LUISS

Dipartimento
di Impresa e Management

Cattedra di Digital Business and Workplace Technology

Blockchain-as-a-Service: new architectures for Data Security in Cloud

Prof. Paolo Spagnoletti

RELATORE

Matr. 242211
Francesco Migliore

CANDIDATO

Anno Accademico 2021/2022

Table of Contents

1. Introduction

Recent years have witnessed an enormous increase in cloud computing utilization.

The COVID-19 outbreak intensified the migration to the cloud, which was already happening in many enterprises. Businesses were required to be able to support and offer essential services to their off-site workers as teleworking became more common.

Because of this, according to CheckPoint Software Ltd. survey about the major cloud security challenges in 2022 [46], more than 98% of businesses employ some sort of cloud-based architecture, and 76% of them have multi-cloud installations that combine services from two or more different cloud providers. Critical business applications are hosted in these cloud environments, which also contain private consumer and business data.

The shift to the cloud necessitates the implementation of cloud security because such cloud-based apps need to be secured from attacks, and any data stored in the cloud needs to be safeguarded from unauthorized access in compliance with any applicable laws.

The Problem of Cloud Data Security

Among the most important cloud security challenges that have to be addressed there are:

- Unauthorized Access
- Stealing or Exposure of Credentials
- Cyberattacks
- Data Leakage
- Cloud Customers' Accounts Hijacking
- Sharing Data with Third Parties
- Malicious Internal Nodes
- Data Privacy and Control

Therefore, it is quite clear that every IT manager dealing with cloud infrastructures reckons that data security especially in public clouds is an aspect that has to be successfully tackled in order to guarantee reciprocal trust between the enterprise and its customers. [47]

Usually, major cloud computing service providers use centralized servers which allows for a cohesive security strategy that defends the entire business from outside threats by overseeing security operations on a corporate level, but it also creates a security difficulty. As a matter of fact, when using a centralized security solution, all security functions are unified in a single appliance, which increases the risk of a single point of failure.

Because security is now a shared duty between the consumer and the cloud provider, cloud computing frequently includes outsourcing trust to a provider. However, the majority of cloud security blunders are the fault of the customer even though data might be extensively exposed via inadequate permission procedures, making businesses vulnerable to intrusions. In addition, regulations like GDPR are becoming more prevalent, which implies public server compliance will probably result in higher cloud prices and less cloud management. Therefore the cloud's promise to improve IT efficiency, flexibility, and scalability is still as true as ever, but security remains an issue. [50]

Using Blockchain to Improve Data Security

Blockchain uses a shared database made up of units of transactions known as blocks that store and encrypt data. A blockchain is created when a time-stamped block joins the filled block ahead of it, and another block joins behind it when it fills with data. The far more popular use is as a distributed ledger, where each participant shares an immutable ledger that only other members with permission can access. [48]

Hence, by providing a record that cannot be altered and is end-to-end encrypted, blockchain can aid IT Managers in the prevention of fraud and unlawful activities supported by the enhancement of cloud data security. It also employs permissions to regulate access, anonymize personal data and reduce privacy concerns. Information, sensitive data and digital assets are also less susceptible to hacking when stored across a decentralized network of computers as opposed to a single server. Big data management and storage on the current public blockchain infrastructure is not always highly scalable, but sharing the data on a cloud platform can boost scalability, making blockchain a useful service that offers stronger data security through decentralization, privacy, and immutability. A major concern with cloud storage is guarding against data theft.

Blockchain provides a way to keep track of past transactions, highlighting any attempts to tamper with the data and is relatively simple to spot efforts to tamper with the data because each block contains a hash that is specific to that block as well as the hash of the previous block. A change to a transaction that has been recorded on a ledger would invalidate the signatures and notify the networks because blockchain data is encrypted, decentralized, and reviewed by all the participating networks. As a result, it is nearly impossible to change a transaction once it has been recorded on a ledger because doing so will lead the networks to become aware of the change. Moreover the numerous nodes in the network that confirm each authorized transaction would need to be compromised simultaneously in order to hack the blockchain and launch a 51% attack which calls for a hostile user to seize control of a certain blockchain network, and is practically close to impossible for this to happen.

However, companies looking to use blockchain to improve their cloud security will need to invest in research and training since it is a relatively new technology and corporate executives will also need to become comfortable with the new methodology. Indeed, adopting blockchain is anticipated to have a wide range of generally positive consequences on business. 64% of participants in a TechRepublic study from March 2022 [49] predicted that blockchain will have some impact on their industry, with the majority of them anticipating a beneficial one.

Blockchain-as-a-Service

During the last five years, the continuous exponential growth and adoption of cloud services and solutions for private users and enterprises led Cloud Service Providers to standardize and differentiate the several models of cloud services offered. [33]

Those models are three and are commonly known as Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS).

IaaS, exploiting virtualization technologies, supplies a cloud computing infrastructure together with servers, storage, operating systems and networks. This service gives to its customers the responsibility to directly manage data, applications, operating systems, middleware and runtime. PaaS empowers developers to build and develop softwares, without the burden of managing storage, infrastructures, operating systems or software updates.

In SaaS there is the higher level of third-party management, in fact this type of solution delivers online softwares, removing the need to download and install applications on the consumer's device. [34]

Another phenomenon that is gaining popularity and awareness in the business world is the blockchain technology. Due to its disruptive nature as an innovation in the IT sector, there are still a few barriers that prevent its widespread adoption. An example of adoption barrier is often seen in technical complexities and considerable costs related to creation, configuration and maintenance of a blockchain infrastructure.

To reduce those adoption barriers and to enable businesses in several industries to benefit from this new technology, many tech companies worked on the re-engineering of cloud computing from the perspective of blockchain implementations. [33] On the basis of already existing cloud services, this new service model deems and provisions blockchain systems or components by a third party to assist customers with the development and/or management of their blockchain initiatives, enabling companies to build and develop blockchain-based services, applications and solutions by accessing a blockchain provider's services. [34]

This emerging blockchain-oriented service model, is known as Blockchain-as-a-Service or BaaS. This new service model makes blockchain adoption far more smoother because it allows customers to keep their focus on the core business rather than struggling with technical obstacles of blockchain. Indeed, BaaS makes customers' life easier by leveraging its cloud-based approach which enables a third-party to install, maintain blockchain networks or to obtain blockchain-related supports.

Logically BaaS has generated great curiosity, becoming very common in the blockchain market as it is an high-speed and relatively low-cost solution and therefore pushing several CSPs to expand their service offerings. Hence with various incumbent BaaS providers, the purpose of each BaaS offered is distinct but common target functions and benefits include security, cost saving, time saving, system integration, ease-of-use, scalability, and control optimization.

Finally, this work will present in the following chapter a detailed analysis and review of recent works and literature addressing this topic, by selecting four main aspects that characterize the major areas of potential application of blockchain with cloud computing.

In chapter 3, is proposed an answer to the research question by presenting the most relevant real-world applications of this two technologies combined together with an emphasis on how data security is achieved and maintained. The last chapters 4 and 5 discuss respectively the conclusions of this research with a glance on possible future research directions and the bibliography of all the sources of cited works.

2. Relevant Literature and Recent Works

In this section, the existing research and works about the specific use of blockchain for data security in cloud computing is studied.

To find relevant targeted papers and studies on this topic, the research approach can be divided in three main steps: aggregation, filtering and analytical evaluation.

During the first step, to address the research question, a systematic literature research was performed using Scopus as the principal scientific database. The major keywords applied to search in the Scopus database were: “Blockchain as a Service” OR “Blockchain Service” AND “Cloud” AND “Computing” OR “Blockchain Service” AND “Cloud Computing” OR “Cloud Computing” AND “BaaS” OR “Blockchain Service” AND “Data” AND “Security” AND “Cloud Computing” OR “Blockchain” AND “Cloud” AND “Security”.

Every paper meeting the targeted keywords set was retrieved in its full-text form to be further analyzed later on in the subsequent step.

In the filtering step, after collecting and aggregating the full texts of the retrieved literature, the research papers’ eligibility is evaluated and compared according to a set of inclusion and exclusion criteria. Lastly, the third step consisted into performing a qualitative analysis and detailed evaluation of the remaining “filtered” papers which met the inclusion criteria in order to empower their purposeful usage to support this thesis’ work on providing solid answers to the research question.

From a systematic literature review, there is remarkable evidence of a significant increase in the number of scientific papers and articles in relevant publications focusing on addressing the usage and implementation of the blockchain in cloud computing settings.

This steady and up-ward trend can be possibly attributed to the rise of attention that this next-generation technology has recently drawn due to its proven security that suits the current informatization era. Precisely, through the authentication of peers that share virtual tokens, encryption and the generation of hash values (Park and Park, 2017) [4].

Hence is worthy to mention that, before being used to pitch into cloud-computing applications, blockchain essentially started as “a way to move Bitcoin from point A to point B, but it is now being used and exploited by a host of big companies to monitor, manage and protect any number of assets around the world as easily as sending an e-mail” wrote Michael Del Castillo [1] for Forbes’ Blockchain 50, a list representing 50 enterprises embracing this technology to speed up business processes, increase security, transparency and to possibly save billions of dollars.

If on one hand is already possible to find in recent literature many applications of this technology in different sectors of the so-called the Industry 4.0, ranging from FinTech to Supply Chain and E-Health, on the other hand there are only quite a few studies addressing its usage for pure data security purposes. One of those works conducted by Joshi et al. [3] shows that in this context (Industry 4.0), which is a catch-all term for a cluster of cutting-edge, industrial, innovative and disruptive technologies that support digital and semi-digital businesses in solidly boosting their efficiency, the Blockchain Technology (BCT) “has the potential to significantly improve data security, privacy and openness for both small and medium enterprises (SMEs) as well as large enterprises” since this technology would not only allow businesses to operate in a smoother and more comfortable fashion but also to uphold their status of being a credible and trustworthy party. This is possible thanks to key features and benefits such as: traceability, integrity, auditability, interoperability, decentralization and security. The authors, in fact, affirm that those characteristics make this technology a “compelling alternative” that can offer solutions to tackle concerns related to Industry 4.0 and to benefit enterprises in terms of competitiveness, efficiency and agility.

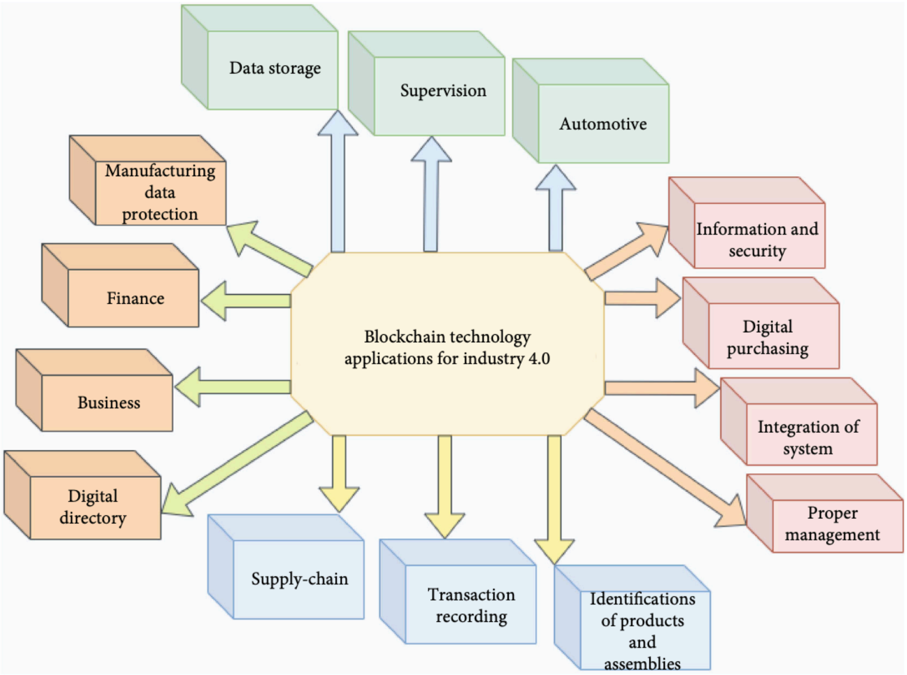


Fig. 1: Blockchain Technology applications for Industry 4.0 (Joshi et. al, 2022)

Another important component which contributed to Industry 4.0 success is the adoption of cloud computing (Shah et al.) [5]. The latter, though, has in first place special architectural capabilities that advance various questions regarding security and privacy. In second place, since cloud computing enables businesses to outsource their required services, it does in fact provide new data protection challenges regarding reliability, integrity and confidentiality becoming indeed a key differentiator and a competitive vantage point among cloud providers (Gong, Nima and Navimipour) [2].

Furthermore, precisely concerning the aforementioned challenges, the authors [2] assert that customers' authority over their data is drastically reduced from the moment that it is sent to the cloud. This in turn makes primitive data security no longer possible and a solution to tackle this problem is seen by Gai et al. [6] where blockchain technology was "integrated with existing cloud infrastructure technologies" by addressing three technical dimensions. First of all analyzing the Blockchain-as-a-Service (BaaS), a progressing cloud-relevant blockchain service model, then by evaluating access control schemes and searchable encryption for security concerns and finally by investigating on both software's and hardware's side the eventual success of cloud datacentres benefitting from blockchain's presence.

Now, from this part of the section, there will be a focus on the main aspects that stood out from this literature review as the key areas in which cloud computing can get the highest potential benefit by integrating or by being supported by blockchain.

These aspects are: security, privacy, data integrity, and trust.

2.1 Security

After the first two COVID-19 pandemic years, it is safe to say that this phenomenon has boosted an increase in digitalization for a lot of industries. In several of those industries a massive quantity of data is uploaded, stored, managed and transferred via cloud services every day. With almost the same frequency though, plenty of cyber-attacks are taking place and being deployed all over the world to hack, steal and possibly resell highly valuable and sensitive data and informations about enterprises' customers or about enterprises themselves. It logically follows that security now more than ever is a very important topic and issue that needs to be addressed.

The employment of blockchain technologies in the cloud will therefore resolve cloud subscribers' trust and security matters, making Service-Level Agreements (SLAs) explicit and available to cloud prospects for a more rapid delivery of the service. [7]

Park et al. [4], in their study, aimed to adapt blockchain security to cloud computing and its secure solutions by surveying and analyzing the trends on generic technology and research studies to date. Subsequently this study discussed the method of providing security via a secure use-and-remove blockchain protocol that required the use of an electronic wallet on the peers's side. This method should ensure the anonymity of users' information in a blockchain-supported cloud computing environment and complete deletion of the same users' information when the service is either fulfilled, cancelled or removed.

Clearly, possible leaks of users' information can be avoided only when the electronic wallet is completely and securely removed by sending the finished message. If instead data is disclosed in the cloud computing environment, monetary and psychological damages might take place due to the leak of sensitive information. Once again it's comprehensible that blockchain, used within the cloud computing environment, can represent a convenient service that provides a more powerful and robust level of security.

Enterprises and organizations must keep up with the research and development of technologies to appropriately face and overcome cybersecurity threats. This is what Raimundo et al. [8] study is all about: to fill a gap in the Internet of Things (IoT) and in the Industrial Internet of Things (IIoT) cybersecurity literature.

In substance, the authors argue, the latest developments in blockchain technologies may bring security enhancements to decentralized systems' architectures of IoT devices to protect against malicious internal users and malwares implanted inside the system.

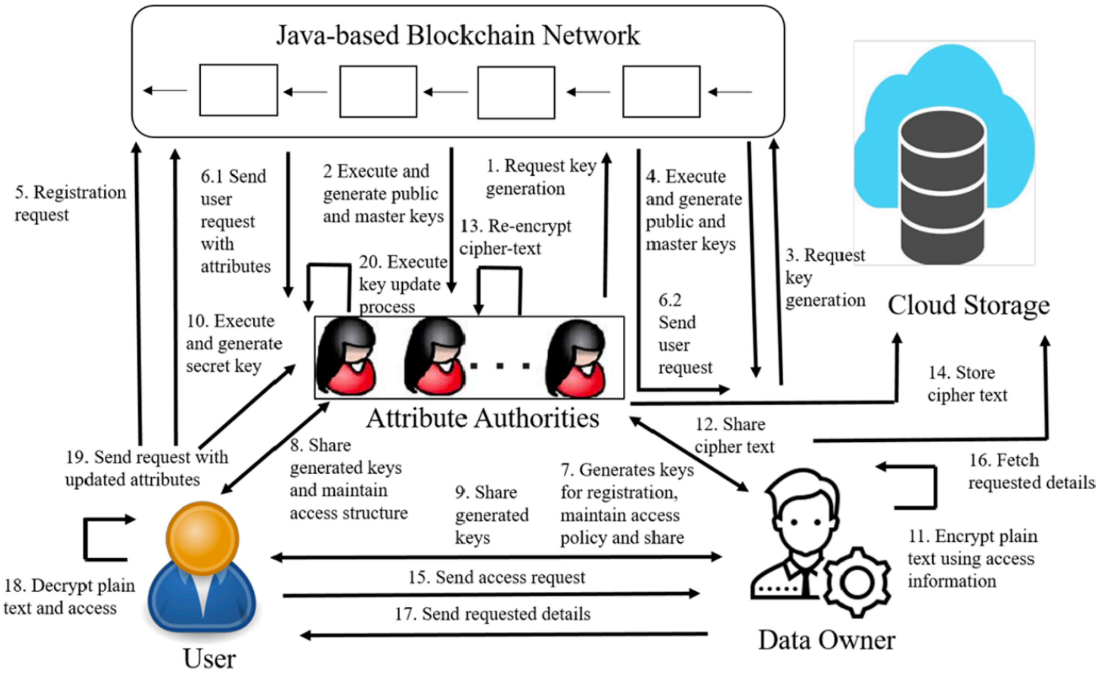
For example, blockchain may contribute to "privacy, security, and non-repudiation of an IoT system via enormous amounts of data generated and several sensor and devices in use as this technology builds a scalable and decentralized end-to-end secure IoT system".

Furthermore, from the study is evinced that "blockchain is also utilized in parallel with cloud computing for higher education, in terms of primary infrastructure topology, by putting together machine learning (ML) and artificial intelligence (AI) on models' training opportunities" [11].

Thus there is the presence of a significantly high correlation between cloud computing and blockchain in preventing attacks against IoT firmware or wireless protocols. This underlines the potentially central role of blockchain technology in the future of cybersecurity in IoT and IIoT, emphasizing that the importance of security is as increasing as the number of wireless-connection devices in the short term, which extends to "virtually all areas of our daily lives that need to be effectively managed" [8].

The proposal of Sharma et. al [9] wants to impose some data security measures before outsourcing data to cloud servers in order to provide a more secure environment. To protect users' privacy, ensure data protection and tackle security issues, the authors proposed a blockchain-based framework with the Ciphertext Policy Attribute-based Encryption

(CP-ABE) algorithm that provides access control and user revocation methods in the cloud storage system. According to their study there is a need to integrate cloud storage and blockchain technology to improve the performance of existing cloud security applications in order to get an architecture that can provide secure and reliable cloud storage services for enterprises and individual users.



Java-based Blockchain Network
Cloud Storage
5. Registration request
6.1 Send user request with attributes
2 Execute and generate public and master keys
1. Request key generation
13. Re-encrypt cipher-text
20. Execute key update process
4. Execute and generate public and master keys
6.2 Send user request
3. Request key generation
10. Execute and generate secret key
Attribute Authorities
14. Store cipher text
12. Share cipher text
19. Send request with updated attributes
8. Share generated keys and maintain access structure
9. Share generated keys
7. Generates keys for registration, maintain access policy and share
16. Fetch requested details
11. Encrypt plain text using access information
18. Decrypt plain text and access
15. Send access request
17. Send requested details
User
Data Owner

Fig. 2: Sharma et al. CP-ABE System Model (2022)

The proposed solution is divided in three main steps: first of all, a java-based blockchain network is designed to register data owners and attribute authority using a key generation algorithm using bilinear mapping-based cryptography. In second place, data owners and attribute authorities store public information in the blockchain structure in a distributed manner, set access policies, and generate the user's secret key to resolve key escrow problems. In the third and last step, the immediate attribute modification is deployed to attain fine-grained access control at the system level with a robust user revocation process.

The evaluations regarding performance, comparative analysis and experimental results point out that Sharma et. al proposed architecture offers a "more efficient and scalable environment to the outsourced cloud data maintaining the effectiveness of existing solutions but providing a better and secure solution".

Another blockchain-based cloud service addressing the security topic is advanced by Pon et al. [10] where a SECure LearningChain (also known as SEC-LearningChain) design with the support of machine learning, blockchain and cloud computing primitives is applied to guarantee data transaction security in a Peer-to-Peer (P2P) network as well as efficiency in data sharing.

This method uses an efficient machine learning algorithm to detect unwanted traffic and intrusions inside the system meanwhile the incorporation of blockchain offers better data transaction and secure services to the cloud system's users. As reported by the authors of the paper, the main benefits of their proposed approach are in first place the ability to handle with low transaction latency a large number of transactions in each block, secondly to achieve high levels of aggregated on-cloud services with low costs and finally to provide rock-solid and reliable security measures against potential cyberattacks.

The SEC-LearningChain architecture is composed by four design models being an attack detection model, a mold blockchain transaction network (MBC-Tnet) model, a machine learning (ML) model and a cloud assessment.

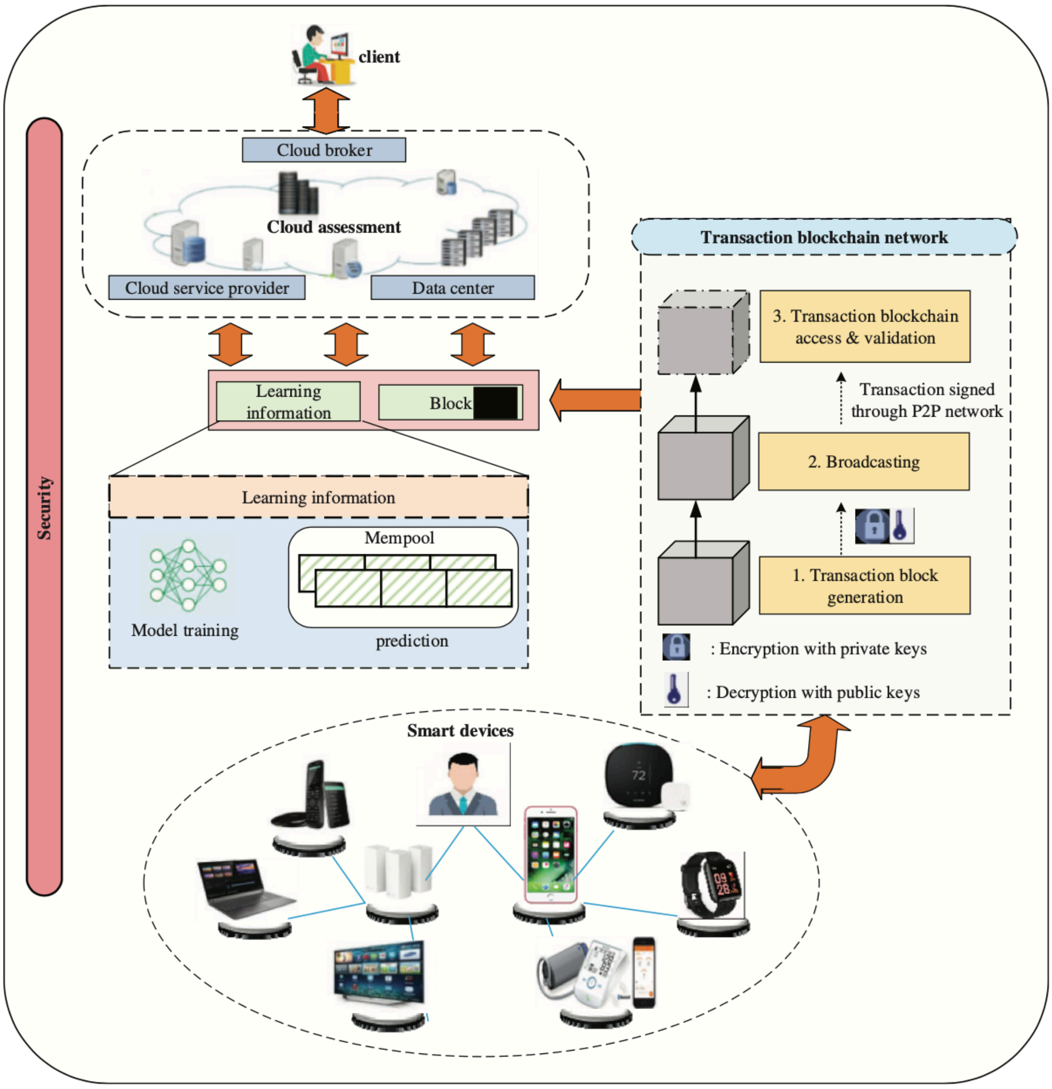

client
Cloud broker
Cloud assessment
Cloud service provider
Data center
Security
Learning information
Block
Learning information
Mempool
Model training
prediction
Transaction blockchain network
3. Transaction blockchain access & validation
Transaction signed through P2P network
2. Broadcasting
1. Transaction block generation
: Encryption with private keys
: Decryption with public keys
Smart devices

Fig. 3: Overview design of the architecture proposed by Pon et al. (2021)

At the beginning, the attack detection model performs a detection of attacks targeting the system's security making use of threshold-based anomalous traffic detectors and examining traffic flow record data from smart devices.

In second place, the MBC-Tnet takes the stage employing the blockchain based on hash function and encryption to validate the identity verification process to address attacks for secure traffic flow record transaction. Subsequently, thanks to a perceptron algorithm the large-scale transaction record is optimized and iterates the ML model with the learning information for transaction output prediction. Finally, the cloud assessment model is designed to enhance the efficiency of the cloud service which manages the stored transaction records, sharing the accessed services across different cloud platforms for each service center. This model is designed not only to enhance efficiency but also to mitigate the risks of malicious attacks and threats putting the cloud users into the position of authorizing trustable transactions through the MBC-Tnet.

The evaluation regarding performance results of the proposed SEC-LearningChain security architecture after being compared with different existing methods such as blockchain based dueling deep reinforcement learning (Dueling DRL), blockchain based distributed machine learning (BC-DML), smart home based on blockchain and cloud computing (SH-BlockCC) and others estimates "an high level of service to be performed on each block, moreover the overall security architecture prevents attacks for traffic record transactions making large-scale smart device data management more efficient and secure with respect to the other existing methods".

Paper	Security	Authentication	Anonymity	Performance	Scalability	Intrusion Detection
[7]	✓			✓		
[4]	✓		✓	✓		
[8]	✓				✓	✓
[11]	✓				✓	
[9]	✓	✓		✓	✓	
[10]	✓	✓		✓		✓

Table 1: Key points of security papers

2.2 Privacy

Alongside security, another major factor for enterprises or individual users who make use of cloud services is privacy. As of today, since data has been considered the new gold, privacy protection is gaining importance for future developments of cloud technology in every applicable field. Moreover considering that data is often processed across multiple clouds, each with their own specificities and constraints, there is the need of a multi-cloud protection system. From recent papers, can be evinced that a substantial amount of research and work has been carried through to strengthen multi-cloud data privacy and to detect internal and external cyber-attacks by mixing blockchain and innovative intrusion prevention technology. According to Casino et al. [13] blockchain is considered as an opportunity for building up the privacy aspects of data and its scalability when combined with efficient cloud storage systems. In their study the usage of decentralized digital identity (DiD) services is suggested to confirm an user's identity, enabling privacy and anonymity in a standardised verification model.

Liang et al. [16] exposed a blockchain-based framework for cloud auditing called ProvChain. This framework aims to keep users' privacy and anonymity intact while incrementing availability. It involves the usage of a record with an immutable time-stamp and a blockchain receipt to verify each data record with the blockchain itself.

It is as well worth to mention the choice of the data unit, such as data chunks, instead of files highlighting the employment of such levels of granularity in cloud computing. From their research it results that a provenance-enabled private cloud has low operating costs meanwhile regarding the incentives for blockchain miners, cloud users might have to pay a fee to make use of the service and the service supplier will instead finance the blockchain network.

Moving on, the study conducted by Alkadi et al. [17] propounds a framework whose goal is to provide security-based distributed intrusion prevention and privacy-based blockchain with smart contracts to IoT networks. This framework, also known as Deep Blockchain Framework (DBF) makes use of the Ethereum Library for its privacy-based blockchain and smart contracts to supply privacy to intrusion detection systems.

As stated in the results, the advised intrusion detection system outperforms other methods of accuracy and detection rate letting the authors come to the conclusion that the proposed architecture makes inter-cloud data sharing faster, cleaner, economically efficient and more open.

Related to the privacy aspect, another element studied from the literature regards healthcare cloud data and smart healthcare systems. Those systems are designed to collect real-time acquired sensitive data about users such as ID, name, locations, health conditions and more. Now more than ever, healthcare data seems very palatable and potentially profitable for cyber attackers. Those attacks, if successfully executed, do not depict an encouraging aftermath scenario for the victims, perhaps, there may be devastating implications and problems for healthcare organizations. For this reason, by decentralizing healthcare cloud data and giving access to it only to pre-authenticated users, we can perceive and behold on one hand to a significant decrease in the chances of successful cyber attacks and at the same time, on the other hand, to an increase in privacy to effectively protect the owners of this data.

El Azzaoui et al. [14] presented a Quantum Cloud-as-a-Service as an efficient, secure, and scalable for complex Smart Healthcare computation. The most distinctive trait of this architectures resides in the combined usage of Quantum Machine Terminal (QMT) and blockchain to boost the feasibility, privacy and security of healthcare cloud data.

Divided into three phases, this proposed architecture employs blockchain in its first phase, as a distributed technology, in first place to create a secure cluster of honest and verified nodes with required rights to access the Quantum cloud and benefit from its offered services. Secondly, prevents the unauthorized access to the Quantum Network to malicious nodes and components of smart healthcare systems such as fake hospitals and thirdly to secure communication between smart hospitals, healthcare providers and research institutions with the QMT at the “edge” layer of the architecture.

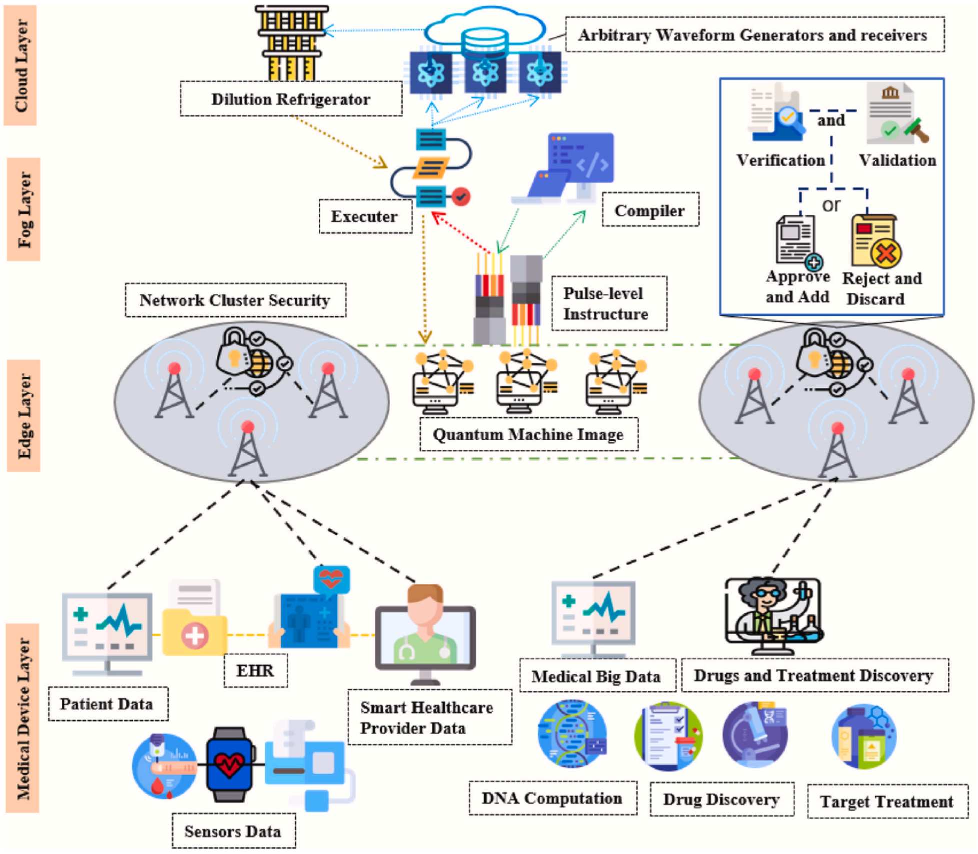


Fig. 4: Blockchain-based Delegated Quantum Cloud architecture overview (2022)

This additional and third employment of blockchain technology tightens even further the security of private data and computation requests, ensuring that Quantum Machine Terminal is blind to the inputs and outputs. The second phase is designed to secure the communication between the QMT and the Quantum Cloud Servers (QCS). This is permitted via the use of Quantum One - Time Pad (Q-OTP) which establishes “an absolute secure communications between two entities where the private key is as long as the message”. Q-OTP allows to benefit of an ensured total communication privacy and security in a secret direct communication environment. The third phase consists in the use of Delegated Quantum Cloud to securely compute the requested patient sensitive data such as drug discovery, DNA sequencing or a search in a database, while preserving information privacy and computation security. Those Quantum Cloud Computations (QCC) are executed at the “cloud" layer in a faster, scalable and more efficient way with respect to any classical computer in use in a Smart Healthcare System nowadays.

Finally, to measure the safety of the proposed architecture, the authors stated that has been performed the computation of the Grover searching algorithm over the fully encrypted data on Quantum Cloud. The subsequently analyzed results underline how feasible is to implement a blockchain-based delegated Quantum Cloud architecture to address medical and smart healthcare big data privacy and security.

Paper	Privacy	Scalability	Verification	Efficiency	Intrusion Prevention	Performance
[13]	✓	✓	✓			
[16]	✓		✓	✓		✓
[17]	✓			✓	✓	✓
[14]	✓	✓	✓	✓	✓	

Table 2: Key points of privacy papers

2.3 Data Integrity

Under the umbrella of cloud data security, data integrity is definitely an aspect that deserves to be taken in consideration and analyzed. Generally speaking, data integrity is a term that describes the action of protecting data from unauthorized deletion, modification or fabrication.

In cloud systems, means preserving information integrity avoiding data loss or modification by unauthorized users. Hence, since data integrity is the basis to provide cloud computing services such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS), a good management of the nodes' authorization to access specific cloud resources and data ensures that valuable digital assets and informations are not abused, compromised, misappropriated or stolen [21].

Usually, Cloud Service Providers (CSP) are trusted to competently maintain data integrity with their inspection frameworks but in any case it is still needed to depend a trusted third-party supervision mechanism (also known as Third-Party Auditors) besides users and CSPs. Anyway even if all those aforementioned measures are taken in order to guarantee data integrity to cloud users, there are issues and challenges to face such as the single-point failure. Almost all TPAs use a clustered architecture with a centralized storage method which if it fails, the whole cloud service becomes inaccessible and making it impossible to any user to retrieve data. In this way the central server logically becomes the bottleneck of the system [20]. The following articles analyzed discuss about addressing the above-said challenge by using blockchain, benefiting from its decentralized nature.

For Jyoti et al. [18] blockchain can boost trust in data integrity and provenance in cloud computing environments. Their proposed decentralized architecture sees each node in the network providing better efficiency and availability than traditional centralized architectures, guaranteeing data integrity proficiency for a cloud computing atmosphere.

Since this solution is cloud-based and blockchain-based, it permanently records every data operation therefore leading to a concrete and reciprocal establishment of trust between data users (DU) and cloud service providers (CSP). Furthermore, is worth to mention that usually the storage of huge data over the blockchain is more expensive because of its distributed nature, but the authors solved this issue employing a system such as the decentralized data saving system known as “Interplanetary file system” (IPFS).

Not only solved this issue, but proposing a Blockchain Smart Contract Data Provenance (BSCDP) method in the cloud environment overcame specific data integrity and provenance problems that traditional methods like the above-mentioned ProvChain [16] have.

First off, in the proposed architecture design, the user’s fingerprint is captured by a fingerprint scanner and then converted into auxiliary encrypted data by the Fuzzy Extractor (FE). The encrypted data is consequently given to the CSP to avoid biometric data leaks. Secondly, following the data user registration, the keys are generated and data is encrypted using an elliptic-curve key based cyclic shift transposition (ECCST) cryptography algorithm to enhance security when sharing the keys.

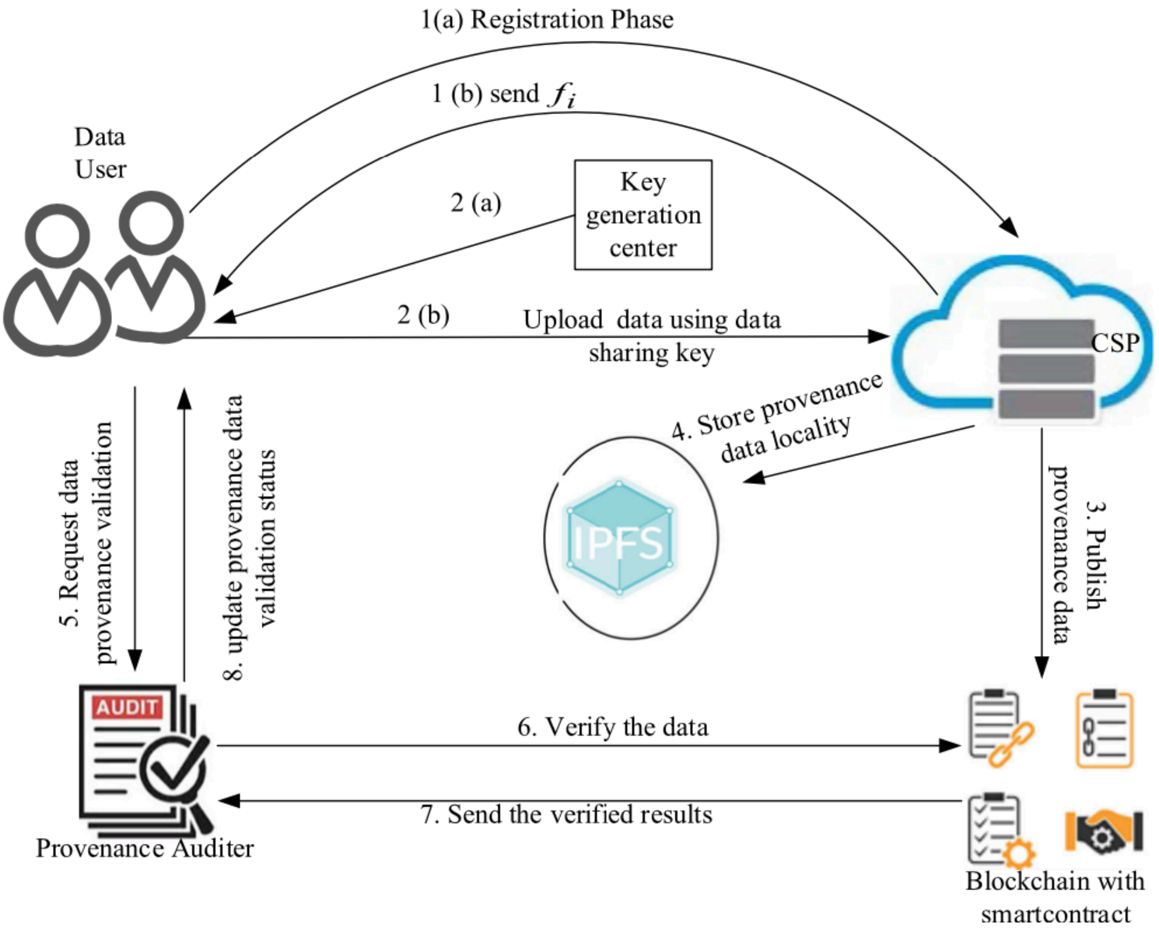

1(a) Registration Phase
1 (b) send f_i
Data User
2 (a)
Key generation center
2 (b)
Upload data using data sharing key
CSP
4. Store provenance data locality
IPFS
3. Publish provenance data
5. Request data provenance validation
8. update provenance data validation status
AUDIT
Provenance Auditer
6. Verify the data
7. Send the verified results
Blockchain with smartcontract

Fig. 6: Proposed architecture of secure BSCDP and integrity collection in cloud environment (2022)

Thirdly, blockchain and the IPFS are employed for provenance and integrity data collection, hash computation, and storing with reduced computational overhead (CO). Precisely, data integrity is maintained by using blockchain-based secure hashing algorithm-3 (SHA-3). Moreover, for better data user access organization, there is also an integration of blockchain smart contracts (SC) with IPFS that enable the development of decentralized cloud storage. By arranging fuzzy-based smart contracts (FSC), the data user can tracks its data and the history of that data.

The data collected is directly stored in IPFS and the DU gets a hash from IPFS to retrieve the data in the future. Finally, the data verification is done by the provenance auditor (PA) by checking the mapping file of IPF and the blockchain, alongside data validity on the user's side.

As far as the authors are concerned, when their proposed BSCDP method is compared to existing ones (such as BHA, ISA and CGA), the former achieves higher security and performance in the cloud environment in terms of insertion time, verification time, response time, total change rate, computational overhead, encryption and decryption time meanwhile scalability affects factors like blockchain's block size and block interval time.

Huang et al. [22] suggested a shared auditing blockchain system for cloud data storage to tackle persistent trust issues involving data holders on one side and cloud service suppliers on the other. In the authors' system both consensus nodes operate as a single TPA, executing auditing delegations and stopping corporations from being untrustworthy and deceptive with one another. This consensus protocol, thanks to its distributed nature, resisted centralization and an incentive method supported the augmentation and maximization of Collaborative Auditing Blockchain (CAB) stability and security.
Additionally, a security review revealed that the architecture benefits from defending cloud data integrity against a wide range of cyberthreats while concurrently, unlike other blockchain-based auditing systems, CAB was being more resource-efficient and functional to data owners and users.

Zhou et al. [19] proposed a scalable blockchain-based integrity verification scheme suitable as well for large-scale IoT data that implements fully dynamic operations such as insertion, deletion, modification and block-less verification. The authors designed and created a scalable homomorphic verification tag based on the Zhang-Safavi-Susilo (ZSS) short signature, which implements basic cryptographic hash functions such as SHA-1 or MD5 to accomplish scalability without the need of recurring to computationally expensive hash algorithms. This scheme, thanks to block-less verification, gives permission to users' data auditing without retrieving it in its entirety. Instead of relying on TPAs, in this scheme the task regarding the integrity verification can be executed without any risk of privacy leakage and with an higher level of protection against collusion cyberattacks thanks to blockchain smart contract technology.

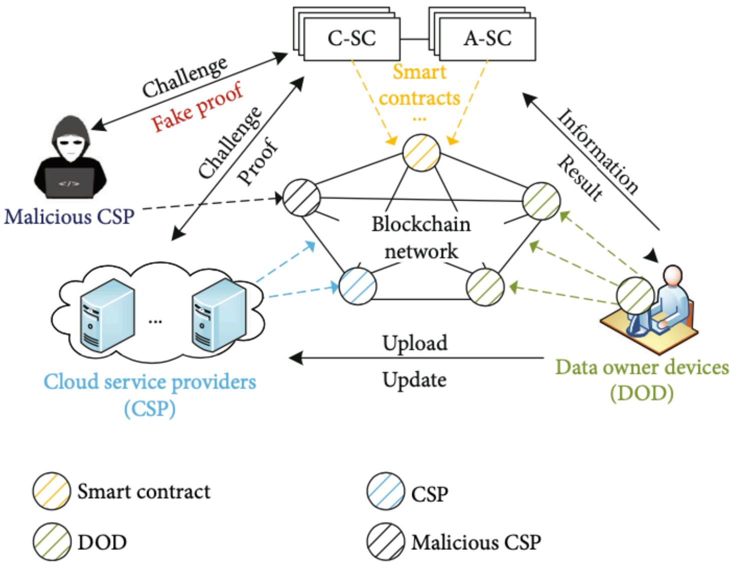


Fig. 7: Zhou et al. proposed network model (2022)

Moreover, a blockchain-based security model is defined to prove that the proposed designed scheme is secure under the security assumption of cryptographic primitives. Lastly the results from the mathematical analysis of the authors' scheme show that the communication complexity of an audit is O(c), where c refers to the number of challenge blocks. Comparing this scheme with existing ones the proposed scheme is the fastest, in matter of time efficiency, to successfully complete an audit.

Witanto et al. [23] focused their study on keeping data integrity in cloud-based AI systems. To this extent, they built a data integrity architecture following the National Institute of Standards and Technology (NIST) cybersecurity framework guidance.

The major point of this architecture is blockchain, since it is a suitable solution to data integrity and trust issues problems in cloud-based AI systems that constantly rise among users and CSPs. Alongside blockchain, smart contracts are used to automate policy enforcement, keep track of and enhance data integrity throughout ML pipeline, and prevent data forgery. To meet the NIST requirements about Identity and Access Control Management, they relied on digital signature to verify users' identity every time the system is entered and services are used.

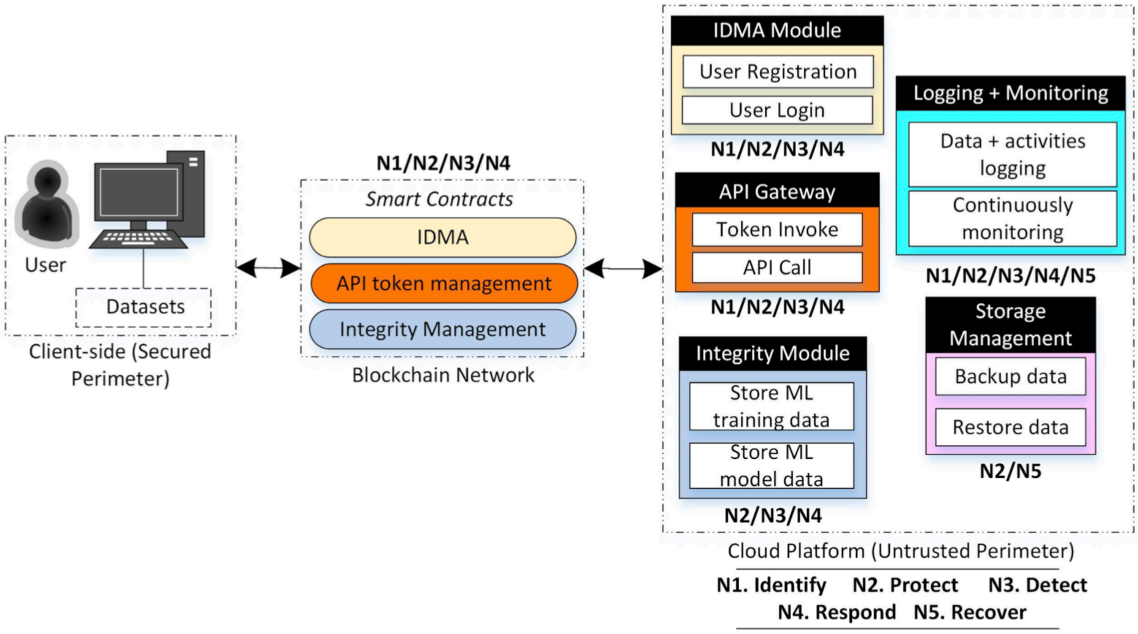


Fig. 8: data integrity architecture for Cloud-based AI Systems (2022)

For Consistency and Completeness related to ML datasets, a hash function ensured no violation of data integrity supported by a correspondent record on the blockchain. To overcome Non-repudiation, the authors' solution required each user to sign data to verify their identity whenever a modification is performed. Finally, through trusted Service Level Agreement (SLA) policy enforcements could be maintained making use of smart contracts to bind trust between service users and CSP who is able to automate the SLA process.

Paper	Data Integrity	Provenance	Trust	Verification	Efficiency	Performance	Scalability
[18]	✓	✓	✓	✓	✓		
[22]	✓		✓		✓		
[19]	✓			✓		✓	✓
[23]	✓		✓	✓			

Table 3: Key points of data integrity papers

2.4 Trust

Nowadays, for most businesses, enterprises and individual users operating on cloud services, it is a major concern to do this activity with a third party they can trust. In fact, after accepting the terms and conditions (T&Cs) of a cloud service provider (CSP) and using the service to outsource data and upload it onto the cloud, the user-side control over every digital asset put on the cloud is essentially lost. This, alongside possible not-so-transparent security warrants on the CSP side might cause a deficit of customer confidence [12].

A solution to this inconvenient involving service providers and the respective consumers, would be the application of a trust mechanism based on blockchain for services' information [15]. In this section relevant literature addressing the aspect of trust will be analyzed and discussed.

The vision of Rong et al. [24] seeks to amplify existing cloud computing services that are able to support multi-cloud infrastructures and seamless integration of cloud-based micro-services. The approach proposed to execute this vision, is called Open Infrastructure as Code (OpenIaC). Built on advances in cloud computing and blockchain, its main mission is to provide a multilayered suite of services based on the principle of Zero-Trust-Architecture (ZTA) achieving secure and trusted interoperability in the midst of a federation of 5G-connected resources on the basis of smart contracts and Decentralized Identity (DID). Precisely, the "gaps" that this solution aims to fill comprehend trust, authentication, service reliability and data control. Lastly, the authors argue that thanks to cryptography and blockchain techniques, is it feasible to form a trusted identity federation between individuals and organizations or among organization themselves. In fact, once again, the decentralized, immutable, traceable and untamperable nature of blockchain on which DID relies on, enables data users to gain back data sovereignty paving the way for a future significant security-oriented redesign of networks and cloud infrastructures.

If on one hand the distributed nature of blockchain is something to leverage in order to ensure better security standards in a blockchain-based system, on the other hand another school of thought states that in a low-trust environment this could also provoke a scarce capacity to control a network increasing the chances of a successful 51% attack.

Therefore in order to meet those two school of thought halfway, Zhu et al. [26] proposed a controllable blockchain data management (CBDM) that making use of a Trust Authority (TA) node allowed users to terminate any potentially malicious action performed on-chain even during a 51% attack. The authors' vision is to incorporate this method, given its performance and security assessment, in a real-world context in the near future.

Returning to the perspective of Industry 4.0 [4] the usage of blockchain could give a crucial advancement to IoT devices for industrial use. This is mainly because there are still many threats to tackle such as interoperability troubles, security vulnerability, absence of trust among parties [29]. Moreover, by combining blockchain and IoT, the chances of data loss or damage can be potentially decreased. Some high-profile use cases of this beneficial combination can be noticed in IOTA, HYPR and XAGE [30].

Kirkman et al. [27] assess that most cloud systems maintain a reliable hardware infrastructure by being supported with attestations from a Trusted Third Party (TTP).
It follows that, to help ease the reliance on TTPs for data monitoring and policy assessment and storage, the study proposed to use blockchain technology. This decision was primarily made since the main goal was to improve and enhance cloud trust with the desire to finally give cloud customers tailored on-chain data movement policies that comprehended detailed insights and informations about how their data was being managed and processed to gain high credibility and decentralizing trust. In addition the proposed method's SLA includes service-level priorities and tiers that the customer and cloud supplier agreed upon.

Another blockchain-based and customer-oriented solution to deal with cloud users' security and trust necessities has been suggested by Singh et al. [28]. In particular, their solution aims to self-adapt according to the functional needs and consistency specs requests of each cloud customer. To make this possible, they exploited a self-adapting Monitor-Analyze-Plan-Execute over a bilateral Knowledge (MAPE-K) approach.

In this case the usage of blockchain made the cloud service benefit of the possibility to offer and guarantee trust, security, openness, privacy and transparency for its subscribers. Hence, all the subscribers could monitor the facilities or consult SLAs or other assets creating an environment with enhanced trust and reduced chances of threats, leaks or frauds.

Paper	Trust	Interoperability	Customer - Oriented	Reliability	Data Management	Performance
[24]	✓	✓		✓		
[26]	✓				✓	✓
[27]	✓		✓		✓	✓
[28]	✓		✓	✓	✓	

Table 4: Key points of trust papers

Keeping in mind this overall recent work and literature review about the different applications and proposed approaches of both blockchain and cloud computing to address data security issues and its sub-aspects like privacy, data integrity and trust, seems pretty evident that there is high interest in doing research, experiments and developments in those fields. Nevertheless, all those studies were just experimental and tested on relatively small-scale environments without any certified or documented real world professional use. Therefore, with a qualitative approach, in the following chapter this work aims to answer to the research question: “how can real-world firms benefit from implementing blockchain with cloud computing for better data security ?”.

3. Research Approach

In this chapter, the focus shifts on answering to the research question formulated in Chapter 2. Hence, real-world solutions and implementations combining the provisioning of blockchain alongside cloud services will be discussed, explored and analyzed in detail.

In addition, it is important to mention that this qualitative approach will mainly cover the security aspects of the following presented solutions for a matter of consistency with the previous chapter's aspects clustering and rationality towards the technologies at stake.

3.1 Blockchain-as-a-Service

The basic concept behind BaaS is that the blockchain network is managed as a service offering, on which customers are allowed to configure and customise their own blockchain settings according to their specific demands or needs, such as blockchain network types and smart contract rules. Therefore, after several practical assessments and evaluations it's considered the most suitable delivery mode for blockchain in industrial settings. Furthermore, BaaS has a great degree of appeal and attractiveness because providers can manage and develop the IT infrastructure, the network and the software to run it, meanwhile client businesses have the opportunity to experiment with blockchain apps and smart contracts. In other words, this blockchain-oriented service model helps companies focus on software development or the provision of other services to customers without managing, updating, and maintaining the platform that hosts the application. Many businesses consider highly valuable the flexibility of a potential BaaS solution. With this service model, companies can leverage the strong points of blockchain technologies (e.g., stronger data security, data provenance, privacy and trust) to work on a secure platform for B2B partnerships based on a high-performance cloud platform without carrying the burden of developing their own blockchain infrastructures, managing software updates or security patches, or investing in expensive in-house computing resources. [34] For the objective of this work the research will be focused on the services offered by major cloud providers such as AWS, IBM and Oracle.

The research will first describe the architecture and cloud deployment and then analyze the key security features of the selected BaaS services.

3.2 Amazon Web Services (AWS)

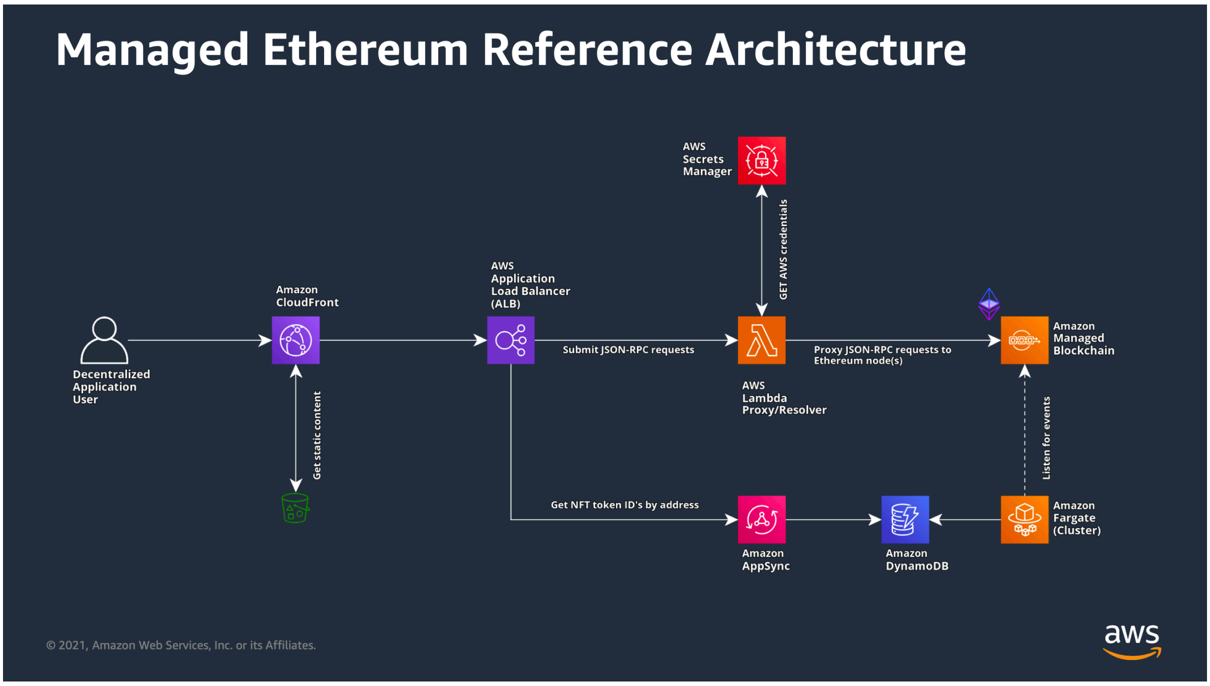
Amazon Web Services, in the second half of the first semester of 2019, added to its range of offered services a complete enterprise blockchain-oriented one. This new solution, called Amazon Managed Blockchain (AMB), is an entirely managed service which supports users in a smoother set-up and management of scalable blockchain networks. [38] AMB totally brings down to zero the overhead required to create the network, smart contract rules and security components, automatically scaling to meet the demands of transactions' volume of running applications. It also makes customers' blockchain network management and maintenance easier and more direct by reducing to the bare minimum the amount of steps required to perform every operation, without sacrificing security, clarity and completeness. Hence, managing certificates, adding new nodes in the network, running security controls and tracking operational performance metrics are just a few clicks away. Furthermore, AMB can fully recreate an immutable copy of blockchain network activity into a completely managed ledger database, the Amazon Quantum Ledger Database (QLDB).

This enables customers and enterprises to track relevant data and easily analyze external network activity and gain insights and valuable informations regarding trends. [39]

Architecture

Amazon Managed Blockchain allows customers in first place to choose between Ethereum and Hyperledger Fabric frameworks according to their preferences and needs and subsequently to add nodes and their permissions to the network meanwhile Amazon manages all the rest.

Ethereum is considered to be the preferable solution for users setting up highly distributed blockchain networks where transparency of data for all nodes is important. In addition, this product enables permissionless and non-stop applications that run autonomously without depending on private infrastructure and anyone can use. It also enables easy access to other data sources on the blockchain and the development of decentralized finance (DeFi). Alternatively, companies can also participate in a public Ethereum blockchain network where participants can be anonymous and aren't necessarily identified in advance.



Managed Ethereum Reference Architecture

AWS Secrets Manager
GET AWS credentials
Amazon CloudFront
AWS Application Load Balancer (ALB)
Decentralized Application User
Submit JSON-RPC requests
Proxy JSON-RPC requests to Ethereum node(s)
Amazon Managed Blockchain
AWS Lambda Proxy/Resolver
Get static content
Listen for events
Get NFT token ID's by address
Amazon AppSync
Amazon DynamoDB
Amazon Fargate (Cluster)
aws

Fig. 9: Amazon Managed Ethereum Blockchain Reference Architecture (2021)

Other features of Ethereum framework are the presence of dedicated Geth nodes managed by AWS, the provision of new nodes in minutes on the Ethereum mainnet, faster sync times, high availability through quick failover of faulty nodes and auto-scaling node storage.

Hyperledger Fabric is instead the optimal choice for customers developing applications that require stringent privacy and permission controls with a known-in-advance set of nodes. Hence, this solution tends to offer more advanced privacy features, with permissioned access meanwhile applications tend to be less decentralized than their public counterparts. It also supports higher transaction rates than are typically possible with public blockchains, therefore being a good option for enterprises that need the practical benefits of decentralization.

From Fig.10 can be assessed that the Amazon Hyperledger Fabric BaaS uses a component-based architecture. Its essential components include the Hyperledger fabric ordering service, members, each member fabric certificate authority (CA) and peer node, and Amazon Web Services (AWS) clients and apps.

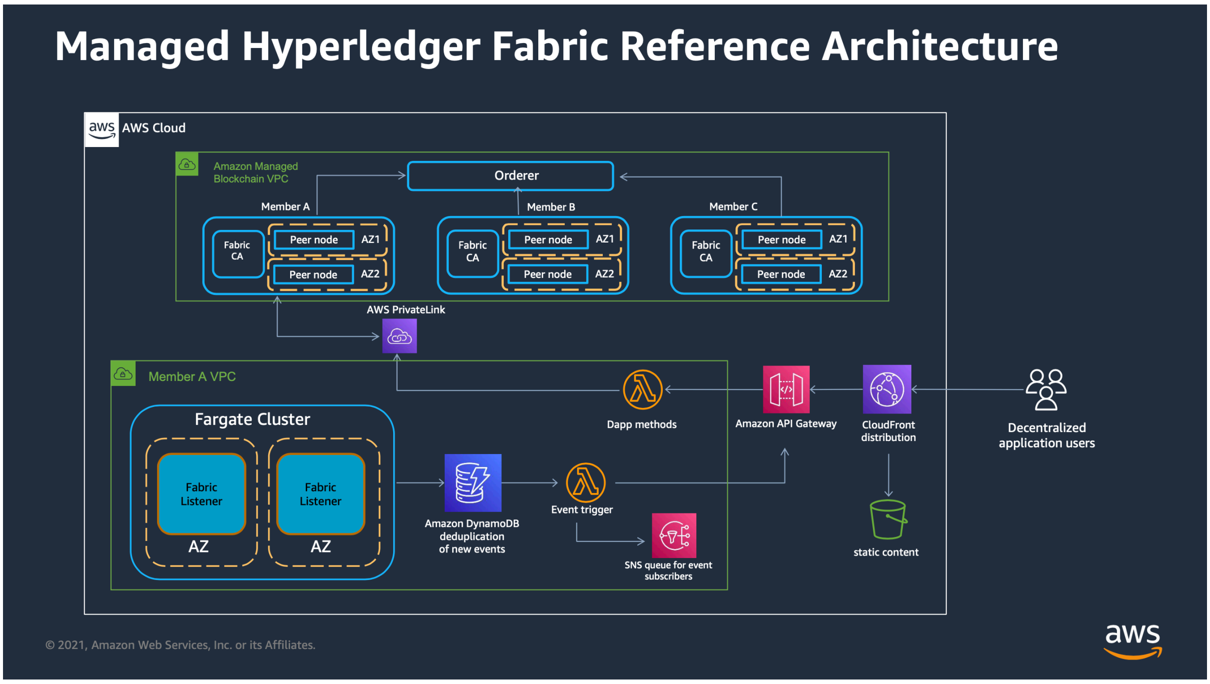

Managed Hyperledger Fabric Reference Architecture
AWS Cloud
Amazon Managed Blockchain VPC
Orderer
Member A
Member B
Member C
Fabric CA
Peer node
AZ1
AZ2
AWS PrivateLink
Member A VPC
Fargate Cluster
Fabric Listener
AZ
Amazon DynamoDB deduplication of new events
Event trigger
SNS queue for event subscribers
Dapp methods
Amazon API Gateway
CloudFront distribution
static content
Decentralized application users
© 2021, Amazon Web Services, Inc. or its Affiliates.
aws

Fig. 10: Amazon Managed Blockchain Hyperledger Fabric Reference Architecture (2021)

Cloud Implementation

Amazon Managed Blockchain operates on Amazon Web Services Cloud, enabling its users to deploy blockchain-based applications using Hyperledger Fabric open source framework or Ethereum, providing interoperability features with other products running on the same framework.

Security

For what concerns security, Amazon Managed Blockchain makes use of a technology named AWS Key Management Service (KMS) to secure Hyperledger Fabric's certificate authority, a component that manages user identities and issues enrolment certificates for securely communicating within the blockchain network. [42] It also relieves users from being concerned to set up their own security devices like hardware security modules (HSM) for this purpose. Among the security aspects it is important to mention the possibility of secure interaction among the customer's Hyperledger Fabric components managed by Amazon Managed Blockchain through Amazon VPC (Virtual Private Cloud) endpoints. Additionally, secure interaction is extended also with blockchain peer nodes from other members in the customer network through an Amazon VPC endpoint in order to endorse transactions.

Hyperledger Fabric’s default ordering service uses Apache Kafka to support the communication of transactions across the network. Even though Kafka meets the needs of providing a messaging platform that is able to deliver transactions in a sequential fashion across the network, it is not optimized to store a complete and comprehensive history of transactional data, making it very difficult to restore historical transactions in case of a failure. For this reason, AMB's ordering service is built using Amazon QLDB technology, which features an immutable change log capable of maintaining the complete history of all uncommitted transactions in the blockchain network, increasing the ordering service durability.

3.3 IBM

IBM Blockchain Platform is the IBM full-stack, managed BaaS offer that can be deployed in several environments according to user’s preferences including IBM Cloud and third-party clouds. No matter how demanding and dynamic its usage in regulated industries could be, the IBM Blockchain Platform aims to guarantee the highest standards of performance and security in any operation performed, from development and network set-up to its daily governance. Its easy-to-use interface results in an intuitive user experience that enables users to comfortably create a blockchain network, manage channels and smart contracts, add new nodes, customize governance policies and supervise identity credentials of network participants. [40]

Architecture

The IBM Blockchain Platform is built around the Linux Foundation’s Hyperledger Fabric.

It is able to offer the crucial elements for creating, managing, and expanding enterprise blockchain solutions without vendor lock-in by leveraging the modularity, performance, privacy, and scalability of Hyperledger Fabric and in turn building on top of important open-source and openly governed technologies. Fig. 11 outlines the three-layer architecture that put together the IBM Blockchain Platform. With a top-bottom approach is possible to describe the system’s architecture.

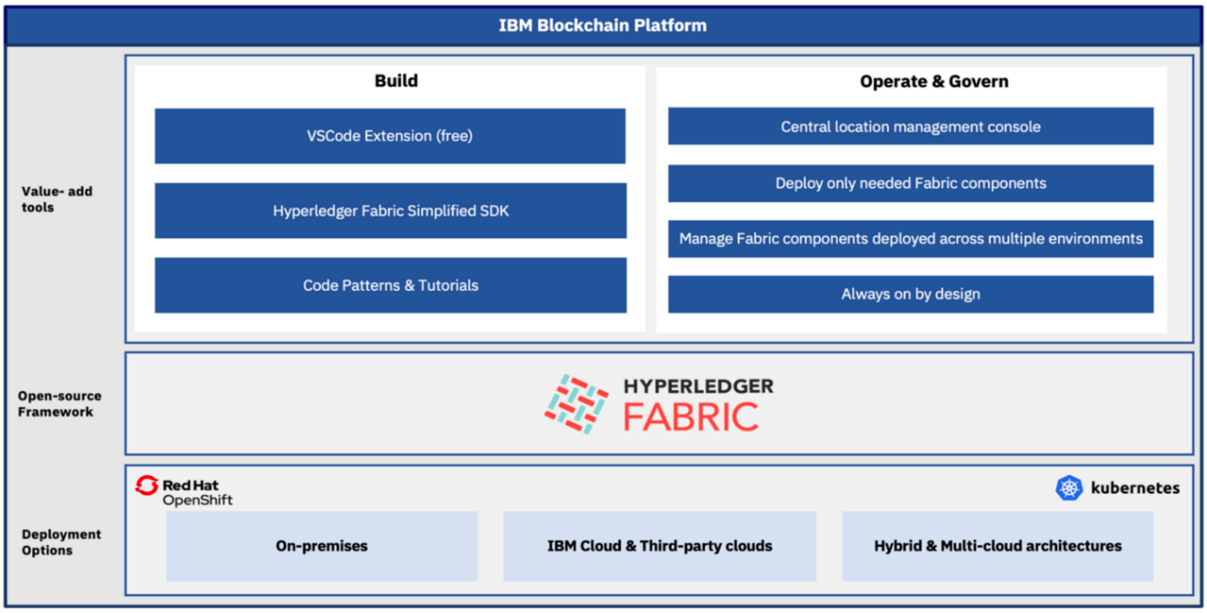

IBM Blockchain Platform
Value- add tools
Build
VSCode Extension (free)
Hyperledger Fabric Simplified SDK
Code Patterns & Tutorials
Operate & Govern
Central location management console
Deploy only needed Fabric components
Manage Fabric components deployed across multiple environments
Always on by design
Open-source Framework
HYPERLEDGER FABRIC
Deployment Options
Red Hat OpenShift
kubernetes
On-premises
IBM Cloud & Third-party clouds
Hybrid & Multi-cloud architectures

Fig. 11: IBM Blockchain Platform Architecture Overview (2022)

The top layer is where the Hyperledger Composer resides. This layer confers to the user the ability to implement value-adding tools in order to create and manage blockchain components and deploy solutions. It also provides the ability to create smart contracts just by providing a simple layer and business level abstraction to implement them rather than writing them from scratch. The middle layer is composed by the open-source Hyperledger Fabric framework and it is employed to create and administer the blockchain components based on Hyperledger Fabric. Moreover, in this layer there are three parts such as certificate authority, peer and ordering service.

Finally in the bottom layer, there are the cloud infrastructure's deployment options such on-premises, IBM Cloud, third-party clouds, hybrid and multi-cloud architectures that use Red Hat OpenShift and Kubernetes mainframes as the base of this layer to supply enhanced performance and a more secure platform environment. [31]

Cloud Implementation

According to the requirements of the ecosystem, clients can administer their peers and other Hyperledger Fabric components using a range of deployment methods through the IBM Blockchain Platform. The IBM BP enables network deployment on both public and private clouds, including IBM Cloud or public clouds from other companies.

Additionally, it has multi-cloud capabilities, which strengthen connections and facilitate interoperability across various businesses independent of infrastructure, enhancing the blockchain business ecosystem. Diving into details, IBM Blockchain Platform on IBM Cloud is based on a Kubernetes architecture which offers more control, security, flexibility, scalability and enhanced developer tools. It gives total control over customers' deployments and certificates thanks to a new user interface that can simplify and accelerate components' deploying process into IBM Cloud Kubernetes Service. Moreover clients can connect to nodes running in any environment (on-premises, public, hybrid clouds) and smoothly connect a single node to multiple industry networks.

For what concerns IBM Support for Hyperledger Fabric, it is important to underline that with this solution clients leverage the full IBM Blockchain Platform solution behind a firewall in their own private cloud or in third-party clouds of their choice. In addition, even though this is a support offering, it also grants access to the same set of certified images, operations console, and Kubernetes operator used in the aforementioned IBM Blockchain Platform on IBM Cloud. Hence, this provides consistent capability and familiar user experience across the two editions.

Security

Differently from permissionless networks, the IBM Blockchain Platform security settings are not based on trust through anonymity.

Thus, nodes participating to business networks must be known ex-ante to the network, in order to estasblish distributed trust amongst a known set of business network nodes. From time to time, regulatory requirements dictate certain information on participants and transactions in a network to be known. Since businesses dealing with sensitive and highly valuable data pretend full confidence that both their transaction data and the transactions themselves are confidential, IBM Blockchain Platform enables stronger security and privacy via three key mechanisms: channels, private-data database, and zero-knowledge proof technologies. Channels are used when data doesn't need to be shared with the entire network. The private-data database is operated simultaneously to the ledger to store private data that may be referenced, securing its privacy. Finally, zero-knowledge proof technologies enable a party who possesses private information to prove to another party that the information satisfies a certain set of properties without revealing the information.

Any blockchain framework's security, scalability, and maturity depend on how well its consensus protocol has been developed and implemented. As was already noted, Hyperledger Fabric's consensus system is set up to let users select the consensus protocol that would work best for their particular business network's requirements. As a result, Hyperledger fabric has emerged as the industry-leading protocol and framework for corporate blockchain networks thanks to open governance of the code base with a distinct purpose.

3.4 Oracle

The Oracle Blockchain Platform (OBP) was introduced to the public in the second half of 2018. The pre-assembled, full, and production-ready OBP gives its users everything they need to build a reliable and secure blockchain network. The Hyperledger Fabric architecture serves as its foundation. It also is a secure, resilient, and scalable platform with continuous monitoring, automated recovery of all network components, and constant replication of configuration changes that is intended for continuous operation. It can be integrated with other Oracle Cloud Platform services, third-party apps, Oracle SaaS, and other blockchain networks. This makes it simple for users to integrate distributed ledgers and smart contracts into a wider corporate process or workflow. Following the initial setup of an OBP instance, clients can expand the blockchain network by including more participants running suitable Hyperledger Fabric releases outside of Oracle Cloud or their own OBP instances. [37]

Architecture

OCI's Blockchain Platform is based on the open source Hyperledger Fabric project from the Linux Foundation, and boasting a number of performance, security and scalability enhancements enables users to easily establish a managed, preassembled blockchain network. It offers a distributed ledger that can only be appended and is shared among a network of nodes and businesses. By doing so, intermediaries are eliminated, complex point-to-point dataflows are replaced, and trusted transactions and a common source of truth are produced. Additionally, Oracle Blockchain Platform's Autonomous Data Warehouse (ADW) can stream transaction history updates, and Oracle Analytics Cloud can deliver robust dashboards, visualizations, and reports.

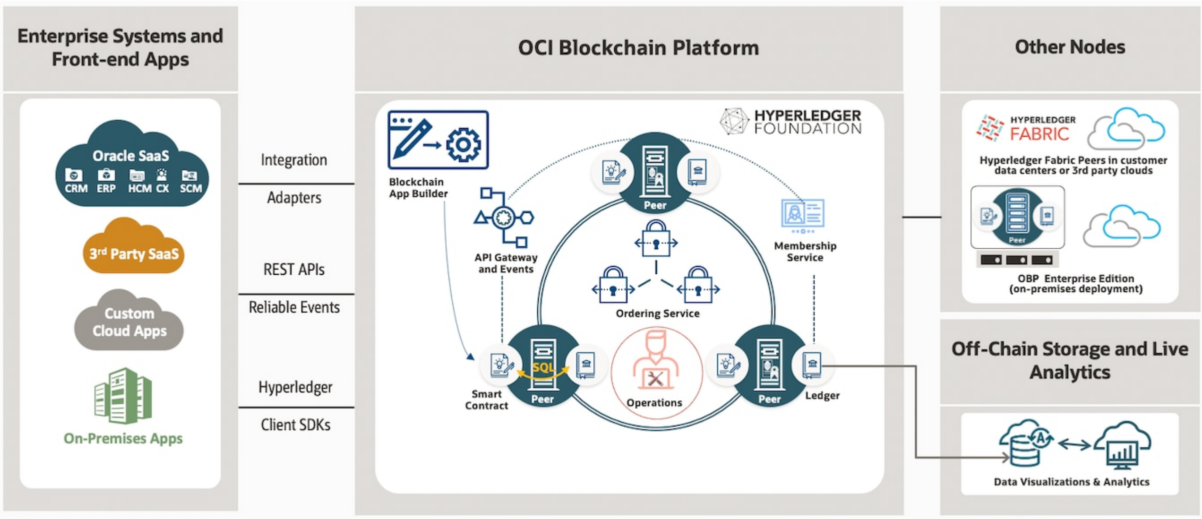


Fig. 12: Oracle Cloud Infrastructure Blockchain Platform Architecture (2022)

Oracle Blockchain Platform manages membership as a permissioned blockchain and connects with Oracle Identity Management to offer role-based access authorizations.

It features an operations console that offers full lifecycle management for smart contracts and gives administrative users access to appealing web UIs and potent REST APIs for updating configurations, adding members, and creating channels and rules. Its architecture is divided into four main components such as the enterprise systems and front-end apps, the OCI Blockchain Platform, other blockchain nodes and containers and finally data services off-chain storage and live analytics.

Furthermore, blockchain peer nodes are able to run business logic that is encoded in smart contracts as business terms, validation criteria, and events meanwhile for multiparty endorsements, they digitally sign the findings using their organization's Public Key Infrastructure (PKI) certificates. [43]

Cloud Implementation

For clients and developers who want to create their own solutions, Oracle offers both on-premises and cloud-based solutions. Precisely, the most relevant offered solutions are a Platform for cloud-based BaaS, which can run on Oracle Cloud and join a multicloud blockchain network by connecting with external nodes and an on-premises blockchain platform, which enables users to set up networks outside of Oracle Cloud or hybrid networks with both on-premises and cloud nodes.

Additionally, always built on the Oracle Blockchain Platform, other services offered include the Intelligent Track and Trace SaaS application which is a ready-to-use SCM tool for corporate users and Oracle Database Blockchain Tables, which provide insert-only tables with hash-linked rows and optional user signatures to give the tamper-evident storage properties of blockchain.

Security

The SKUs offered for Oracle Blockchain Platform are Standard and Enterprise.

By automatically duplicating its components across Oracle Cloud's three Availability Domains or Fault Domains, the latter offers high availability. In addition by raising the resources now allotted to the nodes, adding more OBP nodes, or scaling out by adding more VMs to host more nodes, it also offers dynamic scalability to manage changing workloads. Dynamic scalability has been added to Oracle Blockchain Platform to improve compatibility with changing workloads. Customers may now dynamically scale out and scale up their setups. [44]

Within a permissioned blockchain network with enrolled members, all businesses use certificates for their identities and exchange digitally signed messages to guarantee security and data integrity. Any access at the network or storage level outside of the blockchain containers is prevented by built-in encryption. Oracle Identity Cloud Service (IDCS) handles user authentication for the console and REST APIs in the cloud. TLS is used to enforce data encryption in transit for all transactions, and Oracle Cloud Block storage offers data encryption at rest.

Additional comprehensive Oracle Cloud security measures include network resilience, availability, geo-redundancy and fully isolated compute environments that separate the execution of customer chaincode (for instance) and Oracle's platform code. In its most recent release, OBP includes fine-grained on-chain access management inside the blockchain in alongside the support for Private Data Collections. The ability to manage and validate on-chain Access Control Lists (ACLs) for rights to access and use any ledger data or smart contract operations is provided to chaincode writers as a result. [45]

3.5 Key Differences Among BaaS Providers

After analyzing the BaaS solutions offered by major providers, it’s useful to highlight the main differences that characterize and differentiate each offer on the market.

First of all, because AWS already has an established cloud infrastructure it is in a better position than other providers and its the only provider to support the Ethereum blockchain.

As an alternative, increased use of local databases (on-premise) will increase reliance on IBM and Oracle services which in turn have already put up their reputation as major blockchain service providers in the market working with a wide range of diverse customers and by boasting an increasing number of enterprise implementations. However, it must be taken in consideration that geographical coverage remains a key complication because interoperability features are constrained to USA-usage only. As geographic coverage expands, opportunities for businesses whose networks cross many geographies will increase. The blockchain benefits of the interoperability relationship are currently limited to single sign-on features, at least for consumers in Europe. Comparatively to Oracle, IBM provides additional cloud alternatives, including deployment using its own public cloud infrastructure, containerization on private clouds or deployment on public clouds from other providers. This links its methodology more closely to the blockchain platform than to the cloud provider (relying on IBM Blockchain Platform to provide the differentiation). For solutions created using the IBM Blockchain Platform, this strategy is more appealing. Furthermore it must be reckoned that every vendor provides extremely secure and scalable solutions, marking the potential added value of business usage of this cutting-edge service.

	Supported Blockchain Architectures	Cloud Implementation	Security	Peculiar Features
AWS	• Hyperledger • Ethereum	• AWS Cloud	• AWS Private Key Management • Amazon Virtual Private Cloud • Amazon QLDB	• Growing inter-framework exchange
IBM	• Ethereum	• IBM Cloud • On-Premises, Third-party private and public • Hybrid Cloud • Multi-Cloud	• Private-data DB • ZKP Technology • SecureKey Tech	• Broad cloud implementation handling • Interoperability
Oracle	• Ethereum	• Oracle Cloud • On-Premises, Third-party private and public • Hybrid Cloud • Multi-Cloud	• Digitally signed messages • Identity Cloud Service • Network resilience • Fine-grained on-chain access management	• Crosswise industry coverage • Interoperability

Table 5: Summary of Analyzed BaaS Providers

4. Conclusions

This work with a qualitative approach aimed to ultimately foster decisional support for privacy-preserving oriented IT managers who are looking for new services and solutions capable of implementing blockchain to enhance cloud data security. It is important to mention that the analysis discussed in Chapter 3 to discuss, compare and contrast the major Blockchain-as-a-Service providers has been limited by the fact that it has been performed only on promotional material retrieved on the respective providers' websites and therefore is not comprehensive of highly detailed or in-depth informations about each service offered.

Nonetheless, this thesis work has permitted to discover that the adaptability of a BaaS solution is quite important for many enterprises. Businesses may benefit from blockchain technologies without having to create their own blockchain infrastructures, manage software upgrades or security patches, or spend money on pricey in-house computing resources and is a good way for developers to make original applications without having to build, maintain, and update their own hardware and software.

Furthermore, BaaS are gaining popularity and business-oriented adoption due to its speedy and cost-effective nature and the number of market participants offering their blockchain cloud solutions has increased competition. Since there is no dominant vendor on the market and each has unique characteristics, client relationships, and features, it is critical to consider how to jointly work on interoperable and multi-cloud solutions with direct competitors to offer flexible customer-facing solutions to get over some "lock in" features that may present challenges for customers.

Finally, the potential industries and use cases covered by BaaS solutions should increase as blockchain becomes more well-known and widely used. The future development of wide industry and use-case coverage in sectors like telecommunications, media, and energy, which are exhibiting sweet spots, is essential because there are also significant prospects in other businesses that leaves space to future research.

5. Bibliography

1. del Castillo, M. (2020). Blockchain 50. [online] Forbes. Available at: https://www.forbes.com/sites/michaeldelcastillo/2020/02/19/blockchain-50/

2. Gong, J., Nima and Navimipour, J. (2021). An in-depth and systematic literature review on the blockchain-based approaches for cloud computing. Springer. doi:10.1007/s10586-021-03412-2

3. Joshi, S., Pise, A.A., Shrivastava, M., Revathy, C., Kumar, H., Alsetoohy, O. and Akwafo, R. (2022). Adoption of Blockchain Technology for Privacy and Security in the Context of Industry 4.0. Wireless Communications and Mobile Computing, [online] 2022, p.e4079781. doi:10.1155/2022/4079781

4. Park, J. and Park, J. (2017). Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions. Symmetry, 9(8), p.164. doi:10.3390/sym9080164

5. Shah, K., Patel, N., Thakkar, J. and Patel, C. (2022). Exploring applications of blockchain technology for Industry 4.0. Materials Today: Proceedings, 62, pp.7238–7242. doi:10.1016/j.matpr.2022.03.681

6. Gai, K., et al. (2020). Blockchain meets cloud computing: a survey. IEEE Commun. Surv. Tutor. 22(3), 2009–2030

7. Heidari, A., Navimipour, (2021). J.N.: A new SLA-aware method for discovering the cloud services using an improved nature-inspired optimization algorithm. PeerJ Comput. Sci

8. Raimundo, R.J. and Rosário, A.T. (2022). Cybersecurity in the Internet of Things in Industrial Management. Applied Sciences, 12(3), p.1598. doi:10.3390/app12031598

9. Sharma, P., Jindal, R. and Borah, M.D. (2022). Blockchain-based cloud storage system with CP-ABE-based access control and revocation process. The Journal of Supercomputing, 78(6), pp.7700–7728. doi:10.1007/s11227-021-04179-4

10. Pon, P. and V, K. (2021). Blockchain based cloud service security architecture with distributed machine learning for smart device traffic record transaction. Concurrency and Computation: Practice and Experience, 34(3). doi:10.1002/cpe.6583

11. Foster, D.; White, L.; Erdil, D.C.; Adams, J.; Argüelles, A.; Hainey, B.; Hyman, H.; Lewis, G.; Nazir, S.; Nguyen, V.; et al. (2019). Toward a cloud computing learning community. In ITiCSE-WGR '19, Proceedings of the Annual Conference on Innovation and Technology in Computer Science Education, Aberdeen, UK, 15–17 July 2019; ACM: New York, NY, USA; pp. 143–155

12. Khan, K.M., Malluhi, Q. (2010) : Establishing trust in cloud computing. IT Prof. 12(5), 20–27

13. Casino, F., Dasaklis, T.K. and Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics, [online] 36(36), pp.55–81. doi:10.1016/j.tele.2018.11.006

14. El Azzaoui, A., Kumar Sharma, P. and Park, J. (2022). Blockchain-based delegated Quantum Cloud architecture for medical big data security. Journal of Network and Computer Applications, 198, p.103304. doi:10.1016/j.jnca.2021.103304

15. Li, R., et al. (2019) : Trust Mechanism of cloud manufacturing service platform based on blockchain. In: 2019 11th International Con-ference on Intelligent Human-Machine Systems and Cybernetics (IHMSC)

16. Liang, X., et al. (2017) : ProvChain: a blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. In: 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID)

17. Alkadi, O., et al. (2020) : A deep blockchain framework-enabled collaborative intrusion detection for protecting iot and cloud networks

18. Jyoti, A. and Chauhan (2022). A blockchain and smart contract-based data provenance collection and storing in cloud environment. Springer. doi:10.1007/s11276-022-02924

19. Zhou, Z., Luo, X., Bai, Y., Wang, X., Liu, F., Liu, G. and Xu, Y. (2022). A Scalable Blockchain-Based Integrity Verification Scheme. Wireless Communications and Mobile Computing, 2022, pp.1–13. doi:10.1155/2022/7830508

20. David Raju, K., Vijay Kumar, K., Rahul Showry, K.A. and Lohit Krishn, B. (2018). Techniques of Providing Data Integrity in Cloud Computing. International Journal of Engineering & Technology, 7(1.1), p.223. doi:10.14419/ijet.v7i1.1.9471

21. Sun, Y., Zhang, J., Xiong, Y. and Zhu, G. (2014). Data Security and Privacy in Cloud Computing. International Journal of Distributed Sensor Networks, [online] 10(7), p.190903. doi:10.1155/2014/190903

22. Huang, P., et al. (2020): A collaborative auditing blockchain for trust- worthy data integrity in cloud storage system. IEEE Access 8, 94780–94794

23. Witanto, E.N.; Oktian, Y.E.; Lee, S.-G. (2022). Toward Data Integrity Architecture for Cloud-Based AI Systems. Symmetry, 14, 273. https://doi.org/10.3390/ sym14020273

24. Rong, C., Geng, J., Hacker, T., Bryhni, H. and Jaatun, M., (2022). OpenIaC: open infrastructure as code - the network is my computer. Journal of Cloud Computing, 11(1). doi:10.1186/s13677-022-00285-7

25. N. Mohamed, J. Al-Jaroodi. (2019). Applying blockchain in industry 4.0 applications, in: 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), doi:10.1109/ccwc.2019.8666558

26. Zhu, L., et al. (2019) : Controllable and trustworthy blockchain-based cloud data management. Futur. Gener. Comput. Syst. 91, 527–535

27. Kirkman, S., Newman, R. (2018) : A cloud data movement policy architecture based on smart contracts and the ethereum block- chain. In: 2018 IEEE International Conference on Cloud Engineering (IC2E)

28. Singh, I., Lee, S.-W. (2017) : Comparative requirements analysis for the feasibility of blockchain for secure cloud. In: Asia Pacific Requirements Engeneering Conference. Springer

29. Q. Wang, X. Zhu, Y. Ni, L. Gu, H. Zhu. (2020) Blockchain for the IoT and industrial IoT: a review, Internet of Things. 100081

30. Blockchain Technology Use Cases You Should Know in 2021 | upGrad blog. (2021). from https://www.upgrad.com/blog/ blockchain-technology-use-cases/

31. Song, J., Zhang, P., Alkubati, M., Bao, Y. and Yu, G. (2022). Research Advances on blockchain-as-a-service: architectures, Applications and Challenges. Digital Communications and Networks, 8(4), pp.466–475. doi:10.1016/j.dcan.2021.02.001

32. Li, D., Deng, L., Cai, Z. and Souri, A. (2020). Blockchain as a Service Models in the Internet of Things management: Systematic Review. Transactions on Emerging Telecommunications Technologies, 33(4). doi:10.1002/ett.4139

33. Gai, K., Guo, J., Zhu, L. and Yu, S. (2020). Blockchain Meets Cloud Computing: a Survey. IEEE Communications Surveys & Tutorials, 22(3), pp.2009–2030. doi:10.1109/comst.2020.2989392

34. Croce, C. and Dragov, R. (2020). Blockchain Platform as a Service Getting Traction in Europe: A Deep Dive on Leading BPaaS Players. IDC

35. Alshurafa, S., Eleyan, D. and Eleyan, A. (2021). A Survey Paper on Blockchain as a Service Platforms Customer Satisfaction and Awareness. International Journal of High Performance Computing and Networking. doi:10.1504/IJHPCN.2021.120739

36. Onik, M.M.H. and Miraz, M.H. (2019). Performance Analytical Comparison of Blockchain-as-a-Service (BaaS) Platforms. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, pp.3–18. doi:10.1007/978-3-030-23943-5_1

37. Price, K. (2020). Oracle® Database Using Oracle Blockchain Platform. Oracle Corporation

38. Colyer, F. (2021). Amazon Managed Blockchain: experimentation and adoption. Amazon Web Services, Inc.

39. Whitepaper, A. (2022). Overview of Amazon Web Services. Amazon Web Services, Inc.

40. IBM (2022). IBM Blockchain Platform Technical Overview. IBM Corporation

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

42. Amazon Web Services (2022). Amazon Managed Blockchain Features. [online] Amazon Web Services, Inc. Available at: https://aws.amazon.com/managed-blockchain/features/

43. Oracle Cloud Infrastructure (2022). Managed Enterprise Blockchain Service. [online] Oracle.com. Available at: https://www.oracle.com/blockchain/cloud-platform/

44. Hall, M. (2022). Announcing the Next Generation of Oracle Blockchain Platform Cloud Service. [online] Oracle.com. Available at: https://blogs.oracle.com/blockchain/post/announcing-the-next-generation-of-oracle-blockchain-platform-cloud-service

45. Limited, I.T. (2020). Making blockchain easier: Oracle Blockchain Platform Generation 2 Cloud release. [online] Available at: https://www.oracle.com/a/ocom/docs/corporate/analystrelations/independent-thought-oracle-blockchain.pdf

46. Check Point Software Technologies Ltd. (2022). The Biggest Cloud Security Challenges in 2022. [online] Check Point Software. Available at: https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/the-biggest-cloud-security-challenges-in-2022/

47. CheckPoint (2021). Top Cloud Security Issues, Threats and Concerns. [online] Check Point Software. Available at: https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns/

48. International, D. (2022). Blockchain, security and the public cloud. [online] DoiT International. Available at: https://www.doit.com/blockchain-security-and-the-public-cloud/

49. TechRepublic (2022). The Current State and Predictions for the Future of Blockchain in the Enterprise. [online] TechRepublic. Available at: https://www.techrepublic.com/resource-library/whitepapers/research-the-current-state-and-predictions-for-the-future-of-blockchain-in-the-enterprise/

50. Cloud Security Alliance (2022). Top Threats to Cloud Computing Pandemic Eleven | CSA. [online] cloudsecurityalliance.org. Available at: https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-pandemic-eleven/