LifeHash®

GOVERNMENT &
LAW ENFORCEMENT

Guide to Blockchain

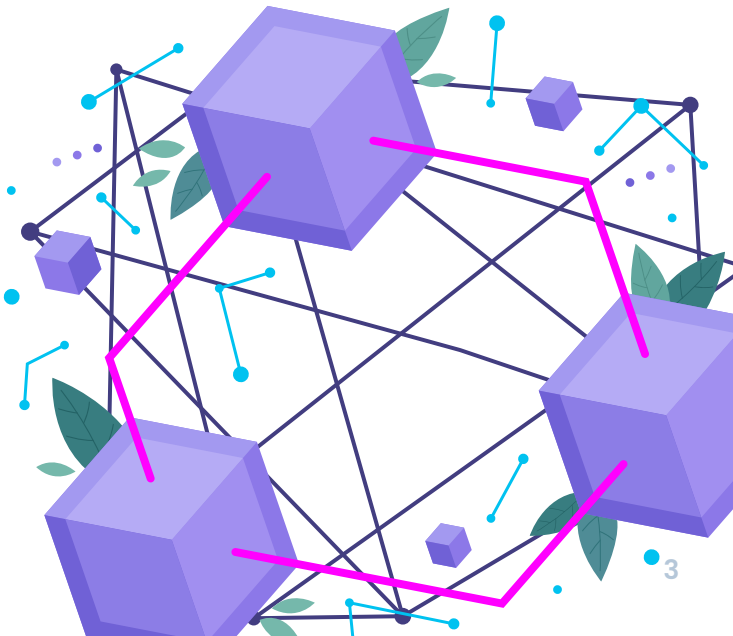
STRAP YOURSELF

(strap yourself in, we're about to rundown some pretty complex tech in about 10mins flat)

Blockchain is most commonly associated with Bitcoin and other cryptocurrencies. While Bitcoin and other cryptocurrencies use blockchain technology to provide transactions, they can provide more than just financial records.

Blockchain records the process of transactions and the tracking of assets. The tracked asset can be a tangible asset, like a house, car, cash or land or an intangible asset, like intellectual property, patents and copyrights.

Ultimately, almost anything can be tracked and traded on a blockchain network.



But, How Does it Work...

Blockchain is a decentralised record of digital transactions distributed between many different computers. Unlike vulnerable conventional databases held on a centralised server, blockchain is decentralised, and no single entity controls it.

The records, or ledger, as it is known, is distributed between users who have access to one shared copy. And, because of this decentralised, distributed system, a majority consensus is required from the network to update the ledger.

When discussing blockchain, three words are going to come up time and again;

- **Distributed** - utilising many computers worldwide that are owned by different entities.
- **Decentralised** - managed by public verification across the network.
- **Encrypted** - a process known as 'hashing' encrypts data sent to the blockchain.

Let's Talk About Encryption...

Before entering a blockchain, complicated mathematical algorithms convert information into a string of characters known as a hash. This process known as hashing ensures that encrypted data is virtually impossible to decrypt. And, a change of even a single point of data will produce a completely different hash value.

Look at the difference between the two hash values below when changing a letter from upper case to lower case in the phrase, Your Digital History!

INPUT	CRYPTOGRAPHIC HASH FUNCTION	DIGEST
Your Digital History	→ # →	928a6e7a0712ecdbcc1591b6ab9f93e9eed96440ee0e07ee250412c35b984dfa
Your Digital history	→ # →	59c00085bda641974fbe88b1794ab0b9ac5937196317c22a806a6d9faa9df6d7

So, Why Call It Blockchain?

The name blockchain originates from the fact that it stores transaction data in blocks.

A block is only open for a fixed amount of time, and once a block is full of transactions, a miner (more about them in a bit) verifies the block and closes it.

Part of the process of verifying a block is to attribute it with a timestamp. This timestamp, combined with the previous block's header, creates the new header.

The system of encrypted headers links each block in an unbreakable chain, hence the name blockchain.

You Could Describe it as... a Database with a Difference!

A traditional database is usually controlled either by an individual user or organisation on a private network. And, the data is stored in a single location, whether cloud storage, hard drive or another form of digital storage.

As you may have guessed, blockchain is the complete opposite of a traditional database. Blockchain is not controlled by a single user or organisation within a private network but is managed and verified by miners across a global network of individual computers or nodes.

Time for a few more definitions...

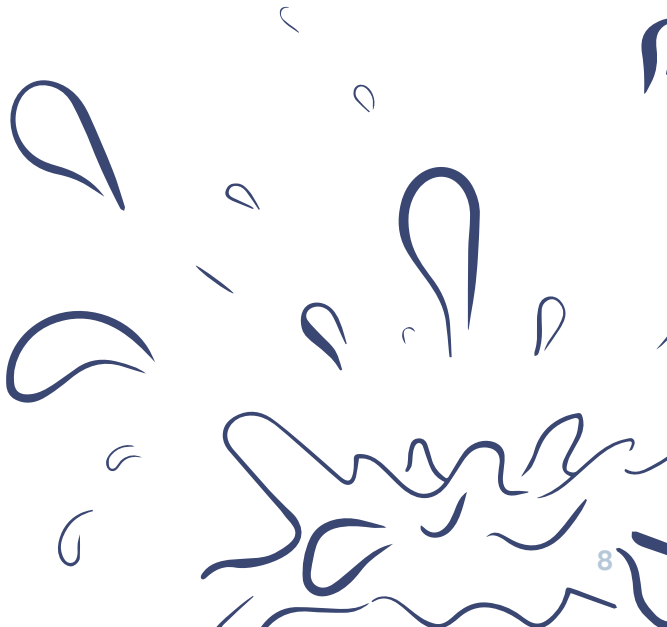
- **Block Explorer** - an online search facility used to view all transactions on a blockchain.
- **Miner** - Specific computing equipment run by people and responsible for validating transactions and adding them to the blockchain.
- **Node** - computers on the network used to receive, validate and execute transactions.

Clear as Mud so far, or Transparent like a Blockchain?

In today's murky world where seemingly ethical businesses are revealed as anything but, blockchain is like a glass of water from a mountain spring, crystal.

Blockchain records transactions across many computers in such a way that they can't be altered. The result is an audit trail of transactions with super high accuracy as it is nearly impossible to falsify data on the blockchain.

Add public access to this ledger through block explorers, and you have just about the most transparent system for recording data on the planet, or off the planet for that matter!



Security in Diversity

Blockchain is not a one-size-fits-all solution, and different measures are needed to cover all the bases. Here's a brief explanation of the different types of blockchain networks;

- **Public**

  Anyone can join and start using the network, the public ledger is accessible to all, and it's entirely decentralised.

- **Private**

  Invite-only and controlled by an institution or group, often used to manage the flow of financial transactions, contracts, medical records, and other sensitive information.

- **Permissioned**

  Members of the blockchain network are known and verified.

- **Consortium**

  Shared by a group of organisations, all of which can add blocks to the chain.

TIME TO RECAP

Time for a Recap before we Blast on to the Benefits

So far, we've covered the basics, but if they're not so basic and you need a quick refresher, here we go.

Blockchain, it's a chronological ledger of encrypted data shared across a distributed, decentralised (remember those words?) network, managed by users and accessible to everyone, with cryptography securing access and consensus creating certainty of the data you share.

And, finally, what you've been waiting for... a numbered list.

The Top 5 Benefits of Blockchain!

Blockchain is already being used across the globe in various applications as industries realise the benefits of the revolutionary technology. Here we look at some of the many benefits of blockchain.

01 Trust

Without total trust in the security, accuracy and provenance of your data, you are vulnerable on all sides. The simple fact that blockchain provides an immutable record of transparent, timestamped transactions between users builds trust and allows you to pursue excellence with confidence.

02 Connection

At a time when global communities are becoming more connected, a universal ecosystem to exchange secure data is needed. Enter blockchain, the ability for information to be verified without the need for a central authority, on a publicly accessible database, means data can be shared in real-time across industries, and everybody gets a copy.

03 Security

A transparent, distributed, decentralised network where all participants agree to the validity of each record without a centralised party. Where all records are individually encrypted, timestamped and linked in a fixed chain of data blocks. Where users can remain anonymous and only need a public key, all results in blockchain being virtually impossible for anyone to hack.

04 Smart Contracts

When speed is of the essence and bureaucracy is slowing you down, smart contracts are your saviour. A computer protocol that can verify, enforce, or negotiate a contract when predetermined conditions are fulfilled effectively streamlines business processes. On or Off-chain, the full potential of smart contracts is expanding every day.

05 Future Proof

The arrival of the Internet of Things (IoT) has created volumes of data that are becoming increasingly hard to verify.
This is slowing operations and decreasing productivity for businesses, which are already being forced to sit on their unused reserves. Blockchain is rapidly scalable and capable of processing the high volumes of data that IoT creates.

Like to see real-world examples? Have a look at law enforcement...

What's the Problem...

Criminal enterprises and individuals at the forefront of technological progress along with an explosion of available data contribute to increasingly complex investigations. Never before has the criminal justice process relied so heavily on electronic evidence, and its integrity, exactness, and reliability are now paramount to the success of many trials.

...and Our Solution

LifeHash has developed Evidential Chain using mobile and web app technology combined with established blockchain from Bitcoin and DigiByte to provide a secure and transparent ecosystem, allowing you to record, retain and manage every aspect of an investigation.

For Example...

A law enforcement agency equipped with Evidential Chain can capture and secure data at the scene as actions occur, utilising QR codes and mobile devices. Evidence is secured using cryptography and resilient public blockchain networks making it traceable, auditable and, of course, impossible to tamper with.

During its journey through the investigation and judicial process, each piece of evidence is scanned every step of the way, building an irrefutable report of continuity. Metadata such as time, date, location and officer ID are attributed automatically, whereas detailed reports of origin, forensic analysis, storage location/condition, transport methods are manually entered. All developed by an expert team of retired and serving police officers, detectives, prosecutors, forensic scientists, forensic investigators, and legal advisors to guarantee truth in evidence.

Here comes the best bit...

The Results

Let's roll with the above example and look at the customer benefits as they happen.

- **Increased Speed,** QR codes and mobile scanning ramp up the recording process
- **Guaranteed Continuity,** simple, accurate and reliable method to ensure evidence is admissible
- **Total Security,** eradicate genuine mistakes, recording errors and tampering.
- **Fully Auditable,** transparent, immutable, public blockchains offer exemplary data recovery

Rewind to the problem...

'Criminal enterprises and individuals at the forefront of technological progress along with an explosion of available data contribute to increasingly complex investigations'

...Fast-forward to the future

- **Criminal Enterprises and Individuals -** Corruption of evidence secured using Evidential Chain will simply be too complex for individuals and a seemingly insurmountable endeavour for even the most technologically advanced criminal enterprises.

- **Explosion of Available Data** - to use to your advantage, managed via fast, secure and scalable public blockchain networks with proven reliability, increasing admissibility of evidence in court.

- **Complex Investigations** - become simple to compile, track and audit, Evidential Chain has been designed by officers aware of the pitfalls in contemporary investigations.

We understand that integrity and continuity of tangible and intangible evidence is vital to the success of any civil or criminal investigation and have created the Evidential Chain to give back the technological advantage to law enforcement.

To Wrap Up, LifeHash Explained in 2 Minutes

Did we mention that we use established blockchain from Bitcoin and DigiByte? Well, there is a good reason for this...

Bitcoin is the original, world-first, decentralised peer-to-peer global payment network. As the original and longest-living decentralised transaction network, Bitcoin enjoys, by far, the most outstanding security and integrity of all blockchains due to the enormous hashing power of its global network. So, we chose it as the foundation for our technology simply because its unmatched level of security provides what we need exactly when it comes to delivering immutable data.

Yet, while Bitcoin offers the best-of-class security, DigiByte offers increased transaction speed and smart contract capabilities.

DigiByte enjoys a broad network of more than 200,000 downloaded nodes worldwide and tens of thousands of active nodes. This network enables DigiByte to create blocks every 15 seconds, 40x faster than Bitcoin, making it especially suitable for applications requiring fast transaction times. The DigiByte network has a long history of security-focused innovation whilst at the same time ensuring scalability. When speed and scalability are of the essence, DigiByte is your answer.

Here comes the rocket science...

The Interplanetary File System (IPFS) is a peer-to-peer (p2p) system for storing and accessing files, websites, applications, and data. Created in an attempt to address the deficiencies of a primarily centralised internet and current data storage, IPFS uses a novel p2p file-sharing system to decentralise both. We firmly believe that it is a solution that can change the way information is shared worldwide and assist in the fight to repatriate data.

A very brief summary of the benefits

- **Resilience** - If traditional servers become unoperational, you're content can not be served. IPFS allows your content to always be available.
- **Freedom** - Censorship by third parties is much more difficult due to IPFS decentralisation.
- **Security** - With a distributed network, there is no single point of attack, making it harder to compromise.

Your Digital Future

At LifeHash, we believe there is a real global need to take back data control from big tech and empower the public with data ownership.

This realisation forms the building blocks for LifeHash and fuels our research into alternative ways of utilising blockchain to shape a more transparent digital future.

We are focused on developing platforms to allow industries to reach another level of technological advancement, whether by streamlining processes through eradication of corruption in data handling or enabling them to provide absolute provenance of their product.

We understand the technology, and you understand your industry, let's work together and use blockchain to create solutions.

We hope you have found this article helpful and are looking forward to discussing your needs.