ISSUE 02
February 2025
WELLINGTON, AOTEAROA

THATSIT CONSULTANTS

TALK TECH

"Insider Tips to Make Your Business Run Faster, Easier and More Profitable"

INSIDE THIS ISSUE:

I am passionate about the use of technology in helping our communities.

Give me a call today for a talanoa to find out whether my team and I can help you improve your security posture and get more out of your existing technology!

- **Jim Tora**
Founder & CEO

WHAT IS BLOCK CHAIN TECHNOLOGY AND HOW DOES IT WORK?

Blockchain technology is changing the world. It is a system designed to keep records safe and secure. But how does it work? Let's find out more about this amazing technology.

What is Blockchain?

Blockchain is some kind of digital ledger. In it, information is stored in a manner that makes it hard to change. This ledger is shared among many computers, each one having a copy of the same ledger.

Information is kept within blocks. Each block maintains a list of transactions. As the block gets filled, it connects to the previous block, forming a linked chain of blocks or a blockchain.

How Does Blockchain Work?

Blockchain works by mining. Miners are computers that solve complex math problems. Once they solve these problems, they add new blocks to the chain.

Each block has a unique code called a hash. This hash helps keep the information secure. If anyone tries to change the information, the hash also changes. That way, it's easy to spot any tampering.

Why is Blockchain Secure?

The blockchain is secure because it is made using cryptography. Cryptography is like a secret code used to protect information. Only the ones who have the right key will be able to read it.

Besides, blockchain is decentralized. That means no one controls it. Several computers are working together to keep it safe.

What Are the Uses of Blockchain?

Many other uses of blockchain exist beyond money. It can track goods in a supply chain, store medical records safely, and even help with voting in elections.

In finance, blockchain powers cryptocurrencies such as Bitcoin. These are digital currencies that people can use online.

How Does Blockchain Impact Our Lives?

Blockchain makes transactions faster and cheaper. It removes the need for middlemen like banks. This saves time and money.

It also introduces transparency. Users can view all the transactions made on the blockchain. These actions help to establish trust among users.

What Are the Challenges of Blockchain?

There are challenges regarding the use of blockchain. Much of the mining is power-consuming. This might not be suitable for the environment.

Besides these issues, there are even more regulatory ones. Governments and agencies don't yet know how to deal with blockchain technology.

What's Ahead for Blockchain?

The future of blockchain is very bright. More industries are exploring its potential every day. In healthcare, it can secure patient data and streamline records. In entertainment, it can protect intellectual property and ensure fair compensation for creators.

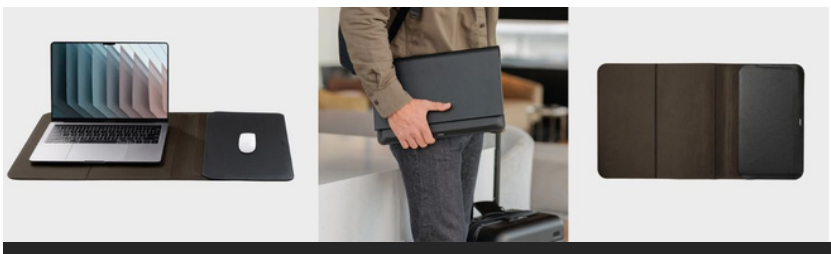
Financial services are also benefiting from blockchain, with faster and more secure transactions. Developers are working on making blockchain more efficient and eco-friendly, addressing environmental concerns.

Blockchain is set to revolutionize various industries.

Want to Learn More About Blockchain?

Blockchain technology is fascinating and holds immense potential. It can transform various aspects of our lives for the better. For example, it enhances security by safely storing and sharing data, which is crucial in healthcare. Its transparency and immutability foster trust, making it ideal for supply chain management. Its decentralized nature makes systems more resilient, while smart contracts automate transactions, increasing efficiency.

Contact us to discover how blockchain can benefit your business or personal projects. Our team is ready to guide you through this transformative technology.



ORBITKEY HYBRID LAPTOP SLEEVE

Orbitkey lets you transform any space into your workspace with its dual-function sleeve/ desk mat.

Made from vegan leather and recycled woven fabric, it combines functionality with eco-friendly materials.

It comes with a magnetic closure and a slim design that fits easily into any bag. The laptop pocket doubles as a mouse pad, making it a perfect on-the-go workspace.

It's made for up to 14″ or 16″ laptops.

ISSUE 02
February 2025
WELLINGTON, AOTEAROA

THATSIT CONSULTANTS

ULTIMATE GUIDE TO ENCRYPTION METHODS

Encryption is a method of securing information. It converts readable data into secret code. Only the right key can decode it. This guide will help you understand different encryption methods.

What is Encryption?

Encryption is like a secret language. It converts regular text into unreadable text. This unreadable text is called ciphertext. Only people who have the right key will be able to convert it into normal text, called plaintext.

Why Do We Use Encryption?

We use encryption to keep our information safe. It makes our data safe from hackers. This is very important for privacy and security.

How Does Encryption Work?

Encryption uses algorithms and keys. An algorithm is a set of rules for solving problems. A key is somewhat like a password that unlocks the secret message.

Symmetric vs Asymmetric Encryption

Symmetric encryption uses the same key for encryption and decryption. The same key is shared between the sender and receiver. It's fast but less secure when the key is shared.

Asymmetric encryption uses two keys: a public key and a private key. A public key can encrypt a message, while a private key can decrypt it. It's more secure since only the private key unlocks the message.

What Are Some Common Encryption Methods

- AES (Advanced Encryption Standard)
- RSA (Rivest-Shamir-Adleman)
- DES (Data Encryption Standard)
- ECC (Elliptic Curve Cryptography)

How Do We Use Encryption in Everyday Life?

- Online Shopping. When you purchase online, your payment information is encrypted. This protects your credit card information against hackers.
- Messaging Apps. Apps like WhatsApp use encryption to keep your messages private. Only you and the person you are chatting with can read them.
- Email Security. Many email services use encryption to protect your emails from being read by others.

What Are the Challenges of Encryption?

- Key Management. If some person loses their key, they probably will lose their data.
- Performance Issues. Encryption could slow down the systems since it needs processing power for encryption and decryption.

How Can You Stay Safe with Encryption?

- Use Strong Passwords. Always use strong passwords for accounts and devices. That will make hacking difficult as it will take time to access.
- Keep Software Up-to-Date. Regularly update your software to protect against security vulnerabilities in software.
- Use Caution with Public Wi-Fi. If you need to use public Wi-Fi, avoid sensitive transactions unless you can encrypt your internet connection using a VPN.

Ready to Secure Your Data?

Encryption helps protect your personal information from threats. Understanding different methods can help you choose the right one for your needs.

If you need help securing your data, contact us today!

CAN PASSWORD MANAGERS BE HACKED?

Password managers keep our online accounts safe. They store all our passwords in one place. But are they hackable?

What Are Password Managers?

Password managers are like digital vaults: they save all your passwords inside themselves. You need only remember one master password, of course. This makes keeping a lot of accounts much easier to handle.

Can Password Managers be Hacked?

They always hunt for ways to steal your information. However, breaking into a password manager is not easy.

How Can You Protect Your Password Manager?

- Choose a Strong Master Password. Use a mix of letters, numbers, and symbols.
- Enable Two-Factor Authentication. 2FA adds a layer of security.
- Keep Software Up-to-Date. Updates fix security issues and keep your data safe.

What Happens If a Password Manager Gets Hacked?

- Change your master password immediately.
- Decide which accounts could be affected and change their passwords as well.
- Consider shifting to another password manager.
- Keep up to date with any security news about your manager.

Is the Use of Password Managers Worth the Risk?

- The benefits of using a password manager usually outweigh the risks. They help you create strong, unique passwords for each account.
- Choosing a reputable password manager with good reviews and security features is key. Do some research before deciding which one to use.

Take Control of Your Online Security Today!

Using a password manager will go a long way in enhancing your online security. If you need help in selecting which one, we're just a contact away.

10 AI TOOLS YOU NEED IN YOUR OFFICE FOR PRODUCTIVITY

- **Smart calendars** use AI to manage your schedule.
- **Task managers** put your tasks in order by deadline or urgency.
- **Email assistants** can filter important emails and even draft replies for you.
- **Virtual meeting helpers** use AI to transcribe meetings in real time.
- **Data visualization** tools create simple charts and graphs that are easy to understand.
- **Predictive analytics** make use of AI to forecast the future with the help of data related to the past.
- **Writing assistants** can help with grammar checks and content ideas.
- **Design tools** powered with AI will create stunning visuals in a jiffy.
- **Chat bots** are AI programs that chat with customers online.
- **Sentiment analysis tools** use AI to understand customer feelings from their messages or reviews.

5 COMMON CYBER THREATS IN 2025

- Phishing attacks will always be in vogue. They make you give away your personal data. Always check the sender's email address. Do not click on suspicious links.
- Ransomware locks your files and demands money to unlock them. Keep your software updated and back up your files regularly.
- Malware is bad software that may cause damage to your computer. Use antivirus software and avoid downloading files from unknown sources.
- Cybercriminals will leverage artificial intelligence for more sophisticated attacks. AI supports them in selecting the right victims.
- There are more and more devices connecting via the internet. Make sure that all devices have updated security measures on them.

BEST PRACTICES FOR SECURE DATA BACKUP

Data backup refers to the creation of a copy of your data. The copy can be used in the event of loss or destruction of the original data.

Backups can be stored on various devices, such as external hard drives, or in the cloud. Having a backup ensures you don't lose important information.

Here are best practices for secure data backup:

- **Use Encryption:** Encryption scrambles your data so only you can read it. This keeps it safe from hackers.
- **Set Strong Passwords:** Use strong passwords for all your backup accounts and devices. This prevents unauthorized access.
- **Regularly Test Your Backups:** Testing ensures that your backups work properly. Try restoring a file to make sure everything is correct.

Take Action to Protect Your Data Today

Don't wait until it's too late to protect your data. Start backing up today!

Secure your important files by following these best practices for data backup. If you need help setting up a secure backup system, we are here.

TECHNOLOGY TRIVIA TIME

Each month you have a chance to win a $50 Amazon Gift Voucher by being the first person to email us with the answer to our Technology Trivia Question of the Month!

The question this month is:

What was the first item purchased using Bitcoin?

The first person to email me at jimtora@thatsitconsultants.com with the correct answer gets a $50 Amazon Gift Card!

Last month's answer was
1994