

Distributed Application Provisioning over Ethereum based private and permissioned Blockchain: Availability modeling, capacity, and costs planning

Carlos Melo, Jamilson Dantas, Paulo Pereira and Paulo Maciel

Received: date / Accepted: date

Abstract Blockchain and Cloud Computing are two of the main topics related to the distributed computing paradigm, and in the last decade, they have seen exponential growth in their adoption. Cloud computing has long been established as the main mechanism to test, develop, and deliver new applications and services in a distributed manner across the World Wide Web. Large data centers host many services and store petabytes of user data. Infrastructure and services owners rule the access to data and may even be able to change contents and attest to its veracity. Blockchain is a step towards a future where the user's data are considered safer, besides being public. Advances in blockchain-based technologies, now, support service provisioning over permissioned and private infrastructures. Therefore, organizations or groups of individuals may share information, service even if they do not trust each other, besides supporting infrastructure management tasks. This paper presents and evaluates models for assessing the availability and capacity-oriented availability of cloud computing infrastructures. It aims at running Blockchain's distributed applications based on the Ethereum blockchain platform and the required expenses to perform service delivery in public and private infrastructures. Most of the obtained results also apply to other blockchains based platforms.

Keywords System's availability · Capacity-oriented Availability · Blockchain · distributed application · Ethereum · cloud computing · cost evaluation.

1 Introduction

Most of the blockchain-based applications try to solve trust problems related to data's privacy, ownership, and control, which are often in possession of a single

Carlos Melo, Jamilson Dantas, Paulo Pereira, and Paulo Maciel
Centro de Informática, Universidade Federal de Pernambuco, Recife, Brazil
Tel.: +55-87-999265912
E-mail: casm3,jrd,prps,prrm@cin.ufpe.br

entity or a group of entities that run massive data centers or that own and manage a respective service, whether this is a social network or even a banking system [34]. Usually, those entities may modify and certify the authenticity of the altered data; also, they can charge high fees for the carried transactions, which goes against what is proposed by blockchain platforms [41].

Besides Blockchain, cloud computing has emerged as one of the leading technologies associated with the distributed computing paradigm, being a direct result of the virtualization technology evolution [38]. Due to virtualization, data centers possess a mechanism to test, refine and develop applications by reducing idle resources, increasing the profit margin, and optimizing resource sharing by hosting and providing any service (infrastructure, software, and platform) over the Internet [21].

Anyone may contract and offer services over cloud computing environments, this on-demand delivery of IT resources can be done via the Internet with pay-as-you-go pricing mechanism, always concerning a Service Level Agreement (SLA), where acceptable rates of availability and performance are established between both environment provider and client or application provider[1]. Besides contracting the cloud computing environments from well-known providers, such as Google Cloud, Amazon AWS and Microsoft Azure, one could deploy their private infrastructure, improving the security and control over the environment, reducing expenses by doing it with free and open-source software, such as Docker and OpenStack.

Blockchain and cloud computing will promote the concept of distributed cloud, which is characterized by adding new values and responsibilities to service users [30]. Therefore, users should be able to use and host distributed services, without the need for large data centers or the information control by large institutions, as well as deploying their own private infrastructure. However, a transition period is required to identify the feasibility of this paradigm, at first we need at least a platform that can be executed either on computer servers or mobile devices, as well as an established pattern to run distributed applications.

The Ethereum platform improved the support for the rapid development of distributed applications by providing a native programming language (Solidity) [6]. Docker container engine has become a community standard for distributed services provision across large and distributed data centers [12].

Ethereum and Docker are stable technologies; each one is present in the daily lives of many persons around the world. However, combining both blockchain platforms and virtualization technology is still in its early steps. Despite that, works have been done to evaluate essential metrics associated with service provisioning, such as the system's availability [2,32], performance [34,31] and capacity-oriented availability [25,36]. Most of them focus only on cloud computing architectures, services, and distributed applications, other ones focused on blockchain platforms. However, as for the best of our knowledge, the present paper is the first one to evaluate the availability and assess the impact of the failures and repairs routines over the capacity planning of blockchain platforms.

As the contribution of this paper, we can list:

- Availability models for blockchain provisioning over cloud computing and virtualized environments managed by Docker;
- Sensitivity analysis evaluation to detect bottlenecks in service provisioning;
- Capacity-oriented availability planning for service provisioning over architectures with a large amount of blockchain computing nodes;
- Cost evaluation and comparison between public and private cloud computing environments on blockchain-as-a-service provisioning.

The remained of this paper is organized as follows. Section 2 presents the works that underlie this research. Already Section 3 shows the background. While the Section 4 presents the support methodology that enable the proposed models construction, as presented in Section 5. Section 6 provides the studies used to demonstrate how feasible are the proposed models. Finally, Section 7 presents the final remarks and future works.

2 Related Works

Over the last few years, authors have devoted their efforts to study and evaluate performance and dependability attributes related to blockchain and cloud computing technologies, in this section, we present some of these remarkable works. To the best of our knowledge, these are the closest related works to what is proposed by the current paper.

Previously in Melo et al., [24,23], we have evaluated a blockchain-as-a-service infrastructure considering Dynamical Reliability Block Diagrams (DRBD) and a set of architectures containing the minimum requirements to deploy a Hyperledger platform over a virtualized environment managed by docker and OpenStack cloud computing platform. The current work is an extension of these two, and are the closest to what is proposed here, which evaluates the availability, capacity-oriented availability, and deployment expenses of an Ethereum private environment. Also, the proposed models here are hierarchically distributed, both Reliability Block Diagrams (RBDs) and Stochastic Petri Nets (SPN) are used in order to represent priority repairs between the nodes on Ethereum environment, we have also used analytical models provided from RBD's K-out-of-N (KooN) blocks to calculate the capacity-oriented availability [16,18].

Pongnumkul et al. 2017 [31] proposed a performance evaluation methodology for blockchain environments, and evaluated the Ethereum and Hyperledger Fabric platforms. The authors concluded that the Hyperledger Fabric has a large throughput and lower latency than Ethereum, which is a clear result of the consensus protocol. Ethereum uses Proof-of-Work (PoW), while the Hyperledger Fabric worked with the Practical Byzantine Fault Tolerance (PBFT) protocol, but now the current versions of the Hyperledger Fabric platform work with Kafka.

Zhang et al., 2018 [40] proposed a method to predict the performance of blockchain environments based on analytical modeling; they used the Ethereum

platform to demonstrate the feasibility of the proposed methodology. The associated metrics evaluated were transactions per second, and the storage space required to store the performed transactions.

In Sukhwani et al., 2017 [34], the authors investigated whether a consensus process using the PBFT mechanism could be a performance bottleneck through Stochastic Reward Nets (SRN) modeling to compute the meantime to complete the consensus process. The PBFT protocol is one of the most used by blockchain platforms. The focus of the current paper is on the availability evaluation of the Ethereum platform.

Later, in Sukhwani et al., 2018 [35], the authors evaluated the performance of Hyperledger Fabric through SRN models, which means that this works the entire platform performance, not only the consensus protocol. Once again, the proposed work differs from ours in the platform and the evaluated metrics.

In Weber et al., 2017 [39], the authors identified some availability limitations of two blockchains, Ethereum and Bitcoin, by measuring and gathering public data. We emphasized the evaluation of an Ethereum private blockchain availability, as well as the current acquisition and maintenance expenses, and the capacity-oriented availability, by proposing and evaluating the availability and capacity-oriented availability models.

Roehrs et al. 2019 [32], the authors proposed the omniPHR blockchain platform, focused on securely sharing personal health information. The authors evaluated through mathematical models and measurement the availability and performance of the proposed platform, considering besides the overall system's availability a set of performance metrics such as transactions per second, CPU utilization, memory, and network utilization.

Aniello et al. 2017 [2] have also proposed a new blockchain platform and evaluated scalability, availability, security, and performance metrics such as transactions per second and response time by considering this platform as an alternative for the traditional distributed database.

In Li et al., 2018 [14], the authors proposed a markovian process to express the relationship between the transaction arrival rate and the server capacity. While in [36] the authors proposed models to evaluate capacity-oriented availability (COA) of general cloud computing environments by considering Virtual Machines as their resources, considering failure and repair routines and their impact over the metric.

As could be seen from previously presented studies, most of the work accomplished focused on performance metrics. At the same time, in the proposed paper, we consider availability models and COA's evaluation, as well as the expenses related to service provisioning in both public and private environments, considering docker containers and compute nodes as resources and performing a sensitivity analysis to detect bottlenecks and the components with the highest impact over the availability metric.

3 Background

This section presents the fundamental concepts about availability evaluation, system modeling, blockchain provisioning, and the Docker engine, which is a community pattern to provide containers.

3.1 Availability Evaluation

Dependability is the ability of a computer system to deliver a service that can be justifiably trusted [4]. This definition considers user perception and system behavior. Evaluating the dependability of a system is usually the result of evaluating at least one of its five attributes: reliability, availability, maintainability, integrity, and safety [5].

The system's instantaneous availability, is the probability that the system is operational at a time t . That is, $A(t) = P\{Z(t)\} = E\{Z(t)\}$, $t \geq 0$, where $Z(t) = 1$ when the system is operational, and $Z(t) = 0$, otherwise, as shown in Figure 1.

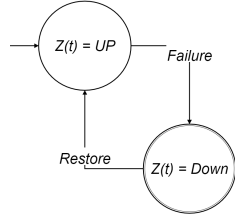


Fig. 1: System's States

The Steady-state availability, which is the one evaluated by this paper and is also called the long-run availability, is the limit of the availability function as time tends to infinity (Equation 1).

$$A = \lim_{t \rightarrow \infty} A(t), t \geq 0 \quad (1)$$

Also, the system's availability may be represented by a ratio between the Mean Time To Failure (MTTF) and Mean Time To Repair (MTTR) of the system (Equation 2).

$$A = \frac{\text{MTTF}}{\text{MTTF} + \text{MTTR}} \quad (2)$$

The MTTF for a system may be computed from Equation 3, where $\mathbf{R}(\mathbf{t})$ is the reliability of that system as a function of elapsed time. The Equation 4 provides a way of computing the MTTR from the values of MTTF, availability (A), and unavailability ($UA = 1 - A$).

$$\text{MTTF} = \int_0^{\infty} R(t) \partial t \quad (3)$$

$$\text{MTTR} = \text{MTTF} \times \left(\frac{UA}{A} \right), \quad (4)$$

As expected, the system's unavailability is the counterpart of the system's availability and can be calculated by $1 - A$. Already the system's downtime, which corresponds to the period where the system is not available, is usually given in units of time, such as in hours per year, in a way that relates time and probability: *Unavailability* $\times 8760h$.

The availability can also be represented by the number of nines [29], as shown in Table 1. For example, a system with four 9's of availability is classified as fault-tolerant, meaning an annual downtime of nearly 1 hour.

Table 1: Service availability in number of nines.

# of 9's	Avail. (%)	System Type	Downtime (year)
1	90	unmanaged	5 weeks
2	99	managed	4 days
3	99.9	well managed	9 hours
4	99.99	fault tolerant	1 hour
5	99.999	high availability	5 minutes
6	99.9999	very high availability	30 seconds
7	99.99999	ultra availability	3 seconds

The system's availability of associated metrics and values usually can be evaluated through simulation, measurement, and analytical models. The latter was chosen due to the high-level system view provided, as well as their great flexibility in adapting parameters and achieving results faster compared to the other two evaluation techniques. Regarding analytical modeling, two main trends are highlighted:

- **Combinatorial or non-state-space** models capture conditions that make a system fail (or to be working) regarding structural relationships between the system's components [37];
- Already **State-space models** represent the system's behavior (failures and repair activities) by a set of states and the occurrence of events that can be expressed as rates or distribution functions. These models allow representing more complex relationships between the system's components than combinatorial models do [19].

Reliability Block Diagram (RBD) [16] and Fault Tree (FT) [17] are among the most prominent combinatorial modeling formalisms, whereas Petri Nets (PN), Continuous Time Markov Chain (CTMC) and Stochastic Automata Networks are well-known state-space modeling formalisms [16,10,37]. In this

paper, RBDs are used to describe the system part that does not present any dependency between components.

Petri Nets [27] is a family of formalism well suited for modeling several system types, including concurrency, synchronization, communication mechanisms, besides supporting deterministic and probabilistic delays. This paper adopts a particular extension of Petri nets, namely Stochastic Petri Nets (SPN) [26], which allows the association of stochastic delays to timed transitions using the exponential distribution. We present an SPN that is used to estimate the overall system's availability associated with a set of metrics such as the system's annual downtime for the blockchain-based application provisioning, this SPN receive input values extracted from an RBD and is used as an input for another RBD, used to estimate the availability of an extensive infrastructure as well as the capacity-oriented availability (COA).

3.2 Docker, Blockchain and Ethereum Platform

Docker is a set of related technologies that includes a container image format and a runtime library, which manages containers' life cycle through APIs and a command-line tool [3]. Docker is the actual pattern for container creation and management; this technology enables users and companies to virtualize their resources and the application only. The virtualized application uses the Kernel of the host operating system, which makes the container images a lot smaller than those from virtual machines managed by hypervisors and require an entire operating system virtualization to run the provided service as KVM and VirtualBox does. This paper evaluates the use of Docker containers running Ethereum blockchain images ¹ to perform a distributed service.

Blockchain technology was first introduced by Satoshi Nakamoto, back in 2008 [28], on the same paper, what later would become just an application of Blockchain was entitled as Bitcoin, an electronic and monetary payment system capable of preventing double expend, as well as a decentralized application, where computational power was the key to keeping data away from malicious users. In 2013, Vitalik Buterin proposed the Ethereum blockchain [6], the first blockchain platform to include a complete program language known as Solidity, and the possibility to develop a distributed application (Dapp) that could be maintained by both users and service providers. The Ethereum platform was the first platform that changes the way that we see blockchain technologies; today, Blockchain is not only a payment system but a distributed platform ready to host any kind of distributed service.

The Ethereum platform is portable, such as the Java computing Language, where the developed applications may run in any environment due to the Java Virtual Machine (JVM). The Ethereum distributed applications (Dapps), which are written in Solidity, runs over the Ethereum Virtual Machine (EVM).

Already an Ethereum node is the client that enables one to participate in an Ethereum network, and many Ethereum clients can turn a device into an

¹ Ethereum: <https://hub.docker.com/u/ethereum>

Ethereum node. Some of the clients are provided by the Ethereum community, such as Geth and Trinity, while others are from third-party developers, which is the case of Parity.

The Ethereum platform can be provided as a cloud service. Blockchain-as-a-Service became a trend among those service providers and will be even more present in daily lives since banking services, and other distributed applications will migrate from traditional cloud models to a more safe and secure mechanism based on Blockchain.

By general means, a blockchain application is based on shared ledgers used to store transactions' records into entities called blocks, inserted one after another into a kind of linked list [11]. Each block, besides storing data about the performed transactions, also has a pointer to the immediately preceding block. Figure 2 shows how a typical blockchain works.

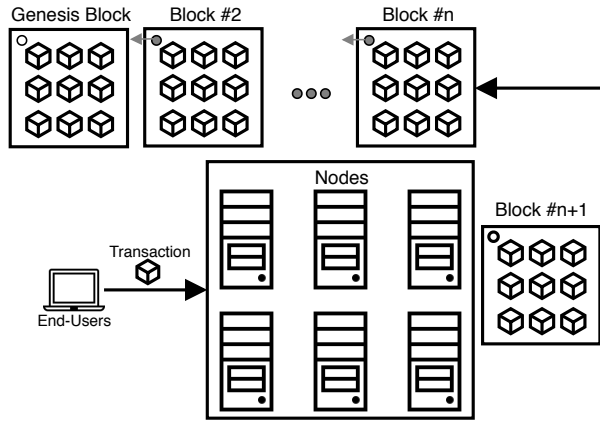


Fig. 2: How does Blockchain Works?

End-user requests to a peer-to-peer network composed primarily of conventional machines or dedicated servers, these machines receive the names of nodes in a P2P architecture and are responsible for executing, ordering, and validating the required transactions. Each transaction is inserted into a block with other transactions, and each block is inserted into what we call a blockchain.

3.3 Sensitivity Analysis

Sensitivity analysis is adopted to determine the most influential factors over a metric of interest [9]. In this paper, the percentage-difference sensitivity analysis technique is applied.

The percentage-difference sensitivity analysis technique is characterized by a sensitivity index known as $S_\theta(Y)$, which indicates the impact of a given measure known as Y for a parameter θ .

Equation 5 shows how the percentage difference index is calculated for a metric $Y(\theta)$, where $\max\{Y(\theta)\}$ and $\min\{Y(\theta)\}$ are the maximum and minimum output values, respectively, computed when varying the parameter θ over the range of its n possible values of interest. If $Y(\theta)$ is known to vary monotonically, only the extreme values of θ (i.e., θ_1 and θ_n) may be used to compute $\max\{Y(\theta)\}$; $\min\{Y(\theta)\}$, and subsequently $S_\theta(Y(\theta))$ [19].

$$S_\theta(Y) = \frac{\max\{Y(\theta)\} - \min\{Y(\theta)\}}{\max\{Y(\theta)\}} \quad (5)$$

Each $S_\theta(Y)$ is calculated by fixing the other parameters' values. The respective impact is computed for each input parameter, and then the most significant impact is found.

3.4 Capacity-oriented Availability (COA)

The assurance of resource availability, considering the occurrence of failures, is a significant challenge for planning a cloud computing infrastructure and services; the same applies to blockchain application. Many techniques have been employed to measure system availability based on the average capacity available - Capacity-oriented availability-(COA) [25] [20].

The COA assesses how the system is delivered, therefore, does not consider only states of availability or unavailability, but the real impact of these factors in service delivery. The COA calculation considers pc_i as the operational processing capacity or the number of available resources at any state s_i , while π_i describes the steady-state availability for the s_i state, a set of all available states is known as US state, also the maximum processing capacity of the system can be represented by MPC . Thus, we can calculate the capacity-oriented availability by solving Equation 6 [16]:

$$COA = \frac{\sum_{s_i \in US} pc_i \times \pi_i}{MPC} \quad (6)$$

4 Methodology

This section presents how we had accomplished our main goals and how this work can be replicated. At first, the required hardware and software resources are defined, as well as their expected behavior. The list of requirements apply to any computer system, including cloud platforms and their respective services, and corresponds to one of the steps of the system's understanding process [13].

The prerequisites to create a blockchain environment based on the Ethereum private platform image include any modern hardware running Linux, MacOSX, or Microsoft Windows 10 Operating System with support to Docker Engine 18+. The Docker Engine is responsible for creating and managing the Ethereum containers.

After listing our relevant requirements and understand how they interact with each other, we may determine a way to evaluate the system, which includes a path to obtain the needed information about it [13]. The Figure 3 shows an organization chart that summarizes our strategy.

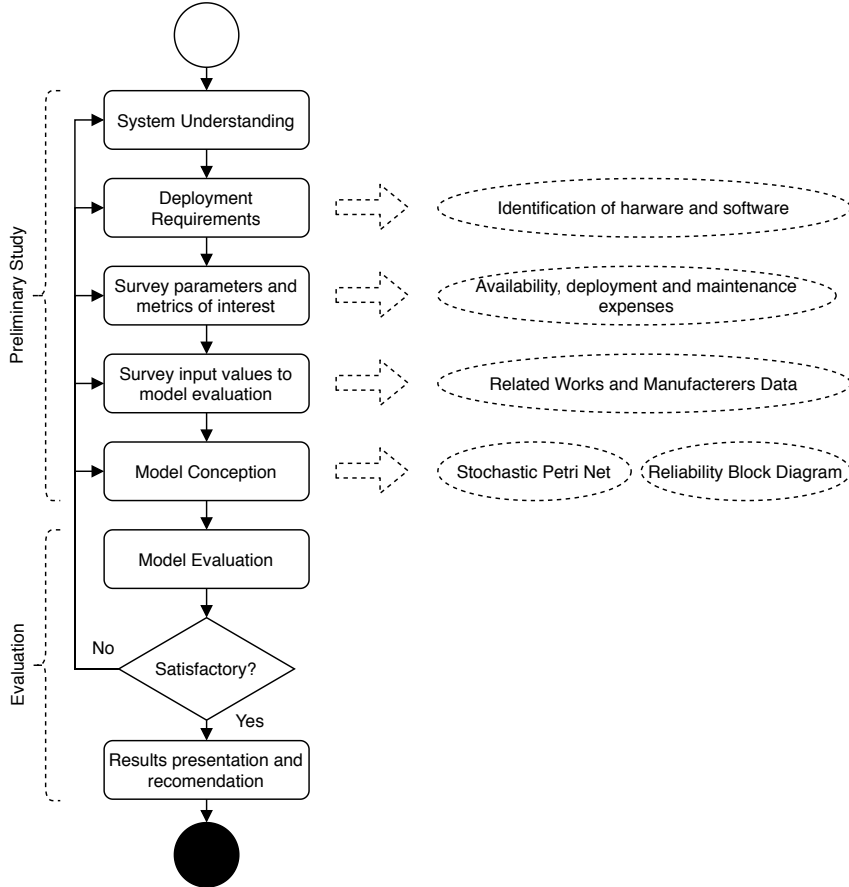


Fig. 3: Supporting Methodology

The rectangles represent each step of the methodology, and arrows connecting the rectangles define the execution order. The evaluator only advances to the next step after the completion of the current one. Already the diamond represents a step that can lead to two different paths, that is if the results are

considered satisfactory, the evaluation proceeds, otherwise, it returns to any of the previous steps, where adjustments will be made until it shows a behavior close to the one expected from a real system. The dashed circles distinguish the subcategories of the methodology steps.

4.1 Preliminary Study

The preliminary study covers the first five steps of the supporting methodology: (1) system understanding; (2) deployment requirements; (3) survey of the parameters and metrics that will be evaluated; (4) a survey of the input values for the models, which are proposed in (5).

System understanding: this step consists of understanding the Ethereum platform as well as the relation between the Docker container engine and the Ethereum image.

Deployment Requirements: Identification of the main requirements for service deployment.

Survey parameters and metrics of interest: The third step corresponds to the establishment of the system metrics that will be evaluated. Choosing metrics and evaluation parameters that have a low impact on the user and administrator perception will lead to a waste of time and resources [13].

Survey input values to models evaluation: Based on the system understanding and as a result of previous activities, we may obtain the input values that will be used by the proposed models by consulting previous knowledge, related works, and manufacturers' specifications.

Models Conception: after defining the parameters, metrics of interest, and the main components required to run the service, it is possible to propose high-level models that allow obtaining a set of preliminary results.

4.2 Evaluation

The evaluation process has two main steps: (I) model evaluation and (II) the presentation and recommendations based on the obtained results.

Model Evaluation: the proposed models were evaluated through the Mercury tool [15], right after it be feeded with an input of the obtained mean time to failure (MTTF) and mean time to repair (MTTR) values; as an output, this step provides the required artifacts to accomplish the data presentation process.

Results presentation and recommendation This step is characterized by data representation, which can be done through graphs and tables and will depend on the audience to which the analyst wishes to present the results. The results will include the proposed models, the availability evaluation of these models, a sensitivity analysis evaluation to identify the components with the highest impact over the availability, and capacity-oriented availability evaluation. The models, evaluations, and raw data can be seen and understood

by designers, analysts, and administrators, but hardly by top management; hence it is important to provide graphical and textual interpretation available to support the decision-making process.

5 Proposed Architecture and Availability Model

This section presents the evaluated environment, considering a baseline architecture managed by a single organization, with a single machine, this environment can host several Ethereum containers or nodes, that could handle or perform transactions for one or more distributed applications. Figure 4 shows a high-level view of the proposed environment. This Figure is based on Ethereum original paper [6] and on cloud service providers, such as Amazon and Google.

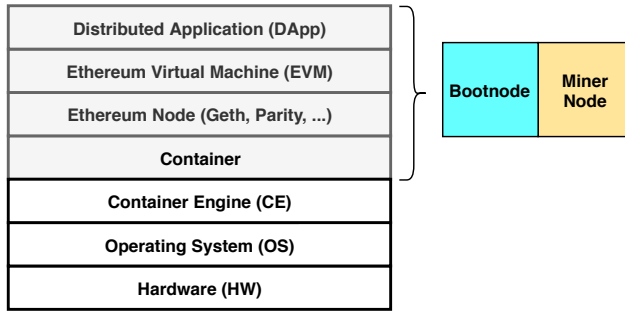


Fig. 4: Service Stack

As can be seen in Figure 4, there are four different components in the proposed environment: the server's Hardware (HW), Operating System (OS), container engine (Docker Engine), and the deployed nodes.

The hardware on this stack considers only the motherboard, CPU, RAM, network, disk, and so on. A power supply unit (PSU) is not considered because the meantime to failure of a component of this type is too high and the impact over the general availability is too low when compared with the other hardware components.

Already an Ethereum node can be both client and server, but it is important to mention that in this paper, we model, evaluate, and consider only the service provider side. That means that the client-side, which could include a client application, or even the network service and the respective Internet Service Provider (ISP) will not be considered for simplification.

The boot node is a dummy node, which can be used only to connect the pairs nodes or other containers so that they can exchange data, transactions, and blocks between themselves, the boot node does not execute any job that requires considerable computational power. However, it is essential because

when an application needs to start or repair, a miner node needs to connect to the boot node first. The miner node is responsible execute computationally intensive jobs by performing transactions and solving puzzles to obtain the credentials to write on the Blockchain.

As already seen in Figure 4, all of the required components for service provisioning are hosted into a single machine. To represent this architecture and the fact that all components must be operational, we considered two-stage modeling. In the first stage, RBDs are adopted to represent nodes. The RBD presented in Figure 5 depicts the node's components.



Fig. 5: Server's RBD

This RBD's components are in series since if one component fails, the whole subsystem fails. After evaluating the server RBD, the respective MTTF is obtained. The MTTR values are discussed later on. Then, we have modeled both nodes, the miner, and the boot node through another RBD. Figure 6 presents the containers RBD, which can be used to represent both types of Ethereum nodes.

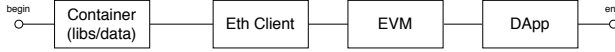


Fig. 6: Containers' RBD

Finally, Figure 7 presents the top-level environment model, which hierarchically relates the two RBDs previously depicted and representing each of the main components in the Ethereum environment. The Service Infrastructure is represented by a Stochastic Petri Net (SPN) due to the dependency between the miner, boot node, and the container engine which is a part of the server.

This SPN depicts three components. The first component is the basic server, whose MTTF_{SE} and MTTR_{SE} are obtained through the evaluation of the previously presented RBD (See Figure 5). The other two components seen in Figure 4 are represented (each) by a single component RBD (See Figure 6). The places (circles) Server_ON, BN_ON, and MN_ON mark the upstate for each component, respectively Server, Bootnode, and Miner Node containers, while their counterpart, that means a mark on places Server_OFF, BN_OFF, and MN_OFF indicates that the component is in a downstate.

Initially, every component is operational or in upstate, each component has a mean time to fail (MTTF) and a mean time to repair (MTTR), these times follow an exponential distribution, and are represented in the model by timed transitions (white squares) connected through arcs (arrows) to the place that corresponds to the component current state (ON or OFF, UP or DOWN).

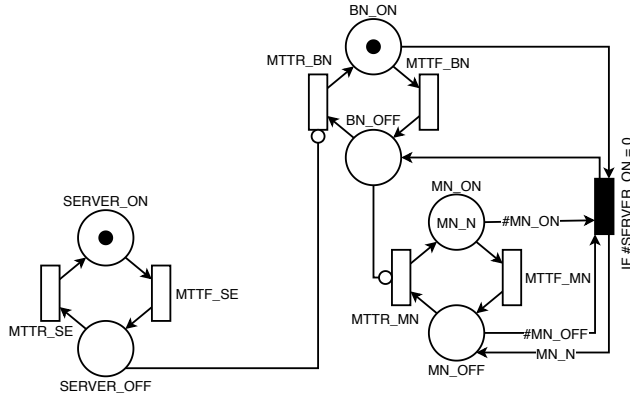


Fig. 7: Service Provisioning - SPN Model

There are two types of arcs in the proposed model, the arc that ends with an arrow is the most common, and indicates the activation of a transition if the requirements are met and the movement of a token (the small black circle inside a place, which indicates the number of resources), while the arc that ends with a circle is called inhibitor arc, there are four of them in the proposed model. An inhibitor arc indicates that a transition can only be activated if some conditions are met, for example, if there is no boot node operational and we need to repair a miner node, the miner node can only be repaired if the boot node has been repaired first, which can be seen as a dependency relationship.

Finally, there are two types of transitions, the already mentioned timed transition that depends on time to activate and the black rectangle, which is the transition called immediate transition, which may be activated if the required amount of tokens are present in the connected place. The proposed model has one immediate transition, used to change the state of a component if this component is dependent from another that failed, for example, if the server enters into a failure state all nodes (miners and boot node) will fail as well, meaning that in this case, the system does not wait for the mean time to fail associated to the timed transitions.

6 Case Studies

This section provides three case studies that demonstrate how feasible are the proposed models: (1) Availability evaluation, (2) Capacity-oriented Availability (COA) evaluation, both of them regarding an application or service provisioning, (3) cost evaluation and comparison between public and private service providers. The first step to accomplish our tasks is to obtain the required system's input values to feed the model and perform the availability evaluation. Some of these values were obtained from a literature review [7, 22, 33], while other ones were extracted from manufacturer charts and white

papers. The values used in this paper can be seen in Table 2. It is important to mention that software-based component has an estimated mean time to repair and can be obtained by measuring the time that usually takes to create or start a new service or component, that tends to be a lower value when compared to hardware components that may demand an entirely new motherboard, CPU or disk to be changed.

Table 2: Input Parameters for Proposed Models

Component	MTTF (h)	MTTR (h)
Hardware (HW)	8760	1.66
Operating System (OS)	2893	0.25
Docker Engine (DE)	2516	0.25
Container	1258	0.25
EVM	788.4	0.25
Eth Client	788.4	0.25
DApp	788.4	0.25

-

6.1 Case Study I - Availability Evaluation

The first case study is the availability evaluation of the proposed models. It is important to mention that this evaluation was performed using the Mercury Tool [15].

We first have evaluated the RBD presented in Figure 5, which could be represented by the expression denoted by $A_{HW} \times A_{OS} \times A_{CE}$, where A stands for Availability. The obtained availability value for this model was 99.96%, corresponding to an annual downtime of 3.28 hours, while the obtained MTTF 1166.48 hours and the respective MTTR was 0.4378 hours.

The second evaluated model was the RBD for the Ethereum nodes (See Figure 6), this evaluation apply to both miner and bootnode, the closed-form equation that represent this model is $A_{Container} \times A_{Eth\ Client} \times A_{EVM} \times A_{DApp}$, the obtained values were 99.9081% of availability, for a MTTF of 271.9 hours and a MTTR of 0.25 hours.

The values obtained from the RBDs evaluation were later used as an input parameter for the Service Infrastructure model, which is the SPN presented in Figure 7. The general availability obtained by the SPN evaluation is 99.82%, resulting in an annual downtime of 8.78 hours. During the downtime period, users can not request or send new transactions to the system. Also, we must mention that only a single miner node was operational on the considered evaluation, we could have many others, as we are going to see on the COA case study. This model's availability was given by the probability of having at least one token in the MN_ON place since, as already mentioned, the boot node is only required when we need to start or repair a miner node. Table 3 resumes the availability metrics obtained through model evaluation.

Table 3: General Availability Values

Model	Availability	Downtime(h/y)	MTTF(h)	MTTR(h)
Server	99.96	3.28	1166.48	0.43
Containers	99.90	8.76	271.9	0.25
SPN	99.82	15.77	990	1.7

As an attempt to detect the components with the highest impact over the system availability, we have applied a sensitivity analysis Through the percentage difference technique using the Mercury tool. To accomplish this task, we fed the model with the required MTTF, and MTTR values for each component, the values presented in Table 2 will be reused. The adopted values vary from +50% to -50% from the original value. Table 4 presents the sensitivity analysis results obtained from the baseline architecture availability evaluation. It is important to mention that the sensitivity analysis can also be applied to check if the used MTTF and MTTR values are close enough to what can be obtained in a real system and to point out where improvements can be made.

Percentage Difference Sensitivity Analysis		
Parameters	Ranking	Sensitivity Index
MTTF _{SE}	1st	0.00109
MTTR _{MN}	2nd	0.00100
MTTR _{SE}	3rd	9.37×10^{-4}
#Miners	4th	6.26×10^{-4}
MTTR _{SE}	5th	4.86×10^{-4}
MTTR _{BN}	6th	1.91×10^{-4}
MTTF _{BN}	7th	1.32×10^{-6}

Table 4: Sensitivity Analysis Ranking

The presented indexes start from the factor with the highest impact over the architecture availability is the MTTF of the server (which is the component that is represented by the RBD of Figure 5 and includes hardware, operating system, and contained engine), which is followed by the MN MTTR and Server MTTR. These components had a higher impact on the environment availability probably because their failure directly impacts the failure of other components; every single component will fail if the server enters into a failure state. Figure 8 shows the behavior of all the factors over the baseline infrastructure availability based on the passage of time in the Percentage-Difference sensitivity analysis evaluation.

The Figure 8 presents a graph for each component and their respective MTTR and MTTF impact over the general availability, the red line on each graph represents the variability of the system's availability based on MTTF and MTTR values changes, has the MTTF of the boot node in the last position. This component presents a minor impact over the system's availability since it can enter into a failure state, and the service will be provided as long as there is a miner node running.

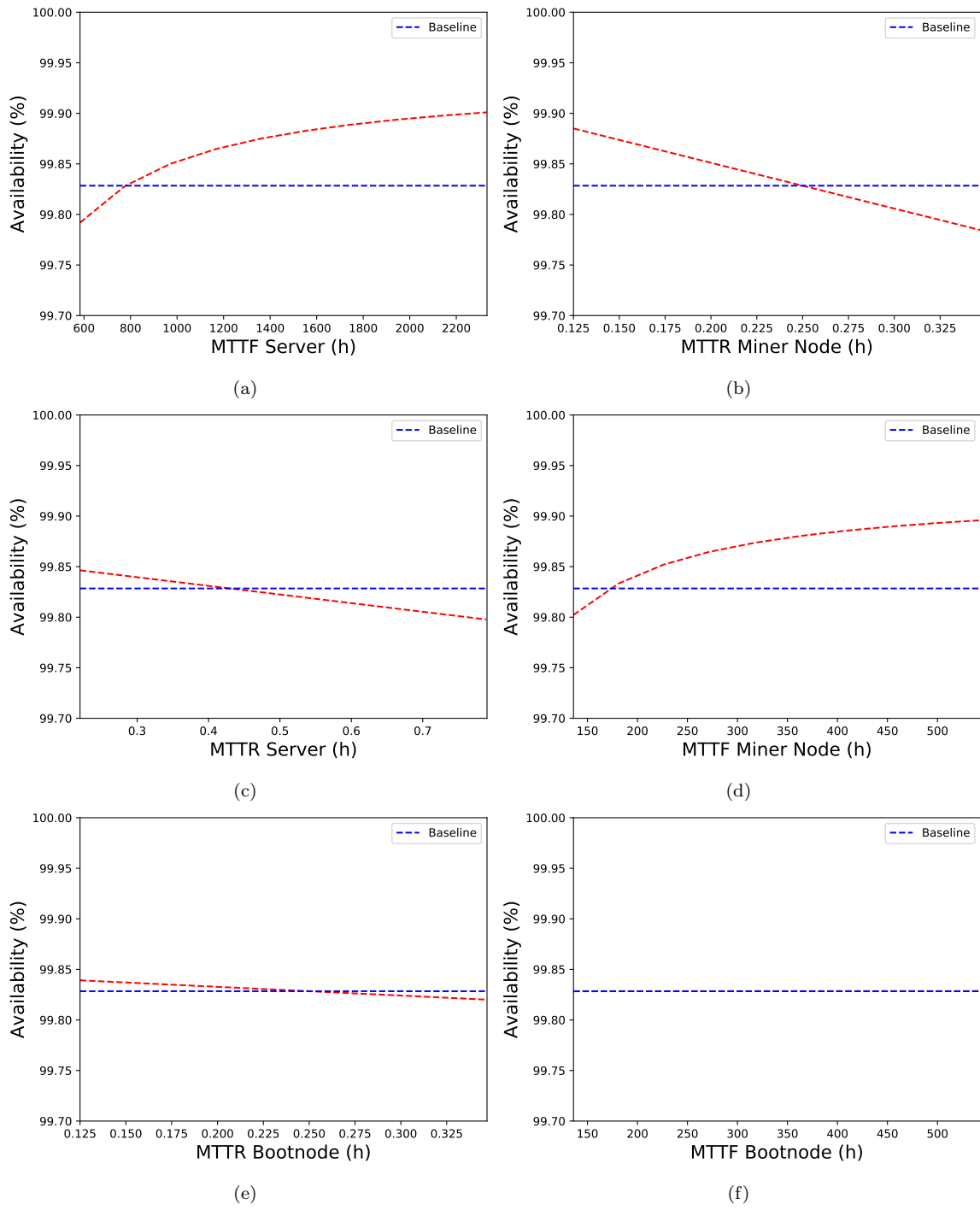


Fig. 8: Sensitivity Analysis

Another essential component is the number of miner nodes. Here, we varied it from 1 to 8 miner nodes and checked the impact of this component on system availability. Figure 9 presents the impact of this component on system availability. From 1 to 2 miner nodes there is a real gain on availability, but after this, two or more, the improvement is almost none.

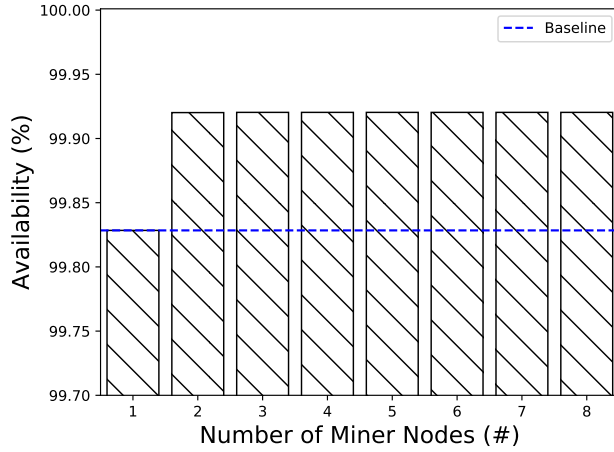


Fig. 9: Impact of the number of miner nodes over the availability

As an attempt to improve the system's availability, we provide a scenario considering multiple nodes in a parallel way, aiming to reach high availability. Using models in a hierarchical way we could distribute the servers and service provisioning in a parallel way, by using a reliability block diagram, we reach to a scenario that is closer to a real-world environment, which is presented in Figure 10.

As an example, we considered up to 4 servers and presented the availability evolution in Figure 11. The general availability reaches five-nines when considering just two nodes (99.999%), implying in an annual downtime of fewer than five minutes.

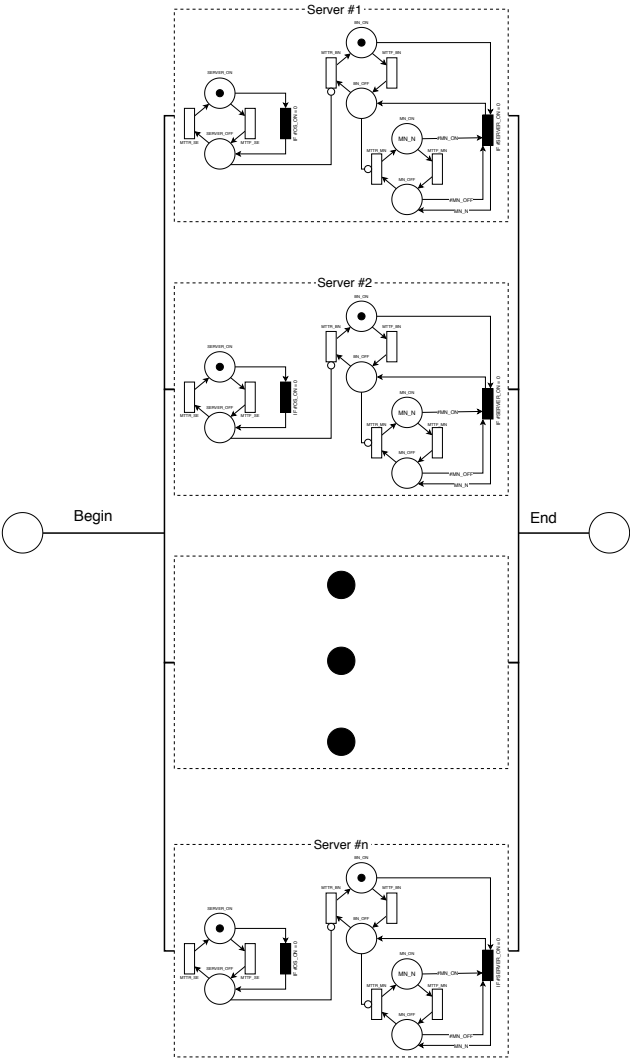


Fig. 10: Multi-server environment

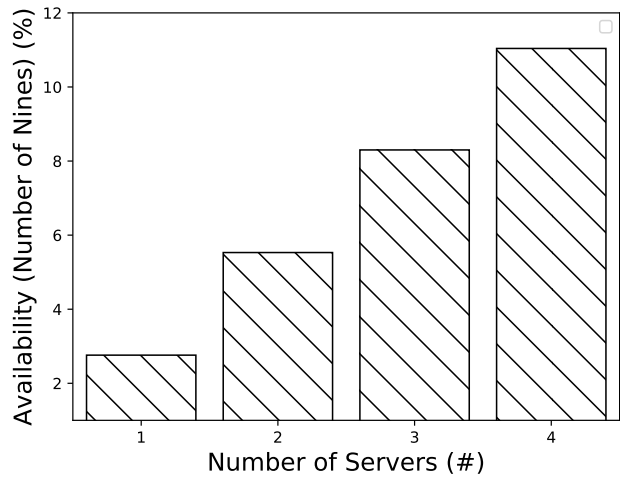


Fig. 11: Availability values for multiple nodes

If we keep adding servers the availability value will have almost no impact on service provisioning, but it will improve the general expenses and on general performance, and in the case of most Blockchain-based applications, the larger the amount of nodes the higher is the time taken to validate or perform a transaction.

6.2 Case Study II - Capacity-oriented Availability

The Capacity-oriented Availability (COA) may be estimated with Markov Reward Models (MRMs), by assigning a reward to each model state corresponding to the system capacity in that condition. Another way of estimating COA is by computing probabilities of being at each system state, multiplying them by the capacity associated with each state, summing up these products, and dividing this result by the maximal system processing capacity. In a private cloud system, COA may be associated with the number of virtual machines or containers that the servers can instantiate, therefore representing the computational work the system can provide regarding the availability values previously obtained.

The capacity-oriented availability of the cloud infrastructure is calculated by dividing the average of service capacity the system can deliver for the maximal service capacity. Therefore, the COA for any configuration of cloud infrastructure can be found following the closed-form equation adapted from [8], which can be expressed by Equation 7.

$$COA = \frac{1}{n} \left(\sum_{k=0}^n ((A_s)^p CTs[k, n](n - k)) + \left(\sum_{j=1}^{p-1} \sum_{k=0}^{NCTj} (A_s(j, p) - A_s(j + 1, p)) \times (CTs[k, NCTj])(NCTj - k) \right) \right), \quad (7)$$

where:

$$CTs[k, n] = \left(\frac{\frac{n!}{(n-k)!} \mu^{(n-k)} \lambda_{ct}^k}{\sum_{i=0}^n \frac{n!}{i!} \lambda_{ct}^{n-i} \mu^i} \right) \quad (8)$$

- $CTs[k, n]$ is a function which defines the probability of state k , from n containers available (P_k);
- $NCTj$ represents the number of containers (NCT) per physical machine (j).

For the proposed case study, a single server can handle a container per core, which means that if the server CPU has eight cores, then it can run up to 8 miner nodes, each one running the Ethereum Virtual Machine and a personal copy of the blockchain/service in its current state. As previously mentioned, the boot node is a dumb node, and it is only required when we need to start a new miner node or repair one that entered into a failure state.

So, as expected, we do not consider its impact on the environment's capacity-oriented availability (COA). We have measured the COA value by varying the number of available resources from 1 to 8, considering an octa-core processor, Figure 12 presents the capacity for a scenario with 1, 2, 3, and 4 servers, each one running up to 8 containers.

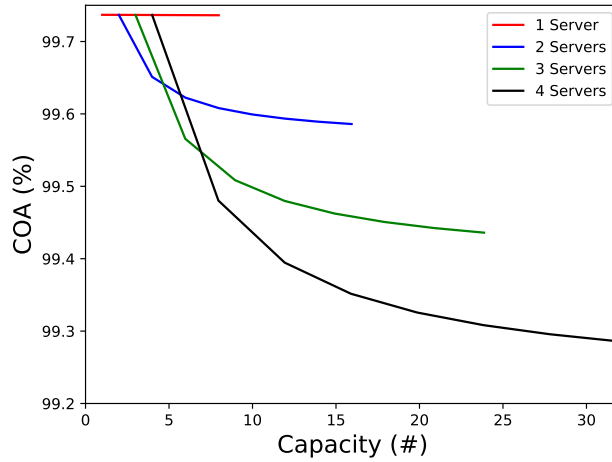


Fig. 12: COA x System's Capacity

As shown in Figure 12, we may see that the more significant the amount of available resource, the lower the Capacity-oriented Availability, which happens since with more resources, we have a higher probability that at least one of these resources enter into a failure state.

6.3 Case Study III - Cost Planning

A three-stage survey characterizes the cost analysis. Which has as a prerequisite the COA analysis previously performed. At the first stage of the survey, the necessary components to provide a cloud computing environment were defined, such as servers, switch, rack, and air conditioning.

In the second stage of the survey, all the acquisition costs for each component were individually analyzed, and by consulting Brazilian and North American websites, the lowest value of each architecture element in the period from 8th to May 14th, 2020, was selected. Table 5 present the cost for each component, as well as the store with the lowest price.

Table 5: Acquisition Costs

Component	Cost (USD)	Store
HPE ProLiant DL360 Gen10	1,884	Amazon
Switch Huacomm HC1709P	63	Amazon
Air conditionair Black+Decker BPACT08	310	Amazon
Rack SRW 15.900	320	Sysracks

The third and last stage of our survey was the technical specification analysis of each environment component, in search of energy power consumption values to calculate the energy cost per unit for one year period. By using the HPE Power Advisor² to estimate the data center energy consumption, we could achieve real values for the energy consumption of the selected components by using Equation 9.

$$\text{kWh} = \frac{\text{Power (W)} \times \text{NHD} \times \text{NDY}}{1000} \quad (9)$$

where NHD stands for the number of hours per day and NDY is the number of days per year that the equipment is operational, so considering that each component would be running for 24 hours a day, seven days a week and a kilowatt-hour cost of 16 cents of American Dollar we could achieve the values presented in Table 6.

Table 6: Energy consumption by year

Component	Power (W)	Energy Expenses/y (USD)
HPE ProLiant DL360 Gen10	122.48	171.87
Switch Huacomm HC1709P	65	91.1
Cooling	187.48	262.77

By considering an eight-core processor for the chosen server, and by using HP Power Advisor (HPA), we estimated the general expenses for one, two, three, and four servers. It is important to highlight that the recommended cooling expenses are equivalent to the total expenses, which means that we will probably spend a dollar with the cooling system for each dollar expended in computing. Table 7 shows the expenses for each scenario. It is important to mention that the acquisition cost for each environment considers a fixed amount of cooling system, switch and rack, the only thing that varies is the number of servers, as can be seen in the first column. In other words, the acquisition cost is defined by the sum of the values for each component on the environment: server + switch + rack + cooling device.

By knowing how much service we can provide (almost eight containers for each server (as already seen in subsection 6.2)), and how much costs to provide service over environments composed by one, two, three and four nodes, we may

² <https://paonline56.itcs.hpe.com/?Page=Index>

Table 7: Maintenance Expenses by Year

#Servers	Total Acquisition (USD)	Maintenance Cost/y (USD)
1	2,577	525.54
2	4,461	777.78
3	6,345	1,636.13
4	8,229	2,837.82

compare the service provisioning of the most popular public cloud computing environments and the proposed private infrastructures.

6.3.1 Public vs Private Cloud

The chosen public cloud computing platforms for comparison to the private environment modeled here are Google Cloud, Amazon AWS, and Microsoft Azure. These three platforms provide Ethereum blockchain environments for distributed application services.

As expected, each one has its peculiarities, we chose a basic container/VM for each platform, the settings are close to the previous stated in this paper, one vCPU, and up to 4 Gib RAM. Table 8 summarizes the selected environments.

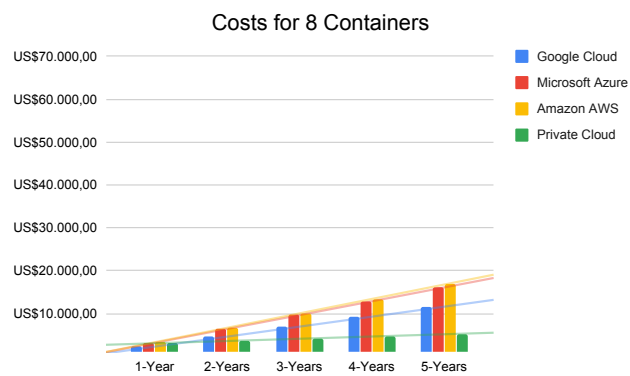
Table 8: Annual Expenses by Instance in Public Clouds

Platform	Instance Type	On-demand /y (USD)	Availability(%)
Google	n1-standard-1	291.24	99.9
Amazon	m3.medium	420.48	99.9
Microsoft	D1s	403,56	99.9

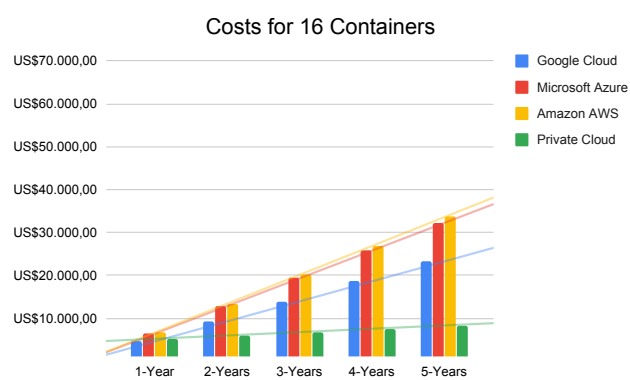
Finally, we compared four different scenarios considering 8, 16, 24, and 32 containers/Virtual Machines in these three cloud computing providers and the use of private cloud computing to deliver the Ethereum platform as a service. Figure 13 present the effective expenses comparison for each platform, including private and public ones.

As can be seen, from both Table 8 and Figure 13 among the public cloud providers, the Google Cloud has the best cost. By considering the life expectancy for a server is from three to five years, we extended our analysis to accommodate this entire period. In general terms, for the first year, the proposed private environment loses to the Google Cloud, which is expected, since the equipment acquisition expenses are higher than the required maintenance expenses.

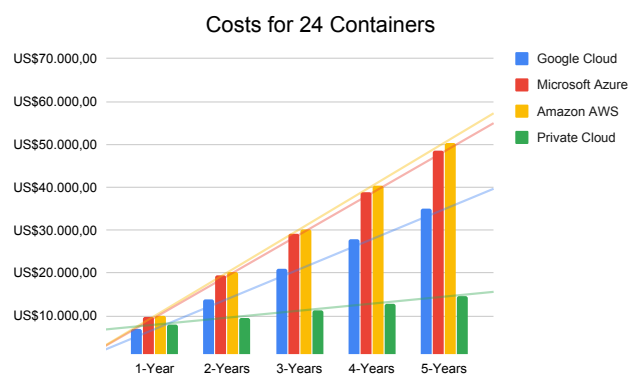
From the tendency, lines are possible to see that Amazon AWS is not a suitable choice, neither the Microsoft Azure. Finally, it is important to mention that this evaluation does not consider maintenance teams' expenses if the decision-maker has to pay someone else to do this work is probably worse to keep a private environment than to contract instances in Google cloud. How-



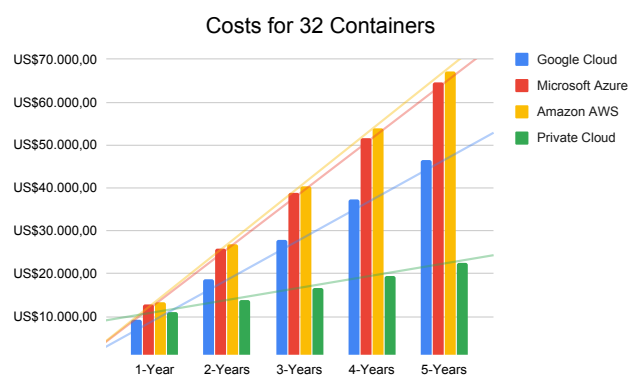
(a)



(b)



(c)



(d)

Fig. 13: Effective Expenses - Public vs Private Clouds

ever, if the distributed application requires high-security, a suitable alternative would be to adopt a private cloud infrastructure at the expense of the cost.

It is important to mention that the availability guaranteed values for those platforms in their respective Service Level Agreements (SLA) are 99.9%, with up to eight hours of annual downtime, which is higher than our first evaluated scenario, that considered only one server, but lower than a scenario with at least two servers (99.999%).

7 Conclusions and Future Works

This paper proposes a set of models to evaluate the availability of a cloud computing infrastructure that provides blockchain-as-a-service. Three case studies demonstrate the feasibility of the proposed models, and help those interested in planning and use blockchains applications based on the Ethereum platform.

The first case study dealt with the proposed models' availability evaluation through the Mercury modeling tool; the baseline environment availability hit 99.82%, then we have performed a sensitivity analysis evaluation and identified the most critical component to provide the service was the service itself. After that, we have evaluated an environment with multiple servers through a reliability block diagram (RBD) that hierarchically distributed the SPN model in order to improve the number of resources that can be delivered to the system's users.

Already the second case study, which was a capacity-oriented availability (COA) evaluation, presented the real amount of resources that could be delivered, due to the presence of the system's failures and repairs routines. This case study showed that the more significant the amount of servers to service provisioning, the lower is the COA, which goes on the counter-hand of the service availability.

The third and last case study evaluated the expenses to provide Blockchain as a service in a private cloud environment, as well as a public platform to host a distributed application based on the Ethereum blockchain platform. Google Cloud has the lowest cost among the public cloud computing service providers, and Amazon has the worst price. The private environment presented the general lower expenses, except for the first year, considering the necessity to buy all required components to accomplish service provisioning.

As future work, we intend to evaluate cost-benefit, as well as the presence of software aging on the environment, aiming to provide a maintenance routine to help to improve the availability of a single server environment and extend the system's life cycle.

Acknowledgements The authors would like to thank the Brazilian Government for the financial support through the Fundação de Amparo a Ciência e Tecnologia de Pernambuco (FACEPE), the Modeling of Distributed and Concurrent Systems (MoDCS) group for the help on improving this research.

Conflict of interest

The authors declare that they have no conflict of interest.

References

1. Amazon: What is cloud computing? (2020). URL <https://aws.amazon.com/pt/what-is-cloud-computing/>
2. Aniello, L., Baldoni, R., Gaetani, E., Lombardi, F., Margheri, A., Sassone, V.: A prototype evaluation of a tamper-resistant high performance blockchain-based transaction log for a distributed database. In: 2017 13th European Dependable Computing Conference (EDCC), pp. 151–154. IEEE (2017)
3. Arundel, J., Domingus, J.: Cloud Native DevOps with Kubernetes: Building, Deploying, and Scaling Modern Applications in the Cloud. O'Reilly Media (2019)
4. Avizienis, A., Laprie, J., Randell, B., Landwehr, C.: Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing* **1**, 11–33 (2004)
5. Avizienis, A., Laprie, J., Randell, B., of Newcastle upon Tyne. Computing Science, U.: Fundamental Concepts of Dependability. Technical report series. University of Newcastle upon Tyne, Computing Science (2001). URL <https://books.google.com.br/books?id=cDkmGwAACAAJ>
6. Buterin, V., et al.: Ethereum white paper. GitHub repository **1**, 22–23 (2013)
7. Dantas, J.: Modelos para análise de dependabilidade de arquiteturas de computação em nuvem. Master's thesis, Centro de Informática - Universidade Federal de Pernambuco (Recife, Brasil) (2013)
8. Dantas, J., Matos, R., Melo, C., Maciel, P.: Cloud infrastructure planning: Models considering an optimization method, cost and performance requirements. *International Journal of Grid and Utility Computing* (2020)
9. Frank, P.M.: Introduction to Sensitivity Analysis. Academic (1978)
10. Garg, S., A, P., M, T., Trivedi, K.S.: Analysis of software rejuvenation using markov regenerative stochastic petri net. In: Proc. In: Sixth International Symposium on Software Reliability Engineering, (ISSRE'95), pp. 180–187. Paderborn (1995)
11. Gupta, M.: Blockchain for DUMMIES. John Wiley & Sons, Inc. (2017)
12. Hightower, K., Burns, B., Beda, J.: Kubernetes: up and running: dive into the future of infrastructure. " O'Reilly Media, Inc." (2017)
13. Jain, R.: The Art of Computer Systems Performance Analysis: Techniques for Experimental Design, Measurement, Simulation, and Modeling. Wiley Computer Publishing, John Wiley & Sons, Inc., New York (1991)
14. Li, Q.L., Ma, J.Y., Chang, Y.X.: Blockchain queueing theory. arXiv preprint arXiv:1808.01795 (2018)
15. Maciel, P., Matos, R., Silva, B., Figueiredo, J., Oliveira, D., Fé, I., Maciel, R., Dantas, J.: Mercury: Performance and dependability evaluation of systems with exponential, expolynomial, and general distributions. In: 2017 IEEE 22nd Pacific Rim International Symposium on Dependable Computing (PRDC), pp. 50–57 (2017). DOI 10.1109/PRDC.2017.16
16. Maciel, P., Trivedi, K., Matias, R., Kim, D.: Dependability modeling. In: Performance and Dependability in Service Computing: Concepts, Techniques and Research Directions (2011)
17. Malhotra, M., Trivedi, K.: Power-hierarchy of dependability-model types. *Reliability, IEEE Transactions on* **43**(3), 493–502 (1994). DOI 10.1109/24.326452
18. Martins Maciel, P.R.: Modeling Availability Impact in Cloud Computing, pp. 287–320. Springer International Publishing, Cham (2016)
19. Matos, R., Araujo, J., Oliveira, D., Maciel, P., Trivedi, K.: Sensitivity analysis of a hierarchical model of mobile cloud computing. *Simulation Modelling Practice and Theory* **50**, 151 – 164 (2015). DOI <https://doi.org/10.1016/j.simpat.2014.04.003>. URL <http://www.sciencedirect.com/science/article/pii/S1569190X14000616>. Special Issue on Resource Management in Mobile Clouds

20. Matos, R., Dantas, J., Araujo, J., Trivedi, K.S., Maciel, P.: Redundant eucalyptus private clouds: availability modeling and sensitivity analysis. *Journal of Grid Computing* **15**(1), 1–22 (2017)
21. Mell, P., Grance, T., et al.: The nist definition of cloud computing (2011)
22. Melo, C., Dantas, J., Araujo, J., Maciel, P.: Availability models for synchronization server infrastructure. In: *Proceedings of the IEEE Int. Conf. on Systems, Man, and Cybernetics (SMC'16)*. Budapest, Hungary (2016)
23. Melo, C., Dantas, J., Maciel, R., Silva, P., Maciel, P.: Models to evaluate service provisioning over cloud computing environments-a blockchain-as-a-service case study. *Revista de Informática Teórica e Aplicada* **26**(3), 65–74 (2019)
24. Melo, C., Dantas, J., Oliveira, D., Fé, I., Matos, R., Dantas, R., Maciel, R., Maciel, P.: Dependability evaluation of a blockchain-as-a-service environment. In: *2018 IEEE Symposium on Computers and Communications (ISCC)*, pp. 00909–00914. IEEE (2018)
25. Melo, C., Matos, R., Dantas, J., Maciel, P.: Capacity-oriented availability model for resources estimation on private cloud infrastructure. In: *Dependable Computing (PRDC), 2017 IEEE 22nd Pacific Rim International Symposium on*, pp. 255–260. IEEE (2017)
26. Molloy, M.K.: On the integration of delay and throughput measures in distributed processing models. Ph.D. thesis, University of California, Los Angeles, USA (1981). AAI8201138
27. Murata, T.: Petri nets: Properties, analysis and applications. *Proceedings of the IEEE* **77**(4), 541–580 (1989). DOI 10.1109/5.24143
28. Nakamoto, S., et al.: Bitcoin: A peer-to-peer electronic cash system (2008)
29. Öhmann, D., Simsek, M., Fettweis, G.P.: Achieving high availability in wireless networks by an optimal number of rayleigh-fading links. In: *2014 IEEE Globecom Workshops (GC Wkshps)*, pp. 1402–1407. IEEE (2014)
30. Onik, M.M.H., Miraz, M.H.: Performance analytical comparison of blockchain-as-a-service (baas) platforms. In: *International Conference for Emerging Technologies in Computing*, pp. 3–18. Springer (2019)
31. Pongnumkul, S.e.a.: Performance analysis of private blockchain platforms in varying workloads. In: *2017 26th International Conference on Computer Communication and Networks (ICCCN)*, pp. 1–6. IEEE (2017)
32. Roehrs, A., da Costa, C.A., da Rosa Righi, R., da Silva, V.F., Goldim, J.R., Schmidt, D.C.: Analyzing the performance of a blockchain-based personal health record implementation. *Journal of biomedical informatics* **92**, 103140 (2019)
33. Sebastio, S., Ghosh, R., Mukherjee, T.: An availability analysis approach for deployment configurations of containers. *IEEE Transactions on Services Computing* (2018)
34. Sukhwani, H., Martínez, J.M., Chang, X., Trivedi, K.S., Rindos, A.: Performance modeling of pbft consensus process for permissioned blockchain network (hyperledger fabric). In: *2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS)*, pp. 253–255. IEEE (2017)
35. Sukhwani, H., Wang, N., Trivedi, K.S., Rindos, A.: Performance modeling of hyperledger fabric (permissioned blockchain network). In: *2018 IEEE 17th International Symposium on Network Computing and Applications (NCA)*, pp. 1–8. IEEE (2018)
36. Torquato, M., Torquato, L., Maciel, P.: Models for capacity oriented availability evaluation of a private cloud. *Revista de Informática Teórica e Aplicada-RITA-ISSN* **2175**, 2745
37. Trivedi, K.S., Hunter, S., Garg, S., Fricks, R.: Reliability analysis techniques explored through a communication network example (1996)
38. Vaqueiro, L.M., Rodero-Merino, L., Caceres, J., Lindner, M.: A break in the clouds: Towards a cloud definition. *Computer Communication Review* **39**, 50–55 (2009)
39. Weber, I., Gramoli, V., Ponomarev, A., Staples, M., Holz, R., Tran, A.B., Rimba, P.: On availability for blockchain-based systems. In: *2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS)*, pp. 64–73 (2017). DOI 10.1109/SRDS.2017.15
40. Zhang, H., Jin, C., Cui, H.: A method to predict the performance and storage of executing contract for ethereum consortium-blockchain. In: *International Conference on Blockchain*, pp. 63–74. Springer (2018)
41. Zyskind, G., Nathan, O., Pentland, A.: Decentralizing privacy: Using blockchain to protect personal data. In: *2015 IEEE Security and Privacy Workshops*, pp. 180–184 (2015). DOI 10.1109/SPW.2015.27