TechTips Newsletter

tech hero

Insider Tips To Make Your Business Run Faster, Easier And More Profitably

August 2018

This monthly publication provided courtesy of Richard Lynn, VP Sales & Marketing, Tech Hero

Our Mission: To build a community of successful minded entrepreneurs that inspires excellence, encourages collaboration and expands the capacity of all members to achieve great things.

Blockchain 101: All you need to know about this red-hot technology

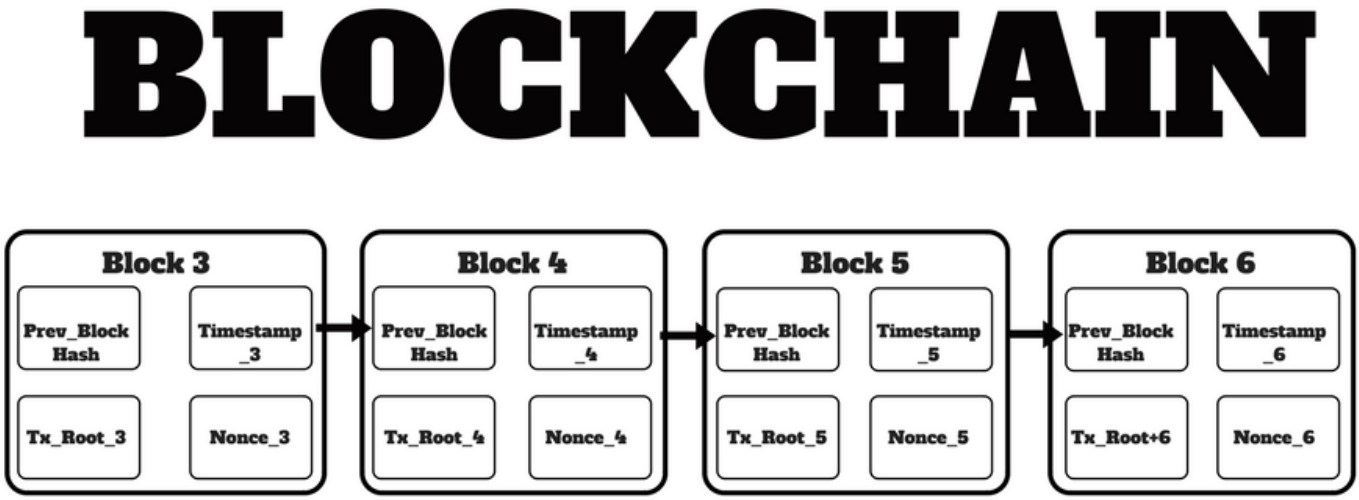
Blockchain is the newest and hottest trend sweeping the world of technology today. Yet, many are unaware of what this new technology is, and what it means for us. In its simplest form, blockchain is a collection of pieces of data that's stored and ordered in a way that makes it almost impossible to tamper with and ideally suited for various data jobs in applications across any industry. While the technology is being adopted at breakneck speed, many are still confused about what exactly blockchain is. This blockchain 101 primer is for them.

Blockchain 101: The 'chain' in blockchain

Core to the idea of blockchain is the idea of, well, the chain. A blockchain is nothing but a string of data that is continuously added to with new pieces of data as transactions occur. Each new piece of data shows progress over time. Just as a physical chain has links, blockchain is made up of many data links in chronological order. Each link relates to the link prior to it.

The advantage is that you can go back into the history of a blockchain and see how it progressed from the first, or "genesis," block. For this model to work it's necessary for each link in the chain to be tamper-proof. This goes back to the concept of immutability. As the saying goes, a chain is as strong as its weakest link. This is true in the case of blockchain, and the good news is that there are no weak links in blockchain. Each piece of data can be completely relied on as a source of truth. Not even a system administrator can go in and manually mess around with the links in the chain.

Data distribution in blockchain



Blockchain is based on a concept called Distributed Ledger Technology (DLT). According to this, data is stored in a distributed manner — meaning that it is stored across multiple peer hosts, and isn't stored centrally. This is a new trend in data storage that has been taking over the world of databases for a couple of years, and blockchain is perhaps the most advanced implementation of distributed data storage.

The advantage of storing data in a distributed architecture is manifold. First, it is secure. If any single node on the network is compromised, there exists an exact copy of its data elsewhere on the network that can be tapped. You can always find the source of truth by comparing conflicting versions of data. In this way, it prevents data loss. Also, when it comes to performance, there's freedom for individual nodes in the network to fail and still rely on other nodes that have the same data. This way the system perform at peak levels as it's not dependent on any single node. The key is to have pieces of data stored randomly across many nodes. This way, together, the nodes always have a complete copy of the data, but alone, none have a complete copy of the data.

Immutability in blockchain

Blockchain data is stored as a ledger. It is a record of transactions and pieces of data that once recorded can't be altered. It functions as the source of truth for the data it records. In this sense, it follows the concept of immutability. This again has been finding strong adoption in the world of computing. Rather than having system components that are continuously modified, the modern paradigm has been to shift toward immutability.

This means that when there's new data added, it gets its own unique and new storage space that's independent from neighboring and previously existing data storage units. This way there's less "drift" — a problem of a component becomes something completely different over time because of constant updates. Immutability lets a system change in a way that's easy to track changes over time. You can always go back into the history and view exact updates separate from the pre-existing condition of the rest of the system.

Bitcoin as proof of blockchain

The best and most widely used example of blockchain in the wild is bitcoin. It is the most popular cryptocurrency today. Many believe it is the future of the financial system while others don't see it becoming mainstream, and are waiting to hear news of its bubble popping. Irrespective of where you fall in this spectrum of reactions toward bitcoin, it pays to acknowledge it as a tectonic change not just in the financial sector, but further, in the world of IT and software delivery as well. This is because of it using blockchain as its core technology. Blockchain is a revolution that's hit core IT practices like data management, and data security.

All transactions in blockchain are publicly accessible. However, the details of the transaction are encrypted. What's publicly viewable is cipher-text. To view the details of the transaction you need a public access key and a private key. It becomes important to handle these keys in a secure manner. The onus of this is on the end user.

The benefit of having publicly viewable transactions is that they can always be used to verify the authenticity and historical record of a blockchain. This brings improved security as fraudsters, if any, will be exposed publicly. Any attempt to fraud will be attached to the identity of a user. In this situation, reputation becomes a prerequisite to conducting business in the world of bitcoin and blockchain.

Security risks of blockchain

Despite having a strong model for data management and an architecture built for end-to-end security, blockchain is not without risks. Indeed, the most vulnerable part of blockchain is where humans interact with the system. Users add new data to a blockchain from their devices that are connected to the network. Endpoint security is key to blockchain.

Blockchain suffers from the traditional IT risks of hacking and mismanagement of access and data. A device in the wrong hands can be used to manipulate blockchain. Passwords and access keys that are accidentally shared can be misused.

A paradigm shift

Blockchain is a paradigm shift in the world of technology and computing. It brings together many bleeding-edge concepts in computing such as distribution, and immutability. It is architected to be fool-proof. This doesn't mean it is a perfect system — no system that involves human interaction can be perfect. But with blockchain, this is the closest we've come yet to have the most secure and efficient system. This is already proved in the case of bitcoin. It's only a matter of time until blockchain finds applications in the world of health care, manufacturing, banking, retail, and more. Blockchain is about to set off a chain reaction. New bitcoin currency is generated every time a user, or "miner," solves a math puzzle to verify the authenticity of an existing blockchain.

vmware PARTNER

PROFESSIONAL SOLUTION PROVIDER

Free Consultation to review your VMware Licensing!

Contact your Tech Hero sales representative to schedule a FREE review of your VMware licensing.

Find out ways to save money, ways to receive free upgrades, and a better understanding on the VMware license models.

tech hero

1-(800) 900-8324 (option 2)

Sales@TechHero.com

Every time a transaction occurs in bitcoin, the transaction needs to be validated to check its identity and to ensure there are no "double spend" issues where the same currency is spent two times simultaneously.

Every time a puzzle needs to be solved for a blockchain, the puzzle has a difficulty score attached to it. The longer the history of a blockchain, the greater the difficulty of the puzzle. Each of these puzzles takes approximately 10 minutes to be solved. How they are solved is unique, too. Every puzzle is processed on numerous peer devices at the same time. This again follows the "distributed" model to ensure no single user bottlenecks the system and that resolution times are constant. It takes compute power and electricity to solve a puzzle. The greater the difficulty level, the more compute power and more time it takes to solve. The user who solves a puzzle is rewarded with a new block of bitcoin currency.

Client Spotlight

FLORIDA HOSPITAL

The skill to heal. The spirit to care.®

Our mission strengthens our commitment to health care. Because of our faith as part of the Seventh-day Adventist Church, we focus on healing the whole person–mind, body and spirit.

Would you like your company highlighted here in our "Client Spotlight"? Then give us a call today at: 1-800-900-8324 x8840.

You will be hit: Your small business guide for preparing a cyberattack response plan

A recent survey carried by Nationwide Insurance showcased something very odd. Of the surveyed small businesses, 63 percent said they have been attacked by cybercriminals. However, 79 percent of the respondents did not have any incident response process in place. Cybercrime is a harsh reality. It's not a question of whether you will be hit by a cyberattack, it's only a matter of when. Eventually, you will upgrade your security systems and make them robust enough to foil advanced hack-attempts. The critical question is — can you do it before the attack! Preparation is the only solution, and this guide to preparing a cyberattack response plan can help you avoid the pain.

Taking stock — Processes, datastreams, people, devices

The thing with cybercrime is – it'll follow the path of least resistance. Your business is as secure as your least secure application, process, data repository, or device. To build a robust and future-ready cyberattack response plan, start like a baby. Leaders of business' digital security programs need to start by taking stock.

- Leaders from each department must be a part — engage with them to enlist all business processes, product lines, and services provided.
- Get all the details about the different business process and the kind of data they create and the applications in use — and who uses them.
- Evaluate the compliance requirements you need to abide by, related to the nature of your data, the method of storing and sharing it, and know all the geographies you operate in, because each one may have different requirements for handling data breaches.
- All this information must be regularly upgraded, so that your business's internal risk management team or an external managed security service provider can build comprehensive risk mitigation plans.

Taking stock (continued) — Security resources

The next phase of your cyberattack response plan is to continue the stock-taking exercise. This time, though, the focus is on taking stock of the currently available security resources.

Corresponding to each disparate "unit" of information identified as relevant for the organization's security program, find out:

- The current methods of digital security in place.
- The number of people responsible for the security preparedness of the unit.
- The external resources (consultancy, managed services) available for the unit's security.

Apart from this, program leaders would do well to:

- Assign priorities and categories (as per criticality) to each unit.
- Challenge how risks are being anticipated, identified, and reported — today.
- Identify the impact of outstanding risk exposure, resulting from lack of adequate coverage.

At the end of this, leadership will be in a good position to evaluate how the organization is currently placed in terms of its readiness for cybercrime.

Build an incident response plan

The homework is now done. With highly contextual information available on the planning desk, it's time for security executives to devise an incident response plan. At this stage, watch out for a common mistake. Your business's security incident response plan should be tailored for your organization. Picking up a template and filling in the blocks, even with diligence and desire, is a questionable practice. In fact, to build yourself a highly relevant and reliable plan – that's why you invested resources in the first two phases — right?

Begin by reviewing the risks — regulatory, competitive, and financial. Talk about the responsibilities of external service providers, which is highly important in the context of the cloud-heavy digital services state that most businesses find themselves in. Ask — what are the current incident response policies, if any? How relevant are they? How often (and reliably) have they been tested?

All these efforts feed into your incident response plan. Here's more on how you can prepare a robust and reliable cyberattack response plan.

Part 1 — Detection

This part of the plan captures details of actions to be taken once an incident is identified. Must include:

- Proper guidelines on documentation of information.
- Communication channels to be adopted.
- Communication matrix: The people and their hierarchy, in terms of who should be informed first.
- Roles and responsibilities of executives in the security response team.
- Identification of media representative — the single point of contact between the outside world and the organization, during the time it's grappling with the incident.

Part 2 — Analysis

This part of the plan outlines best practices to make help managers decide on aspects such as:

- The right people are put together to analyze the security incident.
- The frequency of follow-ups that the incident leader must do to make sure the analysis doesn't get stuck anywhere.
- The mechanism for granting special accesses and privileges that analysts might need to speedily respond to the incident

Part 3 — Containment, eradication, and recovery

This part of the plan covers details of the actions people need to take for the remediation of the situation:

- Building workarounds to ensure business continuity, and to arrest the flow of the damage caused by the security breach.
- Re-prioritizing the work of IT teams to make sure they have adequate resources to help business teams regain access to lost information.
- Quickly remedying the identified problem (for instance, upgrading an application with the latest security patch or the mass-changing of passwords.)
- Intelligently expanding the scope of checks after addressing the burning problem, and leveraging the communication matric established in Part 1 to manage internal communications.
- Preparing a disclosure case to reveal the news of the security breach to the public and regulatory authorities.

Part 4 — Post-incident actions

A lessons-learned meeting, adequately timed after the incident, is a step in the right direction. It should also become an opportunity to challenge the reliability of your incident response plan and to identify scope for improvements in it.

2018's Cutting Edge Network Security Solution:

Cisco Umbrella

Cloud Delivered Enterprise Security

As the industry's first Secure Internet Gateway in the cloud, Cisco Umbrella provides the first line of defense against threats on the internet.

As a secure internet gateway, Cisco Umbrella helps you tackle the challenges of mobility, SaaS, and branch transformation by offering a single platform that secures access to and use of the cloud, SaaS applications, branch offices, and endpoints.

It's your first line of defense against threats -- anytime and anywhere your users access the internet, traffic goes through Umbrella first. By delivering security from the cloud, not only do you save money, but it also provides more effective security. Here's how:

1. DNS & IP layer enforcement

Umbrella uses DNS to stop threats over all ports and protocols — even direct-to-IP connections. Stop malware before it reaches your endpoints or network.

2. Intelligent proxy

Instead of proxying all web traffic, Umbrella routes requests to risky domains for deeper URL and file inspection.

3. Command & control callback blocking

Even if devices become infected in other ways, Umbrella prevents connections to attacker's servers. Stop data exfiltration and execution of ransomware encryption.

Call Tech Hero today to sign up for your free trial!

(800) 900-8324 x2

If one or more employees were responsible for the laxity that led to the data breach, you must find out what they did or didn't do and ensure the causes that led to the failure are never repeated again.

A cyberattack response plan is not optional

Not only are data breaches getting extremely common, but many of them are now targeted exclusively at businesses, because of the "value" that cybercriminals can draw by stealing data and holding operations to ransom. Be prepared, there's somebody out there plotting to sneak in and attack your business soon. If you don't have a cyberattack response plan today, you'd better have one by tomorrow.