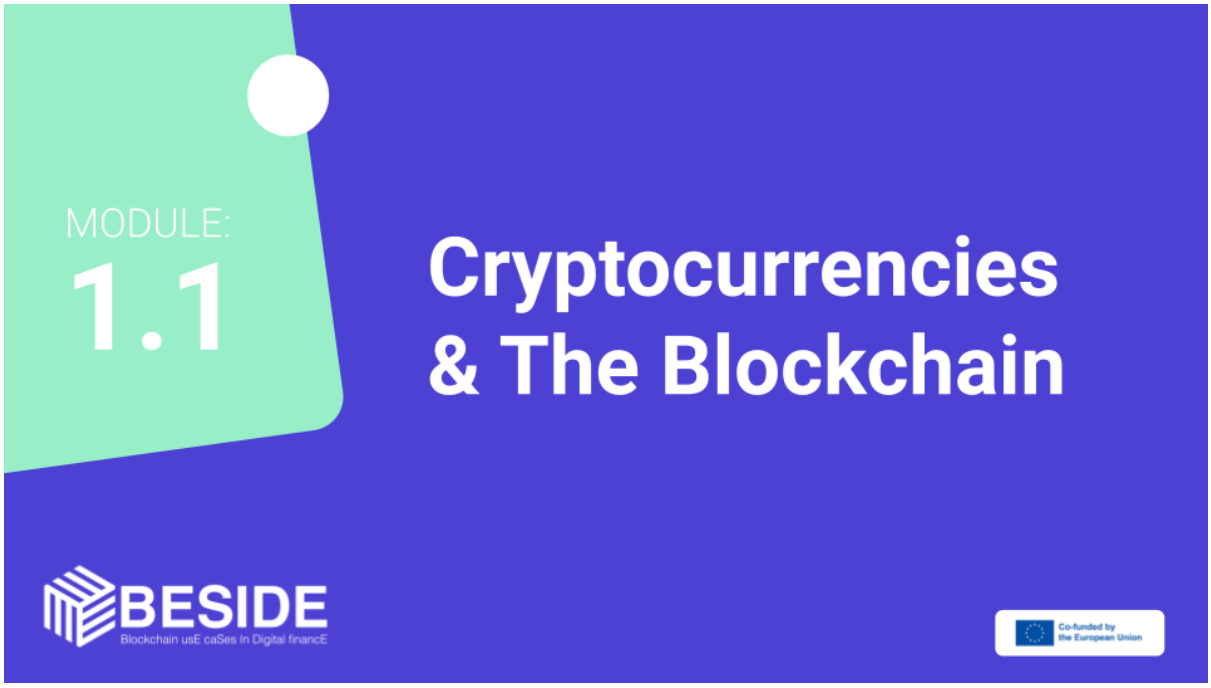
1.1 Cryptocurrencies & The Blockchain

In recent years, cryptocurrencies, NFTs, and the Blockchain are all topics making headlines. Unfortunately, these concepts may be challenging to grasp. This module aims to serve as an introductory guide, shedding light on the fundamental aspects of blockchain technology, digital currencies like Bitcoin and Ethereum, and various types of tokens, including NFTs. This is intended to be your first step toward a better understanding of these technologies that are reshaping the digital landscape.



In its most simplified form, a public blockchain is a shared append-only ledger that enforces certain rules while allowing anyone read and write access. This distributed digital ledger is a way for users to deterministically achieve consensus on a common reality without the need for any centralised parties to keep records and govern the process. Blockchain technology was first introduced by Bitcoin, though the term “Blockchain” was never specifically mentioned in the original Bitcoin whitepaper.

Bitcoin was designed to function as a peer-to-peer electronic cash system with a native, independent currency and monetary system tied to participation in the maintenance of the network and

Co-funded by the European Union
Blockchain usE caSes In Digital financE – BESIDE – 2022-1-DE02-KA220-VET-000089587 is funded by Erasmus+.
Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

processing of transactions. For the first time in history, there was a globally standardised currency that anyone can use, but nobody can monopolise control over.

While this in itself is a historic achievement, researchers interested in the technology quickly realised other potential use cases in which such a system might yield significant benefits and potentially revolutionise how we transact, exchange value, and keep records. Examples include the standardised recording of land titles, providing financial services to all regardless of factors such as location and access to legal documents, decentralised sharing economy platforms, self-sovereign digital identity, automated royalty payments for digital content, and even technology-enabled systems to support and improve governmental functions.

Blockchain technology primarily enables two functions: digital scarcity enabling value transfer and decentralised processing and validation of transactions that are immutably stored in a chronologic ledger; the emphasis with regard to more advanced applications beyond basic party-to-party asset transfer is on the latter.

1. Scarcity & The Double Spend Problem

While digital scarcity certainly plays a role, decentralised computation and execution of transactions can be used to create systems and protocols for a wide variety of use cases. The innovation here is that neither trust among participants nor the involvement of a central governing party is necessary for anyone to participate in a system or use an application.

In 2008, the Bitcoin whitepaper was published in which a decentralised peer-to-peer ledger of transactions organised into time-stamped “blocks” was proposed. By employing incentives which ensure validating nodes behave honestly without needing to be trusted, the ledger is able to record a shared “truth”.

Co-funded by the European Union
Blockchain usE caSes In Digital financE – BESIDE – 2022-1-DE02-KA220-VET-000089587 is funded by Erasmus+.
Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Bitcoin uses cryptographic puzzles, which can only be solved through trial and error, as a challenge for validating nodes. In this context, these network participants are also called “miners”. When a miner solves a puzzle, they receive a reward, paid in the native currency BTC, and may add a block to the chain. The block updates the account balances of all users in accordance with any transactions included in the block. Since there is a consensus shared by the network about how many coins are in each wallet users cannot spend more than they have, enabling digital scarcity.

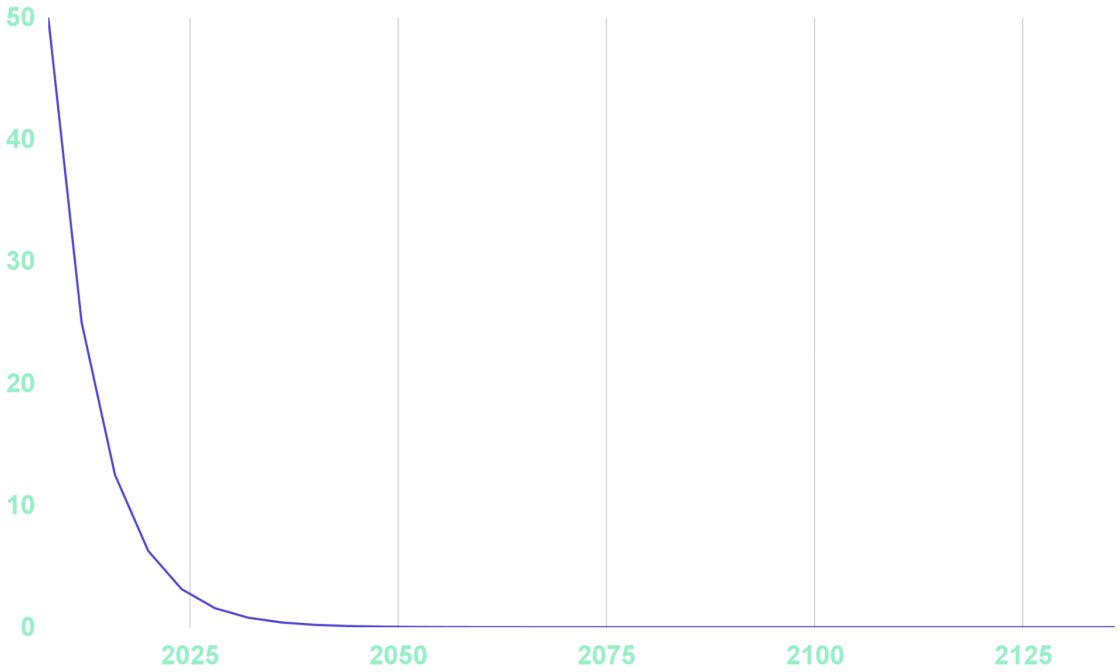
2. Cryptocurrencies

Blockchains that allow anyone to participate in the process of reaching consensus require a form of native digital currency to incentivise network security. Users also use this token for the payment of transaction fees associated with all transactions on a certain network. In the case of Bitcoin, the native cryptocurrency is also called Bitcoin, or BTC.

Other blockchain networks typically have their own native cryptocurrency such as Ether on Ethereum, Litecoin on Litecoin, and so on. These currencies all come with their own individual monetary policies. Bitcoin, for example, was created with a fixed maximum supply of 21 million coins. Rewards for miners are automatically halved every 210,000 blocks produced by the network - roughly every 4 years considering the Bitcoin network creates a block every 10 minutes. The following chart shows Bitcoin’s planned mining reward progression.

Co-funded by the European Union

Blockchain usE caSes In Digital financE – BESIDE – 2022-1-DE02-KA220-VET-000089587 is funded by Erasmus+.
Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.



Other networks have different rules for their respective native currencies. Ether, for example, does not have a maximum supply. Rewards for participating in consensus are fixed and a certain percentage of transaction fees are burned. Depending on the level of transaction fees, the total supply of Ether may increase or decrease. The native currencies are what is known as cryptocurrency.

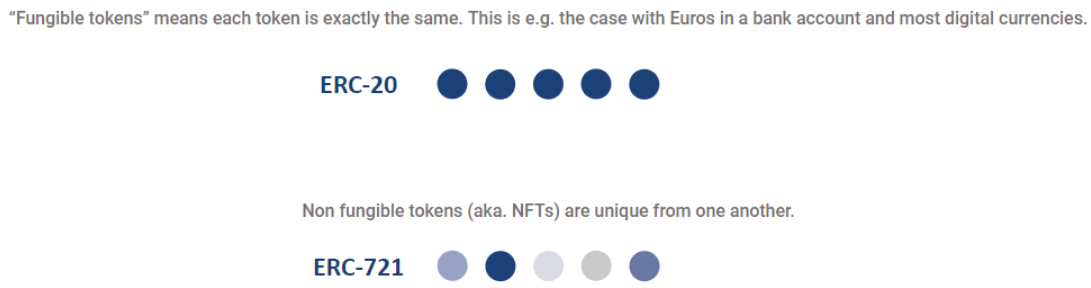
3. Smart Contracts, Tokens, and Decentralised Computation

Beyond native cryptocurrencies, an ecosystem with a variety of digital assets has begun to evolve. While Bitcoin was purpose-built as a peer-to-peer digital cash platform, other blockchain networks support more customisable functionalities and support for programming languages. Pieces of software written and deployed on a blockchain network are typically called “smart contracts” while blockchains which support their deployment are termed “smart contract platforms”. Beyond storing account balances, they are also able to store a “state” of data.

One of the most notable use cases of smart contracts is the creation of tokens. Tokens are digital assets that exist on a blockchain, created through the deployment of a smart contract. Unlike native cryptocurrencies like Bitcoin or Ether, which are integral to their respective blockchain networks,

Co-funded by the European Union
Blockchain usE caSes In Digital financE – BESIDE – 2022-1-DE02-KA220-VET-000089587 is funded by Erasmus+.
Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

tokens are secondary assets that leverage the underlying infrastructure of a smart contract platform. The creation of tokens is generally governed by a set of rules encoded within the smart contract, specifying attributes like supply cap, divisibility, and ownership rights. These tokens can represent anything from a unit of value in a decentralised application, to ownership of a physical asset like real estate, to a vote in a governance system. Because they are programmable, tokens can have a wide array of functionalities and use-cases, including but not limited to utility tokens, governance tokens, non-fungible tokens (NFTs), and more. In fact the only difference between NFTs and fungible tokens is the supply, as showcased below:



There are of course many different types of token contracts based on specific use cases they may need to fullfill. Token contract standards are set in the form of ERC standards. ERC 20 and ERC 721 are currently the most common token types.

Smart contracts may also be used to deploy programs made up of "if, then" statements. In this case, smart contracts act in the same way a vending machine does. If payment for and selection of an item is available as inputs, the process of dispensing the selected item is executed. Since this execution happens on-chain, i.e. through the same consensus process as discussed above, this transaction is trustless. This concept is called decentralised computation. Decentralised computation and execution of transactions can be used to create complex systems and protocols for various use cases. The innovation here is that neither trust among participants nor the involvement of a central governing party is necessary for anyone to participate in a system or use an application.

A simple example of a smart contract in action is the "payment splitter" contract which distributes any received cryptocurrency to various parties according to predefined conditions as showcased below.

Co-funded by the European Union

Blockchain usE caSes In Digital financE – BESIDE – 2022-1-DE02-KA220-VET-000089587 is funded by Erasmus+.
Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Decentralised computation via a smart contract network allows for guaranteed neutral execution of pre-defined logic. This is useful as it removes the need for trust when engaging in even complex transactions. Decentralised computation is practical when building so-called Decentralised Applications (dApps). User-facing applications utilising a blockchain in its back-end. Currently, the primary use for dApps is in finance, primarily on the Ethereum blockchain. Decentralised finance (DeFi) is an umbrella term for decentralised exchanges, lending protocols, derivatives, insurance, and more. All logic for such applications is written ahead of time in the form of a smart contract and published on a blockchain. Once published, the code cannot be changed but it can be audited by all parties. The logic outlined in the contract is executed when a party interacts with the contract. This allows parties to engage in complex transactions without the need to trust one another - the operation is trustless. There is no need for a bank, a government, a notary, an escrow agent, or any other middleman whose role traditionally is to help overcome issues of trust. This has the potential to drastically streamline and disintermediate a wide variety of transactions, even beyond finance.

4. Conclusion and Future Outlook

The emergence of a universally accessible and non-monopolistic digital currency through Bitcoin was just the beginning; innovations in the space have burgeoned to encompass a myriad of applications far exceeding mere “a to b” financial transactions. Blockchain's core features of digital scarcity and decentralised validation have provided fertile ground for advancements in various domains. Through the facilitation of smart contracts, tokens, and decentralised computation, blockchain has enabled the creation of an entirely new digital asset ecosystem.

Co-funded by the European Union

Blockchain usE caSes In Digital financE – BESIDE – 2022-1-DE02-KA220-VET-000089587 is funded by Erasmus+.
Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

As the underpinning technology matures and sees more widespread adoption, blockchain's potential to democratise access to financial services, introduce transparent and auditable governance models, and offer more efficient, trustless systems cannot be overstated. The decentralised nature of these systems could substantially reduce the need for intermediaries, lowering costs and barriers to entry in various sectors, from real estate to supply chain management and beyond. However, as with any transformative technology, challenges such as scalability, energy consumption, and regulatory ambiguity remain. These must be addressed to fully realise the breadth of blockchain's potential impact.

In sum, blockchain technology represents a seismic shift in the way humanity transacts, governs, and interacts. Whether it's the mainstream adoption of cryptocurrencies, the rise of Decentralised Finance (DeFi), or the conceptualisation and realisation of self-sovereign identities, the influence of blockchain is undeniable and only likely to grow. The coming module covers various use cases, suggests how use cases may be evaluated, and more.

Co-funded by the European Union

Blockchain usE caSes In Digital financE – BESIDE – 2022-1-DE02-KA220-VET-000089587 is funded by Erasmus+.
Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.