2021-1-IE01-KA220-VET-000032943

Co-funded by the
Erasmus+ Programme
of the European Union

TrainChain
Blockchain Training for Start Ups

PR1-T3 Core Content

Module 0 – Introduction to Blockchain Technology

Author: CCSDE

PROJECT ID:

Grant agreement	2021-1-IE01-KA220-VET-000032943
Programme	Erasmus+
Key action	KA220-VET - Cooperation partnerships in vocational education and training
Field	Vocational Education and Training
Project acronym	TrainChain
Project title	TrainChain - Blockchain Training for Start Ups
Project starting date	28/02/2022
Project duration	24 months
Project end date	27/02/2024

REVISION HISTORY

Version	Date	Author	Description	Action	Pages
1.0	31/07/2022	CCSDE	Creation	C	8

(*) Action: C = Creation, I = Insert, U = Update, R = Replace, D = Delete

REFERENCED DOCUMENTS

ID	Reference		Title
1	2021-1-IE01-KA220-VET-000032943		TrainChain Agreement
2			

APPLICABLE DOCUMENTS

ID	Reference		Title
1			
2			

Contents

1. Introduction

1.1 Module Description

In the first part of the module, we will…

- Discover the new world of blockchains,
- Understand why they matter,

In the second part of the module, we will…

- Identify the three types of blockchains,
- Deepen our knowledge of how blockchains work.

1.2 Module Goals

1.3 Learning Objectives

1.4 Learning Outcomes

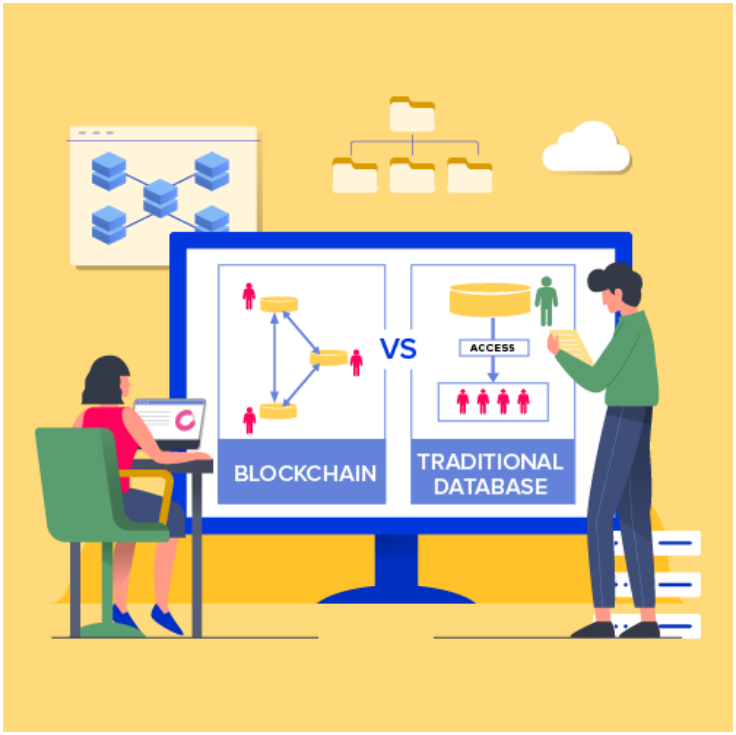
2. Main Content

2.1 Blockchain

Originally, blockchain was just the computer science term for how to structure and share data. Today blockchains are hailed the fifth evolution of computing.

Blockchains are a novel approach to the distributed database. The innovation comes from incorporating old technology in new ways. You can think of blockchains as distributed databases that a group of individuals controls and that store and share information.

There are many different types of blockchains and blockchain applications. Blockchain is an all-encompassing technology that is integrating across platforms and hardware all over the world.



What Blockchains Are

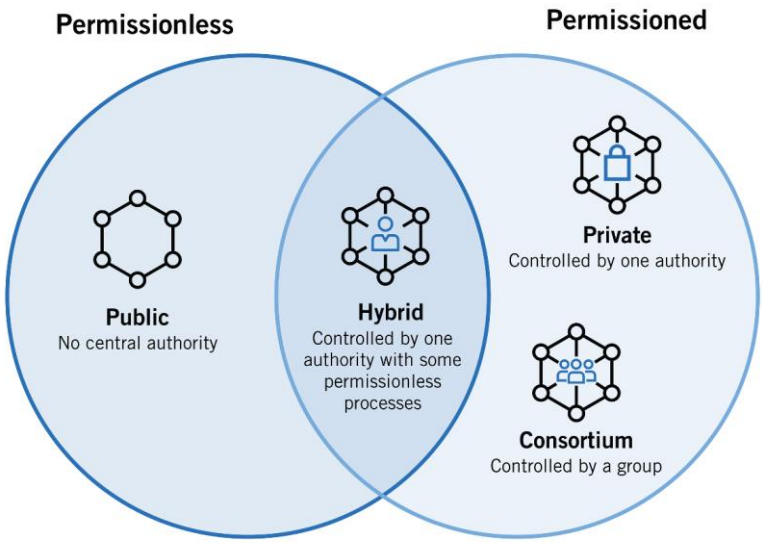
A blockchain is a data structure that makes it possible to create a digital ledger of data and share it among a network of independent parties. There are many different types of blockchains.

- Public blockchains: Public blockchains, such as Bitcoin, are large distributed networks that are run through a native cryptocurrency. A cryptocurrency is a unique bit of data that that can be traded between two parties. Public blockchains are open for anyone to participate at any level and have open-source code that their community maintains.

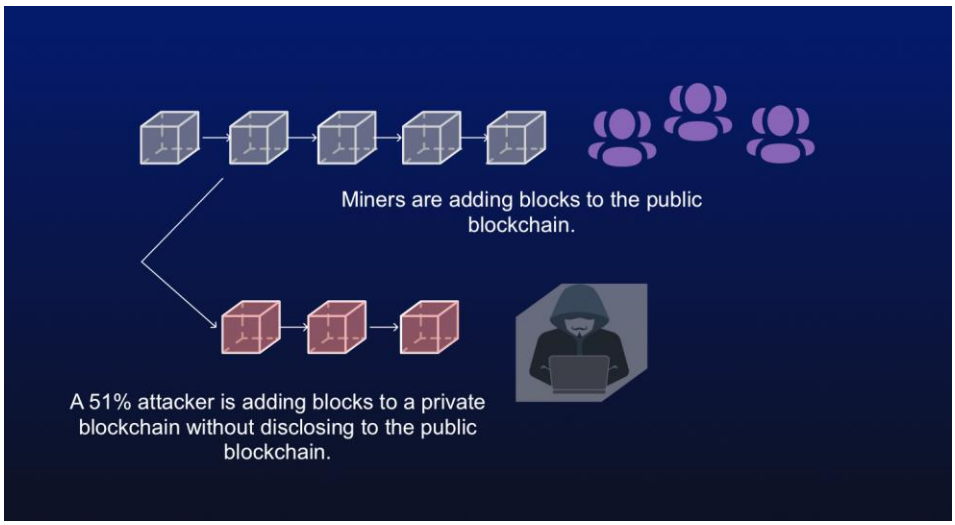
- Permissioned blockchains: Permissioned blockchains, such as Ripple, control roles that individuals can play within the network. They're still large and distributed systems that use a native token. Their core code may or may not be open source.

- Private blockchains: Private blockchains also known as distributed ledger technology (DLT) tend to be smaller and do not utilize a token or cryptocurrency. Their membership is closely controlled. These types of blockchains are favoured by consortiums that have trusted members and trade confidential information.

All three types of blockchains use cryptography to allow each participant on any given network to manage the ledger in a secure way without the need for a central authority to enforce the rules. The removal of central authority from the database structure is one of the most important and powerful aspects of blockchains.



Blockchains create permanent records and histories of transactions, but nothing is really permanent. The permanence of the record is based on the dependability and health of the network. In the context of blockchains, this means that if a large portion of the blockchain community wanted to change information written to their blockchain, they could. Cryptocurrency is used as a reward to incentivize lots of users to facilitate the healthy function of the network through competition. If the records are changed inappropriately, this is known as a 51 percent attack. Small networks with few independent minors are vulnerable because it doesn't take much effort to change their information, and powerful miners could do so and gain extra cryptocurrency.

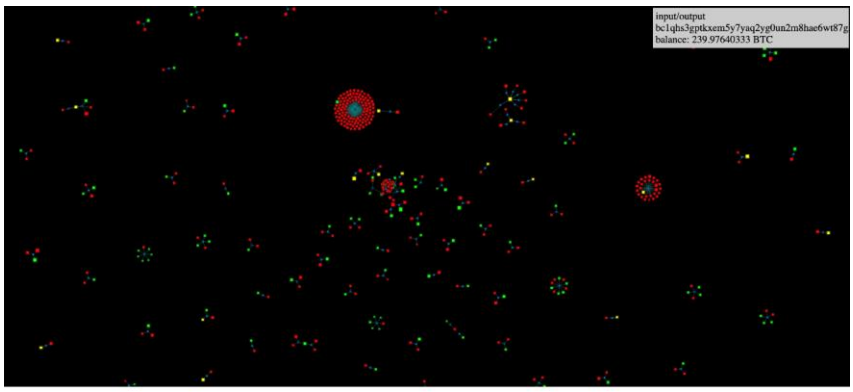


What blockchains do

A blockchain is a peer-to-peer system with no central authority managing data flow. One of the key ways to removing central control while maintaining data integrity is to have a large distributed network of independent users. This means that the computers that make up the network are in more than one location. These computers are often referred to as full nodes."

Figure 1-1 shows a visualization of the structure of the Bitcoin blockchain network. You can see it in action at http://dailyblockchain.github.io.

Με σχόλια [Ma1]: Figures are not referenced, and some of them are illegible



To prevent the network from being corrupted, not only are blockchains decentralized but they often also utilize a cryptocurrency. Blockchain networks produce cryptocurrencies as an incentive to maintain the integrity of the network. Many cryptocurrencies are traded on exchanges like stocks.

Cryptocurrencies work a little differently on each blockchain. Basically, the software pays the hardware to operate. The software is the blockchain protocol. Well-known blockchain protocols include Bitcoin, Ethereum, Ripple, Bitcoin Cash, Stellar, and EOS. The hardware consists of the full nodes that are securing the data in the network.

Why blockchains matter

Blockchains are recognized as the "fifth evolution" of computing because they're a new trust layer for the Internet. Before blockchains, trust was established by central authorities that would issue certificates. One you may be familiar with is Secure Sockets Layer (SSL) client certificates. An SSL certificate is the "green lock" that is next to a web domain. It lets you know you're on a secure website. SSL certificates have proven to not be fool proof. Certificates have been stolen from the domains of the Central Intelligence Agency (CIA), the U.K.'s Secret Intelligence Service (commonly known as MI6), Microsoft, Yahoo!, Skype, Facebook, and Twitter. Relying on a third party allows for a single point of failure.

Blockchains, on the other hand, establish trust in novel ways. Proof-of-work (POW) blockchains require miners to have a full and accurate history of their transactions to participate on the network. Proof-of-stake (POS) blockchains create trust by requiring

nodes that are processing transactions to "stake" some cryptocurrency that may be forfeited if they're caught defrauding the network. Private blockchains build confidence by distributing data across a network of connected but independent participants that are known by each other and can be held accountable. Each type of blockchain uses different incentive systems to establish trust that participants in the network will cooperate in keeping a full and unaltered history of each transaction, or entry that is made within the database they share.

When data is permanent and reliable in a digital format, you can transact business online in ways that, in the past, were only possible offline. Everything that has thus far remained analogue, including property rights and identity, can now be created and maintained online. Slow business and banking processes, such as money wires and fund settlements, can now be done nearly instantaneously. The implications for secure digital records are enormous for the global economy."

Blockchains are important because they allow for new efficiency and reliability in the exchange of valuable and private information that once required a third party to facilitate, such as the movement of money and the authenticity of identity. This is a big deal because much of our society and economy has been structured around establishing trust, enforcing trust when it's broken, and third parties that facilitate trust. You can imagine how blockchain can be utilized to fix areas that have proven to not be fool proof, such as voting, supply chain management, money movement, and the exchange of property.

The Structure of Blockchains

Each blockchain is structured slightly differently. However, Bitcoin is a great blockchain to study because it was used as a template for most subsequent blockchains. The data on Bitcoin is structured so that each full node (the computers running the network) contains all the data in the network. This model is compelling from a data persistence point of view. It ensures that the data will stay intact even if a few of the nodes become compromised. However, because every node has a full copy of the history of transactions, since the very beginning, and every transaction in the future, it requires that the entries be as small as possible from a storage capacity point of view.

Comparatively, other distributed networks you may have heard of like Napster and Pirate Bay are an online index of data. Individual files are shared from specific nodes in

the network. This allows sharing of large files. However, because the data you may be interested in is not available on all the participants in the network, obtaining the data you're interested in is problematic. It's also difficult to know if the data that you're pulling down is intact, has not be corrupted and/or contains information you don't want, such as a virus.

The way that Bitcoin coordinates the organization and input of new data comprises three core elements:

1. **Block**: A list of transactions recorded into a ledger over a given period. The size, period, and triggering event for blocks is different for every blockchain.

Not all blockchains are recording and securing a record of the movement of their cryptocurrency as their primary objective. But all blockchain do record the movement of their cryptocurrency or token. Think of the transaction as simply being the recording of data. Assigning a value to it (such as happens in a financial transaction) is used to interpret what that data means.

2. **Chain**: A hash that links one block to another, mathematically "chaining" them together. This is one of the most difficult concepts in blockchain to comprehend. It's also the magic that glues blockchains together and allows them to create mathematical trust.

The hash in blockchain is created from the data that was in the previous block. The hash is a fingerprint of this data and locks blocks in order and time."

Although blockchains are a relatively new innovation, hashing is not. Hashing was invented over 30 years ago. This old innovation is being used because it creates a one-way function that cannot be decrypted. A hashing function creates a mathematical algorithm that maps data of any size to a bit string of a fixed size. A bit string is usually 32 characters long, which then represents the data that was hashed. The Secure Hash Algorithm (SHA) is one of some cryptographic hash functions used in blockchains. SHA-256 is a common algorithm that generates an almost-unique, fixed-size 256-bit (32-byte) hash. For practical purposes, think of a hash as a digital fingerprint of data that is used to lock it in place within the blockchain.

3. **Network**: The network is composed of full nodes. Think of them as the computer running an algorithm that is securing the network. Each node contains a complete record of all the transactions that were ever recorded in that blockchain.

The nodes are located all over the world and can be operated by anyone. It's difficult, expensive, and time-consuming to operate a full node, so people are incentivized to operate a node because they want to earn cryptocurrency. The underlying blockchain

algorithm rewards them for their service. The reward is usually a token or cryptocurrency, like Bitcoin."

2.2 Main Blockchain Applications & Evolution

Blockchain applications are built around the idea that network is the arbitrator. This type of system is an unforgiving and blind environment. Computer code becomes law, and rules are executed as they were written and interpreted by the network. Computers don't have the same social biases and behaviours as humans do.

The network can't interpret intent (at least not yet). Insurance contracts arbitrated on a blockchain have been heavily investigated as a use case built around this idea.

Another interesting thing that blockchains enable is impeccable record keeping. They can be used to create a clear timeline of who did what and when. Many industries and regulatory bodies spend countless hours trying to assess this problem. Blockchain-enabled record keeping will relieve some of the burdens that are created when we try to interpret the past.

The Blockchain Life Cycle

Blockchains originated with the creation of Bitcoin. It demonstrated that a group of individuals who had never met could operate online within a system that was desensitized to cheat others that were cooperating on the network.

The original Bitcoin network was built to secure the Bitcoin cryptocurrency. It has around 5,000 full nodes and is globally distributed. It's primarily used to trade Bitcoin and exchange value, but the community saw the potential of doing a lot more with the network. Because of its size and time-tested security, it's also being used to secure other smaller blockchains and blockchain applications.

The Ethereum network is a second evolution of the blockchain concept. It takes the traditional blockchain structure and adds several new programming languages that are built inside of it. Like Bitcoin, it has over 10,000 full nodes and is globally distributed. Ethereum is primarily used to trade Ether and create smart contracts. The most popular Ethereum smart contract is the ERC 20. It allows for the generation of interchangeable tokens. These tokens can be used for fundraising purposes.

There is a third evolution in blockchain technology that is under active development addressing speed and data size constraints. Fixing these issues will enable blockchain

technology to be used more "realistically with mainstream applications. It will take several years before it is clear what structure will win out.

Popular new developments include sharding, a type of database partitioning that separates large databases into smaller parts called data shards. An Ethereum development effort called fork choice rule splits the Ethereum blockchain into several parallel networks. It may allow Ethereum to scale more efficiently and reduce the congestion on the network, increasing transaction speeds and lowering transaction costs.

Another popular scaling theory is called POS. Broadly, POS is the concept of putting up tokens or cryptocurrency as a bond for processing transactions. If the node is corrupted and does not process the transactions accurately, the node may forfeit their tokens or cryptocurrency.

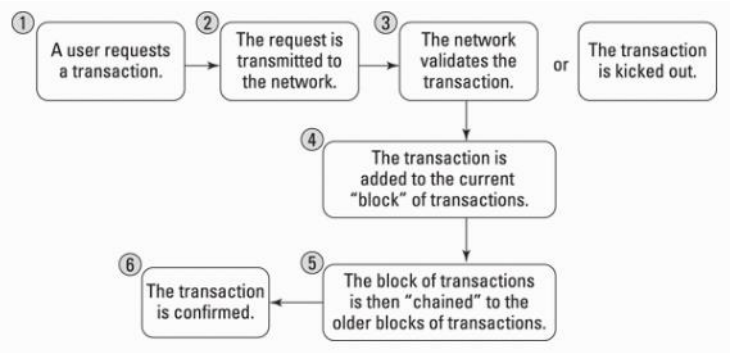
Με σχόλια [Ma2]: Is this an acronym?

A third effort to scale blockchain technology utilizes trusted nodes. For example, the Factom network operates with federated nodes and an unlimited number of auditing nodes. These nodes are trusted with ensuring the system. Factom's elected network is small, just over 60 nodes. To hedge for security risks, Factom anchors itself into other distributed networks to piggyback on the security of more extensive systems. Factom also partitions its network into smaller, faster, more easily managed parts called chains. Factom has faster transaction speeds and lower transaction costs than POW blockchains.

Consensus: The Driving Force of Blockchains

Blockchains are powerful tools because they create honest systems that self-correct without the need of a third party to enforce the rules. They accomplish the enforcement of rules through their consensus algorithm.

In the blockchain world, consensus is the process of developing an agreement among a group of commonly mistrusting shareholders. These are the full nodes on the network. The full nodes are validating transactions that are entered into the network to be recorded as part of the ledger.



Each blockchain has its own algorithms for creating agreement within its network on the entries being added. There are many different models for creating consensus because each blockchain is creating different kinds of entries. Some blockchains are trading value, others are storing data, and others are securing systems and contracts.

Bitcoin, for example, is trading the value of its token between members on its network. The tokens have a market value, so the requirements related to performance, scalability, consistency, threat model, and failure model will be higher. Bitcoin operates under the assumption that a malicious attacker may want to corrupt the history of trades in order to steal tokens. Bitcoin prevents this from happening by using a consensus model called "proof of work" that solves the Byzantine general's problem: "How do you know that the information you are looking at has not been changed internally or externally?" Because changing or manipulating data is almost always possible, the reliability of data is a big problem for computer science.

Most blockchains operate under the premise that they will be attacked by outside forces or by users of the system. The expected threat and the degree of trust that the network has in the nodes that operate the blockchain will determine the type of consensus algorithm that they use to settle their ledger. For example, Bitcoin and Ethereum expect a very high degree of threat and use a strong consensus algorithm called proof of work. There is no trust in the network.

On the other end of the spectrum, blockchains that are used to record financial transactions between known parties can use a lighter and faster consensus. Their need for high-speed transactions is more important. Proof of work is too slow and costly for them to operate because of the comparatively few participants within the network and immediate finality need for each transaction. They also do not need a token or

cryptocurrency to incentivize transaction processing. So, they eliminate these things from their system and run faster and cheaper than POW systems."

2.3 Other Blockchains in use

Thousands of blockchains and blockchain applications are in existence today. The whole world has become obsessed with the ideas of moving money faster, incorporating and governing in a distributed network, and building secure applications and hardware.

You can see many of these public blockchains by going to a cryptocurrency exchange.

The following figure shows the altcoin exchange for Poloniex (https://poloniex.com), a cryptocurrency trading platform."

Blockchains are moving beyond the trading value market and are being incorporated into all sorts of industries. Blockchains add a new trust layer that now makes working online secure in a way that was not possible beforehand.

Current blockchain uses

Most up-and-running blockchain applications revolve around moving money or other forms of value quickly and cheaply. This includes trading public company stock, paying employees in other countries, and exchanging one currency for another.

Blockchains are also now being used as part of a software security stack. The U.S. Department of Homeland Security has been investigating blockchain software that

secures Internet of Things (IoT) devices. The IoT world has some of the most to gain from this innovation, because it's especially vulnerable to spoofing and other forms of hacking. IoT devices have also become more pervasive, and security has become more reliant on them. Hospital systems, self-driving cars, and safety systems are prime examples.

Initial Coin Offerings (ICOs) are another exciting blockchain innovation. They're a type of smart contract that allows the issuer to offer a token in exchange for investment funds. Often used as a non-dilutive fundraising option, entrepreneurs globally have raised billions of dollars. Governments and regulators have been quick to crack down on ICOs. The tokens may be unlicensed securities, and the offering may be defrauding investors. The technology is impressive even if compliance issues are still being addressed.

One of the fantastic innovations inherent in ICO tokens is that they're a self-clearing and self-settling instrument. In our current system for trading securities, there are two types of clearing agencies: clearing corporations and depositories. Clearing corporations audit transactions and act as intermediaries in making settlements. Depositories hold securities certificates and maintain ownership records of the securities. Blockchains perform both these functions for tokens without needing third parties to audit and retain possession of the assets.

Future blockchain applications

Larger and longer-run blockchain projects that are being explored now include government-backed land record systems, identity, and international travel security applications.

The possibilities of a blockchain-infused future have excited the imaginations of business people, governments, political groups, and humanitarians across the world. Countries such as the UK, Singapore, and the United Arab Emirates see it as a way to cut cost, create new financial instruments, and keep clean records. They have active investments and initiatives exploring blockchain.

Blockchains have laid a foundation where the need for trust has been taken out of the equation. Where before asking for "trust" was a big deal, with blockchains it's small. Also, the infrastructure that enforces the rule if that trust is broken can be lighter. Much of society is built on trust and enforcement of rules. The social and economic implications of blockchain applications can be emotionally and politically polarizing because blockchain will change how we structure value-based and socially based transactions.