic expressions and recorded in a blockchain. Data owners would have complete say over who has access to their information thanks to their efforts.

Zhang et al. [114] also addressed medical data, but in the context of a personal health information-sharing scenario, they proposed a public keyword encryption approach. PHI data was intended to be stored on a private blockchain deployed in a private cloud, while PHI indexes were intended to be maintained on a consortium blockchain accessible via encrypted search. This work's time-controlled revocation kept users' data safe from the honest but nosy physicist. The physician was unable to use the trapdoor in the future to access the patient's information once the key word search procedure had been completed.

There was also the option of combining with other technical approaches in this field. In a recent paper [94], researchers combined attribute-based encryption and SSE to create a blockchain framework with flexible permissions and searchable encrypted keywords. By pre-collecting the user's search fee, the smart contract ensured a fair payment process. While the fair pay algorithm in [94] was successful in rewarding users when CSPs were honest, it was not successful in punishing dishonest CSPs. Thus, under the condition of a malevolent service provider, the fair payment mechanism in [94] was not as effective as [110] [111] [113].

Summary: Cloud customers can search their outsourced data thanks to searchable encryptions. Since the CSP(s) could be either benignly curious or malicious, the results of encrypted searches could be off. Using blockchain's transaction verification and smart contract features, we were able to produce trustworthy search results. Equal compensation was also a major factor. A malicious user could get the right information and then refuse to pay. Even if the payment method was poorly conceived, users were still able to pay for the incorrect search results. Time commitments inherent in either the transaction or the smart contract ensured that all parties were paid fairly. The aforementioned problems of SSE have been addressed by the vast majority of blockchain-based searchable encryption thus far. More study was needed on the use of blockchain in PEKS.

VI. BLOCKCHAIN FOR REDUPLICATING INFORMATION IN THE CLOUD

Cloud-Based Data Redundancy Checking

By 2025, the cloud is expected to store over 88 Zettabytes of data, with 75% of that being copied [118]. Most cloud storage providers (CSPs) use data deduplication in their StaaS products (like Dropbox or Google Drive) to increase efficiency. This technology has the potential to benefit both CSPs and end users by decreasing operational costs (such as those associated with electricity and infrastructure) and enhancing efficiencies (such as those associated with data storage). However, significant security issues persisted in deduplication methods.

The Seybold Report
ISSN 1533-9211

To protect the privacy of information that has been transferred to a cloud server, cipher-texts may be used. The effectiveness of the deduplication was impacted, however, because CSPs typically forbid users to encrypt their information by conventional encryption means (such as AES) [119]. Instead, cyphertext deduplication was accomplished via the use of convergent key encryption [120]. Convergent encryption was hypothesized to be a subset of message-lock encryption (MLP) [121]. Additionally, the authors demonstrated that the MLP lacked semantic security. A TTP for delivering tags that helped with the duplicate check was included in the following study [122]. Our research suggests that the centralization of this method is the primary source of its potential difficulties. If the TPP were to go down, the deduplication mechanism would be useless. Adversaries can conduct side-channel attacks against a source-based deduplication system by breaking into the TTP and retrieving file tags.

Furthermore, the deduplication procedure posed a threat to data integrity. Deduplication reduced the number of potentially vulnerable copies to one. This meant that data stored on the device could be permanently deleted in the event of a service interruption or a rogue administrator. Users' data in the cloud, where deduplication was applied, needed to be audited to ensure its safety. Reliable auditing can be attained by utilizing a trusted authority that does not rely on a single point of failure [124].

Deduplication of Cloud Data Using Blockchain

The current blockchain-enabled methods mostly concentrate on a decentralized multi-cloud data-replication scheme. The incentive of a high deduplication rate and fault tolerance performance led to the adoption of blockchain technology to regulate multi-cloud deduplication operations. Blockchain was first used in multi-cloud deduplication management by CloudShare [125]. User-side encryption was used to protect the system from malevolent servers that were in on the conspiracy. The immutability of blockchain transactions ensured the privacy and security of the user data. Multiple CSPs were able to swiftly synchronize file information thanks to blockchain's facilitation, allowing them to dynamically direct a deduplication mechanism. A smart contract-based cloud deduplication system was presented by Li et al. [126], [127]. To ensure file integrity, recoverability, and resistance to side-channel attacks, a business smart contract (BSC) would periodically perform Proof-of-Retrievability (PoR) using a challenge-and-response protocol. After the server has completed the Proof-of-Responsibility (PoR) challenge, the TSC is automatically issued and transaction and payment management are conducted without any more intervention on the part of the BSC. Distributed storage helped [128] outperform [126] thanks to its automated file rebuilding.

Although blockchain-based cloud deduplication is extremely important, not enough has been done in this area until now. A major roadblock was the inherent incompatibility between the high-redundancy of blockchain data and the desire for deduplication. There was no workable alternative wherein a blockchain would be able to recreate a deduplicated cloud storage system. It appeared that blockchain was used as a component in a larger system to guarantee the safety of cloud data storage. Previous efforts put file tags on the blockchain while the actual files themselves stayed off-chain. In this configuration, system security and data integrity could be improved while just a negligible amount of storage space was required.

The Seybold Report
ISSN 1533-9211

VII. CLOUD RESOURCE DISTRIBUTION ENABLED BY BLOCKCHAIN

Allocation of Resources in the Cloud

Maximizing energy use and optimizing computation efficiency are two typical targets of cloud resource allocation [129] [130]. It's common knowledge that cloud data centers store vast amounts of data, and that number only grows as services expand and networks expand. When there is a lot of work being done in the cloud, the data center has to use a lot of power. To cut down on service fees, cloud data centers are working to build an energy-aware task scheduling mechanism, and a blockchain-powered allocation technique is one solution [131] [132]. The blockchain was used by Zhang et al. [133] to try and improve the computational power of mobile edge computing. This research sought to find a solution to the combined computation offloading and coin loaning problem by focusing on the lowest possible cost of computation. Byzantine Fault- Tolerant (BFT) networking was created by Xu et al. [134] to ensure the safety of data while maintaining high performance. This study looked at two scenarios, one with a single Byzantine fault and another with numerous faults.

Scheduling tasks' "distance" from consumers is one-way cloud resource allocation issues are sorted [135]. That is to say, there are several levels at which problems might be classified. Task scheduling in the cloud works to improve datagram exchanging and cloud federations at the infrastructure level. The platform-level optimum migration problem and the virtual machine-to-hardware mapping issue are both typically addressed by task scheduling. Finally, problems at the application layer focus on meeting strictly defined optimization criteria, such as Quality of Service (QoS) or energy efficiency standards.

The difficulty arises from the fact that, when taking into account various factors, most cloud resource scheduling problems are NP-hard problems. One common type of trade-off in scheduling challenges involves the time complexity versus the energy cost. Time and money spent on exhaustive approaches like liner programming [136] grow exponentially with the number of variables. High-efficiency scheduling has been proposed using evolutionary methodologies [137], such as genetic algorithms, ant colony optimization, and particle swarm optimization.

Most existing scheduling solutions, however, were not able to execute real-time scheduling since they were based on a centralized control center, making them look rigid in responding to users' diverse needs. By enabling the development of a decentralized resource scheduling system, blockchain technology offers a potential solution to the problem presented by the control center.

Allocating Cloud Resources with Blockchain Technology

It has come to our attention that some of the technical aspects of blockchain, such as the construction of a trustworthy platform (visible and traceable token transactions) and the use of smart contracts, are being integrated into cloud resource allocations.

Financial incentive tokens could be used to create a decentralized incentive structure for resource allocation. Each Electric Vehicle (EV) could be thought of as a mobile cloudlet and a

The Seybold Report
ISSN 1533-9211

moving power plant, according to the innovative Vehicular Ad hoc Networks (VANETs) design described by Liu et al. [126]. To facilitate dynamic resource reallocation, idling electric resources from EVs were pooled into a source pool that was directly influenced by crypto coins. Proof of Data Contribution (PoDC) consensus was used to determine how data contributions between moving cars would be compensated. The "energy coin" was used to incentivize the provision of other resources, such as power. This blockchain-based approach allocated resources proportionally to the number of tokens held by each EV. A large number of coins indicates the owner actively participates in collaborative management. Owners with more coins may have cheaper access to the resource pool, which may encourage them to contribute more frequently. One interpretation of this mechanism is token-based resource allocation. However, due to a lack of assessments, the efficacy of this strategy has not been thoroughly studied.

Most current cloud systems rely on a central broker to provide resources for one or more specific application scenarios; one of these scenarios is the supply of infrastructure services. To achieve a transparent allocation procedure, Ghosh et al. [138] presented a method that eliminates the need for a central broker. Consequently, blockchain-enabled resource allocation was identified as a promising approach to building a reliable and open cloud federation [139]. In another paper [140], the "FlopCoin" was used to provide efficient compute offloading between mobile devices and cloud servers. To incentivize users to carry out the offloadable duty, FlopCoin was developed. The availability and standing of team members were also taken into account while allocating resources. Pricing strategies were discussed, with both fixed pricing and auction procedures taken into account for the resource price.

Reinforcement learning's popularity in the field of resource allocation has skyrocketed alongside the popularity of machine learning itself. To efficiently collect data from the cloud and share it securely, Liu et al. [128] presented a collaborative framework that makes use of deep reinforcement learning and smart contracts. Following up on their previous research, Xu et al. [141] first integrated a reinforcement learning algorithm into a smart contract to optimize request migration in a distributed cloud computing environment. Off-policy temporal-difference learning (Q-leaning) was proposed as a solution to the issue, and it proved to be both effective and realistic in its modeling of the migration problem, in which both reward and transfer probability were uncertain.

To summarize, some blockchain-based systems incentivize resource allocation by issuing tokens due to the cost-effective nature of the blockchain. Tokenized incentive-based cloud resource allocation may boost resource share and energy costs. In some implementations, a reinforcement learning algorithm is included in the blockchain itself. This would allow cloud data centers to distribute their resources more efficiently. There was a lack of study on the topic of scheduling cloud resources using a blockchain. One possible direction for future study is the integration of incentive and optimal allocation approaches [43].

The Seybold Report
ISSN 1533-9211

VIII. BLOCKCHAIN DATA OFFLOADING FROM THE CLOUD

While blockchain systems have many desirable properties, such as security, transparency, and fault tolerance, blockchain-based applications frequently require robust backend service capabilities. As a first point, the majority of blockchains used proof-of-work consensus. PoW blockchain's limited computational capacity prevented it from being implemented on mobile communication devices like smartphones [26], [142]. One possible way out of this predicament is to outsource the solving of this cryptographic puzzle game. Second, due to the blockchain system's poor throughput and great redundancy, it could be prohibitively expensive to store all data on-chain using only locally available hardware. To solve this problem, you might use a scalable off-site storage provider.

PoW has been a key consensus mechanism in blockchain systems ever since Bitcoin was introduced [143]. PoW mechanisms need miners to solve a cryptographic puzzle to earn the privilege of packaging a block. PoW is computationally exhausting for every node in the blockchain network, despite its excellent fault tolerance and security. Therefore, such a large computing cost is prohibitive for resource-constrained edge devices. Similarly, resource-constrained machines had a hard time carrying out complicated smart contract execution [5]. Smart contracts were offered as a unique method to improve smart grid task allocation in the paper [144]. A smart contract was implemented to dynamically and automatically manage the energy supply. The system employed a reinforcement learning strategy adaptable to a dynamic setting. Also highlighting the auto-control feature of smart contracts is the implementation of a contractual routing protocol in the Internet of Things [145]. To overcome this difficulty, some researchers have begun to offload computational work between devices and cloud servers.

Revenue Sharing with Users Offloading

From the point of view of the miner and the user of the service, offloading strategies have been developed to increase the profitability of the PoW cryptographic game. These works presuppose that the cost of a unit of energy has already been established by some sort of regulatory body. To improve computational efficiency, the profit optimization problem was reformulated as one that sought to reduce overall costs.

To maximize overall net revenue, the authors of work [146] suggested a mobile edge computing based compute offloading and content caching joint system, which they evaluated using a metric that factored in both task delay and energy usage. This was because the optimization task involved minimizing costs, and the unity energy price was fixed. For computationally indifferent mining tasks, two offloading strategies were developed. The first approach involved sending the entire mining job A (m,n) to a nearby access point that was linked to a cloud server. The second method broke down the overall mining job into smaller tasks that were then assigned to individual devices. To find a way to tackle this distributed optimization problem, the optimal offloading choice was built using the Alternating Direction Method of Multipliers (ADMM) [147] algorithm. Rayleigh fading, noise, channel attenuation, and CPU cycling were all taken into account within the context of practical radio wireless communications, as was the relationship between users and time efficiency. At the same time, the power requirements

The Seybold Report
ISSN 1533-9211

of both the dynamic (CPU) and static (static) circuit components. The results of a continuation of the work [146] are provided in [148]. As in [146], two offloading mechanisms were proposed to work in tandem with the ADMM algorithm to maximize total net revenue. Offloading and caching measurements also made use of stochastic geometry techniques. In contrast to [146], the deadline restriction in [148] is based on the likelihood of an orphaning block rather than the anticipated overall delay. As a result of these tests, the distinction between probabilistic and deterministic constraints became clear. Probabilistic constraints were found to be more profitable than deterministic ones. The optimization took the token cost into account when making decisions. Model performance and miner preference under varying deterministic backhaul restrictions (BH) were extensively discussed in this paper. The approach relied so heavily on adjacent network nodes (edge devices) that its performance in the actual world could be affected by the total number of nodes involved.

In their follow-up studies, Liu et al. [149] implemented a blockchain offloading approach in video streaming systems to facilitate user engagement. Video transcoding is a computationally intensive process, hence it was necessary to offload it to local servers. The offloading was designed to increase the typical transcoder's earnings in tokens. There's potential for offloading at the small cell base station level and the Device-to-Device (D2D) user level. The team then applied a distributed ADMM-based approach to the non-convex issue. This blockchain network's block size was dynamically adjusted to accomplish the aforementioned optimization.

As Mobile Terminals (MT) offloaded computationally intensive PoW operations to the Edge Servers (ES), studies [150], [151] focused on the entire reward from the MT's vantage point. Consideration was given to ensuring that all MTs were treated fairly. As an expanded version of [151], we focused mostly on [150]. To accommodate both single ES and many ESs scenarios, two distributed optimized algorithms were presented. The non-convex Total Reward Optimization (TRO) problem was split vertically into two subtasks (TRO-sub and TRO-top) by the solution. Since TRO-sub was a convex optimization problem, it could be solved using either bisection-search or diminishing step size in a single or many ES. The TRO-top was optimized using a randomized search in the multiple ES case, and a linear search with a short step to determine the best viable interval that maximized the sub-problem in a single ES case. The proposed strategy outperformed equal allocation in terms of total reward, as demonstrated by the experiments.

Offloading with a focus on social welfare

Here, we zeroed in on an auction-based offloading approach to maximize CSP income or societal welfare. The resource price was dynamically set via auction in response to miners' demand. As a result, we could make good use of the cloud's abundance of resources. To maximize the social welfare of cloud/edge service providers, Jiao et al. [152] used an auction technique to allocate and price resources on edge servers. From the user's vantage point, the auction process for mining had two distinct phases of appraisal. In the first phase, miners had no idea how many people would ultimately win or how much material would be at stake. By the anticipated gain, the bid was also referred to as an ex-ante value. In the following iteration, the miners factored in the auction outcome and calculated an ex-post valuation. The expected

The Seybold Report
ISSN 1533-9211

reward multiplied by the network effect was used to define the ex-post valuation. In this work, an empirical definition of the network effect was provided by an S-curve function, which outlined the trade-offs between the number of miners, the robustness of the blockchain network, and the resources allotted to each miner under the constant demand model.

To maximize social welfare, as defined by the gap between the sum of ex-post valuations and the total cost of CSPs, an optimal algorithm was developed for resource providers [152]. In this study, a greedy mechanism was applied in the winner selection process to maximize social welfare. Following the finalization of the winning set, the Vickrey-Clarke-Groves (VCG) [157] technique aided in the determination of compensation. According to these five claims, the auction algorithm is trustworthy, considerate of individual preferences, computationally efficient, and socially beneficial. ETRA [158] was a similar social welfare maximizing auction mechanism with three stages. Auction procedures included pairing bidders with possible winners, pairing cloudlets with application servers, and allocating available resources.

However, only the constant demand case was studied in [152]. Both constant-demand and multi-demand approaches to creating a miner's auction scheme were addressed in the comprehensive work [153]. Instead of relying on the empirical assumption, the authors of [153] instead derived the network effect by curve fitting the data from actual experiments. Under the knapsack constraint, maximizing social welfare in multi-demand bidding was a non-monotonic submodule maximization problem. To solve this NP-hard problem, a sub-optimal approximation technique was developed. The FLRS and MDB auction methods were developed to produce a suboptimal level of social welfare through multi-demand bidding. The above-mentioned achievements [152], [153] took server and blockchain network resource limitations into account, but the impact of real-world communications impairments (such as Rayleigh fading, noise, and channel attenuation) was not evaluated.

The above-mentioned literature [152, 153, 158] only considered one social welfare maximization model for service providers, which caught our attention. In the actual market situation, there

As a result, a double auction process [159] that factors in CSP contests should form the basis of the strategy for allocating and pricing available resources.

In the multi-CSP setting, Li et al. [154] used a recursive two-sided auction to maximize social efficiency while protecting user anonymity. Trading management between competing CSPs and miners was handled by a broker built on smart contracts. The process began with the broker gathering miners' needs. It was able to retrieve the hidden information in each double auction integration without compromising the privacy of CSPs/users and adjust the bidding, pricing, and allocation method to maximize utility. To ensure maximum market efficiency, the broker used an algorithm that maximized societal welfare.

The Seybold Report
ISSN 1533-9211

Profit-driven CSPs Offloading

From a CSP standpoint, there are a few things to think about, including energy efficiency and cost reduction. Since most network nodes are severely resource-constrained, Qiu et al. [160] argued that direct blockchain application was impossible in IoT and other networking settings. The research indicated that a practical approach to lowering the restriction was to combine agent mining with cloud mining. It was noted by Chen et al. [132] that blockchain mining and computing offloading needed to be viewed together. With more people participating, the problem became more complicated when computation and mining were taken into account. To lessen the burden of computing, the authors of [132] created a distributed algorithm that relies on communication between different nodes in a network.

In addition, some studies have attempted to model the dynamics between the selfish service provider and users by employing game theory. To model price, Xiong et al. [161], [162] employed a Stackelberg game with two phases. In this game, the service provider played the role of the leader, while the miners played the role of the followers. When the equilibrium was attained, the provider's profit was maximized. Second, a two-stage Stackelberg game model was applied to the interaction between cloud/fog providers (CFPs) and rational miners in a subsequent study [156]. In the second stage's sub-game, miners (or followers) fix their prices to maximize resource usefulness at the provider-determined price. Leaders in the cloud/fog industry have set prices to maximize provider profits. The Stackelberg game consisted of two stages, each of which was a subgame. To maximize both CFP's profit and the miner's resource utility, backward induction was used to reach Nash equilibrium.

Furthermore, both uniform and discriminatory approaches were considered in this paper. The results of the experiments showed that under discriminating pricing, CFP profits and miner demand for resources were both higher than they would have been under uniform pricing.

To maximize service provider revenue, Luong et al. [155] used a deep neural network for monotone transformation, allocation, and pricing. However, this machine learning-based approach took into account only a single resource unit.

To help mobile users crack the PoW puzzle, we covered offloading tasks and allocating resources. We concluded that there were three objects to be optimized during the offloading process.

Miners' overall revenue was maximized by a dynamically tuned mining and PoW job offloading strategy. Game theory was used to determine the sweet spot where service providers might make the most money. The overall utility of the system, which is a measure of social welfare, might be maximized through the use of an auction process. The use of deep learning technology in pricing and auction with many service providers, as well as the evaluation of trade-offs between social welfare optimization and provider profit maximization, are examples of potential future studies in this area.

The Seybold Report
ISSN 1533-9211

IX. BLOCKCHAIN MINING EQUIPMENT FOR THE CLOUD

The growing complexity of the blockchain mining process has made the in-house deployment of miners a costly and space-consuming endeavor. Thanks to advancements in visualization and parallel computing, cloud computing has the potential to be a scalable, pay-as-you-go model with excellent computational performance. In this part, we examined delay and energy costs as two technological factors. Cloud-based blockchain mining offered a clear advantage over the conventional method. The centralization of cloud settings was responsible for the benefits, which included hardware resource optimization that led to greater efficiency and reduced energy use. The efficiency with which PoW was executed in a cloud data center was mostly determined by the computational power of its processing units [163]. As a result, there have been studies and solutions developed to improve mining success through better hardware design and fabrication [164]. CPU, GPU, FPGA, and ASIC are the four generations of hardware that have contributed to the optimization of computational tasks in cloud data centers [165] [166]. To increase the number of nodes in BFT protocols, Liu et al. [167] presented a hardware-assisted approach for secret sharing.

Assembler-based Cloud Mining

SHA256 [143] is the algorithm that solved the Bitcoin mining cryptic map riddle. The mining of bitcoins was characterized as a CISO issue with limited input and high output [168]. Using the supplied nonce, Merkle root, and time stamp, miners attempted to solve the CISO problem and achieve the H2 objective. However, the CPU's processing power was limited. To increase mining efficiency, the mid-state buffer [169] hashes the seed data before the nonce is generated, resulting in a consistent hash value. In addition, [168] discussed nine enhancements that speed up CPU mining.

However, GPU and ASIC miners have recently been developed, which goes against Nakamoto's 1 CPU 1 vote guarantee. Litecoin et al. [170] employed SCRYPT [171], which required a lot of processing power and storage space to mine, to attract CPU miners. Similarly, Ethash is the basis of Ethereum's Proof-of-Work system. The mining speed for Ethash was significantly affected by the amount of RAM available to the process.

The Cloud Mining CPU, which is based on graphics processing units and field-programmable gate arrays, was developed for use in cloud mining. In mining, arithmetic logic units were unnecessary but registers and branch prediction units were not. As a result, using a central processing unit (CPU) for mining was a fruitless endeavor. While it is not possible to parallelize the SHA256 computation rounds, it is possible to test many nonces at once using parallel computing [165]. There are two things to think about while building a GPU cloud mining center.

The first advantage would be reduced hardware overhead. In [169], a GPU miner that doesn't break the bank was presented. For faster SHA256 calculations, this miner opted for AMD's 7970 GPU rather than NVidia's. Additionally, instead of the usual 8x or 16x PICe slot found on a commercial motherboard, a single slot was chosen to cut down on GPU overhead. The 16x AMD GPU connector and the single PCIe slot were linked with a cheap PCIe converter.

The Seybold Report
ISSN 1533-9211

As a result, there was significantly less burden on each GPU. One such NVIDIA GPU mining accelerator was developed by Ekbote et al. [172]. In this study, the authors created a CUDA-based framework for efficient general-purpose computing in the mining industry. The experiments conducted for this article demonstrated the superiority of GPUs over CPUs during mining.

Second, a well-thought-out and efficient power and cooling system design is essential. Using phase charging materials, Skach [173] created a data center with a thermal time cooling system. The day's high heat has been mitigated, and at night, the cooling power of nature can be fully utilized. Recent 2-phase cooling systems for blockchain miners were explored by Kamp et al. [174].

The Field Programmable Gate Array (FPGA) offered versatility and could be programmed to speed up a particular class of computation problems, such as those encountered in the mining industry. Xilinx's FPGA lacks the cooling and processing power necessary to handle mining tasks. Some hackers [175] created an open-source specialized FPGA miner by excluding unnecessary I/O and RAM components.

GPU Mining C. Mining with ASICs

A technology known as application-specific integrated circuits (ASICs) allows designers to create specialized chips for one use case. As a result, there may be an incentive to create the ASIC miner, which has a more efficient layout for locating the hashed value. It is possible to attain a high hash rate performance with a cheap cost of resources. Based on their FPGA miner, Butterfly Labs (BFL) [176] released an ASIC miner in 2012. This miner has a top speed of 1,500GH/s and was built on 65nm technology. A miner fabricated at 110 nm on a TSMC in 2013 was proposed by Avalon et al. [177]. With 60W, this product might achieve 66Gh/s. The exponential growth in ASIC miner performance that Moore's law predicted was made possible by advances in transistor fabrication technology. The most recent offering from Avalon, the AvalonMiner 852, was made using 16-nm technology. It had the potential to reach 15TH/s while only consuming 100W/T. Bitmain's [178] miner took over 70% of the market in 2019. The 7nm miner was their initial suggestion. At a reasonable amount of power, it can reach 40TH/s.

Summary: There were four generations of cloud mining hardware covered. CPU mining was the first method used. During the PoW consensus phase, it ensured complete decentralization. The GPU miner, albeit energy-intensive, provided a large hash rate. The FPGA miner could be customized to work with any mining algorithm. Unfortunately, the FPGA miner's processing power was inadequate. To address this issue, a specialized ASIC miner that is both energy-efficient and hash power-sufficient has been frequently employed since 2014. ASIC miners are capable of balancing speed and efficiency, but they lack the adaptability of FPGA miners. When a new consensus process was implemented, FPGA miners had to rewrite their logic, but they could keep using the same hardware. But the logic of an ASIC can't be altered after tape-out has occurred. That's why the rate at which the consensus would shift would determine how long ASIC miners would last. It's also possible that mining operations in the cloud won't be

The Seybold Report
ISSN 1533-9211

carried out consistently. The ASIC cloud's diversity results from the wide variety of mining tasks. The FPGA allowed the cloud data center to maintain homogeneity. Consequently, continued research into the trade-offs between homology and efficiency in cloud data centers is highly recommended.

X. BLOCKCHAIN AND CLOUD STORAGE

From the perspective of mass data storage, storing blockchain data on the cloud is an alternative that helps alleviate the limitations imposed by the blockchain's block size limitation. For optimal block size and blockchain functionality, the question of what information should be included in blocks is of paramount importance. Additionally, industries like healthcare [75] and smart cities [179] can benefit from employing blockchain technology to enable trustworthy data exchange across institutions. Zheng et al. [180] warned of the risks associated with centralized data storage and showed how to use blockchain technology to safely share medical records. Another study [181] tackled the issue of medical data exchange and evaluated the efficacy of blockchain in facilitating collaboration between several parties. A study by Qian et al. [179] showed that data exchanged between organizations may be done safely. Recent efforts, however, have centered on exploring the feasibility of integrating cloud storage with existing blockchain methods. Attempts were running into a number of roadblocks, including multi-chain cooperation.

Storing Hash Values On-Chain

Despite blockchain's ability to store immutable data on-chain, its capacity was low. The 1MB limit on Bitcoin blocks, for instance, means they can't be utilized to store a lot of data [36]. However, PC and mobile users may find the complete node size of the blockchain network intolerably huge if a large amount of data is stored on-chain. Therefore, off-chain [182] storage was developed to address this issue. CSPs might provide users with a scalable off-chain storage solution by offering storage-as-a-service. Throughput can be increased by using a unique multi-sidechain setting, as presented by Guo et al. [183].

The blockchain-based automatic access control system developed by Zyskind et al. [87] made use of an off-blockchain key-value store. User information was encrypted in the first place for security reasons. After that, the Distributed Hash Table (DHT) based distributed cloud that stores data off-blockchain received the ciphertext. The public ledger just stores the hash value of a file. Together, user privacy and the performance of the blockchain system benefited from this endeavor. The researchers in the supplementary research [88] employed off-chain storage for their Enigma secure multi-party computing system.

Sun et al. [184] also used off-chain technologies to store massive amounts of electronic health record data. Addresses for electronic health record data were recorded on-chain, while the actual EHR data were encrypted and housed in a separate, off-chain database managed by the data owner. Attributed-based signature was introduced in this study to ensure the safety of off-chain data storage and exchange. Before the EHR data could be shared, the owner had to sign the address using his credentials. Once the address was signed, it was added to the distributed

The Seybold Report
ISSN 1533-9211

ledger. When retrieving data, users must first validate the owner's signature. Each file's hash pointer was likewise saved on-chain by Rifi et al. [185]. Rifi's research made extensive use of IPFS, which is an off-chain database.

In light of the aforementioned research, Shafagh et al. [186] utilized blockchain technology to realize trustworthiness in off-chain storage access control and key management. Blockchain served as the "control layer" in their implementation. Distributed cloud storage is used to address blockchain scalability difficulties. Similar to work [87], data that doesn't belong on the blockchain can be kept in a decentralized cloud server using DHT technology.

In-line the file's hash pointer is recorded on-chain, as we've already established in our discussion of how metadata storage functions. A malevolent insider could not compromise the data in this manner, yet the data were uncontrolled. Zhu [15] offered a voting mechanism with tunable outcomes using on-chain metadata to address this issue. This study addressed the problem of collusion attacks on data alteration. Users were able to take advantage of cloud server space for free as part of this project. The efficiency of blockchain storage was significantly improved as a result of these efforts. To keep the system secure and manageable, three types of tamper-resistant metadata (such as voting records, file modification histories, and hash values of modified data) were recorded on the blockchain. In this method, the document's on-chain metadata served as a transparent and verifiable record of all the versions and revisions that had been applied to it. Users would thus have easy access to a history of file revisions. As a result, the system was more manageable than those previously cited. By carefully selecting the appropriate metadata on-chain, a balance was struck between storage efficiency and data security. Extensive testing demonstrated the method's security, scalability, protection of user privacy, and invulnerability to forgery.

The decentralized PingER model was built using blockchain technology in this study [187]. Off-chain file storage locations and metadata such as Merkle roots with raw data leaves were recorded in a distributed ledger. Transferred raw data to a DHT-based storage system for distributed monetary agents. Off-chain storage systems can be made more secure with the use of on-chain information by enabling access restriction and identity verification. Summary: In this article, we looked at some off-chain solutions that can help you overcome the storage constraints of the blockchain. A blockchain's scalability, storage efficiency, and verification time all improved once it adopted off-chain storage. As can be seen from the aforementioned literature, one of the primary challenges in developing the on/off-chain system was striking a balance between data security and the efficiency of the blockchain system. The off-chain data may be safer and more manageable if associated metadata of various types are stored. But if there's a lot of information stored on the blockchain, it may slow things down. Therefore, learning how to pick the right data to store on-chain to address scalability and security concerns could be a fruitful area for future study.

The Seybold Report
ISSN 1533-9211

XI. BLOCKCHAIN IN CLOUD COMPUTING, EDGE COMPUTING, AND IoT

In cloud computing

Blockchain technology can be used to build a distributed network of computers that can then exchange information and resources. Because of this, businesses can function without relying on any one particular service provider. A decentralized network of computers outside of a single organization's control is an alternative.

Increased security, scalability, and availability are just a few of the benefits that such a system can offer [188].

It also enables the development of novel applications that would be impossible to implement using more conventional cloud computing models. For instance, a distributed file storage system that is both more secure and more resilient than current alternatives may be built using a decentralized network of nodes.

Blockchain's cloud computing uses are most often linked to the Internet of Things (IoT). The term "Cloud of Things" is used to describe the growing trend of internet-enabled gadgets and everyday items. It covers everything from automobiles and wearables to factory machinery and household goods [189] [190].

It is anticipated that CoT would produce a flood of data that will require extensive archiving, processing, and analysis. This is due to the widespread adoption of the Internet of Things (IoT) for reasons such as asset tracking and inventory management across numerous sectors. By 2030, Statista predicts there will be 29 billion IoT devices in use around the globe.

Businesses can improve data management and security with the help of blockchain technology implemented in cloud computing. The information gathered by IoT devices, for instance, may be stored in an immutable and secure blockchain-based system. Additionally, the storage capacity of most IoT devices is quite little.

However, the cloud can store vast amounts of data, thus establishing the significance of CoT.

Each computer in a blockchain-based cloud network must keep its copy of the blockchain. Each node in the network receives the latest version of the blockchain whenever a new transaction is added to the ledger.

This paves the way for a data management system that is not just transparent but also safe and decentralized.

The blockchain cloud may also alter the way information is handled. Its potential applications range from medical record keeping to food safety monitoring [190].

In Edge computing

General-purpose servers and processors may not be up to the task of processing blockchain transactions quickly because of the large amount of processing power needed. Companies like NVIDIA, which produces GPUs, are reaping the rewards of the increased demand brought on by blockchain and cryptocurrencies.

The Seybold Report
ISSN 1533-9211

This is mostly unaffected by edge computing, while it is possible that GPUs and high compute processors would be more common in edge computing infrastructure because many edge computing applications require a large data transfer rate. These low-delay types need these features anyhow.

However, the way modern network topologies are constructed also contributes to the lag time experienced by blockchain networks. Similar to how traffic travels in the cloud, for blockchain nodes to communicate with one another, data must go through the complete network and back. By eliminating the requirement for data to travel through the core network, an edge computing network can facilitate novel server-to-server data flows.

Developing a business model that facilitates developer access to edge cloud infrastructure is a significant obstacle in the field of edge computing. An application developer may have to interact with each telecom operator to make sure their product works for customers in different countries and across borders if edge computing technology continues to be fragmented across telecom providers. The developer's ability to ensure a constant (low-latency) experience is compromised without this [192].

In IoT

If blockchain technology were implemented, it might help IoT systems immensely. As the number of connected devices and objects continues to rise, there will be more opportunities for interaction. The internet will serve as a conduit for the growing number of gadgets that will attempt to communicate with one another. Since most data in IoT devices resides on centralized servers, this would provide a number of problems. Figure 6 shows how the process flows, with the devices interacting via the centralized network and the data flowing via the centralized server. However, the expanding requirements of IoT and its applications were giving the impression that IoT entailed massive systems that incorporated cutting-edge technologies. The centralized server model will not scale well in such massive IoT deployments. The majority of current Internet of Things implementations rely on a central server for their functionality. The Internet of Things relies on sensor devices to collect data from the targeted objects and relay that data to a centralized server over a wired or wireless network. User requests and preferences were taken into account while conducting analytics on the central server. Similarly, the analytical and processing needs of the existing internet are met by the desires of the large-scale IoT system [193] [194].

The Seybold Report
ISSN 1533-9211

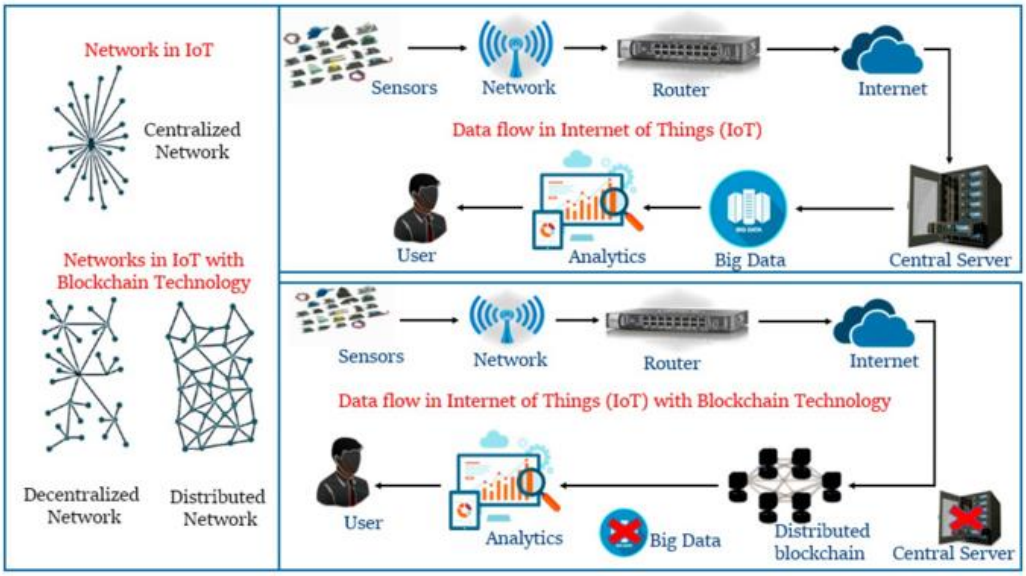

Figure 6: Data Flows in IoT Networks, Types of IoT Networks, and IoT Data Flows Utilizing Blockchain Technology

XII. PRIMARY RESULT AND DISCUSSION

Results

Several perspectives, including those of similarity, connectedness, and originality, are used to explain the study's key conclusions.

Similarity: The fact that they both rely heavily on a decentralized/distributed networking environment is the fundamental commonality between the two technologies. Cloud data centers may provide their services in a centralized fashion, however, distributed/decentralized cloud settings such as multi-tenant clouds, heterogeneous cloud deployment, and external service providers remain. As a result of these shared characteristics, we find that equivalent technical care is given to each. Both technologies address sophisticated controls (such as resource allocations) to improve service quality from a user's point of view. One may compare a smart contract to a cloud controller. Many of the same service concepts underpin blockchain and cloud computing as well, including BaaS and X-as-a-Service.

Blockchain and cloud computing have comparable network-relevant concerns (such as security and privacy difficulties) because they both rely on distributed networks. Identity leakage and data mining-based attacks are two examples of cloud computing cyber dangers that also apply to blockchain networks, although the specifics of the attacks themselves may vary. There is a risk of privacy leakage when mining blocks because the data they contain is accessible to all authorized users. It's very much like when information is kept on distant cloud servers. When a linkage attack is effective, even for an anonymous cloud dataset, privacy may be leaked. Two technologies are under siege from both external and internal sources of danger.

The Seybold Report
ISSN 1533-9211

Furthermore, improving the performance of blockchain systems is a major study area, much like the optimization of cloud systems. Improvements have been made to the architecture of both systems, as well as the hardware, the allocation strategy for resources, and the provenance of data.

Our research shows that blockchain technology and cloud computing can communicate with one another. To begin, BaaS is a cloud computing-based service model. Providing BaaS services is a strategy used by many IT businesses to expand into new customer bases. Most existing BaaS architectures largely consist of blockchain infrastructure and backend support. Second, the blockchain system benefits from the abundance of cloud computing resources, which help to fortify security, boost efficiency, and enhance service quality. Hardware-related supports are also addressed in the supplementary offers, such as blockchain-specific hardware (for example, processors designed specifically for use in blockchain applications). To create a reliable setting for cloud applications, consensus mechanisms are crucial. Smart contracts, because of their autonomous nature, have vast potential across a variety of cloud applications, including, but not limited to, resource allocation and intelligent manufacturing. Our research shows that smart contracts are a key integration point between blockchain and cloud resources, Table 1 data management specificity with and without blockchain.

Ingenuity: New models for providing services have been made available to the general public in recent years. Value innovations, which can be broken down into two categories, are the key inspiration for the innovative use of blockchain and clouds. The primary goal is to improve upon the current setup. Cloud solutions have limitations, such as a lack of control and a lack of trust, which blockchain technology is utilized to address. When integrated into preexisting cloud models, blockchain's benefits are seen as a valuable enhancement. Alternative creative path: making something of worth out of nothing. Blockchain systems rely on cloud computing for resource provisioning such as infrastructure and software, giving rise to a novel service model (BaaS). BaaS is still in its infancy, and more study is needed before it can be tailored to meet specific needs.

Data Managment Specifity	Cloud with out Blockchain	Cloud with Blockchain
Data access	Users can acess data online	Use data encryption and hashing
Viability of data	Data is mutable	Data is immutable
Data control	Centrilized (relies on 3rd parties)	Decentrilized (not involve 3rd parties)
Data integrity	Not guarantee the full data integrity and tamper-free data.	Full data integrity, tamper-free data
Security	Vulnerable to cyber attacks	Strong data security

Table 1: **Data Management Specificity With and Without Blockchain**

The Seybold Report
ISSN 1533-9211

Discourse

In this part, we provide a brief overview of a few key difficulties and opportunities.

Challenges: First, more work needs to be done in several areas, including architecture, communication, and consensus mechanisms, to support BaaS operations in multi-cloud (cloud federation). Due to the immaturity of the multi-chain method, interoperability between various BaaS service providers remains a significant obstacle. Second, there are numerous obstacles to overcome when trying to prove the origin of data stored in the cloud using blockchain technology. Verifying if data are used by unexpected parties in a network setting is still difficult. It's also unclear if the information stored in blocks refers to genuine things in the real world, such as animals or computers. There is a need for further technical advancement in various fields. Third, blockchain security still faces significant obstacles. There are security flaws in every layer of existing blockchain systems at the moment, from the blockchain infrastructure to the smart contract. Blockchain has the potential to improve security, but there are still numerous problems to be fixed, including those related to privacy, hardware threats, and complex network node settings. Finally, certain parameters of blockchain system performance, including throughput capacity, energy cost, and data storage, have not reached other mature active systems. Possibilities for Study: While blockchain and cloud computing are the primary focus of this work, other linked technologies should not be overlooked for updates and future research. Based on our research into previous works on other types of integrations, such as software-defined networks [195], the Internet of Things [196], and cloud radio access networks [190], we conclude that future integrations may have more comprehensive coverage that incorporates many network-related technologies. Additionally, the improvement of the BaaS service model will be a matter of interest in both academic and business circles. To cater to a wide variety of customer needs, it is important to provide a wider range of services (such as those connected to artificial intelligence (AI) or security access management). Additionally, specialized services for tracking the history of data and objects will flourish. Attaching things in the real world to digital resources could spark a technological revolution. In addition, studying blockchain's security and privacy flaws is a must. Attacks on blockchains (such as smart contract attacks) and new blockchain-cloud security risks need to be addressed in future research. In conclusion, high performance will continue to be a focus in the blockchain-cloud industry. To better handle complicated or heavy-workload scenarios, advancements in both software and hardware are required.

XIII. CONCLUSIONS

This paper uses blockchain technology to solve a few technical considerations for cloud computing reengineering. The effort involves three technological aspects: service, security, and performance. In particular, this article details recent efforts to re-engineer cloud data centers with the help of blockchain technology by focusing on the following areas: the BaaS service model; blockchain-enabled cloud access control; blockchain-enabled cloud data provenance; blockchain-based cloud searchable encryptions; blockchain-based cloud data deduplication; smart contract-based cloud applications; blockchain-powered offloading; blockchain hardware

The Seybold Report
ISSN 1533-9211

development; and blockchain-enabled cloud data deduplication. The primary results of this paper give a theoretical foundation for further research into blockchain-enabled reengineering of cloud datacenter.

References

1) Tanweer Alam,"A Reliable Communication Framework and Its Use in Internet of Things (IoT).",International Journal of Scientific Research in Computer Science, Engineering and Information Technology © 2018 IJSRCSEIT | Volume 3 | Issue 5 | ISSN : 2456-3307.

2) Ahmed Rahman Abdulzahra Al-Obaidi, Seyed Ebrahim Dashti "corresponding author", Saba Atiyah Mashaan, Mohammed Ahmed Kadhim Al-khafaji, "proposed new secure hybrid mobile cloud computing to improve power and delay," , Journal of New Zealand Studies NS35,2023 .

3) Seyed Ebrahim Dashti, Amir Masoud Rahmani,"Dynamic VMs placement for energy efficiency by PSO in cloud computing,"2015.

4) Seyed Ebrahim Dashti, Ahmed Rahman Abdulzahra Al-Obaidi, Saba Atiyah Mashaan,"An Overview of Deep Learning Methods in the Internet of Things Technology in regular life," ,Computer Integrated Manufacturing Systems,2023.

5) Seyed Ebrahim Dashti, Mohammad Zolghadri, Fatemeh Moayedi,"Improving flexibility in cloud computing using optimal multipurpose particle swarm algorithm with auction rules",2022.

6) Mostafa Ghobaei-Arani, Ali Asghar Rahmanian, Mohammad Sadegh Aslanpour, Seyed Ebrahim Dashti '"CSA-WSC: cuckoo search algorithm for web service composition in cloud environments,", Soft Computing,2018.

7) Seyed Ebrahim Dashti, Hoasain Zare ," Increase the Efficiency of the Offloading Algorithm in Fog Computing by Particle Swarm Optimization Algorithm,", Journal of Intelligent Procedures in Electrical Technology,2023.

8) F. Hardwick, R. Akram, and K. Markantonakis, "Fair and transparent blockchain based tendering framework-a step towards open gover- nance," in 17th IEEE Int'l Conf. TrustCom. New York, USA: IEEE, 2018, pp. 1342–1347.

9) N. Fabiano, "Internet of Things and blockchain: legal issues and privacy. the challenge for a privacy standard," in IEEE Int'l Conf. on IoT. IEEE, 2017, pp. 727–734.

10) W. Meng, E. Tischhauser, Q. Wang, Y. Wang, and J. Han, "When intrusion detection meets blockchain technology: a review," IEEE Access, vol. 6, pp. 10 179–10 188, 2018.

11) K. Biswas and V. Muthukkumarasamy, "Securing smart cities using blockchain technology," in 18th Int'l Conf. on HPCC. Exeter, UK: IEEE, 2016, pp. 1392–1393.

12) R. Cole, M. Stevenson, and J. Aitken, "Blockchain technology: impli- cations for operations and supply chain management," Supply Chain Management: An Int'l J., vol. 24, no. 4, pp. 469–483, 2019.

13) K. Gai, Y. Wu, L. Zhu, M. Qiu, and M. Shen, "Privacy-preserving energy trading using consortium blockchain in smart grid," IEEE Trans. on Industrial Informatics, vol. 15, no. 6, pp. 3548–3558, 2019.

14) I. Eyal, A. Gencer, E. Sirer, and R. V. Renesse, "Bitcoin-ng: A scalable blockchain protocol," in 13th USENIX Sym. on Networked Systems Design and Implementation, 2016, pp. 45–59.

15) L. Zhu, Y. Wu, K. Gai, and K.-K. R. Choo, "Controllable and trust- worthy blockchain-based cloud data management," Future Generation Computer Systems, vol. 91, pp. 527 – 535, 2019.

16) E. Heilman, F. Baldimtsi, and S. Goldberg, "Blindly signed contracts: Anonymous on-blockchain and off-

The Seybold Report
ISSN 1533-9211

blockchain bitcoin transactions," in Int'l Conf. on Fin. Crypt. & Data Sec. Springer, 2016, pp. 43–60.

17) N. Herbaut and N. Negru, "A model for collaborative blockchain-based video delivery relying on advanced network services chains," IEEE Communications Magazine, vol. 55, no. 9, pp. 70–76, 2017.

18) D. Qin, C. Wang, and Y. Jiang, "Rpchain: a blockchain-based academic social networking service for credible reputation building," in Int'l Conf. on Blockchain. Springer, 2018, pp. 183–198.

19) Y. Xu, G. Wang, J. Yang, J. Ren et al., "Towards secure network computing services for lightweight clients using blockchain," Wireless Communi. and Mobile Comp., vol. 2018, 2018.

20) F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2084–2123, 2016.

21) M. Khalilov and A. Levi, "A survey on anonymity and privacy in bitcoin-like digital cash systems," IEEE Communications Surveys & Tutorials, vol. 20, no. 3, pp. 2543–2585, 2018.

22) M. Conti, E. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3416–3452, 2018.

23) X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," FGCS, p. 1, 2017.

24) T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A state of the art survey," IEEE Commu- nications Surveys & Tutorials, vol. 21, no. 1, pp. 858–880, 2018.

25) Q. Feng, D. He, S. Zeadally, M. Khan, and N. Kumar, "A survey on privacy protection in blockchain system," Journal of Network and Computer Applications, vol. 126, pp. 45–58, 2019.

26) R. Yang, F. Yu, P. Si, Z. Yang, and Y. Zhang, "Integrated blockchain and edge computing systems: A survey, some research issues and challenges," IEEE Communications Surveys & Tutorials, p. 1, 2019.

27) M. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. Rehmani, "Applications of blockchains in the internet of things: A comprehensive survey," IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1676–1717, 2018.

28) H. Dai, Z. Zheng, and Y. Zhang, "Blockchain for internet of things: A survey," IEEE IOT J, vol. 6, no. 5, pp. 8076–8094, 2019.

29) J. Xie, H. Tang, T. Huang, F. Yu, R. Xie, J. Liu, and Y. Liu, "A survey of blockchain technology applied to smart cities: Research issues and challenges," IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2794–2830, 2019.

30) M. Samaniego and R. Deters, "Blockchain as a service for IoT: cloud versus fog," in IEEE Int'l Conf. on IoT. IEEE, 2016, pp. 433–436.

31) W. Viriyasitavat, D. Li, Z. Bi, and A. Sapsomboon, "New blockchain- based architecture for service interoperations in Internet of Things," IEEE TCSS, vol. 6, no. 4, pp. 739–748, 2019.

32) Y. Chen, J. Gu, S. Chen, S. Huang, and X. Wang, "A full-spectrum blockchain-as-a-service for business collaboration," in IEEE Int'l Conf. on Web Services. Milan, Italy: IEEE, 2019, pp. 219–223.

33) Q. Lu, X. Xu, Y. Liu, I. Weber, L. Zhu, and W. Zhang, "uBaaS: A unified blockchain as a service platform," Future Generation Computer Systems, vol. 101, pp. 564–575, 2019.

34) W. Zheng, Z. Zheng, X. Chen, K. Dai, P. Li, and R. Chen, "Nutbaas: A blockchain-as-a-service platform," IEEE Access, vol. 7, pp. 134 422– 134 433, 2019.

35) A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in The 2nd Int'l Conf. on Open and Big Data. IEEE, 2016, pp. 25–30.

The Seybold Report
ISSN 1533-9211

36) C. Esposito, A. D. Santis, G. Tortora, H. Chang, and K. Choo, "Blockchain: A panacea for healthcare cloud-based data security and privacy?" IEEE Cloud Computing, vol. 5, no. 1, pp. 31–37, 2018.

37) X. Liu, A. Liu, T. Wang, K. Ota, M. Dong et al., "Adaptive data and verified message disjoint security routing for gathering big data in energy harvesting networks," JPDC, vol. 135, pp. 140–155, 2020.

38) J. Singh and J. Michels, "Blockchain as a service (baas): Providers and trust," in IEEE European Sym. on Security and Privacy Workshops. London, United Kingdom: IEEE, 2018, pp. 67–74.

39) IBM, "IBM developer: Blockchain," https://developer.ibm.com/technologies/blockchain/, 2019.

40) Oracle, "Oracle blockchain blog," https://blogs.oracle.com/blockchain/ blockchain-use-cases, 2019.

41) Microsoft, "Microsoft azure," https://azure.microsoft.com.

42) Amazon, "Blockchain on AWS," https://amazonaws-china.com/cn/blockchain.

43) Keke Gai, Senior Member, IEEE, Jinnan Guo, Liehuang Zhu,"Blockchain Meets Cloud Computing: A Survey,"IEEE,2020.

44) M. Samaniego and R. Deters, "Using blockchain to push software- defined IoT components onto edge hosts," in Int'l Conf. on BDAWT. ACM, 2016, p. 58.

45) A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in IEEE Sym. on S&P. IEEE, 2016, pp. 839–858.

46) C. Melo, J. Dantas, D. Oliveira, I. Fé et al., "Dependability evaluation of a blockchain-as-a-service environment," in IEEE Sym. on Comp. and Communi. IEEE, 2018, pp. 00 909–00 914.

47) J. Lee, "BIDaaS: Blockchain based ID as a service," IEEE Access, vol. 6, pp. 2274–2278, 2017.

48) Y. Xu, J. Ren, Y. Zhang, C. Zhang, B. Shen, and Y. Zhang, "Blockchain empowered arbitrable data auditing scheme for network storage as a service," IEEE TSC, vol. PP, no. 99, p. 1, 2019.

49) H. Chen and L. Zhang, "FBaaS: Functional blockchain as a service," in Int'l Conf. on Blockchain. Springer, 2018, pp. 243–250.

50) Q. Lu, X. Xu, Y. Liu, and W. Zhang, "Design pattern as a service for blockchain applications," in IEEE Int'l Conf. on Data Mining Workshops. IEEE, 2018, pp. 128–135.

51) H. Zhang, E. Deng, H. Zhu, and Z. Cao, "Smart contract for secure billing in ride-hailing service via blockchain," Peer-to-Peer Networking and Applications, vol. 12, no. 5, pp. 1346–1357, 2019.

52) A. Karinsalo and K. Halunen, "Smart contracts for a mobility-as-a- service ecosystem," in Int'l Conf. on QRS-C. Lisbon, Portugal: IEEE, 2018, pp. 135–138.

53) P. Marandi, C. Gkantsidis, F. Junqueira, and D. Narayanan, "Filo: consolidated consensus as a cloud service," in USENIX Annual Technical Conference, Denver, CO, USA, 2016, pp. 237–249.

54) G. Kumar, R. Saha, M. Rai, R. Thomas, and T. Kim, "Proof-of- work consensus approach in blockchain technology for cloud and fog computing using maximization-factorization statistics," IEEE IOT J, vol. PP, no. 99, 2019.

55) Z. Zhou, B. Wang, M. Dong, and K. Ota, "Secure and efficient vehicle-to-grid energy trading in cyber physical systems: Integration of blockchain and edge computing," IEEE Trans. on Systems, Man, and Cybernetics: Systems, vol. PP, no. 99, p. 1, 2019.

56) D. Reinsel, J. Gantz, and J. Rydning, "The digitization of the world: from edge to core," 2018.

57) M. Westerkamp, F. Victor, and A. Kupper, "Tracing manufacturing processes using blockchain-based token

The Seybold Report
ISSN 1533-9211

compositions," Digital Com- munications and Networks, vol. PP, no. 99, p. 1, 2019.

58) 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 Proceedings of the 17th IEEE/ACM international symposium on cluster, cloud and grid computing. IEEE Press, 2017, pp. 468–477.

59) A. Ramachandran and M. Kantarcioglu, "Smartprovenance: a dis- tributed, blockchain based dataprovenance system," in Proceedings of the Eighth ACM Conf. on Data and Application Security and Privacy. ACM, 2018, pp. 35–42.

60) Q. Xia, E. Sifah, K. Asamoah, J. Gao, X. Du, and M. Guizani, "Med- share: Trust-less medical data sharing among cloud service providers via blockchain," IEEE Access, vol. 5, pp. 14 757–14 767, 2017.

61) J. Gao, K. Asamoah, E. Sifah, A. Smahi, Q. Xia, H. Xia, X. Zhang, and G. Dong, "Gridmonitoring: Secured sovereign blockchain based monitoring on smart grid," IEEE Access, vol. 6, pp. 9917–9925, 2018.

62) R. Neisse, G. Steri, and I. Nai-Fovino, "A blockchain-based approach for data accountability and provenance tracking," in The 12th Int'l Conf. on Avail., Reli. and Sec. ACM, 2017, p. 14.

63) A. Al-Mamun, T. Li, M. Sadoghi, and D. Zhao, "In-memory blockchain: Toward efficient and trustworthy data provenance for hpc systems," in IEEE Int'l Conf. Big Data. IEEE, 2018, pp. 3808–3813.

64) D. K. D. Tosh, S. Shetty, X. Liang, C. Kamhoua, and L. Njilla, "Con- sensus protocols for blockchain-based data provenance: Challenges and opportunities," in IEEE 8th Ann'l Ubiquitous Computing, Electronics and Mobile Communication Conf. IEEE, 2017, pp. 469–474.

65) A. Maw, S. Adepu, and A. Mathur, "ICS-BlockOpS: Blockchain for operational data security in industrial control system," Pervasive and Mobile Computing, vol. 59, p. 101048, 2019.

66) W. Oliveira, D. Oliveira, and V. Braganholo, "Provenance analytics for workflow-based computational experiments: A survey," ACM Comput- ing Surveys, vol. 51, no. 3, p. 53, 2018.

67) M. Interlandi et al., "Titian: Data provenance support in spark, "Proceedings of the VLDB Endowment, vol. 9, no. 3, pp. 216–227, 2015.

68) P. Buneman and W. Tan, "Data provenance: What next?" ACM SIG- MOD Record, vol. 47, no. 3, pp. 5–16, 2019.

69) F. Zafar et al., "Trustworthy data: A survey, taxonomy and future trends of secure provenance schemes," JNCA, vol. 94, pp. 50–68, 2017.

70) Z. Xiao and Y. Xiao, "Security and privacy in cloud computing," IEEE Communications Surveys & Tutorials, vol. 15, no. 2, pp. 843–859, 2013.

71) P. Ivie and D. Thain, "Reproducibility in scientific computing," ACM Computing Surveys, vol. 51, no. 3, p. 63, 2018.

72) S. Zawoad, R. Hasan, and K. Islam, "SECProv: trustworthy and efficient provenance management in the cloud," in IEEE Conf. on Computer Communications. IEEE, 2018, pp. 1241–1249.

73) S. Ali, J. Wang, M. Bhuiyan, and H. Jiang, "Secure data provenance in cloud-centric internet of things via blockchain smart contracts," in SmartWorld. Guangzhou, China: IEEE, 2018, pp. 991–998.

74) Muniswamy-Reddy and M. Seltzer, "Provenance as first class cloud data," ACM SIGOPS Operating Systems Review, vol. 43, no. 4, pp. 11–16, 2010.

75) T. McGhin, K. Choo, C. Liu, and D. He, "Blockchain in healthcare applications: Research challenges and opportunities," JNCA, vol. PP, no. 99, p. 1, 2019.

The Seybold Report
ISSN 1533-9211

76) K. Gai, Y. Wu, L. Zhu, Z. Zhang, and M. Qiu, "Differential privacy- based blockchain for industrial Internet of Things," IEEE Transactions on Industrial Informatics, vol. PP, no. 99, p. 1, 2019.

77) G. Liang et al., "Distributed blockchain-based data protection frame- work for modern power systems against cyber attacks," IEEE TSG, vol. 10, no. 3, pp. 3162–3173, 2018.

78) Y. Chen, L. Wang, and S. Wang, "Stochastic blockchain for IoT data integrity," IEEE TNSE, vol. PP, no. 99, p. 1, 2018.

79) J. Lopez and J. Rubio, "Access control for cyber-physical systems interconnected to the cloud," Computer Networks, vol. 134, pp. 46– 54, 2018.

80) M. Qiu et al., "Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in financial industry," Future Generation Comp. Syst., vol. 80, pp. 421–429, 2018.

81) S. Rane and A. Dixit, "BlockSLaaS: Blockchain assisted secure Logging-as-a-Service for cloud forensics," in Int'l Conf. on Security & Privacy. Springer, 2019, pp. 77–88.

82) Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, "Smart contract- based access control for the internet of things," IEEE IOT J, vol. 6, no. 2, pp. 1594–1605, 2018.

83) S. Rouhani and R. Deters, "Blockchain based access control systems: State of the art and challenges," arXiv:1908.08503, 2019.

84) I. Sukhodolskiy and S. Zapechnikov, "A blockchain-based access control system for cloud storage," in IEEE EIConRus. Moscow, Russia: IEEE, 2018, pp. 1575–1578.

85) S. Wang, X. Wang, and Y. Zhang, "A secure cloud storage framework with access control based on blockchain," IEEE Access, vol. 7, pp. 112 713–112 725, 2019.

86) D. Nguyen, P. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for secure EHRs sharing of mobile cloud based e-health systems," IEEE access, vol. 7, pp. 66 792–66 806, 2019.

87) G. Zyskind and O. Nathan, "Decentralizing privacy: Using blockchain to protect personal data," in IEEE Security and Privacy Workshops. IEEE, 2015, pp. 180–184.

88) G. Zyskind, O. Nathan, and A. Pentland, "Enigma: Decentral- ized computation platform with guaranteed privacy," arXiv preprint arXiv:1506.03471, 2015.

89) D. Nguyen, J. Park, and R. Sandhu, "Dependency path patterns as the foundation of access control in provenance-aware systems." in TaPP, 2012.

90) Q. Xia, E. Sifah, A. Smahi, S. Amofa, and X. Zhang, "Bbds: Blockchain-based data sharing for electronic medical records in cloud environments," Information, vol. 8, no. 2, p. 44, 2017.

91) M. Rahman, M. Hossain, G. Loukas, E. Hassanain, S. Rahman, M. Al- hamid, and M. Guizani, "Blockchain-based mobile edge computing framework for secure therapy applications," IEEE Access, vol. 6, pp. 72 469–72 478, 2018.

92) A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, "Fairaccess: a new blockchain-based access control framework for the internet of things," Secur. & Communi. Netw., vol. 9, no. 18, pp. 5943–5964, 2016.

93) O. Novo, "Blockchain meets iot: An architecture for scalable access management in iot," IEEE IOT J., vol. 5, no. 2, pp. 1184–1195, 2018.

94) S. Wang, Y. Zhang, and Y. Zhang, "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems," IEEE Access, vol. 6, pp. 38 437–38 450, 2018.

95) M. S. Ferdous, A. Margheri, F. Paci, M. Yang, and V. Sassone, "Decentralised runtime monitoring for access control systems in cloud federations," in IEEE 37th Int'l Conf. on Distributed Computing Systems.

The Seybold Report
ISSN 1533-9211

IEEE, 2017, pp. 2632–2633.

96) S. Alansari, F. Paci, and V. Sassone, “A distributed access control system for cloud federations,” in IEEE 37th Int’l Conf. on Distributed Computing Systems. IEEE, 2017, pp. 2131–2136.

97) F. Schiavo, V. Sassone, L. Nicoletti, A. Reiter, and B. Suzic, “Faas: Federation-as-a-service: The sunfish cloud federation solution,” in FaaS: Federation-as-a-Service: The SUNFISH Cloud Federation So- lution, 2016.

98) D. Song, D. Wagner, and A. Perrig, “Practical techniques for searches on encrypted data,” in Proceeding 2000 IEEE Sym. on Security and Privacy. S&P 2000. IEEE, 2000, pp. 44–55.

99) D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, “Public key encryption with keyword search,” in Ann’l Int’l Conf. on the Theor. and App. of Crypt. Techni. Springer, 2004, pp. 506–522.

100) P. Golle, J. Staddon, and B. Waters, “Secure conjunctive keyword search over encrypted data,” in Int’l Conf. on Applied Cryptography and Network Security. Springer, 2004, pp. 31–45.

101) J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, “Fuzzy keyword search over encrypted data in cloud computing,” in 2010 Proceedings IEEE INFOCOM. IEEE, 2010, pp. 1–5.

102) G. Poh, J. Chin, W. Yau, K. Choo, and S. M. Mohamad, “Search- able symmetric encryption: designs and challenges,” ACM Computing Surveys, vol. 50, no. 3, p. 40, 2017.

103) X. Chen, J. Li, X. Huang, J. Ma, and W. Lou, “New publicly verifiable databases with efficient updates,” IEEE Trans. on Dependable and Secure Computing, vol. 12, no. 5, pp. 546–556, 2015.

104) Z. Fu, J. Shu, X. Sun, and N. Linge, “Smart cloud search services: verifiable keyword-based semantic search over encrypted cloud data,” IEEE Trans. on ConsR Elec., vol. 60, no. 4, pp. 762–770, 2014.

105) R. Cheng, J. Yan, C. Guan, F. Zhang, and K. Ren, “Verifiable searchable symmetric encryption from indistinguishability obfuscation,” in The 10th ACM Sym. on ICCS. Singapore: ACM, 2015, pp. 621–626.

106) L. Chen et al., “Blockchain based searchable encryption for electronic health record sharing,” FGCS, vol. 95, pp. 420–429, 2019.

107) Y. Zhang, C. Xu, J. Ni, H. Li, and X. Shen, “Blockchain-assisted public-key encryption with keyword search against keyword guessing attacks for cloud storage,” IEEE TCC, vol. PP, no. 99, p. 1, 2019.

108) J. Niu, X. Li, J. Gao, and Y. Han, “Blockchain-based anti-key-leakage key aggregation searchable encryption for IoT,” IEEE Internet of Things Journal, vol. PP, no. 99, p. 1, 2019.

109) P. Jiang, F. Guo, K. Liang, J. Lai, and Q. Wen, “Searchain: Blockchain- based private keyword search in decentralized storage,” Future Gener- ation Computer Systems, 2017.

110) Y. Zhang, R. Deng, X. Liu, and D. Zheng, “Outsourcing service fair payment based on blockchain and its applications in cloud computing,” IEEE Trans. on Services Computing, 2018.

111) Y. Zhang, R. H. Deng, J. Shu, K. Yang, and D. Zheng, “Tkse: trust- worthy keyword search over encrypted data with two-side verifiability via blockchain,” IEEE Access, vol. 6, pp. 31 077–31 087, 2018.

112) C. Cai, X. Yuan, and C. Wang, “Towards trustworthy and private keyword search in encrypted decentralized storage,” in IEEE Int’l Conf. on Communications. IEEE, 2017, pp. 1–7.

113) S. Hu, C. Cai, Q. Wang, C. Wang, X. Luo, and K. Ren, “Searching an encrypted cloud meets blockchain: A decentralized, reliable and fair realization,” in IEEE Conf. on Computer Communications. IEEE, 2018, pp. 792–800.

114) A. Zhang and X. Lin, “Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain,” Journal of medical systems, vol. 42, no. 8, p. 140, 2018.

The Seybold Report
ISSN 1533-9211

115) F. Han, J. Qin, and J. Hu, "Secure searches in the cloud: A survey," Future Generation Computer Systems, vol. 62, pp. 66–75, 2016.

116) A. Choudhuri et al., "Fairness in an unfair world: Fair multiparty computation from public bulletin boards," in SIGSAC Conf. on CCS. Dallas, USA: ACM, 2017, pp. 719–728.

117) L. Luu, J. Teutsch, R. Kulkarni, and P. Saxena, "Demystifying incen- tives in the consensus computer," in 22nd ACM SIGSAC Conf. on CCS. ACM, 2015, pp. 706–719.

118) IDC, "Idc report," https://www.emc.com/collateral/analyst-reports/idc- digital-universe-are-you-ready.pdf.

119) Y. Shin, D. Koog, and J. Hur, "A survey of secure data deduplication schemes for cloud storage systems," ACM Computing Surveys, vol. 49, no. 4, p. 74, 2017.

120) J. Douceur, A. Adya, W. Bolosky, P. Simon, and M. Theimer, "Reclaim- ing space from duplicate files in a serverless distributed file system," in The 22nd Int'l Conf. DCS. IEEE, 2002, pp. 617–624.

121) M. Bellare, S. Keelveedhi, and T. Ristenpart, "Message-locked encryp- tion and secure deduplication," in Ann'l Int'l Conf. on the Theor. and App. of Crypt. Techni. Springer, 2013, pp. 296–312.

122) S. Keelveedhi, M. Bellare, and T. Ristenpart, "Dupless: server-aided encryption for deduplicated storage," in Presented as part of the 22nd USENIX Security Sym., 2013, pp. 179–194.

123) D. Harnik, B. Pinkas, and A. Shulman-Peleg, "Side channels in cloud services: Deduplication in cloud storage," IEEE Security & Privacy, vol. 8, no. 6, pp. 40–47, 2010.

124) J. Yuan and S. Yu, "Secure and constant cost public cloud storage auditing with deduplication," in IEEE Conf. on Communications and Network Security. IEEE, 2013, pp. 145–153.

125) Y. Li, L. Zhu, M. Shen, F. Gao, B. Zheng, X. Du, S. Liu, and S. Yin, "Cloudshare: Towards a cost-efficient and privacy-preserving alliance cloud using permissioned blockchains," in Int'l Conf. on Mobile Networks and Management. Springer, 2017, pp. 339–352.

126) H. Liu, Y. Zhang, and T. Yang, "Blockchain-enabled security in electric vehicles cloud and edge computing," IEEE Network, vol. 32, no. 3, pp. 78–83, 2018.

127) J. Li, J. Wu, L. Chen, and J. Li, "Deduplication with blockchain for secure cloud storage," in CCF Conf. on Big Data. Springer, 2018, pp. 558–570.

128) C. Liu, Q. Lin, and S. Wen, "Blockchain-enabled data collection and sharing for industrial iot with deep reinforcement learning," IEEE Trans. on Industrial Informatics, 2018.

129) K. Gai et al., "Dynamic energy-aware cloudlet-based mobile cloud computing model for green computing," JNCA, vol. 59, pp. 46–54, 2016.

130) K. Gai, M. Qiu, and H. Zhao, "Energy-aware task assignment for mobile cyber-enabled applications in heterogeneous cloud computing," JPDC, vol. 111, pp. 126–135, 2018.

131) X. Qiu, L. Liu, W. Chen, Z. Hong, and Z. Zheng, "Online deep reinforcement learning for computation offloading in blockchain- empowered mobile edge computing," IEEE Transactions on Vehicular Technology, vol. 68, no. 8, pp. 8050–8062, 2019.

132) W. Chen, Z. Zhang, Z. Hong, C. Chen, J. Wu et al., "Cooperative and distributed computation offloading for blockchain-empowered indus- trial Internet of Things," IEEE IOT J, vol. 6, no. 5, pp. 8433–8446, 2019.

133) Z. Zhang, Z. Hong, W. Chen, Z. Zheng, and X. Chen, "Joint compu- tation offloading and coin loaning for blockchain-empowered mobile- edge computing," IEEE IOT J, vol. 6, no. 6, pp. 9934–9950, 2019.

134) J. Xu, K. Ota, M. Dong, A. Liu, and Q. Li, "SIoTFog: Byzantine- resilient iot fog networking," Frontiers

The Seybold Report
ISSN 1533-9211

of Information Technology & Electronic Engineering, vol. 19, no. 12, pp. 1546–1557, 2018.

135) Z. Zhan, X. Liu, Y. Gong, J. Zhang, H. Chung, and Y. Li, "Cloud computing resource scheduling and a survey of its evolutionary ap- proaches," ACM Computing Surveys, vol. 47, no. 4, p. 63, 2015.

136) S. Kumar and P. Balasubramanie, "Dynamic scheduling for cloud reliability using transportation problem," Journal of Computer Science, vol. 8, no. 10, 2012.

137) Y. Li, Z. Zhan, Y. Gong, W. Chen, J. Zhang, and Y. Li, "Differential evolution with an evolution path: A DEEP evolutionary algorithm," IEEE Trans. on Cybernetics, vol. 45, no. 9, pp. 1798–1810, 2015.

138) B. Ghosh, S. Addya, A. Satpathy, S. Ghosh, and S. Chakraborty, "To- wards a democratic federation for infrastructure service provisioning," in Int'l Conf. on SCC. Milan, Italy: IEEE, 2019, pp. 162–166.

139) M. Yang, A. Margheri, R. Hu, and V. Sassone, "Differentially private data sharing in a cloud federation with blockchain," IEEE Cloud Computing, vol. 5, no. 6, pp. 69–79, 2018.

140) D. Chatzopoulos, M. Ahmadi, S. Kosta, and P. Hui, "Flopcoin: A cryptocurrency for computation offloading," IEEE Trans. on Mobile Computing, vol. 17, no. 5, pp. 1062–1075, 2018.

141) C. Xu, K. Wang, and M. Guo, "Intelligent resource management in blockchain-based cloud datacenters," IEEE Cloud Computing, vol. 4, no. 6, pp. 50–59, 2017.

142) Y. Zhang, R. Deng, X. Liu, and D. Zheng, "Blockchain based efficient and robust fair payment for outsourcing services in cloud computing," Information Sciences, vol. 462, pp. 262–277, 2018.

143) S. Nakamoto et al., "Bitcoin: A peer-to-peer electronic cash system," 2008.

144) K. Gai, Y. Wu, L. Zhu, L. Xu, and Y. Zhang, "Permissioned blockchain and edge computing empowered privacy-preserving smart grid net- works," IEEE IOT J, vol. 6, no. 5, pp. 7992–8004, 2019.

145) G. Ramezan and C. Leung, "A blockchain-based contractual routing protocol for the internet of things using smart contracts," Wireless Communications and Mobile Computing, vol. 2018, 2018.

146) M. Liu, F. Yu, Y. Teng, V. Leung, and M. Song, "Joint computation offloading and content caching for wireless blockchain networks," in IEEE INFOCOM WKSHPS. IEEE, 2018, pp. 517–522.

147) W. Shi, Q. Ling, K. Yuan, G. Wu, and W. Yin, "On the linear convergence of the admm in decentralized consensus optimization," IEEE Trans. on Signal Processing, vol. 62, no. 7, pp. 1750–1761, 2014.

148) M. Liu, F. Yu, Y. Teng, V. Leung, and M. Song, "Computation offloading and content caching in wireless blockchain networks with mobile edge computing," IEEE Trans. on Vehicular Technology, vol. 67, no. 11, pp. 11 008–11 021, 2018.

149) M. Liu, F. Yu, Y. Teng, V. Leung, and M. Song, "Distributed resource allocation in blockchain-based video streaming systems with mobile edge computing," IEEE Trans. on Wireless Communications, vol. 18, no. 1, pp. 695–708, 2019.

150) Y. Wu, X. Chen, J. Shi, K. Ni, L. Qian, L. Huang, and K. Zhang, "Optimal computational power allocation in multi-access mobile edge computing for blockchain," Sensors, vol. 18, no. 10, p. 3472, 2018.

151) Y. Wu, J. Shi, X. Chen, K. Ni, L. Qian, and K. Zhang, "Optimal multi-access computation offloading for mobile blockchain," in IEEE Int'l Conf. on Communi. Sys. IEEE, 2019, pp. 198–203.

152) Y. Jiao, P. Wang, D. Niyato, and Z. Xiong, "Social welfare maxi- mization auction in edge computing resource allocation for mobile blockchain," in IEEE Int'l Conf. on Communi. IEEE, 2018, pp. 1–6.

153) Y. Jiao, P. Wang, D. Niyato, and K. Suankaewmanee, "Auction mecha- nisms in cloud/fog computing resource allocation for public blockchain networks," IEEE TPDS, vol. PP, no. 99, p. 1, 2019.

154) Z. Li, Z. Yang, and S. Xie, "Computing resource trading for edge- cloud-assisted internet of things," IEEE

The Seybold Report
ISSN 1533-9211

Trans. on Industrial Info., 2019.

155) N. Luong, Z. Xiong, P. Wang, and D. Niyato, "Optimal auction for edge computing resource management in mobile blockchain networks: A deep learning approach," in IEEE ICC. IEEE, 2018, pp. 1–6.

156) Z. Xiong, S. Feng, W. Wang, D. Niyato, P. Wang, and Z. Han, "Cloud/fog computing resource management and pricing for blockchain networks," IEEE IOT J, 2018.

157) V. Krishna, Auction theory. Academic press, 2009.

158) C. Xia, H. Chen, X. Liu, J. Wu, and L. Chen, "ETRA: efficient three-stage resource allocation auction for mobile blockchain in edge computing," in 24th Int'l Conf. Par. & Dist. Syst. IEEE, 2018, pp. 701–705.

159) J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," IEEE Trans. on Industrial Informatics, vol. 13, no. 6, pp. 3154–3164, 2017.

160) C. Qiu, H. Yao, C. Jiang, S. Guo, and F. Xu, "Cloud computing assisted blockchain-enabled internet of things," IEEE TCC, vol. PP, no. 99, p. 1, 2019.

161) Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, "When mobile blockchain meets edge computing," IEEE Communications Magazine, vol. 56, no. 8, pp. 33–39, 2018.

162) Z. Xiong, S. Feng, D. Niyato, P. Wang, and Z. Han, "Optimal pricing- based edge computing resource management in mobile blockchain," in IEEE Int'l Conf. on Communi. IEEE, 2018, pp. 1–6.

163) P. Fairley, "Blockchain world-feeding the blockchain beast if bitcoin ever does go mainstream, the electricity needed to sustain it will be enormous," IEEE Spectrum, vol. 54, no. 10, pp. 36–59, 2017.

164) I. Magaki, M. Khazraee, L. Gutierrez, and B. M. Taylor, "Asic clouds: specializing the datacenter," in 2016 ACM/IEEE 43rd Ann'l Int'l Symp. on Comp. Archi. IEEE, 2016, pp. 178–190.

165) N. Amit, M. Wei, and C. Tu, "Extreme datacenter specialization for planet-scale computing: Asic clouds," ACM SIGOPS Operating Systems Review, vol. 51, no. 1, pp. 96–108, 2018.

166) M. Taylor, "The evolution of bitcoin hardware," Computer, vol. 50, no. 9, pp. 58–66, 2017.

167) J. Liu, W. Li, G. Karame, and N. Asokan, "Scalable byzantine con- sensus via hardware-assisted secret sharing," IEEE Trans. on Comp., vol. 68, no. 1, pp. 139–151, 2018.

168) N. Courtois, M. Grajek, and R. Naik, "Optimizing sha256 in bit- coin mining," in Int'l Conf. on Cryptography and Security Systems. Springer, 2014, pp. 131–144.

169) M. Taylor, "Bitcoin and the age of bespoke silicon," in 2013 Int'l Conf. on CASES. IEEE, 2013, pp. 1–10.

170) C. Lee, "Litecoin," 2011.

171) C. Percival, "Stronger key derivation via sequential memory-hard functions."

172) B. Ekbote, V. Hire, P. Mahajan, and J. Sisodia, "Blockchain based remittances and mining using cuda," in 2017 Int'l Conf. On Smart Technologies For Smart Nation. IEEE, 2017, pp. 908–911.

173) M. Skach, M. Arora, C. Hsu, Q. Li, D. Tullsen, L. Tang, and J. Mars, "Thermal time shifting: Leveraging phase change materials to reduce cooling costs in warehouse-scale computers," in ACM Sigarch Computer Architecture News, vol. 43, no. 3. ACM, 2015, pp. 439–449.

174) A. Kampl, "Bitcoin 2-phase immersion cooling and the implications for high performance computing," Electronics Cooling, vol. 20, no. 1, 2014.

175) S. Ziegenbalg, "Btcminer - open source bitcoin miner," https://open cores.org/projects/btcminer.

176) butterflylab, "Butterflylab," https://butterflylabs.com/category/bitcoin/.

177) Avalon, "Avalon," https://canaan.io/.

178) Bitmain, "Bitmain," https://www.bitmain.com/.

The Seybold Report
ISSN 1533-9211

179) Y. Qian, Z. Liu, J. Yang, and Q. Wang, “A method of exchanging data in smart city by blockchain,” in 20th Int’l Conf. on HPCC. Exeter, United Kingdom: IEEE, 2018, pp. 1344–1349.

180) X. Zheng et al., “Blockchain-based personal health data sharing system using cloud storage,” in 20th Int’l Conf. Healthcom. Ostrava, Czech Republic: IEEE, 2018, pp. 1–6.

181) X. Liang et al., “Integrating blockchain for data sharing and collab- oration in mobile healthcare applications,” in 28th Anu’l Int’l Symp. PIMRC. Montreal, QC, Canada: IEEE, 2017, pp. 1–5.

182) R. Khalil and A. Gervais, “Revive: Rebalancing off-blockchain pay- ment networks,” in ACM SIGSAC CCS. ACM, 2017, pp. 439–453.

183) J. Guo, K. Gai, L. Zhu, and Z. Zhang, “An approach of secure two-way- pegged multi-sidechain,” in ICA3PP. Melbourne, Australia: Springer, 2019, pp. 551–564.

184) Y. Sun, R. Zhang, X. Wang, K. Gao, and L. Liu, “A decentralizing attribute-based signature for healthcare blockchain,” in 27th Int’l Conf. on Computer Communi. and Networks. IEEE, 2018, pp. 1–9.

185) N. Rifi, E. Rachkidi, N. Agoulmine, and N. Taher, “Towards using blockchain technology for iot data access protection,” in IEEE 17th Int’l Conf. on Ubiquitous Wireless Broadband. IEEE, 2017, pp. 1–5.

186) H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, “Towards blockchain-based auditable storage and sharing of iot data,” in Cloud Computing Security Workshop. ACM, 2017, pp. 45–50.

187) S. Ali, G. Wang, B. White, and R. Cottrell, “A blockchain-based decentralized data storage and access framework for pinger,” in 17th Int’l Conf. TrustCom. New York, USA: IEEE, 2018, pp. 1303–1308.

188) R. Chaudhary, A. Jindal, G. Aujla, S. Aggarwal, N. Kumar, and K. Choo, “BEST: Blockchain-based secure energy trading in SDN- enabled intelligent transportation system,” Computers & Security, vol. 85, pp. 288–299, 2019.

189) Yi Li a, Meiqin Tang,"Blockchain-powered distributed data auditing scheme for cloud-edge healthcare system,"Cyber Security and Applications, 2023.

190) Kaiyu Wang, Zhiying Tu, Zhenzhou Ji, Shufan He,"Faster service with less resource: A resource efficient blockchain framework for edge computing,"Computer Communications, 2023.

191) He Xue, Dajiang Chen, Ning Zhang, Hong-Ning Dai, Keping Yu,"Integration of blockchain and edge computing in internet of things: A surve",Future Generation Computer Systems,2023.

192) Aaliya Sarfaraz, Ripon K. Chakrabortty, Daryl L. Essam,"The implications of blockchain-coordinated information sharing within a supply chain: A simulation study,"Blockchain: Research and Applications,2022.

193) Seyednima Khezr, Abdulsalam Yassine & Rachid Benlamri,"Towards a secure and dependable IoT data monetization using blockchain and fog computing ,"Cluster Computing, 2023.

194) Haoyu Wang, Jianwei An, "Dynamic stochastic game-based security of edge computing based on blockchain ,", The Journal of Supercomputing, 2023.

195) Nallapaneni Manoj Kumara,Pradeep Kumar Mallickb,"Blockchain technology for security issues and challenges in IoT,",Procedia Computer Science, 2018 .

196) P. Sharma, S. Singh, Y. Jeong, and J. Park, “Distblocknet: A distributed blockchains-based secure SDN architecture for IoT networks,” IEEE Communications Magazine, vol. 55, no. 9, pp. 78–85, 2017.

197) X. Ling, J. Wang, T. Bouchoucha, B. Levy, and Z. Ding, “Blockchain radio access network (B-RAN): Towards decentralized secure radio access paradigm,” IEEE Access, vol. 7, pp. 9714–9723, 2019.