Business and Technology Drivers for Decentralized Cloud Systems

A major technological advance in the computing industry has been the adoption of cloud system models. The US National Institute of Standards and Technology (NIST) defines cloud computing as:

> *[A] model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.*[1]

But what is the frontier of the current cloud systems model and its offerings, and how can the present cloud model mature to address continued access, security and privacy challenges? These challenges are the drivers for extending the boundaries of the current cloud model to conform to and mitigate industry and technological pressures.

In the competitive business market and with fast-moving technology advancements, cloud providers must respond to and comply with cost management, security and performance burdens placed on various business stakeholders due to the shortcomings of the classical centralized cloud model. This has led to the birth of a new derivative of centralized cloud systems: decentralized cloud systems.

Prior to the cloud, organizations had to commit to large investments in computing infrastructure, applications and extensive IT operations. The first phase of the cloud evolution (cloud 1.0) introduced Software as a Service (SaaS), which created a virtual place to store data and applications (apps), disrupting standard IT operations with à la carte business process applications built on virtualization with no upfront investment. Then, cloud 2.0 disrupted the IT infrastructure of application development with offerings of Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). Cloud 2.0 allowed organizations to take control of their data and introduced services such as big data, artificial intelligence (AI) and machine learning (ML), along with development concepts such as containerization.[2, 3]

Emerging cloud 3.0 technologies will be driven by the ability to compute anywhere and will use a scale-and-adapt approach. Cloud 3.0 will disrupt application development in organizations across all industries. It will be based on building high availability and decomposing software into loosely connected subcomponents called "microservices."[4, 5] It will lead to organizations adopting and migrating to the decentralized cloud.

A *Forbes* article notes that:

> *[The decentralized web] has led to the rise of distributed apps or decentralized apps (Dapps) where there will be no single point of failure and no central authority. They are transparent, have a greater level of encryption, have better heuristic methods to secure and are completely trustless.*[6]

ROBERT PUTRUS | CISM, CFE, PE, PMP

Is a professional with senior management experience in the areas of IT, cybersecurity, regularity and internal controls compliance, managed services, global transformation programs, portfolio and program management, and IT outsourcing. He has published many articles and white papers in professional journals, some of which have been translated into multiple languages. Putrus is quoted in publications, articles and books, including those used in Master of Business Administration programs in the United States. He can be reached at *https://www.linkedin.com/in/robert-putrus-cism-pmp-cfe-pe-8793256/.*

Decentralized cloud systems are enabling the reconfiguration of the Internet to create a distributed global system that is less dependent on web platforms and data centers.

One of the most significant benefits of the decentralized web is the ability to access data from anywhere. One example of decentralized cloud computing is blockchain technology.

Blockchain

Blockchain is a decentralized system that stores data across multiple networks of computers. Blockchain applications are used in recording and storing transactions for cryptocurrencies. Blockchain can be applied to cryptocurrency, cybersecurity, accounting and record keeping, supply chain and healthcare.

A blockchain network is a technology infrastructure that is distributed and uses digital ledger technology to encrypt, track and secure all transactions on the network. Blockchain networks are immutable, meaning every transaction and record that is transmitted over a blockchain network is unable to be changed, altered or edited.[7]

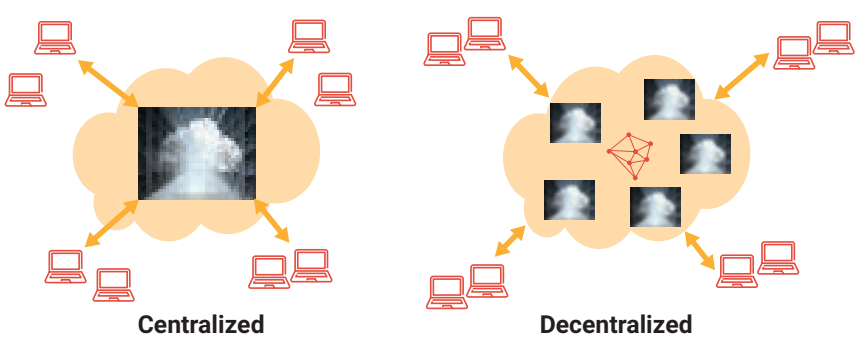
In a decentralized blockchain network, no user has to know or trust any other user. Individual members on the network have a copy of the exact same data in the form of a distributed ledger. If a member's ledger is altered or corrupted in any way, it will be rejected by the majority of the members on the network.

LOOKING FOR MORE?

- Read *Certificate of Cloud Auditing Knowledge Study Guide. www.isaca.org/CCAK-Study-Guide*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's *https://engage.isaca.org/onlineforums*

FIGURE 1

Centralized vs. Decentralized Cloud Systems



Drivers of the Decentralization of Cloud Systems

The current cloud offers several advantages to organizations such as integration of centralized information systems, ease of access and cost effectiveness in investing and managing evolving technologies.

However, centralized cloud systems face major issues, most notably privacy and security. Centralized cloud systems are maintained by third parties that transfer and store data. The centralized cloud is vulnerable to several security threats such as malware, ransomware and man-in-the-middle (MitM) attacks.

Therefore, the market is witnessing a movement toward a decentralized cloud that supports multiple user access and ensures data security at the same time (**figure 1**). In a decentralized cloud system data are stored on multiple computers or on the entities taking part in the decentralized cloud. Data are encrypted, fragmented and then distributed across multiple hosting nodes (computers) worldwide.

The drivers of decentralized cloud systems relative to business and technology are privacy and security. Decentralized cloud systems are enabling the reconfiguration of the Internet to create a distributed global system that is less dependent on web platforms and data centers. The adoption of the decentralized cloud accelerated with the increase in remote work.[8]

The goal is to build a better Internet for the sake of creating automated services.

Data Privacy Concerns

Providers of centralized cloud services offer easy access to data and large data storage capacity. However, because only a small number of organizations control the major market share of cloud services, the risk to consumers includes price fixing, policy dictation, cyberattacks, loss of data and numerous privacy concerns.

Accessing data in a public cloud through the Internet introduces daunting uncertainties regarding where an organization's data are stored and by whom they are managed. There are also concerns about the lack of ownership and control when relying on third-party cloud service providers.

The primary function of decentralized cloud systems is to protect private and confidential data from unauthorized access and from transfer by

external parties. Organizations cannot compromise on privacy. As such, many organizations are contemplating the adoption of emerging technologies such as blockchain as a viable solution.

Unlike in a centralized cloud, in a decentralized cloud with decentralized storage systems, multiple copies of the data are created, which eliminates the risk of data loss if a site goes down.

Security Concerns

The adoption of cloud models by various entities such as governmental agencies and public and private organizations has led to the institution of various compliance regulations with requirements for compliance.

The IT industry presented the decentralized cloud for consideration as an alternative to current cloud systems. Most decentralized clouds are based on blockchain technology, which offers transparency and reliability through cryptography.

Decentralized cloud systems implement client-side encryption enabling increasing security, privacy and control over users' data.

With a centralized cloud and in a given hosted facility, data are stored in a centralized location. In a decentralized cloud, the data are stored on the distributed nodes to ensure redundancy and avert server failure. In addition, the suspension of accounts and denials of services are significantly reduced. This eliminates a single point of failure and service interruption. Decentralized cloud systems store data in multiple computers connected through decentralized peer-to-peer (P2P) networks. These networks enable quicker data transfer in a decentralized cloud through nearby peers rather than through the servers hosted in a physical location.[9]

In a decentralized cloud, all data are encrypted. In addition, data are split and distributed over vast computers/nodes. It is close to impossible for any single node to access what is being stored on a decentralized computer network.

The Outlook for Decentralized Cloud Systems

Cloud computing and cloud storage have created many opportunities for organizations to save costs, increase security, increase flexibility, increase mobility, and enhance disaster recovery. However, the cybersecurity threats presented by a centralized cloud architecture have forced technologists to react to market demands for more robust protection. Some threats impact the core processes and foundations of data integrity, accountability, privacy, access control, authentication and authorization. Cloud decentralization is a solution that addresses the fundamentals of data privacy and security.

Blockchain has transformed the classical cloud architecture to create a market opportunity for more robust and predictable cloud outcomes with the implementation of an encryption algorithm. It complies with the market demand for assurance for data confidentiality, security and resilience concerning the cloud. In addition, blockchain technology, with its distributed ledger, enables many applications to ensure redundancy, confidentiality and transparency.

Making a comparative analysis of centralized vs. decentralized cloud systems may help organizations determine whether they can quickly adopt the new cloud model or if it makes more sense to stay with their current model. **Figure 2** illustrates an example comparison; however, the comparison can be amended based on similarities or differences in the attributes of both systems.

It is close to impossible for any single node to access what is being stored on a decentralized computer network.

Limitations of Decentralized Cloud Systems

Despite its potential, a decentralized cloud does have limitations. There are a number of challenges that need to be addressed, including:

- The technology is relatively new and will require time for adoption.
- Because the technology is relatively new, users may encounter problems when attempting to integrate multiple applications (and their data dependencies) in decentralized cloud systems.[10]
- A decentralized cloud lacks accountability for lost data or misplaced transactions.
- There is not a guarantee of privacy and security. A decentralized cloud will be a target of malicious actors who will form malicious nodes and execute hub attacks.

FIGURE 2

Comparative Attributes of Centralized vs. Decentralized Cloud Systems

Category	Centralized Cloud	Decentralized Cloud
Architecture	It provides scalability to infrastructure.	It provides scalability to infrastructure.
	Infrastructures have the entirety of data and resources stored in one geographical location.	Infrastructures have data and resources stored in a variety of different geographical locations.
	Networks are built based on traditional networks (i.e., data transmission takes place through a central server, becoming slow at the peak times).	Most infrastructures are built based on blockchain networks. Peer-to-peer technology is used to decentralize storage.
	Infrastructure requires that the enterprise trust the administration of the cloud provider because it is a centralized computer architecture.	No individual user has access to more permissions than another on a blockchain network. It is a distributed computer architecture.
	It relies on and trusts central providers.	No one has to know or trust anyone else. Decentralized clouds are based on blockchain, which offers transparency and reliability through cryptography.
Performance	The speed of data transfer relies on the servers hosted in a physical location, among other factors.	The speed of data transfer is higher in a decentralized cloud because it is based on peer-to-peer communication.
	It may impose capacity constraints and tends to have higher costs.	It is more cost effective because computing power and storage are not finite.
Security-General	A variety of security concerns include unauthorized access, malicious insiders, cyberattacks and insecure interfaces. It is also susceptible to data loss due to outages and has a single point of data failure.	Blockchain technology infrastructure is distributed and uses digital ledger technology. It is more resilient to outages due to geographical redundant technology.
Security-Cyberthreats	Data are susceptible to cybersecurity threats.	Security measures are inherited from the blockchain networks based on decentralized cloud computing infrastructures.
Security-Data Privacy	Data are not always encrypted.	Data are encrypted both in transit and at rest.
	Data can be encrypted using encryption software before being uploaded to the cloud. Data stored in the cloud are mostly encrypted.	Data are stored in a variety of geographical locations (geo-redundancy). Each piece of a data file is encrypted separately.
Security-Data Integrity	For redundancy, a multicloud solution that replicates data across multiple cloud computing providers can be used.	Geo-redundancy is the practice of storing data across a variety of locations.
	Physical integrity of the data is ensured due to physical security controls used at the cloud center. However, malicious insiders are a risk.	Data cannot be changed or edited by other users intentionally, in a malicious manner or by mistake.
	Computing infrastructures are easily affected by geographical outages or disasters.0	Cloud computing replicates resources and data across different locations automatically.
Cost Model	The cost model is scalable, easy to use and pay-as-you-go.	The cost model is scalable, easy to use and pay-as-you-go.
Use	It is the most widely used and accepted infrastructure.	It is less utilized by consumers and enterprises. Adoptability and acceptance are on the rise given the number of benefits that come with the decentralized cloud and its ability to protect and secure data.

- Compliance with laws and regulations is needed. A decentralized cloud requires a high degree of central support and monitoring to substantiate the evidence of IT controls.
- Developers are addressing rising performance-related challenges. For some, when data are dispersed across many storage devices, performance can be volatile.
- Users need to overcome the lack of trust when using P2P technology, bypassing centralized regulatory authorities.
- Security assurance continues to be a concern.

Conclusion

Decentralized systems change the game when it comes to cloud technology. They are a derivative of the current centralized cloud systems, but they offer a remedy for lack of data ownership and control, data breaches and security risk, increasing storage costs and low transmission speeds. Data privacy and data security are the main concerns when using centralized cloud systems, but in a decentralized cloud, data are more secure and kept private, file loss and data loss are diminished, download speeds are quicker, and it is easier to transfer files. In addition, in a decentralized cloud, there is no single point of failure, which increases reliability and redundancy in the event of failure.

For example, the transactions of digital currency are verified and the records are maintained by a decentralized system using cryptography rather than by a centralized authority. Cryptography provides secure communication techniques for the recipients in the presence of malicious adversaries.

The business demand for secure and inexpensive storage technology has paved the way for organizations to invest in and build momentum for decentralized cloud adoption, and blockchain has been a major factor in this change.

However, there are several challenges when integrating decentralized cloud systems,[11] including technology design and the need to further assure enterprises that privacy laws and IT security of the cloud can be guaranteed. The use of peer-to-peer communication in a decentralized network lacks accountability for lost data.

Decentralized cloud computing may present the solution to the challenges of the centralized cloud; however, the technology is still in the development stage and it may take several years to fully mature and be accepted by enterprise users.

The business demand for secure and inexpensive storage technology has paved the way for organizations to invest in and build inertia for decentralized cloud adoption.

Endnotes

1 Mell, P.; T. Grance; Special Publication (SP) 800-145 *The NIST Definition of Cloud Computing, National Institute of Standards and Technology (NIST)*, USA, September 2011, *https://csrc.nist.gov/publications/detail/sp/800-145/final*

2 Fu, T.; "Top Three Challenges to Cloud 3.0," The New Stack, 20 May 2020, *https://thenewstack.io/top-3-challenges-to-cloud-3-0/*

3 IQVIA, "Evolution to Cloud 3.0 and Roadmap for Adoption," 12 August 2019, *https://www.iqvia.com/library/white-papers/evolution-to-cloud-30-and-roadmap-for-adoption*

4 *Op cit* Tu

5 *Op cit* IQVIA

6 Balanagu, R.; "The Evolution of Decentralized Cloud," *Forbes*, 23 February 2022, *https://www.forbes.com/sites/forbestechcouncil/2022/02/23/the-evolution-of-decentralized-cloud/?sh=37f381f03bcc*

7 Liu, W.; "Research on Cloud Computing Security Problem and Strategy," Institute of Electrical and Electronics Engineers (IEEE) 2nd International Conference on Consumer Electronics, 17 May 2012, *https://ieeexplore.ieee.org/document/6202020*

8 Beatrice, A.; "The Time Is Ripe for Companies to Adopt Decentralized Cloud Storage," Analytics Insight, 23 April 2021, *https://www.analyticsinsight.net/the-time-is-ripe-for-companies-to-adopt-decentralized-cloud-storage/*

9 Arcana Network, "How Does Decentralized Cloud Storage Work?" *Medium*, 8 September 2021, *https://medium.com/arcana-network-blog/how-does-decentralized-cloud-storage-work-a4f36fe7dddc*

10 Müller, A.; A. Ludwig; B. Franczyk; "Data Security in Decentralized Cloud Systems—System Comparison, Requirements Analysis and Organizational Levels," *Journal of Cloud Computing*, 28 June 2017, *https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-017-0082-3*

11 Haritonova, A.; "Decentralized Data Storage: Pros, Cons and Prospects," Pixelplex, 16 August 2021, *https://pixelplex.io/blog/decentralized-storage/*