An Enterprise Blockchain Solution for an Infrastructure-as-a-Service Platform

Jason Feibelman, jason.feibelman@gmail.com (A paper written under the guidance of Prof. Raj Jain)

Download

Abstract:

Current technology is limited by its operating system and infrastructure in terms of deployment, interoperability, and security. This paper will propose an infrastructure-as-a-service (IaaS) solution to provide a more secure, high-speed infrastructure, which will facilitate the development process by offering a universal deployment platform. We will explore Quorum and Hyperledger Fabric as potential blockchain solutions for generic frameworks for transacting and communicating within the proposed network. Moreover, this proposed platform will help create a set of standards for development, enterprise networks and blockchains, and cloud computing. This will leverage knowledge in blockchain technology, networking, and the Internet of Things (IoT).

Keywords:

Networking, Infrastructure-as-a-Service (IaaS), Cloud Computing, Blockchain, Virtual Private Cloud (VPC), Virtual Private Network (VPN) Hyperledger Fabric, Quorum, Internet of Things (IoT)

Table of Contents

---

1. Introduction

Infrastructure-as-a-service (IaaS) providers supply cloud computing infrastructure from which individuals or organizations can access their resources in the cloud through virtualization, which abstracts a computer's software from its hardware, typically by running multiple virtual machines (VM) on a single machine. IaaS has many advantages, including scalability, on-demand resource provisioning, flexibility, and providing a high level of infrastructure customization [IaaS19]. Cloud computing is a general term that refers to a wide array of services that provision and deliver highly customizable computing services to users on demand. Some services include data storage, running applications, and video streaming [Laberis19]. This paper proposes an IaaS platform where the respective networking and security benefits of cloud computing and blockchain technology are intrinsic to the platform's design. Before discussing the proposed IaaS solution, it is important to understand the problem that the solution helps to solve.

Companies, including Amazon, Google, and Microsoft, presently lease cloud computing space. However, this technology is primarily utilized by developers for professional applications, which limits how extendable and usable it is for the average consumer. Currently, the primary way for consumers to interface with such cloud technology is over the Internet through a browser or application. This platform aims to expand accessibility of more advanced technologies that can be readily used by any individual by leveraging a cloud computing based architecture. As a result, consumers will be able to interface with their personal cloud in a variety of ways and directly reap the benefits of cloud computing. Moreover, consumers typically have countless devices with different files and operating systems, and it can often be difficult to transfer data between different platforms. The proposed IaaS platform helps solve this problem by providing one backend that an individual can access across countless devices.

Another current issue deals with continuous deployment and integration. Currently, when developers wish to create an application, they often have to develop various versions for different platforms, which can be very costly. Currently, there is no platform that supports a singular deployment mechanism, which sets up an application on many different operating systems. The proposed IaaS platform intends to solve this problem as it will supply businesses and developers with a singular platform that supports continuous deployment and integration, which provides a more secure, scalable, and efficient infrastructure.

The last major problem this platform addresses is standardization. Newer technologies typically lack complete standards as to how they should be implemented. For interoperability, further standards must be created for such technologies, namely blockchain and cloud computing. While committees such as the National Institute of Standards and Technology and the Institute of Electrical and Electronics Engineers have begun creating standards, there are not nearly enough for complete interoperability [IEEE19]. The infrastructural solution proposed in this paper helps to solve this problem by natively incorporating continuous development, deployment, and

integration, and providing a standardized platform to develop applications for all operating systems. Similarly, the solution creates a standardized, validated identity for each user that can be easily extended, such as for authentication, by any 3rd party platform.

Technology is now an integral part of daily life, and all generations are increasingly demanding improved connectivity and new technologies. This paper proposes a blockchain-based solution for an IaaS platform in which many of the benefits of blockchain technology and cloud computing are native to its architecture. As a result, individuals will receive improved security, faster speeds, and newer technologies. Likewise, organizations will get a more efficient, secure architecture for hosting applications. Before describing the platform, it is important to introduce the networking and blockchain technologies that will be leveraged.

2. Network Architecture

Networking is often at the core of most enterprise-based technological solutions. The network is one of the most fundamental aspects of IaaS solutions as it defines the rules for communication. For this IaaS platform, the network must be configured as private for enterprise cloud computing and must properly distribute resources. This section will discuss the network architecture that will be the foundation of the platform proposed in this paper. First, the network's components must be defined.

2.1. Network Components

A virtual private network (VPN) extends a network, which is typically less secure, and encrypts its traffic. The platform proposed in this paper will exist within a VPN, which contains numerous VM's, each granted specific permissions for various purposes. Within the VPN, many VM's will be provisioned as virtual private clouds (VPC). Each VPC gives its respective user their own private space in the cloud on shared infrastructure by separating the individual's resources based on private IP subnets, and all VPCs will be connected over virtual local area networks [Cloud19]. This network architecture will result in the highest level of availability, scale, and redundancy and will provide the foundation for the proposed IaaS solution.

2.2. Network Structure

This section will explore the structure of the network used by the platform proposed in this paper. An overlay network will be created on top of the physical network using a virtual extensible local area network. This network's architecture consists of a VPN composed of a central authority, many central server clusters, and many VPCs as can be seen in Figure 1. Many components of this VPN will leverage blockchain technology and communicate over the infrastructure that was defined by this section.

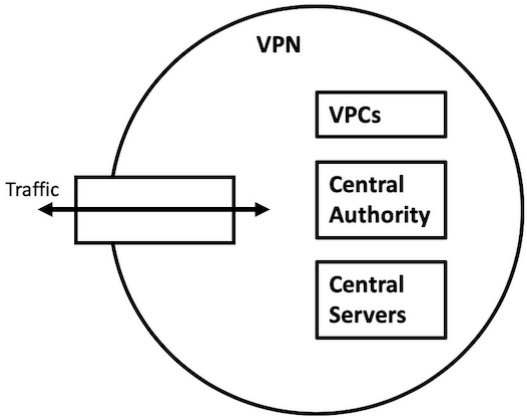

Figure 1: Network Architecture

3. Blockchain

In recent years, blockchain technology has been gaining traction and is becoming more widely accepted. Blockchain has many applications in law, finance, communications, and more. This section gives a brief introduction to blockchain development paradigms and specifies how blockchains will be implemented in the platform proposed in this paper.

3.1. Development Paradigms

A blockchain system consists of a network of machines, called nodes. This system contains a ledger, which defines how the blockchain is stored. Some examples include using directed acyclic graphs for hashgraphs or using the restricted shared ledger structure, which consists of numerous smaller ledgers only shared between specified, authorized parties [Xu19]. The main development paradigms for this blockchain system will be deployment and consensus protocol [Laurence19].

Deployment

Blockchains can be deployed in a public, private, or consortium manner. Public blockchains allow participation by anyone over the Internet while permission-less blockchains grant equal rights to all participating nodes. In contrast, permissioned blockchains allow an authority to have control over the nodes by granting them specific rights. Such permissions may include transacting, validating blocks, or even joining the network. Private blockchains allow a single authority to have full control over the blockchain network and its participants [Xu19]. Likewise, consortium blockchains are the same as private blockchains, except control is distributed across multiple organizations.

Consensus Protocol

The choice for consensus protocol has tremendous implications in terms of both security and scalability, especially for private permissioned blockchains. The consensus mechanism

determines how different nodes within a network reach agreements as to whether a transaction was valid. Once consensus is achieved, the transaction is non-refutable. The choice of consensus protocol must revolve around the security vulnerabilities of the predesignated blockchain network. For example, a common requirement for public, decentralized blockchain consensus algorithms is to be Byzantine fault-tolerant, which refers to protecting against an attack where some nodes within a network could be malicious and distribute inaccurate information [Byzantine17].

3.2. Blockchain Platforms

This section compares the Quorum and Hyperledger Fabric platforms for implementing enterprise blockchains. However, before exploring these platforms, it is important first to analyze a simpler decentralized blockchain platform called Ethereum. The development of Ethereum was a significant advance in the blockchain community as it enabled the use of smart contracts, which are custom, externally invoked, executable programs that are deployed and run within a blockchain network. Smart contracts can be used for custom transactions between multiple parties or for executing code, which will be run when the contract is validated and added to the blockchain [Xu19]. Such programs are run by the Ethereum VM, are developed using Solidity, and can be designed to run on or off the actual blockchain. This paper assesses Quorum and Hyperledger Fabric as enterprise blockchain solutions since neither platform will require a cryptocurrency for validating nodes in their consensus protocols.

Quorum

Quorum was created by J.P. Morgan and is a permissioned Ethereum-based distributed ledger technology that revolves around financial transactions. Quorum maintains a single, shared blockchain that is validated by every node within the network. Importantly, it provides various consensus algorithms, high performance, and the ability to provision the blockchain as private or public, which determines whether a transaction's details are exposed [Quorum19]. Quorum also supports Ethereum smart contracts according to this architecture such that private smart contracts are only validated by participating parties. This structure for private contracts has tremendous implications for financial transactions and investment strategies [Quorum18]. Quorum's public and private smart contract structure is derived from Ethereum, where Solidity is used to program smart contracts. Through such smart contracts, assets can be easily tokenized to create their digital equivalents that can be easily transacted on the blockchain [Xu19]. One of Quorum's most popular consensus algorithms for enterprise blockchains leverages the Raft protocol [Raft14] to provide high throughput and transaction finality for private and consortium blockchains where Byzantine fault tolerance is not required. In this protocol, the leader node in the Raft creates a new block as a new transaction flows in, which will likely become the head of the blockchain, after which the Raft comes to a consensus, and the entry is appended to the ledger [Raft19].

Hyperledger Fabric

Created by the Linux Foundation, Hyperledger Fabric is a private, permissioned blockchain platform that has been developed with a modular architecture and does not depend on any cryptocurrency. What makes this platform so unique is that it creates private, shared channels

between specified nodes such that for each channel, only its participants maintain a shared ledger of the channel's transactions [Xu19]. For every channel, each participant maintains a shared ledger that has both a world state and a transaction log. The world state is the ledger database and describes its current state at any time while the transaction log tracks all previous transactions that have resulted in the current world state [Hyperledger19]. This blockchain platform is highly customizable in terms of consensus protocol, shared ledger, its modular design, and smart contracts, which leverage container technology and is implemented through chaincode. All members of a Fabric network have validated identities using a membership service provider [Xu19].

3.3. The Blockchain Implementation

Since the blockchain will be implemented within a VPN, the platform will use private, permissioned blockchains for this enterprise solution. Rather than being fully centralized or decentralized, this architecture will allow the platform to be partially centralized and decentralized, where certain nodes will be granted the ability to transact and others the permission to validate such transactions [Xu19]. The platform will utilize two different types of enterprise blockchains for transactions and communications between different parties. These blockchains will leverage platform identities provisioned by the authentication protocol to validate additions to the chain.

Authentication

For authentication, the central authority will maintain a distributed ledger among various nodes provisioned for authentication. During authentication, the central server will verify a user's login details and then generate a temporary token, which will allow the user to maintain a persistent connection to their VPC for a set amount of time. Once a device has been connected to the VPC for the first time, it will be given the user's private key and will be remembered by the VPC for future access. Each entry in the central authority's distributed ledger will contain a platform identity, which maps a certified identity to a digital identity, as shown in Figure 2. The certified identity is provisioned on account creation and defines an individual's identity within the platform. This includes their login details, basic information, and internal details, such as their VPC endpoint and proof of certification. Before an account is made, a proof of certification is generated that certifies the identity of the user or organization. Only one account can be made for each individual entity, which is strictly enforced through comprehensive identity verification. On the other hand, a digital identity consists of public and private keys and any membership service provider identities provisioned to the user.

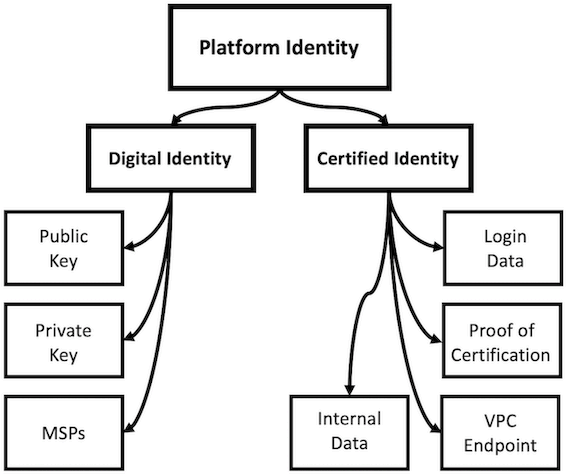

Figure 2: Platform Identity Hierarchy

While a certified identity is immutable, a digital identity is not. If an application needs to provision a new digital identity within the VPN, it will send a request to the central authority, which then may validate the newly provisioned identity. Since a certified identity is immutable, a VPC will be permanently provisioned for that user and, while it can be shut down, the association between the VPC and the individual can never be deleted. This structure gives individuals the ability to associate physical assets or money with their platform identity and to transact with other users. This ledger is a requirement for the proposed enterprise solution since the law requires a company to know the identities of its consumers. Blockchain technology was not included in the authentication solution since the ledger is completely centralized within the central authority, and since the digital identity is mutable.

Transaction

To track the transactions of money and assets, a private, permissioned blockchain will be utilized where all nodes within the VPN are permissioned to access and store it. First, the users involved in the transaction will sign it using their private key, and the transaction will be added to a block. Then, the block will be validated by designated nodes within the central servers and authority, which will then distribute the updated blockchain across the network. It is important to note that there is only a single blockchain in this model. Furthermore, this platform will provide open-source libraries to developers, which allow them to implement investment strategies and trading algorithms within their own VPC.

Quorum supports private smart contracts for financial transactions and asset-backed tokens, making it a viable solution for this blockchain. There is no requirement to protect against the Byzantine fault attack since this blockchain is private and permissioned. Thus, Quorum's Raft-based consensus algorithm will be used. Quorum uses public and private keys for identification, which allows an individual to use their digital identity to transact.

Communication

The final implementation of blockchain technology will be utilized for specialized communication within the network between different nodes. Rather than using a single blockchain, the platform will maintain many privately shared blockchains between predefined nodes that follow a publish/subscribe mechanism for communication. However, the platform will provide a fairly loosely defined blockchain template that is easily extendible and customizable by developers for both 1st and 3rd party applications. Thus, developers will be able to define and implement custom protocols that leverage this communications blockchain for specific use cases, such as decentralized applications that run across many VPCs or for exchanging information between different individuals or organizations.

Hyperledger Fabric provides a high level of customization, smart contracts, and privately shared channels and ledgers, making it an excellent solution for this communication blockchain. This blockchain technology utilizes membership service providers, and thus can easily leverage the platform's digital identities for identification. Furthermore, its flexible framework and modular design make it extremely extendible for developers to use Hyperledger Fabric to implement their own protocols and applications.

4. Platform

This section discusses the functionality of the proposed IaaS platform. For the average consumer, the platform's fundamental feature is the VPC. For every user, this platform provisions a unique VPC, which can be stopped manually or from timing out but never disassociated from the user or terminated. This is a direct result of the platform identity architecture.

4.1. Platform Identities

As previously stated, platform identities are comprised of certified and digital identities. As a result, this framework allows individuals to associate monetary and physical assets with their online identity. The proposed IaaS platform will enable users to transact and trade such assets using the transaction blockchain, which is shared within the IaaS platform. The platform identity framework will manage the permissions and private keys for a user such that this identity can be used across the various blockchains and within the VPN. While users' identities will be hidden from one another, the central authority will know the exact identities of who is transacting. This is necessary as it is required both by law for enterprises and by the authentication protocol in order to interface with VPCs.

4.2. Interfacing

One of the main goals of the proposed platform is to provide users with a personal cloud that can be accessed anywhere and developers with a standardized platform for developing applications that can immediately be deployed on all current operating systems and devices. This section proposes the various interface methods for users to communicate with their VPC and the architectural benefits of provisioning VPCs into environments.

Current Hardware

Individuals can access their VPC over SSH or HTTPS. Additionally, for this proposed IaaS solution, there will need to be a software application developed for all existing operating systems so that users can easily access their VPC. The platform's software application will provide a simple, fluid graphical user interface to provide users with an array of different mechanisms to interface with their VPC.

It is important to note that to deploy an application, many different versions must be developed for various platforms to create a truly universal platform. This problem is exactly what the platform proposed in this paper helps to solve, creating a standardized platform that supports continuous development, deployment, and integration. Once an application is launched on this IaaS platform, it will be available for download and use on all VPCs and will be accessible by any device regardless of its operating system.

Custom Adapters

In contrast, individuals would also access their VPC using a remote controller, a monitor, and a custom HDMI adapter that maintains a persistent wireless connection to the VPC. Finally, the platform will enable users to interface with their VPC over a special VPC Link, which is essentially a wireless router that will first authenticate into a VPC over Wi-Fi, and then create a wireless network that will forward all traffic directly to the VPC. For the best performance and security, it will be recommended that the VPC Link and adapter are used together.

Environments

The interface architecture must not only allow users to access their VPC from any device at any given time, but it must also support parallel access from multiple devices to a single VPC. Thus, VPCs will leverage environments that provide a variety of features, including simplicity, modularity, and supporting handoff between devices. An environment can be thought of as a new desktop screen to interface with that users can provision for themselves. Within each environment, users can instant message, utilize the internet, play games or launch applications much like modern desktops do today. Through the platform's interface, users will be able to easily access all environments, create new ones, switch between them, or have multiple open at once. Environments are highly customizable and can be configured so that its state is saved or reset on disconnection. All environments belonging to a user share that individual's VPC resources within the VPN. By leveraging the modular environment approach, the cloud computing technology intrinsic to this platform becomes much more extendable since a VPC can now be accessed by virtually any device or operating system that has the proper authentication.

4.3. Communication

Within the platform, a user's VPC has access to both the overarching VPN and the Internet. However, the proposed IaaS model renders all traffic and transactions within the VPN faster and more secure than with the outside Internet. This significant benefit is primarily due to network architecture and blockchain technology. Consider a corporation that uses this platform's central

servers to host its applications or web services. Any networking request made from a user's VPC that leverages the internal infrastructure, such as to a central server or another VPC within the VPN, would have its traffic encrypted and offer extremely high performance. This section will discuss the communication protocol native to the proposed IaaS model and explore the potential for 3rd party development.

Native Publish/Subscribe Protocol

The platform will have multiple native protocols that define mechanisms for communication between different individuals' and organizations' VPCs that use the Hyperledger Fabric communication blockchain framework, which will be available to all developers. This section will define just one native protocol for communication that will utilize the available Hyperledger Fabric framework according to the publish/subscribe mechanism proposed by Nejc Zupan et al. Every publish and subscribe transaction is validated by its participants and permanently added to the shared blockchain belonging to the specific channel's participants. This architecture will utilize Kafka, a real-time publish/subscribe data streaming service, to act as a proxy. For each channel, Kafka will forward notifications for data received to all of its subscribers [Zupan17], as can be seen in Figure 3, which reveals two independent publish/subscribe processes in red and blue with respect to the highlighted publishing nodes.

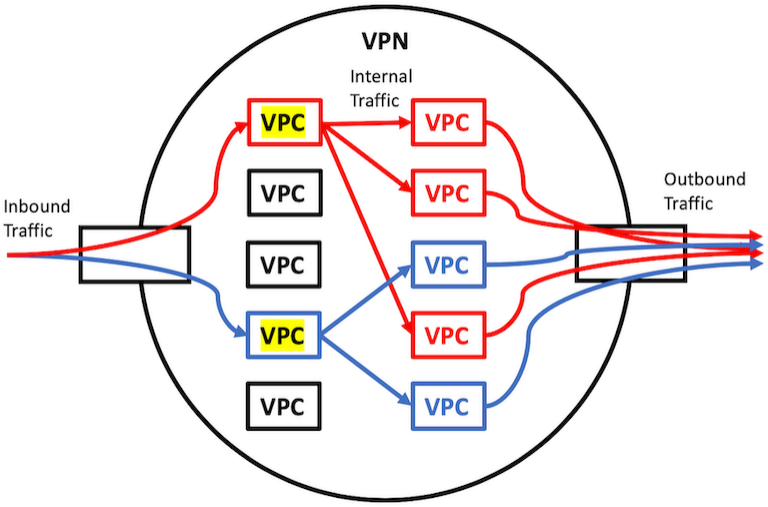

Figure 3: Publish/Subscribe Communication Mechanism

One potential application of this protocol is the private sharing of data between separate parties that require a permanent ledger and a publish/subscribe mechanism. One example is a supply chain tracking system that leverages the notification-based system for real-time updates on shipping, production, etc. Another potential application is that it will provide an organization, which has many devices or property residing within the VPN, the ability to monitor, contact, and maintain all devices from one node. Further, another potential application is for Internet of Things (IoT) devices that connect to a user's VPC and share data over this publish/subscribe mechanism. In contrast, other potential communication mediums include using TCP without blockchain or leveraging a potential mechanism in a 3rd party application.

3rd Party Development

This platform's central servers will offer a variety of consumer and enterprise hosting services, facilitating easy deployment of applications into an open marketplace within the VPN. Once applications are approved by the central authority, they can be downloaded by users onto their individual VPCs. This IaaS architecture will provide developers with continuous deployment and integration. The Hyperledger Fabric communication blockchain framework and the platform's modularized, flexible architecture, will spur a large open-source development community and make it extremely easy to develop, deploy, and leverage open-source 3rd party libraries. This has tremendous implications for some of the hottest Computer Science fields, including Machine Learning and Artificial Intelligence, since novel software developments could immediately be integrated into the platform in the form of 3rd party libraries and applications, making them immediately accessible on any device as a result of having all devices linked to a single VPC. However, these open-source libraries can only be leveraged for development specific to this proposed IaaS platform. Continuous deployment and improved security will be intrinsic to application design, given the blockchain communication framework and the potential of large open-source community of libraries immediately available to all developers.

5. The Platform's Potential

This section discusses some potential applications and additions to the IaaS platform and discusses how each problem identified in the introduction was addressed. Recall that this architectural design requires creating an application for all operating systems to interface with VPCs. As a result, users are no longer constrained by any single enterprise operating system, and applications can be developed that are much more secure, scalable, and usable. This blockchain template has the potential to be implemented for a wide array of applications, including decentralized enterprise applications like supply chain management or for creating agreements using smart contracts. Similar to how this platform provides a standard for identities, which allows the digital ownership and trading of monetary and physical assets, it also has the potential to provide a standard for centralizing medical records and other private documentation between different authorized organizations. Despite the wide array of applications, there are still many additions that should be made to the platform.

5.1. Future Additions

First, a fundamental addition to this IaaS platform must be a complete operating system. While its architecture and some fundamental protocols have been defined by this paper, a more complete design is needed for a complete enterprise solution. Namely, more 1st party applications must be developed to provide a greater variety of features to the user. Another potential future addition could be creating a more efficient architecture by shifting towards distributed computing to provide on-demand resources rather than provisioning dedicated resources that can start, stop, and time out. Lastly, this technology has tremendous potential in IoT.

5.2. Internet of Things

Incorporating IoT into the intrinsic structure of the platform will leverage the generalized communication blockchain template for a secure, partially decentralized IoT communication platform. IoT devices would share data with a VPC in real-time, providing a central location for individuals and organizations to manage their devices. Additionally, the IoT platform could be extremely flexible and be configured to utilize a variety of communication mediums, including the discussed publish/subscribe Hyperledger Fabric mechanism.

5.3. Related Products

This section will explore two alternative products. First, Amazon Web Services provides a comprehensive cloud computing solution, is currently one of the most popular platforms, and provides scalability, security, and redundancy. However, Amazon Web Services is mainly targeted towards businesses and developers since it is not usable without technical knowledge. Another extremely popular IaaS platform is Microsoft Azure, which provides a public cloud infrastructure for deploying and building applications. This technology is currently the farthest along in providing a singular deployment platform but is currently limited by its reliability. The shortcomings of these two technologies demonstrate why a complete IaaS solution is needed.

6. Summary

In summary, this modular solution provides a secure, high-speed infrastructure with native continuous deployment, development, and integration, which is easily extendable by programmers through the open-source development community. This infrastructure will allow new software to be immediately integrated into existing applications and will facilitate the development process by providing a single deployment platform. It will leverage Quorum and Hyperledger Fabric blockchain technology to provide a generic framework for transactions and communications. Both consumers and businesses, ranging from farmers to large corporations, will be able to reap the direct benefits of this blockchain-based networking technology through its various applications, such as in IoT, finance, or supply chain management. Finally, the proposed platform will help create a set of standards for development, enterprise networks and blockchains, and cloud computing.

References

1. [Xu19] X. Xu, "Architecture for Blockchain Applications," Springer, 2019, 9783030030346, MOBIUS, http://searchmobius.org/iii/encore/record/C__Rb34931288__SArchitecture%20for%20blockchain%20applications__Orightresult__U__X6?lang=eng&suite=cobalt
2. [Laurence19] T. Laurence, "Blockchain for Dummies," John Wiley & Sons, 2019, 9781119555018, MOBIUS,

http://searchmobius.org/iii/encore/record/C__Rb35247401__SBlockchain%20for%20dummies__Orightresult__U__X6?lang=eng&suite=cobalt
3. [Cloud19] "Virtual Private Cloud vs. Private Cloud: What's the Difference?", an article describing the impact of virtualization for private clouds, https://symmetrycorp.com/blog/virtual-private-cloud-vs-private-cloud-whats-difference/
4. [Laberis19] B. Laberis, "What Is the Cloud?", O'Reilly Media, 2019, 9781492052906, O'Reilly Safari, https://www.oreilly.com/library/view/what-is-the/9781492052913/
5. [IaaS19] "SaaS vs PaaS vs IaaS: What's the Difference and How To Choose," a webpage detailing the architectural differences between IaaS and other types of platforms, https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/
6. [Hyperledger19] "Hyperledger Fabric - A Blockchain Platform for the Enterprise," the documentation for Hyperledger Fabric, https://hyperledger-fabric.readthedocs.io/en/release-1.4/
7. [Quorum19] "Quorum," the documentation for Quorum, https://github.com/jpmorganchase/quorum/
8. [Quorum18] "Introduction to Quorum: Blockchain for the Financial Sector," the usage of Quorum in the financial industry, https://medium.com/blockchain-at-berkeley/introduction-to-quorum-blockchain-for-the-financial-sector-58813f84e88c
9. [Byzantine17] "Byzantine Fault Tolerance: The Key for Blockchains," Byzantine faults and requirements for specific blockchain networks, https://www.nasdaq.com/articles/byzantine-fault-tolerance-key-blockchains-2017-06-29
10. [Raft14] "The Raft Consensus Algorithm," the GitHub page for Raft, https://raft.github.io
11. [Raft19] "Raft-based consensus for Ethereum/Quorum," Quorum's implementation of the Raft consensus algorithm, https://github.com/jpmorganchase/quorum/blob/master/docs/Consensus/raft.md
12. [Zupan17] N. Zupan, K. Zhang, and H. Jacobsen, "Demo: HyperPubSub: a Decentralized, Permissioned, Publish/Subscribe Service using Blockchains," Middleware, 2017, Pages 15-16, https://dl.acm.org/citation.cfm?id=3155018
13. [IEEE19] "IEEE Blockchain," current progress towards standardizing blockchain, https://blockchain.ieee.org/standards

List of Acronyms

- Virtual Private Network (VPN)
- Virtual Private Cloud (VPC)
- Virtual Machine (VM)
- Infrastructure-as-a-Service (IaaS)
- Internet of Things (IoT)

Last Modified: December 10, 2019
This and other papers on latest advances in computer networking are available on line at http://www.cse.wustl.edu/~jain/cse570-19/index.html
Back to Raj Jain's Home Page