Raritan®

A brand of legrand®

BlockOps:
Getting Your Blockchain Infrastructure Off to the Right Start

A White Paper by Raritan

Introduction

Blockchain is a promising technology for many markets. With the decentralized network of trust that blockchain enables, large numbers of stakeholders can engage in secure data exchanges, financial transactions, and other multi-party business processes without depending on centralized clearinghouse authorities—which can add cost, friction, and a potential single point-of-failure to markets where agility and stakeholder sovereignty have become increasingly desirable.

These enticing new possibilities are leading companies in diverse markets from finance and healthcare to transportation, and consumer products to launch blockchain pilot initiatives.

But like all digital technology initiatives, blockchain isn't just about software. It's also about hardware. To pilot your blockchain initiatives appropriately, you must provision your infrastructure resources to both support those initial pilots and lay the foundation to perform at scale if, and when those pilots lead to live, competitively critical production implementations.

That's why, in addition to considering the business implications of your emerging blockchain trials, you also need to think about the implications of blockchain for your data center infrastructure.

*This notion of best practices for operation of the infrastructure that supports your organization's blockchain participation — or **"BlockOps"** — is integral to blockchain success.* And, based on the experiences of early adopters, the following three sets of BlockOps best practices are already surfacing.

BlockOps Best Practice #1: Capacity and Density Planning

Anyone following the blockchain hype cycle is well-aware of the intense compute and energy requirements associated with Bitcoin and other cryptocurrencies that first put blockchain on the map. These intense infrastructure requirements are driven by the so-called Proof of Work "mining" activities that require participants seeking to add to their cryptocurrency holdings to solve highly complex cryptography problems that demand massive CPU cycles.

Commercial blockchain applications will differ significantly from cryptocurrencies — and thus are not likely to require anything quite as compute-intensive as Proof of Work mining. They will, however, require intense compute activity for the hashing and cryptography necessary for establishing and maintaining trust across blockchain networks.

Some blockchain networks require mechanisms similar to Proof of Work that make it computationally impractical to attack trust across a broadly distributed blockchain. Others are moving to Proof of Stake or Proof of Authority models. In private blockchains, central authorities may maintain trust for participant identities — while retaining the distributed ledger model for tracking transactions themselves.

Regardless of which model a particular commercial blockchain application may take, compute-intensive cryptography will be key to success, because 1) the basic mechanism of trust in such networks is the creation of hashes for each new block and 2) blockchains keep getting longer over time.

The hardware capacity necessary to support commercial blockchain applications with high transaction volume over an extended period is still unclear. But it is likely to be significant, so if your organization is planning to get involved in one or more blockchain initiatives, it is critical to not underestimate:

- The **capital cost** (or opex, if obtained under an IaaS model) of compute, I/O, and storage capacity required for blockchain participation over the long term.
- **Associated opex costs** such as energy, cooling, and floor and rack space.
- **Other ownership costs** such as systems monitoring, more aggressive OS patching, log capture, systems troubleshooting, etc.
- Additional **network and processing capacity** for interfacing blockchain applications with existing enterprise applications, such as back-end ERP systems of record.
- **Highly variable power consumption** by CPUs required to handle intense peaks in cryptographic computation.

We are all going to learn more about precise requirements for capacity and cost in these areas as commercial blockchain applications become more commonplace — and as the industry settles on an increasingly standardized set of hashing and cryptographic models. But whether we deploy our blockchain infrastructure on-premise, in the cloud, or under some hybrid model, we should not minimize its total cost of ownership of the long term.

BlockOps Best Practice #2: Infrastructure Segmentation

DevOps arose to address a major problem in the relationship between developers and infrastructure operations. Business stakeholders and development teams were working together to create new applications and application updates at a faster pace — and then just threw the resulting code "over the wall" to operations. This created a variety of problems, including technical snafus in the deployment of new code in production, slower time-to-benefit, and unexpected infrastructure costs.

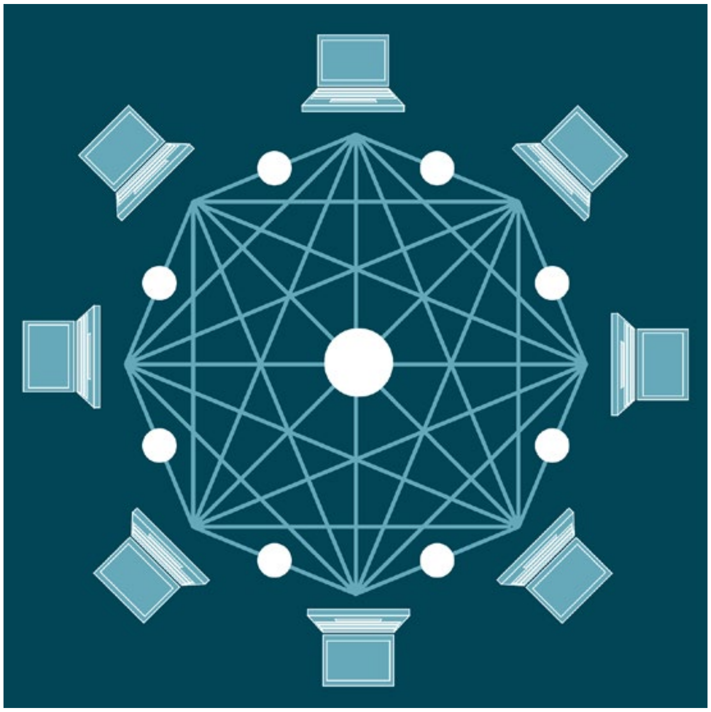
DevOps addresses this problem by improving collaboration between developers, QA staff, and operations teams, and by streamlining the process by which ideas become code live applications in production.

Similar issues emerged as technologies such as analytics, machine learning, and AI became more popular. Here again, business stakeholders and data science professionals often moved forward enthusiastically without fully considering infrastructure implications — which can be considerable when pulling together enormous volumes of disparate data, applying sophisticated algorithms to that data, and then delivering equally sophisticated visualizations of the results. To address these issues of performance at scale, organizations adopted collaborative disciplines similar to DevOps — sometimes referred to as "DataOps" (for Big Data processing) and/or "AIOps" (for supporting intensive algorithmic processing of that data).

The same pattern is continuing with blockchain. Business stakeholders and blockchain technology SME's have already begun to pilot emerging use-cases — but rarely if ever include infrastructure operations staff in those early-stage discussions.

In part, this may be because best practices such as server and storage virtualization have "spoiled" the business by enabling flexible allocation of capacity for traditional applications as needed on-demand. But blockchain behaves very differently from both traditional deterministic applications and the new wave of non-deterministic AI/machine learning systems. This is why BlockOps is now necessary.

For example, because blockchain applications often depend on real-time responses to hashing requests for new transactions, even the smallest micro-cut or other instability in server power may interrupt a critical cryptographic process at the exact wrong time. To address this potential problem, blockchain infrastructure may require the use of uninterruptible power supplies (UPSs) in a way that other infrastructures do not.

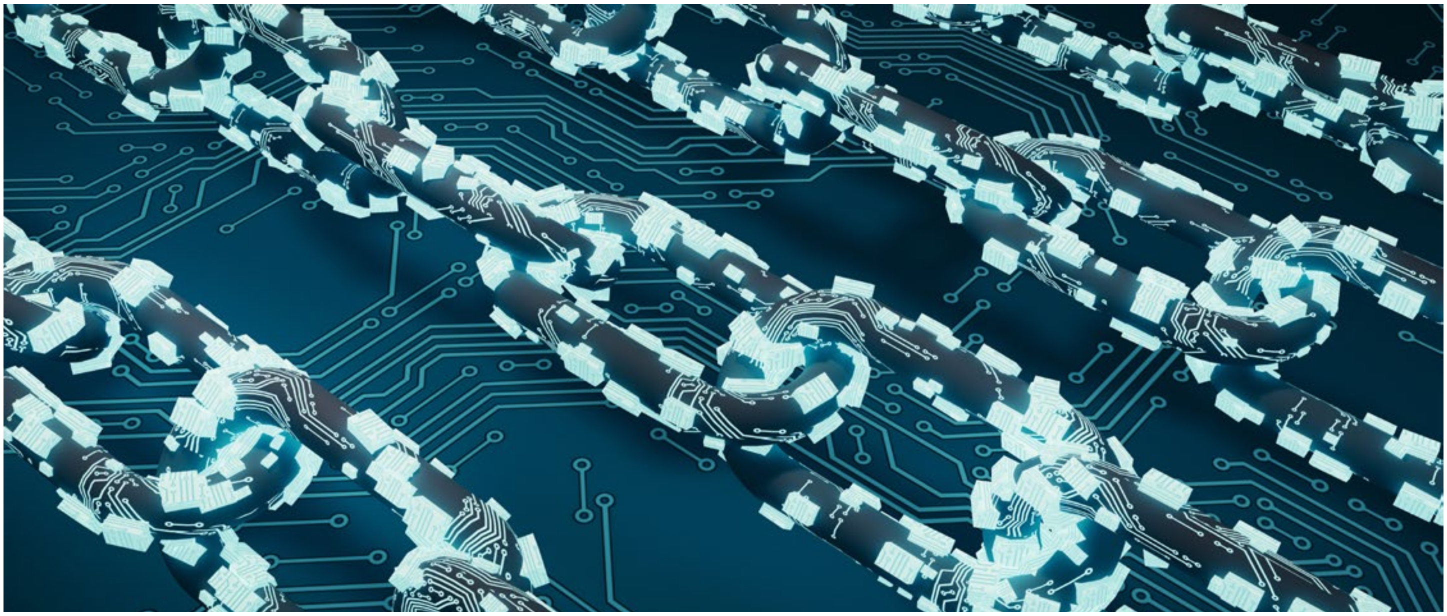


Particularities such as these suggest that — in addition to being included in discussions about potential blockchain initiatives as early as possible — infrastructure ops leaders also fully segment blockchain pilots on separate purpose-specific racks.

This segmentation provides multiple benefits, including:

- Clear visibility into the unique behaviors and workload characteristics of blockchain applications.
- The ability to experiment with blockchain-specific infrastructure configurations — including specialized CPUs, cooling, power supplies, and energy metering.
- Avoidance of adverse impacts of experimental (and potentially volatile) blockchain infrastructure behaviors on other business applications.

In the early days of Bitcoin, no one expected that cryptocurrency mining would wind up consuming as much electricity as the entire country of Ireland — and that, left unchecked, it could reach an astounding 7.7 gigawatt worldwide. Similarly, enterprise IT ops teams don't want to get caught by surprise when it comes to cost and capacity. So segmented blockchain infrastructure "sandboxes" are essential.



BlockOps Best Practice #3: Governance and Audit

The unknowns you face as your organization begins piloting blockchain go beyond performance, reliability, and cost. There are also serious security and compliance issues to consider — as well as the integrity of the data center itself.

From a security perspective, blockchain is still largely untested and unproven. Compute-intensive Proof of Work requirements are certainly a deterrent against distributed denial of service (DDoS) attacks, but that doesn't make blockchain hack-proof. On the contrary, high-profile cryptocurrency thefts have already shown that blockchain applications are as vulnerable to flawed coding and inadequate identity controls as any other type of software.

Also, the interest of cybercriminals and malicious state actors in blockchain is likely to rise as the technology becomes more widely utilized — since the rewards for hacking non-cryptocurrency blockchain applications are still rather limited. As utilization rises and the stakes get higher, more sophisticated attacks will be almost certain.

From a compliance perspective, regulatory agencies are already demonstrating serious concern about blockchain. Without a centralized point of control, blockchain applications pose new challenges for compliance auditors. Many blockchain variants, in fact, enable the kind of anonymity and/or identity masking that facilitates regulatory bypass.

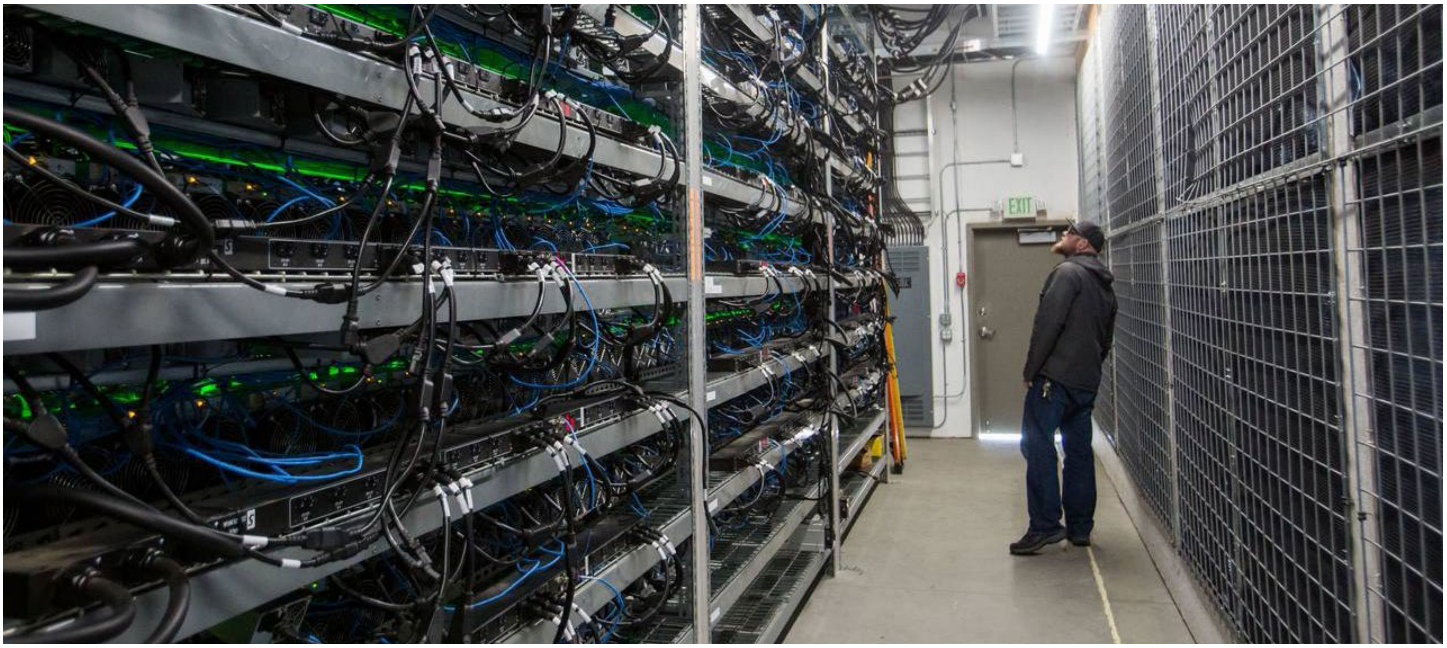
Due to this potentially heightened possibility of malfeasance, regulatory agencies may impose particularly stringent audit requirements on blockchain participants — especially in highly regulated industries such as financial service and healthcare.

Rigorous auditing of blockchain activity is not only necessary for regulatory compliance. Internal governance mandates also make it important to maintain ongoing real-time and historic visibility into blockchain-related infrastructure activity. This visibility is necessary to mitigate the risk of inadvertent human error, to understand the real cost of blockchain participation, and to develop replicable best practices for continuously driving down cost and risk as the business engages in a growing number of different blockchains.

For these reasons and others, blockchain governance and audit best practices include:

- **Robust capture** of all blockchain-related system activity logs and related audit data.
- **Rack-level physical security** and logging of all remote and hands-on staff maintenance activities.
- **Use of analytics and/or data science methods** to detect trends and anomalies from behavioral baselines.
- **Blockchain-specific escalation procedures** to alert IT, business, and risk management stakeholders about potentially noteworthy events and trends.

It is worth noting that all these governance and audit best practices are in large part supported by the previously suggested best practice of infrastructure segmentation.



High density Raritan PX2 PDUs with dual inlet and 10kAIC circuit breaker per outlet with metering and switching, deployed in a high density crypto-mining facility in the United States.

A BlockOps Action Plan for Data Center Managers

The above three best practices offer some initial guidance regarding how data center leaders can best support their organizations' foray into blockchain. However, even before those forays are piloted, there are several steps you can and should take to make sure you're in a position to optimally contribute to your organization's blockchain initiatives:

1) Educate yourself now. Blockchain is a rapidly evolving technology category. At the very least, you should become knowledgeable about its basics. Just remember that you want to learn about commercial blockchain applications and their emerging use-cases — not cryptocurrency mining per se.

2) Get in the conversation. If there are already discussions about blockchain going on among business executives and IT innovation leaders, you need to get involved now. The hard-won lessons of DevOps, DevSecOps, AIOps, and the like is that digital initiatives always run more smoothly when infrastructure managers have a seat at the table from the get-go. Explain to your company's blockchain leaders that BlockOps is essential for successful pilots and reliable, cost-efficient long-term blockchain participation.

3) Plan and provision your blockchain sandbox early. Another lesson of DevOps and related disciplines is that infrastructure can't be the "Department of No" that chronically poses an impediment to digital initiatives. To avoid this, appropriately prioritize the implementation of blockchain infrastructure to get ahead of the curve. Otherwise, you could lose your seat at the blockchain planning and strategy table.

4) Stay connected. When technology trends hit, they hit fast and hard. We've seen it happened repeatedly — with PC LANs, with the web, with mobility, and with AI. So regardless of how you personally feel about blockchain and its utility for your business, keep your eyes on the trendlines. Also stay connected with peers and vendors who can share lessons learned as the technology continues to evolve at a rapid pace.

Blockchain offers a lot of possibilities when it comes to transactions and interactions between businesses. It may even change the way data center infrastructure itself is bought and leased between enterprises and multiple cloud providers — as well as the way data center managers purchase energy within microgrids.

So, don't wait until a blockchain initiative lands on your desk before you get up to speed on it. Get educated and involved now so you can successfully meet your organization's needs in the future — and not have your work life turned upside-down in the process.

Lessons from Cryptocurrency

Cryptocurrency is a special use-case for blockchain that typically attempts to create an alternative to national fiat currencies. Corporate blockchain initiatives are more focused on enabling ecosystems of trust for transactions, supply chains, smart contracts and the like without depending on a central clearinghouse.

However, because the most intense and large-scale implementations of blockchain to date have been associated with cryptocurrency, it's worthwhile to take note of the BlockOps challenges cryptocurrency participants have faced. A few examples include:

- **The importance of remote power control.** Highly unstable cryptomining workloads have often led to peak workloads that caused CPUs and GPUs past their technical tolerances. Cryptominers learned about the importance of implementing PDUs that enable remote shut-down and reboots to protect hardware and ensure business continuity without having to wait for a technician to get to the rack.
- **Outlet-level metering.** In the case of co-lo hosting, chargebacks for high power consumption can be a shock to both the service provider and the customer. Credible outlet-level metering is a necessity — as is the ability to correlate spikes in consumption with associated spikes in blockchain activity that may cost-justify additional energy costs.
- **Re-thinking business continuity.** With traditional applications, ops teams tend to think in terms of failovers and/or the backup of data and code — which essentially exist independent of each other and can be reconstituted as needed. With blockchain, data cannot actually be "lost," since it is replicated everywhere. Instead, it is encryption key management that must be thoroughly protected and/or reconstituted. Otherwise, there is no way to regain access to the blockchain.

About Raritan

Raritan began developing KVM switches for IT professionals to manage servers remotely in 1985. Today, as a brand of Legrand, we are a leading provider of intelligent rack PDUs. Our solutions increase the reliability and intelligence of data centers in 9 of the top 10 Fortune 500 technology companies. Learn more at Raritan.com