UNIT 4
CUTTING-EDGE TECHNOLOGY

COLOMBIA POTENCIA DE LA VIDA

TIC

TALENTO TECH

Región 3 Cauca Y Nariño

OBJECTIVES OF THE UNIT

- Facilitate a comprehensive understanding of essential blockchain concepts, terminologies, and the historical context of cryptocurrencies, as well as to enhance participants' technological literacy, enabling them to navigate and engage in discussions on blockchain-related topics.

- Build language proficiency in cloud computing, emphasizing vocabulary, technical concepts, and effective expression of ideas related to cloud architecture patterns

COLOMBIA POTENCIA DE LA VIDA

WARM UP ACTIVITY

TIC

STOP ONLINE

VOCABULARY ACTVITY

https://stopots.com/es/

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

Universidad Tecnológica de Pereira

COLOMBIA POTENCIA DE LA VIDA

IDIOM OF THE DAY

TIC

A COG IN THE MACHINE

Being a small, and often insignificant, part of a bigger system or organization

*He felt like he was a **cog in the machine**, so he quit his job and decided to do something different.*

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

Universidad Tecnológica de Pereira

COLOMBIA POTENCIA DE LA VIDA

TIC

WHAT IS CRYPTOCURRENCY?

Cryptocurrency, sometimes called crypto-currency or crypto, is any form of currency that exists digitally or virtually and uses cryptography to secure transactions. Cryptocurrencies don't have a central issuing or regulating authority, instead using a decentralized system to record transactions and issue new units.

Cryptocurrency is a digital payment system that doesn't rely on banks to verify transactions. It’s a peer-to-peer system that can enable anyone anywhere to send and receive payments. Instead of being physical money carried around and exchanged in the real world, cryptocurrency payments exist purely as digital entries to an online database describing specific transactions. When you transfer cryptocurrency funds, the transactions are recorded in a public ledger. Cryptocurrency is stored in digital wallets.

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

Universidad Tecnológica de Pereira

COLOMBIA POTENCIA DE LA VIDA

USEFUL CRYPTOGRAPHY TERMINOLOGY

TIC

CRYPTOGRAPHY

The practice and study of techniques for securing communication and data by encoding information in a way that only authorized parties can understand.

DIGITAL CERTIFICATE

An electronic document that uses cryptography to bind the identity of an entity, such as a person or a website, to a public key.

SYMMETRIC ENCRYPTION

A type of encryption where the same key is used for both encrypting and decrypting the data.

ASYMMETRIC ENCRYPTION

A type of encryption that uses a pair of keys, one for encrypting and another for decrypting, providing a higher level of security.

SSL (SECURE SOCKETS LAYER)

A protocol that ensures the secure communication of data over a computer network, commonly used on the internet to secure transactions and sensitive information.

ENCRYPTION

the process of converting information or data into a code, especially to prevent unauthorized access.

READING ACTIVITY

“Securing Online Transactions: A Cryptography Guide”

Many of us navigate the online world, buying, selling, or communicating without a second thought. But have you ever wondered how your information stays safe while it travels across the vast web? The answer is simple: cryptography for digital certificates. This blog will walk you through the ins and outs of cryptography, making it easy for you to appreciate its role in securing your online transactions.

What is cryptography?

Cryptography is a bit like a secret code. But instead of passing notes in class, this code helps secure your online transactions. It's a method of scrambling your data into an unreadable format, which can only be decoded with a special key. This process is crucial in protecting your sensitive information from prying eyes.

Cryptography for digital certificates is like a digital stamp of authenticity. It uses cryptography to validate the identity of the sender and receiver. It assures that the message comes from a trusted source and hasn't been tampered with en route.

Let's highlight some key points about cryptography:

Scrambles data: Turns readable data into a coded format.
Uses keys: A special key is needed to decode the information.
Secures transactions: Protects your sensitive information during online transactions.
Validates identity: In the case of digital certificates, cryptography validates the identity of parties involved.

In a nutshell, cryptography is the superhero who keeps your online world safe and secure.

COLOMBIA POTENCIA DE LA VIDA

TIC

Why cryptography matters in online transactions?

Imagine you're shopping online for a new pair of shoes. You find the perfect pair, add them to your cart, and proceed to checkout. At this point, you're asked to enter your credit card details. Now, wouldn't you want to make sure that your credit card information remains confidential? Of course, you would! And that's when cryptography steps in.

Cryptography for digital certificates is like a secret handshake between your computer and the online shop. It ensures that the information you send is only accessible to the online shop and no one else. Not only does it protect your credit card information, but it also ensures that the online shop is who they say they are. It's like having a bouncer for your online transactions—keeping the bad guys out and letting the good guys in.

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

Universidad Tecnológica de Pereira

Here's why cryptography matters in online transactions:

Keeps your data private: Cryptography ensures that your sensitive information (like credit card details or personal information) remains confidential during transmission. It's like sending your data in a sealed envelope instead of a postcard.

Verifies authenticity: With cryptography for digital certificates, you can be sure that the website you're interacting with is genuine. It's like checking the ID of a person before trusting them with your house keys.

Prevents tampering: Cryptography ensures that the data you sent reaches the recipient as it is, without any changes. It's like making sure your mail doesn't get opened or altered during delivery.
So, while you're enjoying your new pair of shoes, take a moment to thank cryptography for making your online shopping experience safe and secure.

SYMMETRIC VS ASYMMETRIC ENCRYPTION

Now that we've seen why cryptography is the silent guardian of our online transactions, let's understand the two main types of encryption methods used in cryptography for digital certificates: symmetric and asymmetric encryption.

Let's start with symmetric encryption. Picture it like a locker at the gym. You put your stuff inside, lock it using a key, and when you're done, you open it with the same key. In symmetric encryption, the same key is used to both encrypt (lock) and decrypt (unlock) the data. It's speedy and efficient, but there's a catch: you need a safe way to share the key with the person who needs to unlock the data. And if the key gets into the wrong hands—well, that's like losing your gym locker key to a sneaky thief.

On the other hand, we have asymmetric encryption. Think of it as a mailbox. Anyone can drop letters (public key) into the slot, but only the person with the unique key (private key) can open it and read the letters. Here, two different keys are used—one to encrypt the data and the other to decrypt it. While it's more secure, it's also a bit slower than symmetric encryption.

So which one should you use? Well, it's like choosing between a bicycle and a car. It depends on what you need. For faster speed, go with symmetric encryption. But if you want more security and don't mind the slower speed, choose asymmetric encryption. Either way, you're ensuring that your online transactions remain safe and secure. And that's a win in our books!

COLOMBIA POTENCIA DE LA VIDA

TIC

HOW TO USE ENCRYPTIONS FOR SECURE TRANSACTIONS?

So, we've chatted about the two types of encryption methods used in cryptography for digital certificates. But you're probably wondering, "How do I actually use this encryption stuff for secure transactions?" Well, I'm glad you asked. Let's dive in.

Firstly, it's worth noting that you don't have to be a secret agent or a coding genius to leverage encryption. Many internet services, like email providers and online shopping sites, already use encryption to protect your information. However, it's always a good idea to know how to double-check.

For starters, always look for the little padlock icon in your web browser's address bar. This symbol indicates that the website you're visiting uses encryption—specifically, the Secure Sockets Layer (SSL) protocol. More on that in another section, so stay tuned!

Next, if you're sending sensitive information like credit card details or social security numbers, make sure to only send it over encrypted channels. For example, an encrypted email service or a secure online payment platform. Remember, the key to secure transactions is to always keep your sensitive information locked up tight with encryption.

Lastly, don't forget about WiFi. Public WiFi networks can be like a gold mine for hackers. So, whenever possible, use a Virtual Private Network (VPN) to encrypt your data and keep it safe from prying eyes.

By following these steps, you're using the power of encryption to protect your online transactions. And trust me, your bank account will thank you!

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

Universidad Tecnológica de Pereira

COLOMBIA POTENCIA DE LA VIDA

TIC

WHAT IS A DIGITAL SIGNATURE?

Imagine you're writing an old-fashioned letter to a friend. At the end of the letter, you sign your name—your unique mark that says "this letter is genuinely from me." A digital signature works in a similar way, but with a fancy tech twist. It's like your handwritten signature but for digital stuff, like emails and online transactions.

So, how does it work? Well, the magic happens thanks to our friend, cryptography. When you create a digital signature, you're using your private key to encrypt data. This encrypted data is the digital signature. It's unique to both you and the specific document or transaction it's attached to.

When the recipient of your message or transaction sees your digital signature, they use your public key to decrypt it. If the decrypted data matches the original document or transaction, bingo! They know two things: the message really is from you (authenticity), and nobody has tampered with it in transit (integrity).

And there you have it. With digital signatures, we're using cryptography for digital certificates to keep our online communication safe and secure. Just like a seal on an important letter, a digital signature gives a stamp of approval that the message or transaction is genuinely from you and hasn't been messed with.

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

Universidad Tecnológica de Pereira

COLOMBIA POTENCIA DE LA VIDA

TIC

HOW TO IMPLEMENT DIGITAL SIGNATURES?

So, you're all set and ready to use digital signatures to amp up the security, huh? Awesome! Here's how you can go about that:

Create a Hash: First, you'll need to produce a hash of the document or transaction you want to sign. Imagine a hash as a digital fingerprint of your data. It's a unique string of characters that represents your specific data. And just like your own fingerprints, even a tiny change in the data creates a whole new hash.
Encrypt the Hash: Next, you'll need to use your private key to encrypt the hash. This creates the digital signature. Remember, your private key is like your secret password in the world of cryptography for digital certificates.
Attach the Signature: Finally, you attach the digital signature to your document or transaction. It's like sealing an envelope with a wax seal in the old days. It's a mark of authenticity and integrity.
And voila! You've just created and implemented a digital signature. But remember, the power of digital signatures comes from the balance of private and public keys. Keep your private key secret, and share your public key openly. That way, anyone can confirm your digital signature is genuine, but only you can create it.

By implementing digital signatures, you're taking a big step in securing your online transactions. You're making the online world a safer place, one digital signature at a time.

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

Universidad Tecnológica de Pereira

HOW TO USE SSL FOR SECURE ONLINE TRANSACTIONS

So, we know that SSL is like a superhero for our data, but how do we use it? You'll be happy to know that it's not as complicated as you might think!

Let's say you're running an online store. You'll want to make sure your customers' payment information is safe, right? This is where SSL steps in. To use SSL, you'll need to get an SSL certificate from a trusted certificate authority. This is a little like getting an ID card that proves you are who you say you are. It's this certificate that allows your website to establish secure connections and use cryptography for digital certificates.

Once you have your SSL certificate, you install it on your website's server. This is usually a straightforward process, and most hosting providers offer guidance on how to do it. After installation, your website's URL will change from http to https. The 's' stands for 'secure' —this shows your website's visitors that their data will be safe with you.

But it's not just about protecting your customers' data. Using SSL also helps to increase your website's ranking on search engines. This is because search engines, like Google, prefer secure websites. So, by using SSL, you're not only protecting your customers but also boosting your website's visibility. It's a win-win!

Remember, the internet can be a bit like the Wild West. It's full of opportunities, but it can also be risky. Using SSL is one of the best ways to protect yourself and your customers. So why not saddle up and give it a try?

BEST PRACTICES FOR SECURE ONLINE TRANSACTIONS

Alright, let's wrap things up with some practical tips for making your online transactions as secure as possible.

Tip 1: Use Strong Passwords This may seem obvious, but you'd be surprised how many people use "password" as their password. Make sure to use a strong, unique password for every online account. Consider using a password manager to keep track of them all. Remember, your password is the first line of defense in online security.

Tip 2: Keep Software Updated This includes your operating system, web browser, and any apps you use for online transactions. Updates often include security patches for known vulnerabilities, so staying updated is a simple way to boost your security.

Tip 3: Use Two-Factor Authentication Two-factor authentication (2FA) adds an extra layer of security to your online accounts. It requires you to provide two types of information before accessing your account. This could be something you know (like a password), something you have (like a phone), or something you are (like a fingerprint).

Tip 4: Be Aware of Phishing Scams Phishing scams try to trick you into giving away your login details or other sensitive information. Be wary of any emails, texts, or phone calls that ask for this information, especially if they claim to be from a bank or other financial institution.

Tip 5: Use SSL and Digital Certificates As we've discussed, using SSL and digital certificates is a great way to secure your online transactions. It ensures that the data you send and receive is encrypted and authenticated, protecting it from prying eyes.

By following these best practices, you can make your online transactions as secure as possible. Remember, when it comes to online security, it's always better to be safe than sorry!

COLOMBIA POTENCIA DE LA VIDA

READING ACTIVITY

TIC

MATCHING AND MULTIPLE CHOICE

MATCHING DESCRIPTIONS WITH CONCEPTS

https://www.liveworksheets.com/es

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

Universidad Tecnológica de Pereira

TECH TAGS FOR PEOPLE

COLOMBIA POTENCIA DE LA VIDA

TIC

COMPUTER WHIZ

A person with a strong interest or skill in computers or technology.

EARLY ADOPTER

A person who starts using a product or technology as soon as it becomes available.

DIGITAL NATIVE

A person born or brought up during the age of digital technology and so familiar with computers and the internet from an early age.

HACKER

An individual with technical computer skills but often refers to individuals who use their skills to breach cybersecurity defenses.

TECH GEEK

Someone who loves all things about technology

GAMER

A person who plays games and especially video games.

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

Universidad Tecnológica de Pereira

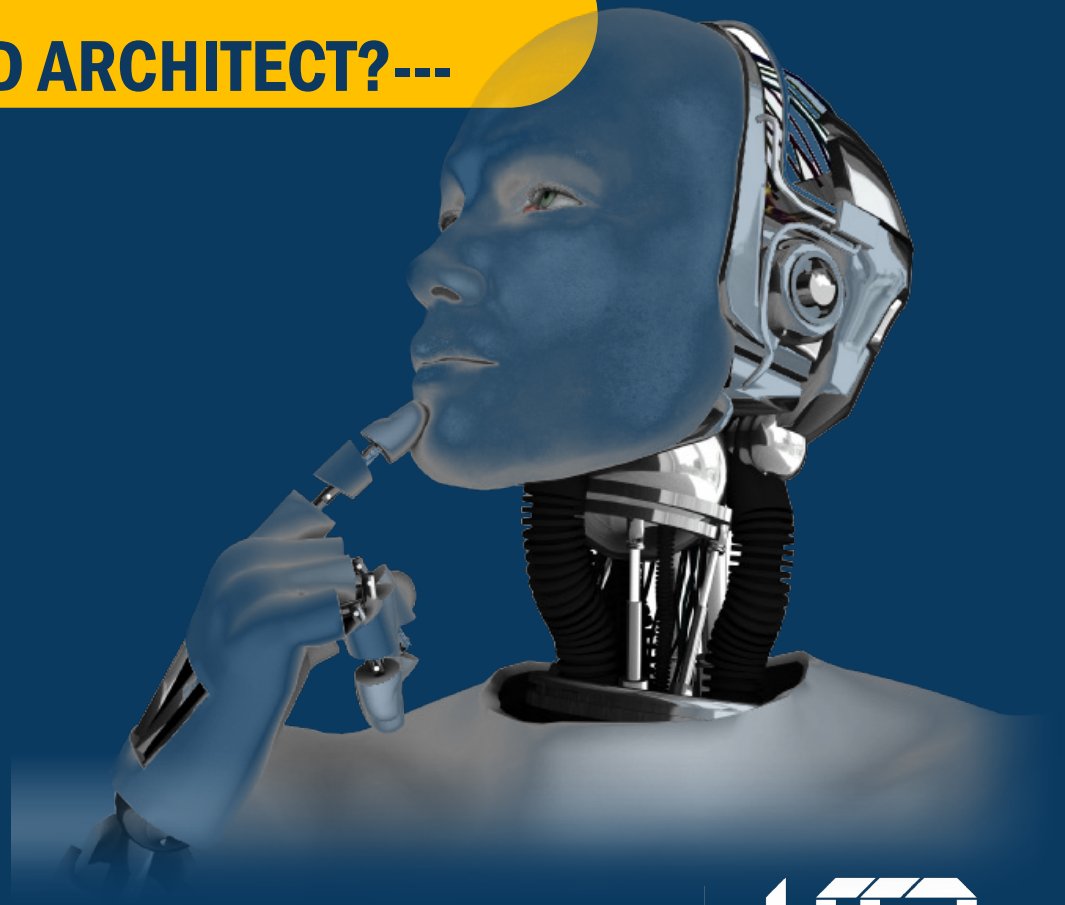
COLOMBIA POTENCIA DE LA VIDA

TIC

VIDEO ACTIVITY

--- SO YOU WANT TO BE A CLOUD ARCHITECT?---

https://youtu.be/F2pXoh3Cmo8?si=5WIOkraAP0s8xhAb



TALENTO TECH

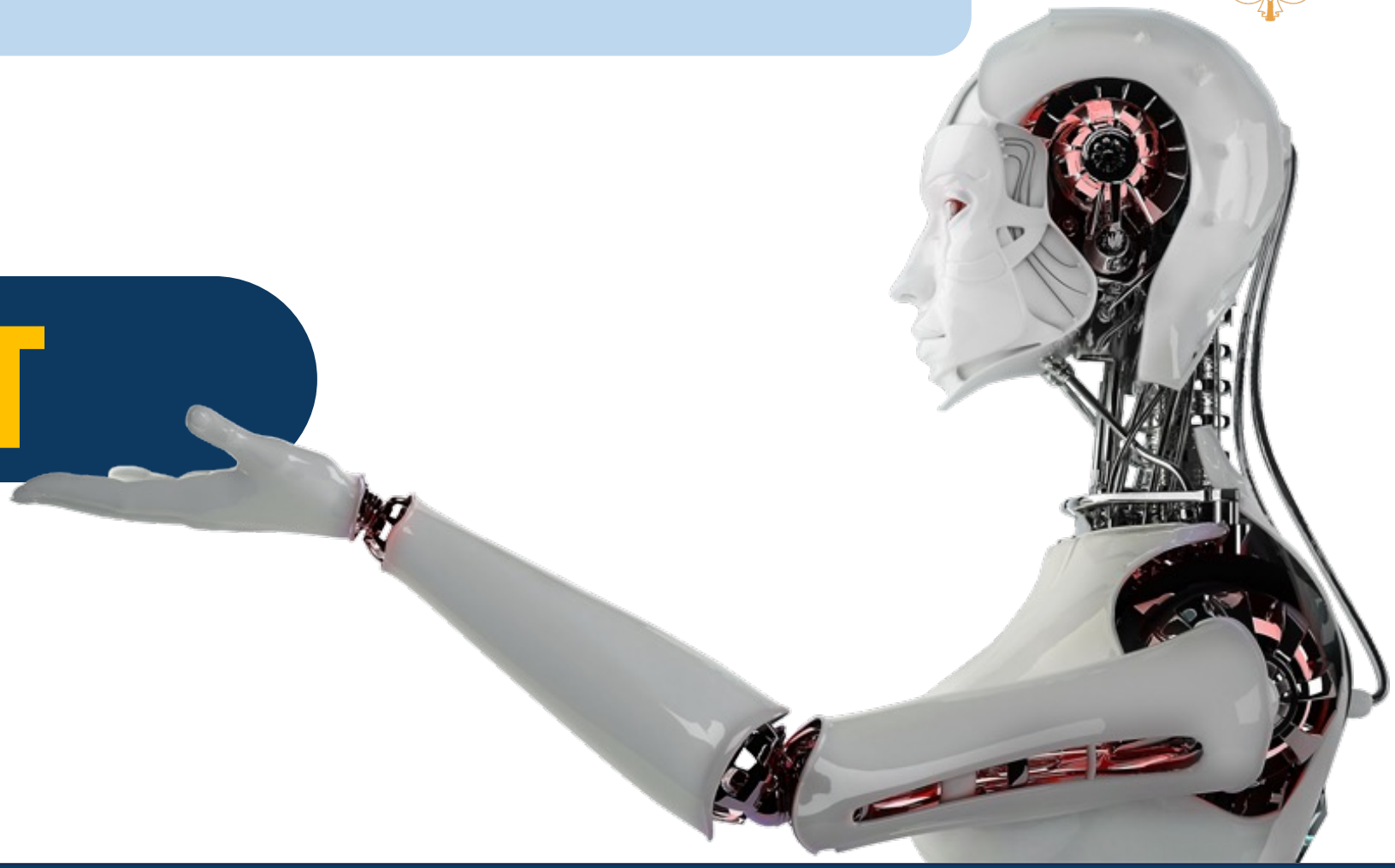
AZ | PROYECTOS EDUCATIVOS

Universidad Tecnológica de Pereira

COLOMBIA POTENCIA DE LA VIDA

VIDEO ACTIVITY

TIC



KAHOOT

VIDEO COMPREHENSION

https://kahoot.it

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

Universidad Tecnológica de Pereira