GENERATION BLOCKCHAIN

Master Curriculum
Blockchain Technology & Cryptocurrencies

www.**generationblockchain**.eu

2022-2024
OERS

By
Frankfurt School of Finance & Management

Co-funded by the European Union

contents

Co-funded by the European Union

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 National Agency. Neither the European Union nor National Agency can be held responsible for them.

01 | INTRODUCTION TO THE COURSE

Welcome to the Course Blockchain Technology & Cryptocurrencies

Before diving into the content, we highly recommend that you review the course syllabus. You can find the most important information related to the course in the syllabus, including:

- Course overview
- Course prerequisites and duration
- Course learning objectives and curriculum outline
- Course timing
- Grading and course completion
- Information about the ERASMUS+ project “Generation Blockchain”

About the ERASMUS Project “Generation Blockchain”

The ERASMUS+ project “Generation Blockchain” aims at contributing to the enhancement of digital learning and teaching in higher education institutions and the development of advanced student skills such that they are better prepared to contribute to the digital transformation of society. This project is a collaboration between University of Szczecin in Poland, Frankfurt School Blockchain Center in Germany, Momentum Educate+Innovate in Ireland, Amsterdam University of Applied Sciences in the Netherlands, European E-Learning Institute in Denmark and University of Porto in Portugal.

This course has been funded with support from the European Commission within the Erasmus+ programme. This course only reflects the views of the project partners, and the Commission and National Agency of the Erasmus+ programme cannot be held responsible for any use which may be made of the information contained therein.

01

MODULE 1

Introduction to Blockchain Technology & Cryptocurrency Curriculum

Co-funded by the European Union

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 National Agency. Neither the European Union nor National Agency can be held responsible for them.

contents module 1

Co-funded by the European Union

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 National Agency. Neither the European Union nor National Agency can be held responsible for them.

01| MODULE 1 Introduction to Blockchain Technology

Chapter Overview

In this module, we will examine a brief history of distributed ledger technologies, specifically blockchain technology and how it is designed (i.e., cryptography, block structure, mining and consensus). This foundation will allow you to understand blockchain technology and it facilitates to make use of current internet protocols while improving and adding to them. Additionally, we will dive into the history of money and especially Bitcoin as the first application of blockchain technology. As a point of reference, we will look at the characteristics of Bitcoin's blockchain, specifically its peer-to-peer network which allows to store transactions, provides transparency and immutability as well as different consensus mechanisms.

Learning Objectives

After the first module, you should be able to:

- Explain the difference between blockchain technology and distributed ledger technology (DLT).
- Discuss blockchain technologies and early money.
- Explain the difference between blockchain and the cryptocurrency Bitcoin.
- Explain how the Bitcoin blockchain works.
- Discuss blockchain characteristics.
- Explain blockchain components such as mining and consensus.
- Explain what a block in a blockchain is composed of.
- Explain how transactions on a blockchain work.
- Discuss the advantages and disadvantages of the consensus mechanisms Proof-of-Work and Proof-of-Stake.
- Explain the three main functions of money.

01| INTRODUCTION TO DLTS & BLOCKCHAIN TECHNOLOGY

Introduction to Module 1

To lay the foundation for this course, we will first introduce you to Distributed Ledger Technology (DLT) and Blockchain as one of its sub-categories.

1.1 What is Blockchain Technology?

On a fundamental level, blockchain technology is a database structure based on the principle of a decentral, immutable, and transparent digital transaction book. With it, assets and information of various forms can be managed, stored, and transferred. The word blockchain refers to its database structure. Each transaction is recorded in the form of a block of data alongside other data required for the transaction to be validated. The details of transaction data will be discussed later in module 1. Each block is cryptographically connected to its precedent and subsequent block. Accordingly, each block confirms its place in the sequence of transactions. As transactions and storage of data occur, these blocks form a chain of data – the blockchain.

A blockchain is a digital ledger controlled by a distributed public computer network. A distinction is made between public (public or permissionless) blockchains and private (private or permissioned) blockchains. More broadly, a ledger refers to an information storage that keeps records of transactions that are intended to be final, definitive and immutable. A distributed ledger is not stored centrally but is stored and updated ledger on many different computers (so-called nodes). A distributed ledger as a specific calibration of a ledger is a ledger that is shared across a set of distributed ledger technology (DLT) nodes and synchronized between the DLT nodes using a consensus mechanism which is designed to be tamper resistant, append-only and immutable containing confirmed and validated transactions or information.

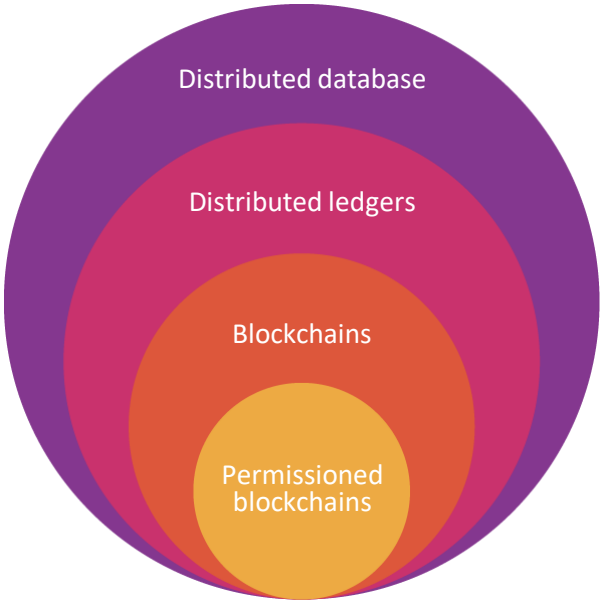


Figure 1: Relationship between distributed ledgers and blockchains

1.2 Different Types of Blockchain Networks

Blockchain systems can be centralized, decentralized or distributed network systems.

Centralized Network

All nodes are connected under a single authority

Decentralized Network

No single authority controls the nodes

Distributed Network

Every node is independent and interconnected with each other

Figure 2: Blockchain network architecture

Within this initial differentiation, there are four main types of decentralized or distributed networks in the blockchain which are public blockchain networks, private blockchain networks, hybrid blockchain networks and consortium blockchain networks.

1

Public Blockchain Networks

Public blockchain networks do not require a central authority to give permission for participation. Per default, a public blockchain network does not restrict access to any user. This equality is also given in the right for all participants to read, edit, and validate the blockchain. Examples for public blockchain networks include Bitcoin, Ethereum, and Litecoin.

2

Private Blockchain Networks

In a private blockchain network, a single organization or institution controls private blockchains which are also referred to as managed blockchains. The authority running the private blockchain determines which participants have rights or rights such as access and voting. Decentralization only exists to a certain degree on private blockchains since they have access restrictions. An example of a private blockchain network is Ripple, a digital currency exchange network for businesses.

3

Hybrid Blockchain Networks

Hybrid blockchain networks combine aspects of private and public blockchain networks. One use-case for hybrid blockchains is in banking, where the central institution can grant public access to digital currency but at the same time keep bank-owned currency private. In this way, part of the data stored on the chain is publicly accessible and part of the data is restricted by access control.

4

Consortium Blockchain Networks

In a consortium blockchain network, there is a group of selected organizations that can govern access, reading and editing rights. This setup is commonly used in industries in which several organizations have common goals and benefit from shared responsibility over goods, data, or assets. For example, the Global Shipping Business Network Consortium is digitizing the shipping industry and increasing collaboration between maritime industry stakeholders.

1.3 Features of Blockchain Technology

Blockchain technology is usually in the form of a decentralized database structure or digital register that transparently records transactions and serves as the basis for many digital currencies. The distinct characteristics of blockchain technology are decentralization, immutability, and transparency. It is ultimately an openly viewable ledger that transparently documents all transactions. Typically, such a ledger is not stored centrally but is stored and updated on many different computers or nodes. The decentralized storage ensures that a blockchain does not have to be managed by a central authority, eliminating the risk of a single point of failure. Next to transparency, blockchain technology has the three following main features:

Decentralization

Decentralization in blockchain refers to transferring control and decision-making from a centralized entity (i.e., individual, organization, group) to a distributed network. Decentralized blockchain networks use transparency to reduce the need for trust among participants. These networks also deter participants from exerting excessive authority or control over one another in ways that degrade the functionality of the network.

Immutability

Immutability means something cannot be changed or altered. No participant can tamper with a transaction once a node has recorded it in the shared ledger. If a transaction record includes an error, one must add a new transaction to reverse the mistake, and both transactions are visible to the network.

Consensus

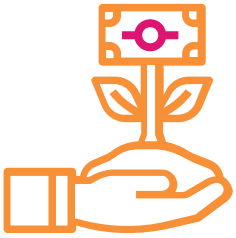
A blockchain system establishes rules about participant consent for recording transactions. You can record new transactions only when the majority of participants in the network give their consent. Figuratively, the blockchain can be thought of as a chain of blocks, each of which links transaction data together. The transactions are combined into blocks, checked for validity, and appended to the previous chain of blocks in a process called Proof of Work (PoW) for Bitcoin. The PoW approach involves solving computational problems that can only be solved through frequent trial and error. This ensures that sufficient work is invested in calculating and securing the transactions. Next to PoW, there is a myriad of other consensus mechanisms that may be chosen for specific use cases based on their specific advantages and disadvantages.

1.4 What Are the Key Components of Blockchain Technology?

Blockchain architecture has the following main components:

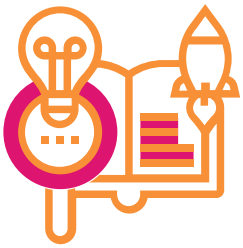
Distributed Ledger

A distributed ledger is the shared database in the blockchain network that stores the transactions, such as a shared file that everyone in the team can edit. In most shared text editors, anyone with editing rights can delete the entire file. Not so in DLT – have strict rules about who can edit and how to edit. You cannot delete entries once they have been recorded.



Smart Contracts

Companies use smart contracts to self-manage business contracts without the need for an assisting third party. Smart contracts are programs stored on a blockchain system that are triggered automatically when predetermined conditions are met. Specifically, smart contracts conduct if-then statements so that transactions can be completed confidently. For example, a lottery may determine that the price money of the lottery is distributed amongst those parties that win the lottery by guessing the numbers correctly. The information about the correct number would be part of the if-then statement.



Public Key Cryptography

Public key cryptography is a security feature to uniquely identify participants in the blockchain network. This mechanism generates two sets of keys for network members. One key is a public key that is accessible to everyone in the network. The other is a private key that is unique to every member. The private and public keys work together to unlock the data in the ledger which will be touched on in a later chapter.

For example, Bob and Alice are two members of a network. Alice records a transaction that is encrypted with her private key. Bob can decrypt it with his public key. This way, Bob is confident that Alice made the transaction. Alice's public key would not have worked if Bob's private key had been tampered with.

1.5 The Difference Between a Database and a Blockchain

Blockchain is a certain type of database management system containing more features as compared to regular databases. Some of the significant differences between a traditional database and a blockchain are the following:

- The control is decentralized in blockchains without damaging trust in the existing data which other database systems cannot achieve to this extend.
- Normally, companies involved in a transaction are not entitled to share their entire database with third parties. In blockchain networks, every participating entity has a (transparent) copy of the current status of the ledger with automatic updates.
- Blockchains are immutable, meaning that you may only insert data, but you cannot edit or delete data.

1.6 Development of Blockchain Technology

The history of blockchain and that of Bitcoin are intertwined. In 2008, the Bitcoin white paper was published. This white paper presented a conceptual design for a decentralized monetary system. The development of blockchain technology has reached new highs since Satoshi Nakamoto as the unknown author, published the Bitcoin whitepaper. In the meantime, possible applications for blockchain technology exist that go far beyond the function of a financial transaction ledger. For example, smart contracts can be used to handle a wide variety of administrative and process applications that a regular blockchain base-layer is not capable of. The execution of these smart contracts can be tracked in real-time - as a logical further development of the open-source idea, the blockchain thus makes open execution possible.

Thus, thanks to the rapid blockchain development, sensitive data such as health data or property relations such as land ownership can be organized and controlled via a blockchain in this way. At the same time, every entry ever made in a blockchain directory can be traced forever and cannot be deleted or changed. Accordingly, companies are interested in researching this technology. The main motivations are the aspects of security, transparency and increased efficiency (in cost, time, workforce and digitalization). The possibility of automating processes via a secure infrastructure while eliminating the risk of data manipulation appears appealing to institutions and companies.

It must be kept in mind that there is no such thing as "the one blockchain." Rather, a blockchain can be designed in very different calibrations. A blockchain used in the administration of a public authority is designed differently than, for example, the most well-known blockchain, the Bitcoin Blockchain, on which a large number of applications are based.

1.7 Benefits of Blockchain Technology as Compared to Traditional Database Systems

Traditional database technologies present several challenges for recording financial transactions. For instance, consider the sale of a property. Once the money is exchanged, ownership of the property is transferred to the buyer. Individually, both the buyer and the seller can record the monetary transactions, but neither source can be trusted with the complete elimination of doubt. The seller could claim they have not received the money even though they have, and the buyer could equally argue that they have paid the money even if they have not.

To avoid potential legal issues, a trusted third party has to supervise and validate transactions. The presence of this central authority not only complicates the transaction but also creates a potential single point of failure and adds vulnerability. If the central database was compromised, both parties could suffer as a consequence. Blockchain could mitigate such issues by creating one ledger each for the buyer and the seller. All transactions must be approved by both parties and are automatically updated in both of their ledgers in real-time. Any corruption in historical transactions will corrupt the entire ledger. These properties of blockchain technology have led to its use in various sectors, including the creation of digital currency like Bitcoin and other use cases which are subject to the next chapter.

02

BLOCKCHAIN USAGE IN DIFFERENT INDUSTRIES

2.1 Financial Market Use Cases for Blockchain Application

International Payments

Blockchain can create secure, efficient, tamper-proof records of sensitive activity. This is beneficial in the context of international payments and money transfers where high transaction fees, various intermediaries, and long settlement times are still the norm. The commercial bank Banco Santander launched the world's first blockchain-based money transfer service in 2018. The so-called "Santander One Pay FX" customers can make same-day or next-day international money transfers. By using blockchain, Santander was able to reduce the number of intermediaries typically required in these transactions and lower the costs of transfers through less manual work required, making the process more efficient.

Capital Markets

In capital markets, blockchain technology can contribute to faster clearing and settlement, the consolidation of audit trails and operational improvements (e.g., tokenizing stocks and less manual work, monitoring of richer data sets, market surveillance, fund portfolio management).

Trade Finance

Traditionally, the common methods of trade financing involve slow processes which interrupt business and hamper liquidity. This is due to the fact that cross-border trade involves lots of data (i.e., country of origin, product details, documentation of transactions). Blockchain technology can automate this data tracking and monitoring.

Regulatory Compliance and Audit

In accounting and auditing decreases the possibility of human error and the correctness of data. Account records cannot be changed once they are recorded on a chain.

Money Laundering Protection

Through the record-keeping on chain, supported by the "Know Your Customer (KYC)," process by which a business identifies and verifies the identities of its clients, coins, tokens and addresses that launder money or a suspected to do so can be blacklisted, leading to detection of fraudulent activities involving funds and business.

Insurance

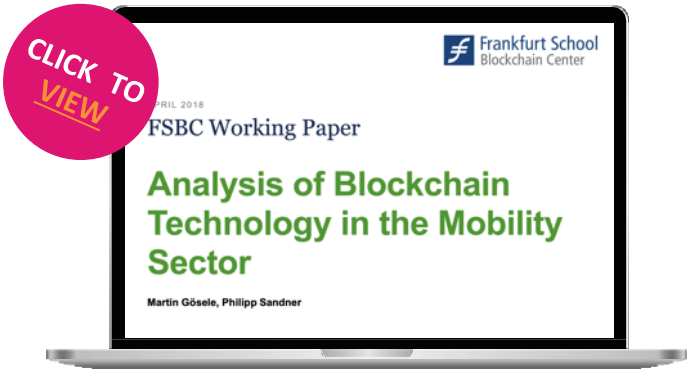
Blockchain in connection with smart contracts in insurance schemes has various application use cases. Moving insurance claims onto a blockchain can lead to the reduction of common sources of fraud in the industry (i.e., by rejecting multiple claims on one incident). There is also the possibility for medical records (or rather only the relevant parts) to be cryptographically secured and distributed between insurance companies, doctors and the patient. Another example would be filing a death claim whereby the manual process of filing claims is replaced with an automated blockchain system.

Peer-to-Peer Transactions

P2P payment services such as PayPal, Swish or Venmo offer fast and cheap transactions with e-money in many parts of the world, though some services restrict transactions based on location. Transaction fees, the risk of hacks and bankruptcies and the need for an intermediary can be reduced or eliminated by introducing a blockchain-based system.

2.2 Industry Use Cases for Blockchain Application

To learn about industry use cases for blockchain application in the mobility sector, read the excursion paper "Analysis of Blockchain Technology in the Mobility Sector" by Prof. Dr. Philipp Sandner and Martin Gösele.



03

WORKING MECHANISMS OF BLOCKCHAIN TRANSACTIONS

3.1 How does a Transaction on Blockchain Work?

Blockchain mechanisms are complex, the following gives a brief overview of transaction processing on blockchains. Start by watching this blockchain demo.

Start by watching this blockchain demo.

You can also try out the blockchain demo tool yourself. To do so, click here.

Record the Transaction

A blockchain transaction shows the movement of physical or digital assets from one party to another in the blockchain network. It is recorded in a data block and includes details such as (e.g., Who was involved in the transaction? When did the transaction occur? How much of the asset was exchanged?).

Figure 3: Sample Bitcoin transaction (Source: Mempool Space, accessed on 27.10.2022)

As indicated in the figure, the transaction ID is the unique identifier used to track the transaction, all transactions are traceable through block explorer websites. The input address indicates who the sending address(es) of the funds is/ are, the output address is the funds receiving addresses. In this case, there is one external receiving address and the input address receives the unspent Bitcoin back via the input address. The transaction information lists details about the transaction such as the amount of fees paid to the miner, the total amount of Bitcoin input. The difference between the total amount of Bitcoin input and output determines the transaction fee.

The block information gives information about the block size (1.12 MB in this example), the median miner's fee that has to be paid to miners in order for your transaction to be included in the block, which miner/ mining farm mined the block and other key information. All transaction data (see Figure 3) is listed for each individual transaction in the block itself. The block information (see Figure 4) is so to speak only the summary of the transaction data within the block. Generally speaking, the Bitcoin block size is around 1MB, though there are proposals and discussions about enlarging the block size to achieve more scalability for Bitcoin as a transaction network.

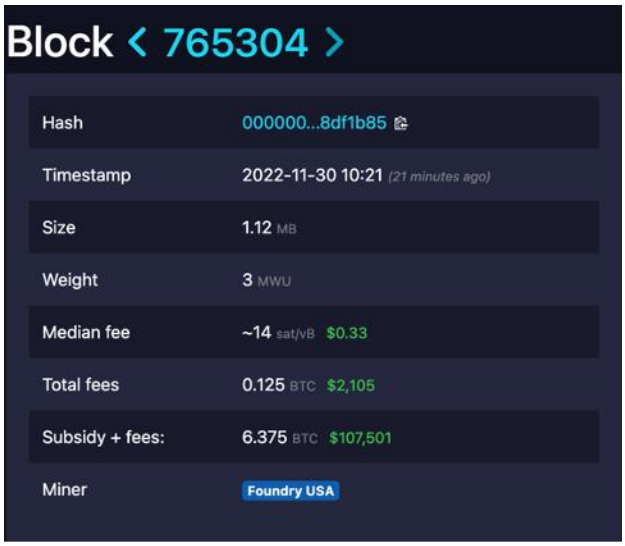


Figure 4: Sample Bitcoin transactions (Source: Mempool Space, accessed on 30.11.2022)

Finding Consensus

Most participants on the distributed blockchain network must agree on the current state of the network and the validity of transactions via using consensus mechanisms. Consensus means that there is a general agreement on the current state of the network. Depending on the type of network, rules of agreement can vary but are typically established at the start of the network. Imagine a group of people going to the movies. If there is no disagreement about a proposed movie selection, a consensus is reached. If a consensus cannot be found, the group could split up and go separate ways. In terms of the blockchain, the process is formalized and reaching consensus means that at least 51% of the nodes in the network agree on the next global state of the network.

Link the Blocks

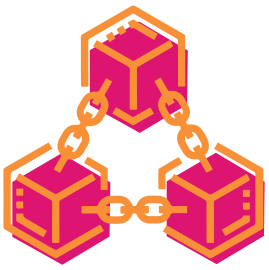
Once consensus has been reached, transactions on the blockchain are written into blocks. A cryptographic hash is also appended to each new block, as was shown in the video previously. The hash then creates the chain linking the blocks together. If the data in the block is edited, the hash value changes which shows tampering. Each additional block re-verifies the previous block.

Share the Ledger

The system then broadcasts the newest copy of the central ledger to all participants in the network which updates the status of the stored copy of the blockchain for all participants. Mining requires significant computational resources and takes a long time due to the complexity of the software process. In exchange, miners earn a small amount of cryptocurrency. The miners act as modern clerks who record transactions and collect transaction fees. All participants across the network reach a consensus on who owns which coins and or tokens.

3.2 What Are the Benefits of Blockchain Technology?

Blockchain technology brings many benefits to asset transaction management:



Advanced Security

Blockchain systems provide the high level of security and trust that modern digital transactions require. There is always a fear that someone will manipulate underlying software to generate fake money for themselves. But blockchain uses the three principles of cryptography, decentralization, and consensus to create a highly secure underlying software system that is nearly impossible to tamper with. There is no single point of failure, and a single user cannot change the transaction records.

Improved Efficiency

Business-to-business transactions can take a lot of time and create operational bottlenecks, especially when compliance and third-party regulatory bodies are involved. Transparency and smart contracts in blockchain make such business transactions faster and more cost and time efficient.

Faster Auditing

Enterprises must be able to securely generate, exchange, archive, and reconstruct e-transactions in an auditable manner. Blockchain records are chronologically immutable, which means that all records are always ordered by time. This data transparency makes audit processing faster.

3.3 What is the Difference Between Bitcoin and Blockchain?

Bitcoin and blockchain might be used interchangeably, but they are two different things. Since Bitcoin was an early application of blockchain technology, people inadvertently began using Bitcoin to mean blockchain, creating this misnomer. As was shown in a previous chapter, blockchain technology has many use cases outside of Bitcoin. Bitcoin is a digital currency that operates without any centralized control and uses blockchain technology as the underlying infrastructure.

04

THE HISTORY OF MONEY

4.1 History of Money

Money itself is as old as civilization, even in the most primitive societies, useful and valuable objects were used as means of payment. Natural or commodity money are generic terms for these early forms of money. In the course of history, a wide variety of things were used as money. These include food, farm animals, weapons, jewelry, clothing and also the shells of snails. Thus, the most widespread means of payment in terms of space and time is the cowrie snail, which is often mistakenly called 'cowrie shell'. Cowries, the most successful means of payment in world history to date, were used in large parts of Africa and Asia. Findings in China even suggest that the cowrie shell was used as money there as early as the 2nd millennium BC. Usually, these types of money were bartered, meaning that you would need to exchange one good that you owned with a different good that you desired, making interchangeability a rough estimation game.

This money in kind or commodity money was replaced with increasing trade by coins, which had exclusively money function. The first coins were struck in the kingdom of Lycia in the 7th century BC. These were shapeless lumps of electrons, a naturally occurring gold-silver alloy. Coinage made trade much easier, and so the new cultural technique of payment spread from Asia Minor to Europe in antiquity. Slowly, coins were also minted in Greece and Rome. Ancient rulers began to stamp their portraits on the coins, which were thus not only a means of payment but also image carriers. With the end of the Roman Empire in the 5th century AD, the ancient era of coinage also ended, and in late antiquity and the early Middle Ages, the circulation of coins throughout Europe declined sharply. It was not until the High Middle Ages, in the 12th century, that the transition from a natural to a monetary economy took place again in Italy, and with it, coins reappeared. However, there was no longer a uniform coinage system as in the Roman Empire. Thus, in the Holy Roman Empire of the German Nation, which was characterized by small states, many different currencies circulated. In the late Middle Ages, the Rhenish florin finally prevailed as a kind of reserve.

Paper money as we know it today did not become established until relatively late. Yet paper money has appeared as a means of payment throughout history, for example in China in the 10th century AD. In Europe, it was introduced much later. It was not until the Bank of England in Great Britain adopted it that it succeeded in creating lasting public confidence in paper money. In 1833, the English government declared banknotes to be legal tender and thus became a pioneer. Due to the rapidly growing economy in the age of industrialization, the supply of money was of essential importance. This led to a gradual move away from precious metal currencies. Coinage became small change.

Money, regardless of its shape or form, is often defined in terms of three functions or services:

1 **Store of value:**
value is upheld or increased over a long period of time.

2 **Unit of account:**
providing a common measure of the value of goods and services being exchanged and has to be fungible, divisible and countable.

3 **Medium of exchange:**
is an intermediary instrument or system used to facilitate trade of goods between parties.

Money can be any good that is widely used and accepted in transactions involving the transfer of goods and services from one person to another. In today's world there are two traditional forms of money, fiat money and commercial bank money. Fiat money, in the form of notes and coins, receives its value because the government declares fiat money to be legal tender, which requires all merchants and traders within the country to accept it as a means of settling debt. By definition, fiat money has an intrinsic value, which is significantly lower. Its value is derived through supply and demand forces. This is the form of currency with which we are most familiar.

An additional form of money is commercial bank money which can be described as claims against financial institutions that can be used to purchase goods or services. What all these types of money have in common are the basic characteristics of money:

1 Durability

2 Portability

3 Liquidity

4 A unit of account

5 Legal tender status

6 Resistance to counterfeiting

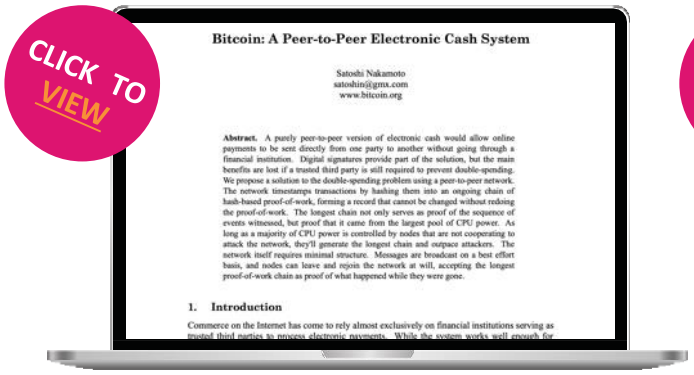
4.2 Introduction to Bitcoin & the Bitcoin Blockchain

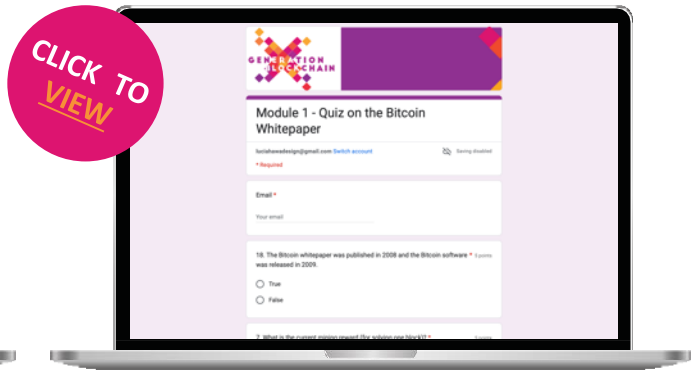
Bitcoin

To understand Bitcoin, it is crucial to read the Bitcoin whitepaper as Bitcoin is the most important crypto asset as measured by market capitalization. Note that you do not have to understand the technological parts in detail at this stage. Reading the white papers is supposed to provide a high-level overview of the intentions of Bitcoin and the mechanics of the technology.

Access the whitepaper here.

After reading through it, test your understanding with this quiz.

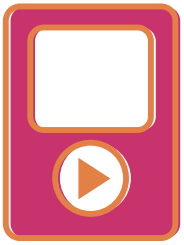




Bitcoin Wallets

What are Bitcoin wallets and which kinds of wallets are there? To get an overview of this topic, listen to the Generation Blockchain Podcast Episode “Bitcoin Wallets”.

Generation Blockchain Podcast Episode “Bitcoin Wallets”



Example of a Bitcoin public key:
Bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh

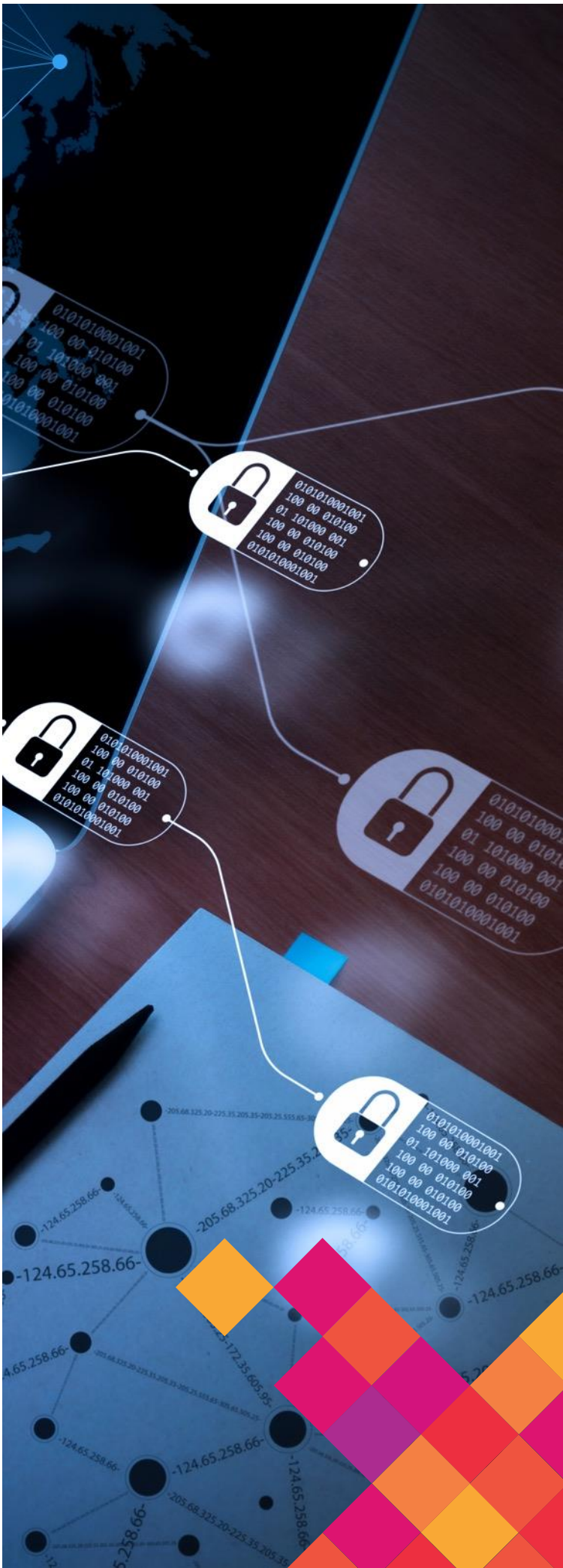
! DO NOT SEND BITCOIN TO THIS ADDRESS, BITCOINS SENT TO THIS ADDRESS WILL BE IRREVERSIBLY LOST!

Bitcoin Network

A public ledger records all Bitcoin transactions, and servers around the world hold copies of this ledger. The servers are like banks. Although each bank knows only about the money its customers’ exchange, Bitcoin servers are aware of every single Bitcoin transaction in the world. Any computer can set up a node. This is like opening your own Bitcoin bank instead of a bank account. Note that setting up a node is not equivalent to being a miner.

Bitcoin Mining

Around the clock and without downtime, people transfer Bitcoins through the Bitcoin network. On the public Bitcoin network, members mine for cryptocurrency by solving complex mathematical crypto calculations to create new blocks. Bitcoin mining is the process of providing computing power for transaction processing, securing and synchronizing the current blockchain status for all users on the network. Mining is a type of decentralized Bitcoin data center with miners all over the world. This process is called mining which is reminiscent of gold mining. Unlike gold mining, there is a reward for useful services in Bitcoin mining. The payout of the respective Bitcoin shares is based on the computing capacity provided. In 2022, the block reward for miners is 6.25 BTC per new block. Miners compete with one another to solve the calculation for the next block the fastest. The block of the miner that manages to solve the cryptographic calculation first is eventually recorded in the next block in the blockchain. The blocks of the other miners are invalid and cannot be appended to the chain. The block time which defines the time it takes to mine a block for Bitcoin is 10 minutes on average. All miners start to solve the puzzle simultaneously. The time to solve the puzzle depends on the current rate of difficulty. If relatively more miners are trying to solve the puzzle at the same time, it will be solved faster on average for a short amount of time until the level of difficulty adjusts to the total number of miners, evening out the block time of 10 minutes. New Bitcoins are not mined based on demand, the total amount of Bitcoin is fixed since its inception (at 21 million) and cannot be inflated by monetary tools. Traditional fiat currency systems, governments or central banks print more money when there is a need. Rather, Bitcoin is mined itself or in the cloud (cloud mining). The system broadcasts each new transaction publicly to the network which means that the nodes in the network share transactions with other nodes. A new block acts like the definitive account book of Bitcoin.



05

INFRASTRUCTURE OF BLOCKCHAIN TECHNOLOGY

Your first touchpoint with the infrastructure of blockchain technology will be learning in-depth about the elements and participants of it (i.e., miners, nodes, hash functions, public-key cryptography, digital signatures and addresses).

5.1 Blockchain Technology

The blockchain documents every transfer of money made within a certain network (e.g., the Bitcoin network). This ensures that no one can spend the same set of their money twice. Through this, blockchains managed to solve the so-called double spend problem in the digital world. Instead of sending out copies of one original item or asset, blockchains enable digital things to exist in only one location at a certain moment in time. Digital money and assets would not be operable if a copy of that money or asset could be sent twice.

5.2 Nodes

The nodes which are a network of computers, run a blockchain and form its core infrastructure. Nodes in the network are exchanging information on new incoming transactions and the formation of blocks. It is important to note that there exist different types of nodes. A full node is a node that maintains a full copy of the blockchain and has offline capabilities whereas a light node does not keep a copy of the blockchain and is more limited in its functionalities (i.e., it only downloads the block header instead of the complete block). Before a light node can be part of a blockchain network (i.e., to send or validate transactions), it needs to be connected to a full node. In this sense, the blockchain network is similar to the infrastructure supporting your phone.

Full nodes can be compared to the cell phone tower that your phone (i.e., the light node) is connecting to. All the antenna stations (i.e., full nodes) – are connected to each other and make up the communication network infrastructure. If you want to make a call with your phone, you need to connect to a cell phone tower first before you can interact with any other mobile phone. Similarly, in the distributed network of a blockchain, the full nodes are up and running most of the time and make up the distributed network. They also maintain a copy of the entire blockchain. You are likely to use a light node if you use a wallet on your phone or computer. In this case, you are going to connect to a full node first before you can interact with the blockchain. Participants of a network decide to run a full node if they want to contribute to the stability and security of the network, but to use cryptocurrencies it is not a necessity.

5.3 Miners & Validators

Every miner is a node in the blockchain network but you do not need to be a miner to run a node. Miners support the network by forwarding information and maintaining a copy of the blockchain, just like all the other nodes. As opposed to non-miner nodes, miners are responsible for creating new blocks in the chain of blocks. Each block in a blockchain is a collective decision on the history of a given point in time. To find a collective decision, the network finds a consensus on which transactions are included in the next block and in which sequence. Not all proposed blocks by miners are the same. One reason for that is that it takes differing amounts of time for new transactions to spread across the entire network, causing differing transaction pools of unverified transactions to gather.

In Ethereum, miners are called validators since Ethereum switched from its Proof-of-Work to the Proof-of-Stake algorithm. A validator is essentially a voter for a new block. The more votes a block receives, the more likely it is that it will be chosen.

The reason why miners have an interest in acting honestly and in the interest of the network is because they are incentivized to behave according to the rules of the blockchain. If an invalid transaction is put into a block, this block has no chance of being the winning block given its faulty data entry. The miner solving the puzzle first is rewarded with the block rewards and/ or the transaction fee that anyone sending a transaction via the Bitcoin and Ethereum blockchain has to pay in order for the transaction to be included in one of the next blocks. The probabilistic chance to receive the block reward and the transaction fees creates the incentive for individuals to purchase and run the costly hardware needed to solve the cryptographic puzzle. The first miner to solve a block receives a reward in the currency that she is mining. The winning miner is allowed to send themselves a transaction with a few coins (depending on the blockchain and cryptocurrency) that did not exist before.

Miners receive the final batch of transaction data, which is then run through a cryptographic algorithm. During this process, a hash, a string of numbers and letters that does not reveal any transaction data, is generated and used to verify validity. The hash ensures that the corresponding block has not been subject to changes. If even one number is off or out of place, the corresponding data generates a different hash. The hash of the previous block is integrated into the next block, so that if anything has been changed in the previous block, the generated hash will change. The hash value must also be below a target value set by the hash algorithm. If the generated hash value is too large, it is generated again until it is below the specified target value.

5.4 Hash Functions

Data verification is an important component when building a data structure on a decentralized network. Only through verification, can participants distinguish between valid data and invalid information. In blockchain systems, hash functions are the mathematical one-way function used as a means to verify data in blockchains at different stages of a data verification (i.e., when creating an address, proving ownership, proving the integrity of the blockchain itself).

All hash functions take inputs of variable length and produce an output of fixed length called the hash value. Has functions are irreversible one-way functions. You cannot translate your hash back into the data that you put in to receive the hash value as was shown in the blockchain demo video. Hash functions are pseudo-random (i.e., they produce seemingly random outputs from two similar inputs). The likelihood of a hash function producing the same output for two or more different inputs is highly unlikely. However, they are deterministic meaning that they always produce the same output from a specific input. In this sense, a hash value is similar to a fingerprint of data. One can verify the integrity of files and detect changes by comparing their hashes. The input can be any type of data (i.e., audio, video, picture) it is not restricted to numbers.

Hash-Mode	Hash-Name	Example
0	MD5	8743b52063cd84097a65d1633f5c74f5
10	md5($pass.$salt)	01dfae6e5d4d90d9892622325959afbe:7050461
20	md5($salt.$pass)	f0fda58630310a6dd91a7d8f0a4ceda2:4225637426
30	md5(utf16le($pass).$salt)	b31d032cfdcf47a399990a71e43c5d2a:144816
40	md5($salt.utf16le($pass))	d63d0e21fdc05f618d55ef306c54af82:13288442151473
50	HMAC-MD5 (key = $pass)	fc741db0a2968c39d9c2a5cc75b05370:1234
60	HMAC-MD5 (key = $salt)	bfd280436f45fa38eaacac3b00518f29:1234
70	md5(utf16le($pass))	2303b15bfa48c74a74758135a0df1201
100	SHA1	b89eaac7e61417341b710b727768294d0e6a277b
110	sha1($pass.$salt)	2fc5a684737ce1bf7b3b239df432416e0dd07357:2014
120	sha1($salt.$pass)	cac35ec206d868b7d7cb0b55f31d9425b075082b:5363620024
130	sha1(utf16le($pass).$salt)	c57f6ac1b71f45a07dbd91a59fa47c23abcd87c2:631225
140	sha1($salt.utf16le($pass))	5db61e4cd8776c7969cfd62456da639a4c87683a:8763434884872
150	HMAC-SHA1 (key = $pass)	c898896f3f70f61bc3fb19bef222aa860e5ea717:1234
160	HMAC-SHA1 (key = $salt)	d89c92b4400b15c39e462a8caa939ab40c3aeeea:1234
170	sha1(utf16le($pass))	b9798556b741befdbddcbf640d1dd59d19b1e193
200	MySQL323	7196759210defdc0
300	MySQL4.1/MySQL5	fcf7c1b8749cf99d88e5f34271d636178fb5d130

Figure 5: Generic hash types (Source: Hashcat, accessed on 15.11.2022)

As the figure shows, there are different hash functions that have different fixed-length outcomes and are used by different blockchains. One of the most commonly used hash functions is the so-called SHA256 (Secure Hash Algorithm 256 bit). The 256 stands for the fixed length of the hash value. There are many hash functions, most of which indicate their fixed length in their name.

5.5 Public-Key Cryptography

Public-Key Cryptography (also known as asymmetric cryptography) grants cryptocurrency holders access to their funds. It offers a way to prove ownership. In symmetric cryptography, you encrypt and decrypt a message with the same key from both ends. This works similarly to a padlock where you use the same key to open (decrypt) and close (encrypt) the padlock. Asymmetric encryption stems from the property of keys always coming in pairs and being used complementary. One of the keys encrypts something and the other one decrypts it. The keys are called public key and private key, also spending key or secret key. Your keys translate to your identity on the blockchain. You receive funds with your public key and send funds with your private key.

Keys and Identity

The idea in cryptocurrencies is that you are receiving funds with your public key and spending them with your private key. The keys are named public and private on purpose since you can share your public key with everyone. You need your private key to spend your funds. Whoever has access to your keys, can access your funds. A public key is similar to your address. You can give it to people that want to send you a letter or package. Your private key is like the key to your postbox. Only this key lets you access your mail and usually, only you have access to it. Your keys are needed for both, sending and receiving transactions. A transaction is on a technical level a message to all nodes in the network. The information in the message is then encrypted via the private keys which are called signing a transaction digitally. This process is not done manually instead, there are wallets that do these steps for the user. Wallets are able to generate and manage keys and encrypt and decrypt.

Generating Keys and Addresses

Funds or data which is sent to a public key can only be accessed by those in possession of the corresponding private key. The public key is derived from the private key via Elliptic Curve Cryptography (ECC). ECC is the most commonly used public-key cryptography scheme in cryptocurrencies, though there are other cryptographic schemes. Cryptography uses one-way functions, and multiplication on an elliptic curve is another one-way function of note. Thus, the derivation of a public key from a private key cannot be reversed.

Digital Signatures

A transaction can only be validated if it has a valid digital signature. The private key associated with the address storing the funds has to sign a transaction. When a transaction is broadcast to the network, all full nodes and miners verify it based on the message, public key or address, and signature. A signature can only be valid or invalid at the end of the verification.

Peer-to-Peer Network

In a P2P network all participants have the same role. Each of them acts as a client (i.e., requesting data) and as a server (i.e., providing data). The advantage of a P2P network is that if one machine becomes unavailable, the machines that are still connected to the network continue to provide services. This system architecture makes blockchain networks resilient to single-points-of-failure.

5.6 Consensus Mechanisms

Mining & Consensus

Every blockchain must choose a mechanism that ensures all participants agree on a single truth regarding the data. Think of it as a standardized way to get all the politicians in a parliament to agree on an opinion as quickly as possible. Since the politicians probably need to discuss it, all participants in a blockchain network also do so by communicating with each other through the network. The communication protocols are implemented in the software that is executed on all participating devices. However, communication is not about a political opinion, but about the data status of the blockchain, such as the transaction history of a currency like Bitcoin. To resolve this issue in blockchain networks, a consensus mechanism is used.

The Problem of the Byzantine Generals

The various consensus mechanisms solve an ancient problem, referred to as the Byzantine generals' problem. The initial dilemma is the following:

A queen is trapped in her castle with her 500 soldiers because the castle is besieged by five armies, each 100 strong. Each army has set up camp near the castle and is under the independent command of one general from each army. The generals must communicate with one another to find agreement on an attack strategy. However, their trust in one another is limited because they suspect that some of them are traitors. If the generals would send a message laying out the tactics and timing of the attack by a messenger from camp to camp, generals loyal to the queen could easily make changes to the message and thus pass false information to the next camp.

Consequently, the alteration of written messages is not a secure means of communication. The spread of misinformation could lead to the victory of the malicious generals given that different camps would not attack simultaneously or not at all. In the 21st century, the basic problem still remains: How can one be sure that a message is authentic and has not been subject to changes and malicious activity?

Authenticity refers to the certainty that counterparties did not forge calls and emails or pretend to be someone else. Tampering means the distortion, deletion, or viewing of the message by malicious parties.

To solve the problem of Byzantine generals, consensus mechanisms are based on two concepts:

1 All generals must first have skin in the game by contributing something to the network that they would not get back in case they behave against the rules. For example, imagine two businessmen who want to start a joint venture, but one of them refuses to invest time or capital. The other businessman who has skin in the game would question the loyalty of the other. This can be applied to decentralized networks.

2 Secondly, the ledger has to be manipulation-free (referring to past and present transactions). A system is tamper-free if the nodes in the network immediately detect any change or deletion of previous transactions and data. All user transactions are recorded, verified and stored on a blockchain.

In the case of the Byzantine generals, one solution could be to let generals pay a high sum up front as a token of their loyalty. Before a general can pass on a message, their identity would need to be proven by a cryptographically secured and unique signature. If one general is sabotaging the attack, the transaction history can give information on the identity of the individual giving the signature. The punishment for maliciousness is financial loss for the general since they are not reimbursed for the deposit made upfront. Reaching consensus in this way is called 'proof-of-stake'. All generals have invested a stake in maintaining the network upfront to participate. Another alternative would be for each general to solve a complex math problem before signing and sending a message is permitted. The general would need to pay a lot of money to workers solving the math problems for them. This method is referred to as Proof of work (PoW). Each general proves his loyalty to the network by consuming costly and time-consuming resources.

Consensus in Distributed Systems

The history of cryptocurrencies, the order in which transactions were validated is crucial to be kept track of. When a network participant creates a transaction, the transaction is broadcast to the entire network. Each node records the new transactions and adds them to its version of the ledger. The versions of the ledger differ slightly from one to the other. If a node is based in the EU and broadcasts a transaction, the nodes that are closest to it receive it earlier than a node based in the US. This results in slightly different versions of the same transaction history. Eventually, all network nodes need to agree on a given order and this is what the consensus mechanism of a blockchain achieves. There are many approaches to reach consensus in a distributed network, the two most prominent ones are the PoW and Proof of Stake (PoS) algorithms.

Proof of Work

The term "mining" is known from Bitcoin, for example. The Ethereum network used to run on PoW as a consensus mechanism transactions have to be packaged into blocks by means of mining and thus confirmed. PoW describes the condition that a participant in the network must have performed honest and provable work in order to confirm a number of transactions. The block reward which miners receive is intended to compensate for the electrical energy expended and the use of special hardware (e.g., ASIC miner or GPU), and beyond that to make a profit from the current block reward and the transaction fees approved in the transactions. PoW is the most widely used method in cryptocurrencies so far. The high stakes involved in mining also ensure that the coins generated through it have a real equivalent value in the form of fiat money.

As robust and proven as the process may be, it is also heavily criticized. The downside of PoW is the usage of electrical energy and the sometimes specially manufactured hardware is consumed at the expense of the environment. The comparison (based on ballpark number estimates) to frequently used services and industries (e.g., Netflix, YouTube) and Bitcoin and Ethereum energy consumption levels puts the energy usage of PoW and PoS into perspective.

	Annualized energy consumption (TWh)	Comparison to PoS Ethereum
Gold mining	240	92,000x
Gold mining	130	50,000x
Bitcoin	130	50,000x
Bitcoin	100	38,000x
YouTube	244	94,000 x
Global data centers	200	78,000x
Netflix	0.45	175x
Netflix	94	36,000x
PayPal	0.26	100x
Gaming in USA	34	13,000x
PoW Ethereum	78	30,000x
PoS Ethereum	0.0026	1x

Figure 6: Comparison of annualized energy consumption of services and industries (Source: Ethereum's energy expenditure, Ethereum Foundation, 2022)

> Estimates of YouTube's energy expenditure have also been broken down by channel and individual videos. Those estimates show YouTube used over 175 times more energy watching Gangnam Style in 2019 than Ethereum uses per year.
>
> Ethereum Foundation, 2022

While the reduction of the carbon footprint of crypto (by use of renewable energy sources) is desirable, one must answer the following question for themselves:

Are the functions that Bitcoin and other cryptocurrencies fulfill worth the energy expenditure that they incur?

Another disadvantage is the division of the community of these projects. There are always two groups. Users, who have to raise the transaction fees and wait for the confirmations, and miners, who have their eye on profit and mostly want to make a political profit on the project for themselves. Suggestions on how to improve the project and its source code implementation usually trigger discussions in which both camps vigorously defend their own interests.

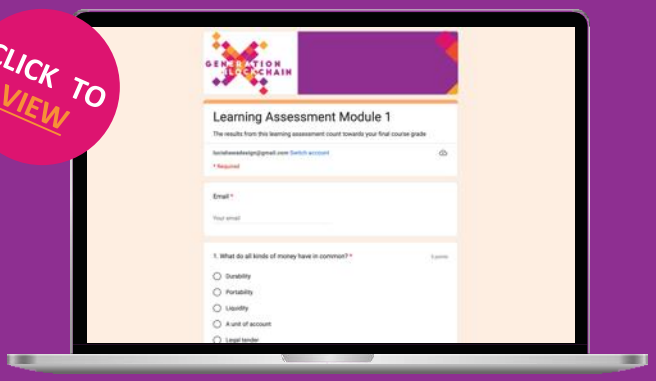
Proof of Stake

As in a stock corporation, for example, in PoS all shareholders have the right to have a say in the consensus. This entitlement to validate a block of new transactions is deterministically (by pseudo-randomness) assigned each time. In this process, shareholders with more assets in their wallets have a slightly higher chance of being selected. On the one hand, they have a higher interest in the functionality of the network and should therefore contribute relatively more. On the other hand, with too heterogeneous a selection of shareholders comes the risk that block confirmations become centralized and empower parties holding large shares of the asset, resulting in an unfair redistribution of wealth. In most cases, in PoS-based blockchains, the corresponding tokens are already "pre-mined" (i.e., created) instead of being slowly flushed to the market through block discovery until the set maximum is reached, as in PoW. PoS blockchains thus, usually already have all shares in circulation and can only pay shareholders who win blocks with transaction fees. Energy consumption is limited to simple use by the participants and is not driven up by complex calculations as it is in PoW consensus mechanisms.

06

LEARNING ASSESSMENT FOR MODULE 1

To test your knowledge, finish this learning assessment as part of your overall grade for the course.
Click here.



01

MODULE 2

Trust in Business

Co-funded by the European Union

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 National Agency. Neither the European Union nor National Agency can be held responsible for them.

contents module 2

Co-funded by the European Union

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 National Agency. Neither the European Union nor National Agency can be held responsible for them.

01| MODULE 2
Trust in Business

Chapter Overview

In this module, the role and means for trust in business (i.e., measurement & processes for trust establishment) and how blockchain technology can redress the establishment thereof are discussed. Further, the module presents different application areas of blockchain technology such as financial and industrial use cases.

Learning Objectives

After the second module, you should be able to:

- Argue the importance and prevalence of trust in business.
- Understand the different dimensions of trust.
- Explain how blockchain technology can enhance trust in certain business processes and fields.
- Understand the prerequisites to place trust in cryptocurrencies and factors influencing this trust.
- Explain which group(s) of people trust cryptocurrencies.
- Reiterate various financial use cases for blockchain technology and their benefits and pitfalls.
- Reiterate various industry use cases for blockchain technology and their benefits and pitfalls.

01| THE ROLE & MEANS FOR TRUST IN BUSINESS

1.1 Measurement & Processes for Trust Establishment

Trust occurs without exception in all business-related activities and scenarios. In fact, it is the foundation of all activities, deals, collaborations, and processes that involve more than one party. In a business context, trust is required with people from inside or outside of the organization. While it is hard to quantify the precise importance of trust, a lack of trust is arguably one of the biggest expenses in business. Trust is a particularly fragile concept, given that it may take years for a manager or an executive to develop the trust of their employees, but can be betrayed within a moment. Trust is the natural result of thousands of tiny actions, words, thoughts, and intentions. Without trust, transactions would not occur, influence could be destroyed, leaders can lose their teams and salespeople can lose sales.

What is Trust?

Trust is a(n) (at least) two-party bilateral social construct that is built when perceived risk and consciousness of vulnerability are outweighed by the perceived benefit that both (or more) parties choose to see before going forward in acting on their intentions. It is a manifold concept made up of thousands of tiny actions, words, thoughts, and intentions. Despite the central role of trust in business today, it can remain unnamed and invisible.

The business strategist David Horsager identified the following eight pillars of trust:

1 **Clarity**
People trust the clear and mistrust the ambiguous

2 **Compassion**
People put faith in those who care beyond themselves

3 **Character**
People notice those who do what is right over what is easy

4 **Competency**
People have confidence in those who stay fresh, relevant, and capable

5 **Commitment**
People believe in those who stand through adversity

6 **Connection**
People want to follow, buy from, and be around friends

7 **Character**
People immediately respond to results

8 **Consistency**
People love to see the little things done consistently

As per “PwC’s Trust in US Business Survey” from 2021, business executives, customers and employers show to think about the same four items when they think about trust: data protection, cybersecurity, treating employees well, ethical business practices and admitting mistakes. Notably, when it comes to points beyond these four elements, the divergences grow. Business leaders tend to take a broader stance on trust including elements of responsibility such as responsible usage of artificial intelligence (AI) and social impact (i.e., sustainable value chain management and ESG reporting). Employees, on the other hand, emphasize more on leadership accountability. This survey merely serves as a benchmark that gives an idea of how much the notion of trust differs depending on socio-economic, demographic, and personal definition. The only statement regarding trust in business that can be made with certainty is that it is a highly complex phenomenon that is yet to be fully understood.

According to the PwC study, established trust in companies pays off in several ways and through various stakeholders: Almost half (49%) of consumers have started or increased purchases from a company because they trust it, and 33% have paid a premium for trust. PwC finds that 44% of customers have stopped buying from a company due to a lack of trust. As for employees, PwC finds that 22% have left a company because of trust issues and 19% have chosen to work at one because they trusted it highly. In other words, one out of five of your employees do not leave for reasons of a higher-paid job or position but because of a lack of trust in the company.

Next to the already mentioned points of data protection, cybersecurity, treating employees well, ethical business practices, and admitting mistakes, customers deemed data protection to be a determinant of trust placed in a company. Data protection is perceived as a necessity and considered the bare minimum for trust not to falter. In a break between theory and practice, business leaders’ actions on trust often do not match what they deem “extremely important”, and these actions often are not addressing consumer priorities. For consumers, the top trust driver is accountability, while only 56% of business leaders deem it to be “extremely important.” Only 46% say that their companies have implemented it.

What builds trust in business for consumers and employees

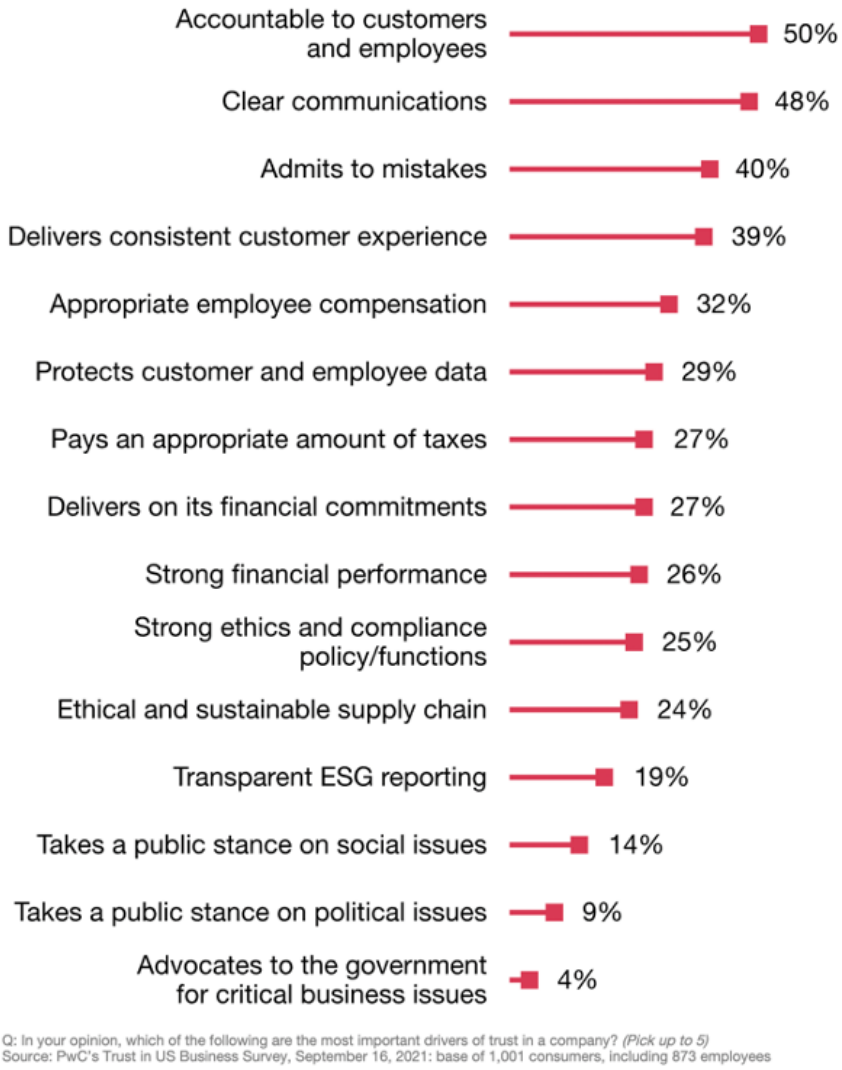


Figure 7: What builds trust in business for consumers & employees (Source: PwC's Trust in US Business Survey, 2021)

When it comes to environmental, social and governance (ESG), 45% of business leaders have implemented transparent ESG reporting — but only 19% of consumers list it among the top five drivers of trust. This disconnect between consumers and businesses may be more complex than it first appears. Consumers care deeply about ESG initiatives such as climate change. However, they may not fully understand what ESG reporting entails, or PwC alternatively supposes that customers may consider it as part of their top two trust drivers (i.e., accountability and clear communications). ESG skepticism may also be a problem. Only 24% of consumers say the main reason for ESG pledges is to do good. Far more (39%) say that the motive for companies lies in self-interest: to build trust with the consumers.

In this next section, a narrower look will be taken at e-commerce trust.

Trust in E-Commerce

With the rise of e-commerce, the concept of consumer trust has been adopted, analyzed, and refined in its meaning and role in the online context. This is to say that different additional layers of complexity have been added to the already diffuse concept of trust in offline business contexts. This particular kind of trust is called online trust and refers to the attitude of the customer which has the confident expectation in an online situation that one's vulnerabilities will not be exploited. E-tailing websites convey more and more humanistic qualities which mimic its retailing equivalent with actual human interaction to foster trust-building. Though there is no pertinent scholarly definition for consumer trust, the elements of confidence in a product or company, assurance for integrity, and reliability are often named in association.

In e-commerce, the importance of the website's design and social cues that convey humanlike features as well as the assurance of transaction are builders for trust in businesses. Further, security, privacy protection, and knowledge-based familiarity of the website and its functions have been found to have a positive as well as significant impact on trust.

Overshadowing all that an online vendor can regulate within his/ her sphere of influence is self-efficacy (i.e., initiation, effort, and persistence of the customer). Self-efficacy assesses how well someone can go through a course of action that is needed to deal with a prospective situation, regardless of the actual skill level of a person. It puts other antecedents for trust in the shade in terms of positive influence on transaction trust. Meaning that if a user cannot navigate well through e-commerce, their trust in the e-commerce shop or is impaired as a result even if the skills of the user play a large role in the impairment. With millennials, there is a relatively high perceived risk associated with online purchases as compared to younger generations. Possible incentives that are perceived benefits in the eyes of the customer entail time and cost savings and increased convenience

Concerning benefits, functional benefits rather than affective trust-based ones are found to influence purchase intention the heaviest in multiple studies. Especially the first two named elements can be connected to cryptocurrencies since their transaction time and cost is lower than with alternative payment service providers. For example, a retailer in the USA selling a product via PayPal costs 2.9% of the sum sent plus $0.30 per transaction within the country. Border crossing trades cost an additional 1.5% of the transaction settling sum. BitPay as a comparable payment service provider in the crypto sector charges only 1% of the sum, regardless of border crossing. This example can be seen as an incentive for the customer and the retailer because, for both sides, the transaction becomes cheaper and thus, more beneficial. The more prevalent the perceived benefit is in the mind of the customer, the more willing he/she is to share their sensitive data. Several studies show that even individuals that are highly concerned with their private data are by a vast majority willing to share their data nonetheless, if they value the product, trust the brand, are offered reward points or other financial incentives. These aspects can often be seen in loyalty point schemes and member rebates. As soon as it is established as initial trust, continuous consumer trust and perceived benefits can be seen as a mental shortcut. Together they serve as a mechanism to reduce transaction- specific uncertainty and influence payment behavior and choice of payment methods. Payment behavior can be broken down from manifold starting points. From country to age, occupation over gender, and financial education-specific segmentation, differences can be pointed out.

1.2 Blockchain Technology for Trust Establishment

First of all, it is important to note that blockchain technology is not a trustless technology but rather a confidence machine. The absence of a trusted authority in charge of managing and coordinating interactions over a blockchain-based network does not make it a "trustless technology". In fact, while trust is less relevant when it comes to the standard operations of a blockchain-based system, it is nonetheless necessary to trust the actors securing and maintaining the underlying blockchain network, to guarantee a sufficient level of confidence in any of the blockchain-based applications operating on top of that network. Blockchain technology thus produces confidence (and not trust) in blockchain-based systems based on the user's understanding of procedural and rule-based working, stemming from derived mathematical knowledge and cryptographic rules and mechanisms and long-standing account of its past performance. It increases confidence in the operations of a computational system which is dependent upon its underlying governance structure. To place confidence in the governing party or parties of the computational system, trust in a distributed web of actors is needed.

To place trust in a distributed web of actors the following questions need to be answered:

1 Is the system governed properly?

2 Can the various actors involved be expected to act in accordance with the blockchain system's rules?

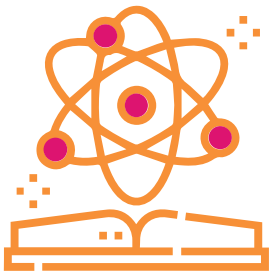
The web of actors includes miners and mining-pools, responsible for processing and validating transactions, large commercial operators, such as cryptocurrency exchanges or custodian wallet providers, who can leverage their market power to unilaterally impose their decisions onto their user-base, as well as core developers and social media influencers, whose voice can contribute to shifting the selling point. Regulators and policy makers also have a role to play in the governance of blockchain-based systems, to the extent that they can introduce legal restrictions and constraints to influence the decisions taken by any of these actors.

The governance of most blockchain-based systems has been constructed in such a way as to distribute trust over many actors, with different interests and preferences, so that no single actor has the capacity to unilaterally affect or influence the operations of the overall network. Problems emerge, however, when standard governance practices are threatened in the case of an emergency that calls for decision-making beyond the scope of ordinary procedure (e.g., as in the case of TheDAO attack on the Ethereum network).

Although it is possible to enhance confidence in the proper operations of blockchain-based systems through the introduction of a series of technological guarantees related to on-chain governance, the robustness of the underlying governance system requires a whole different set of constraints that extend beyond the scope of a purely codified protocol and code-driven rules. Hence, in order to ensure a proper level of confidence in such blockchain-based systems, it may be necessary to introduce a series of procedural and substantive constraints related to off-chain governance, addressing both situations of normalcy and states of exception.

If we take another look at David Horsager's eight pillars of trust, the following theoretical statements for blockchain technology can be derived:

1



Clarity

People trust the clear and mistrust the ambiguous

Data inserted into a blockchain is clear, transparent, and immutable. It is clear where data is coming from and how and under which parameters it was inserted into the blockchain system and keeps the same record of a ledger no matter which user looks at it.

2

Compassion

People put faith in those who care beyond themselves

Blockchain as a neutral technology cannot assert compassion unless programmed to do so (i.e., act according to rules and code)

3

Character

People notice those who do what is right over what is easy

Consensus mechanisms incentivize miners, validators, nodes, developers, and participants in a network to do what is right over what is easy. Doing what is right over what is easy is thus not the easier way but the only way in a blockchain-based system

4

Competency

People have confidence in those who stay fresh, relevant, and capable

In a sense blockchain technology is an iteration step of digitalization and digitization at the same time. While digitalization is referring to making processes such as sending money digital digitization means moving real-life objects onto a blockchain and making it thus digital, tradable, and divisible. blockchain systems can be seen as more relevant and capable than many other innovative technologies.

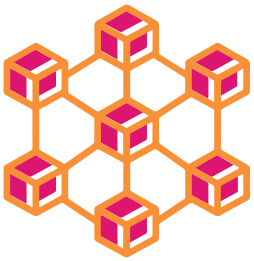
5

Commitment

People believe in those who stand through adversity

Decentralized and censorship-resistant blockchain technology cannot be altered and is committed to a truthful display of reality as fed into the blockchain at a given point in time. Changes made throughout time in a blockchain can be tracked and pinned down.

6



Connection

People want to follow, buy from, and be around friends

Though blockchain technology is a neutral technology and does not have the ability to build interpersonal connections with its users in the case of cryptocurrencies there is communities building around a network that can act as interpersonal relationships to one to follow by from and be around as well as learn from. Crypto communities often share the same vision and mission for a cryptocurrency project they also often collaborate on projects together giving a feeling of belonging.

7

Contribution

People immediately respond to results

In the case of cryptocurrencies and permissionless blockchain systems people can immediately participate and contribute to the network and the protocol.

8

Consistency

People love to see the little things done consistently

As the rules of a blockchain system are set out from the beginning and cannot be altered unless a 50% majority is reached blockchain technology can be considered consistent by nature. depending on the network many blockchain systems are up and running 24/7 which can also be viewed as a means of consistency. Though there are improvement proposals in blockchain systems to change rules as needed blockchain systems generally stay consistent in that they are often times backward compatible with previous versions of the system or alternatively they create spin-offs of an existing blockchain (a so- called fork).

Three Measurable Areas of Trust

In 2018, PwC's conducted the Global Blockchain Survey which found that 45 percent of companies investing in blockchain technology believe that lack of trust among users will be a significant obstacle in blockchain adoption. Reasons provided for this assessment include uncertainty with regulators and concerns about the ability to bring business networks together. PwC makes suggestions to close this trust gap early by planning cybersecurity and compliance frameworks that regulators and stakeholders will trust from the initiation of blockchain development within a company.

Looking at data from supply chain networks across the retail industry, PwC identifies three key measurable areas often considered the foundation of enterprise trust:

1 **Validity of data**
An organization has, to the extent and to the effect, accurately sourced information that holds true when shared with the consumer.

2 **Governance of data**
An organization has defined fair business rules to manage data and to align with business processes.

3 **Reliability of data**
An organization acts consistently and proactively, in a timely, thought-driven manner.

Generally speaking, enterprises tend to hesitate to embrace emerging technology, especially one that requires a new method in sharing data which blockchain technology would require them to do. Blockchain technology delegates data management back to the consumer and to regulatory bodies. Blockchain Technology cannot only shift trust mechanisms within single business entities but rather in whole industries. For example, in supply chain management. The more companies embrace blockchain, the more networking effects come into place. Supply chain management on-chain can only make sense if all steps along the chain are tracked by all participating parties. As soon as one or more steps and suppliers are not participating, the chain is incomplete and significantly inhibited in its purpose.

With more than a decade of this transformative technology, through the rise of digital commerce, trusting business networks have raised significant questions in transforming IT. As a result, this transformation has redefined technical stacks and has developed new data models. However, technology cannot scale trust within a transaction, hence, to reduce the cost of trust, PwC identified quantifiable metrics in the scope of their study.

Quantifying Trust

Today, blockchain presents an interesting predicament in corporate America with businesses siloed by traditional infrastructures and long-standing processes. With the rise of blockchain technology, businesses are demanding data quality reviews prior to progressing into solutions that apply automated business logic across a value chain. Another issue is presented by the quality of data that is inserted into a blockchain system by an oracle. A so-called oracle is the source of inputs from the real world, oracles thus connect blockchains to external systems.

Although trust is a qualitative attribute, the measure of trust depends on quantifiable metrics. Quantifiable measurements of trust as identified by PwC include:

1 **System behavior**
Programs and applications that capture the movement of data, as exhibited by transactions, consensus, or votes.

2 **Content analysis**
Using techniques like Natural Language Processing (NLP), deep learning and AI/ML to analyze structured and unstructured data.

3 **IoT & digital identities**
IoT devices, QR codes, and web-based identities for cybersecurity.

4 **Social layer**
Considering human actors, social aspects, user incentives and motivations, culture, levels of digital literacy, access to technology.

By capturing quantifiable data, enterprises begin to establish governance with a collection of automated business processes, improving regulatory compliance and safeguarding the customer experience. The expansion of blockchain data depends on the migration of enterprise legacy data into building blocks, defining rules for each block that results in enhancements to business outcomes as measured by revenue, customer satisfaction, leaner processes, and automation of manual processes.

Blockchain in the Public Sector

Developing blockchain solutions for the public sector also requires a decision for the blockchain stack. The main issue to solve in the public sector is social trust by the public. To increase trust in the public sector, it needs to be considered which information needs to be captured and stored in the blockchain as well as which information should not be included. In the permanent record to support the goal of trust. This is then followed by consideration of the blockchain protocols, architectures and other technical considerations that deliver the necessary capabilities.

A choice must be made regarding the distributed ledger technology protocols (i.e., Ethereum, Hyperledger, Corda, Quorum), the network options (e.g., public, private, hybrid or consortium), governance mechanisms, security, and cost/duration indications (initial investment and annual operating costs).

In this approach, the initial three-layer design and implementation paradigm is expanded by the social layer (i.e., human actors, social aspects, user incentives and motivations, culture, levels of digital literacy, and access to technology).

1 **A data layer**
The ledger itself is an ”immutable” store of transactional data and/ or records, including considerations of data usability, privacy, and security, authenticity,
reliability, integrity, etc.)

2 **A technical layer**
The technology stack, including distributed ledger protocols, consensus mechanisms, architectures, peer-to-peer networks, data storage, etc.

Adopting this approach encourages consideration of important design trade-offs among the layers that could help avoid potential misalignments between the technology and its intended area of application, as well as encourage faster adoption and more transformative outcomes for governments.

Trust in Cryptocurrencies

After having looked at trust in the context of blockchain technology, we will now focus on trust in cryptocurrencies specifically. As there is no single entity behind Bitcoin that can help with customer service requests, a user that holds their Bitcoin in self-custody, can in the event of losing their keys for access to their Bitcoins not be recovered in any way. In a sense, instead of trusting payment service providers, trust is replaced upon the payer holding their own cryptocurrency.

There is evidence that trust in an algorithm is more likely when information on others who have adopted it already is available rather than the actual accuracy of an algorithm. Anecdotal evidence and reviews from people that we know, and trust can be a bigger driver of trust than the factual accuracy of an algorithm's working mechanisms. In the case of blockchain technology, this could mean that anecdotal evidence of people or executives we trust could make us more likely to place trust in the technology. There are different attributes that impact trust in cryptocurrencies. Trust is found to be linked to transferability, immutability, and openness. Cryptocurrencies, such as Bitcoin, could make international transfers much easier, with lower transaction fees than those charged by traditional commercial banks. Since cryptocurrencies could become an alternative method for international money transfers, several commercial banks worldwide are looking into launching their own cryptocurrencies.

Other trust-fostering factors are ledger immutability and openness - the former securing safe and fair transactions and the latter making the transaction information accessible to the public. Immutability means that the transaction history provided on Bitcoin ledger cannot be manipulated, revised, or deleted. Openness refers to the availability of the data on the Bitcoin blockchain to everyone, rendering the system completely transparent. Openness creates transparency, while immutability creates accountability. Transparency is considered as the key element in trust creation. The degree of transparency and accountability offered by Bitcoin or other cryptocurrencies is unparalleled to that of any traditional financial institution. When technology provides a high enough level of transparency and accountability, it eliminates the necessity of a trusted central authority to govern the system. In other words, it is essentially the core properties of blockchain technology that facilitate the creation of trust in cryptocurrencies.

The geographic locations in which crypto communities are is also where crypto hubs are forming (i.e., through the founding of crypto or blockchain technology-enabled companies, providing point of sales for cryptocurrencies in stores are more frequent, laws and regulations are laxer). These individuals meet the criteria of being at least somewhat knowledgeable and familiar with cryptocurrencies. Exemplarily, Berlin has a district in which almost all stores accept cryptocurrencies as a means of payment, the IT University of Copenhagen offers a Blockchain summer school, in 2018 the Czech Republic counted 147 Bitcoin-accepting stores in 2018 and Malta is also referred to as Bitcoin Island.

It is not possible to assess trust in cryptocurrencies fully as it consists of various layers, angles, and depends on the technical set-up, jurisdiction and what cryptocurrencies are used for.

Who trusts Bitcoin?

Trust in Bitcoin as a means of payment and investment vehicle is more prevalent in segments that fit the profile of male, between 20 and 35, are financially well-educated, and have high levels of self-efficacy in handling crypto payments. The adoption of blockchain technology is measured by how well it is understood and trusted.

Lack of knowledge is found to significantly limit trust and usage intention. Another trust influencing factor is the reinvolvement of a third-party payment service provider. It does not necessarily mean that by introducing a payment service provider, Bitcoin's features lose their trait of being perceived as a trustless system. It can be even beneficial for building trust to have a tangible contact company. In terms of functional benefits, retailers can mitigate volatility risk and shift the financial risk connected to Bitcoin. To sum up, it depends heavily on the convictions of individuals whether increased trust in cryptocurrencies is achieved by reintroducing a third party or by removing the third party.

Established trust in existing payment methods does not significantly influence usage frequency (for example ApplePay, PayPal, etc.). Trust also does not appear to be an irrefutable prerequisite for usage, especially not for payment methods that customers are completely unfamiliar with and thus, hold a higher perceived risk of uncertainty. Bitcoin does fulfill the requirements of acting as a payment method in that it has comparable features such as trustworthiness, transaction speed, cost, crossing international borders, etc. to other existing payment methods. Even though initial trust in Bitcoin as a payment method is not established with most people, it does not mean that Bitcoin as a payment method would only be used by those that trust it. Trust in Bitcoin in general and trust in Bitcoin as a payment method are two different things where trust in one does not necessarily imply that trust in the other is established as well, though there is a tendency that those who do trust Bitcoin also trust it as a payment method.

To gain an understanding of what a fair valuation for Bitcoin is, watch this Generation Blockchain video.

02

APPLICATION AREAS OF BLOCKCHAIN TECHNOLOGY

2.1 Financial Use-Cases

Stock market trading itself has already undergone a disruptive change in the recent past. Electronic trading, clearance and settlement systems have against what was believed previously not really eliminated jobs on the trading floor. Rather, only some regional exchanges have become unprofitable and insignificant, and with them and, as a result, a number of professions. This innovation has led to an enormous increase in efficiency in stock exchange trading. As a result, trading volumes and turnover have increased, transaction costs have decreased, and new exchange products and jobs have been created. The significance of the world's leading stock exchanges has increased the technological revolution. For this reason, further efficiency gains for example through blockchain technology in secondary trading and settlement are likely to be unpromising. Other areas of application for blockchain technology promise greater innovation potential and thus higher profits.

Issuing securities

The issuing process of securities on the primary market for example is currently still costly and complex. Blockchain technology could generate effects similar to those of electronic trading for the secondary market. The Bank of the State Baden Württemberg (LBBW) in Germany and Daimler AG have issued a prototypical bond with blockchain technology as pioneers. This indicates that the efforts to develop applications with added value are being intensified not only among FinTechs as is often believed. One application that has already widespread application are so-called initial coin offerings (ICO). The similarity in name to an initial public offering (IPO) is not coincidental with the issuance of shares on the primary market. An IPO in the analog market is lengthy and costly since many disclosure requirements and stock exchange regulations must be complied with. It, therefore, made sense to use the instrument outside of regulation in the digital world to raise capital. As an example, one can now delineate from the ICO's how the incorporation (or subjection) of these issues into financial regulation is taking place. If necessary, the authorities are also prepared legally to enforce equal treatment.

Electronic payment & business processing

Another area of application for blockchain technology is electronic payment and business processing. This involves both, the more efficient of conventional payment transactions as well as the replacement of business processing. The advantages of blockchain technology should be the speed, security, and trustworthiness of processing. In leading industrialized countries, especially the European Union it should be difficult to compete here with the European System of Central Banks (ESCB) in international payments. In contrast, blockchain may find high acceptance in economic regions with trust deficits, security gaps, and/or inefficient payment processing. However, this advantage will only come to fruition if there are numerous interfaces and bridges to the real world exist.

This requires the affordability of goods and services of all kinds with cryptocurrency. It is rather unlikely that this will be the case in, of all places, countries or regions where traditional payment systems and other innovations are not yet established. The Bundesbank and the ECB, in monitoring blockchain developments and the digital currency markets have so far concluded that the processes and costs of their systems are significantly more efficient and cost-effective. Nevertheless, both institutions are also testing blockchain technology in order not to miss out on new developments, if necessary. Another potential savings from blockchain technology, which could result from the lack of regulatory and financial oversight costs for this type of payment processing, is only true as long as the number of payment flows is not systemically relevant.

Payments Across Borders

Multinational banks such as UBS and British Barclays use blockchain to streamline back-office operations and settlement, which could potentially decrease US$20B expenses for third-parties involvement. For example, in 2019 Barclays invested US$5.5 million in startup called Crowdz that helps businesses to promote B2B cash turnover. As a result, it offers alternative ways of payment collection and automation of e-invoices. Another renowned Spanish bank has cooperated with the DLT-based company to add visibility to their international payments and dramatically accelerate them.

Pressured adoption of blockchain technology

If, on the other hand, they have reached a significant scale and would be used across the board to pay for goods and services, these services would not be concealed from financial supervision. At the latest, regulation would then be created. Blockchain activities in the financial system that remain outside of regulation would then, at best, have the meaning of a black market and would then, if necessary, also be relevant under criminal law.

New business models

The potentially most promising application of distributed transaction registers is to be seen in the linking of banking transactions and real economic business processes. Broader use of pay-per-use processes, real-time settlement of transactions in value chains and cash-flow-oriented corporate financing with smart finance can be expected. These represent new services whose forms of financing will be digital and automatized. Their settlement does not necessarily require an artificial currency. On the contrary, virtual currencies will be able to conquer this market as a payment medium only if transparency increases, fraud disappears, and value stability is established and controlled. In any case, this will further revolutionize the financial services business. In addition to FinTechs, which are often the focus of attention, and which are using innovative solutions to drive the competitors with innovative solutions, established financial service providers are also experimenting with digital process solutions. They have the advantage here, of the functionality, security, and costs of the existing systems and processes and can leverage this expertise.

Cost reduction

One motivation for the development of distributed ledger applications in the Finance arises from the high costs of banking and financial regulation. Avoidance of these costs in the provision of financial services can bring significant competitive advantages. Due to the inefficiency of many regulations, most digital market players are unlikely to view the elimination of supervision as a loss of security or stability. An elimination of regulation in digital business processes is therefore unlikely to be detrimental to business.

The potential applications of blockchain or distributed ledgers in the financial industry are extensive and vary in their level of development. The tendency their use is worthwhile if the security, speed, and efficiency of financial services can still be improved. Transaction costs can be reduced on a large scale, and the innovative service providers can generate high returns from the resulting efficiency gains. The prerequisites for such a triumphant advance of distributed, digital register transactions are in place in the application areas: Securities issuance (primary market), securities trading (secondary market), payment transactions, financing of pay-per-use, and digital payment. While in the areas of secondary trading and payment transactions, the challenges of finding a technical solution and at the same time the efficiency improvements of the last few years through innovative solutions are already considerable, there is still great potential for the new technology in the primary market and in financing technology. In addition, completely new fields of application for blockchain will emerge with the shared economy as well as the usage-based transfer and payment of assets. In the business areas that are already digitally advanced, blockchain and distributed transaction registers will represent additional options to further develop existing further develop existing systems and processes. In other areas, where time and costs are currently still high, the new technologies will trigger radical changes. Especially in the issuance market for securities has seen considerable movement with ICOs. The regulation of ICOs that is currently regulation of ICOs demonstrates the systemic relevance already achieved. Regulatory equal treatment will not reduce the importance of the financial instrument. On the contrary, it can be assumed, especially after legal clarification, that the underlying technology will significantly simplify and modernize the analog issuance process. For new applications, blockchain technologies will be used exclusively from the outset.

With regards to the players in the financial markets of the future, it can be summarized that established competitors, who are at the forefront of development, will continue to play an important role in the future due to their market and customer will continue to play an important role in the future. Of the many FinTechs many companies will not reach the profitability threshold and will disappear or be acquired by other competitors. However, some of the start-ups in the financial industry will certainly rise to become large, profitable market players. A more precise forecast of which providers these are, cannot be given at present. The state and its supervisory institutions have so far been able to follow the innovations from an observer's perspective.

To dive into a specific financial use case of blockchain technology, watch this Generation Blockchain video on the digital euro and digital dollar and how they work.

Click here to watch the Generation Blockchain video on the digital euro and the digital dollar.

2.2 Industrial Use-Cases from the Energy Sector

The Brooklyn Microgrid is a blockchain-based P2P energy trading platform that is run by Transactive Grid. Transactive Grid is a partnership between LO3 Energy, Consensys, Siemens and Centrica. This microgrid is located in the Gowanus and Park Slope communities in Brooklyn, New York. It has successfully completed a three-month trial run of P2P energy trading between community members in Brooklyn.

With Microgrid, prosumers can sell their energy surplus directly to their neighbors. This is achieved by the use of Ethereum-based smart contracts and the so-called practical Byzantine Fault Tolerance (PBFT) consensus mechanism. The first trial included 5 prosumers and 5 neighboring consumers and resulted in the first-ever energy transaction recorded in blockchains worldwide. The energy surplus is measured by smart meters that can conduct physical energy measurements and record data, and sequentially transformed in equivalent energy tokens that can be traded in the local marketplace. Tokens indicate that a certain amount of energy was produced from the solar panels and can be transferred from a prosumer's smart meter wallet to end-consumers via blockchain. Tokens are burned by the consumer's smart metering device, as purchased energy is used in the house. Microgrid users interact with the platform by specifying their individual price preferences in the form of willingness to pay or sell electricity. The platform can display location-specific and real-time energy prices. In the initial phase of the project, users manually trigger an agreement in the platform, whose terms are recorded in the blockchain. The ledger records contract terms, transacting parties, volumes of energy injected and consumed as measured by metering devices and crucially the chronological order of transactions. In addition, payments are automatically initiated by self-executed contracts. Every member of the community can have access to all historic transactions in the ledger and verify transactions for themselves.

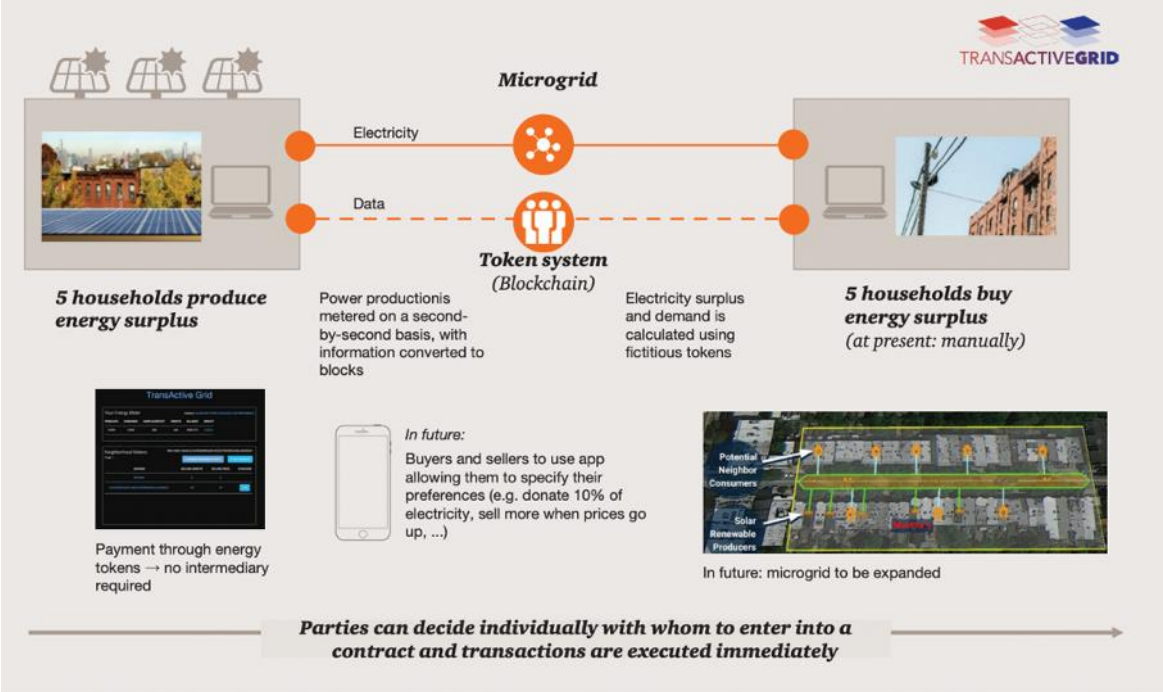


Figure 8: BrookylnGrid project (Source: Microgrid, 2022)

During the trial phase, more than 300 houses and small businesses, including around 50 prosumers and one small wind turbine generator, have signed for the next phase of development, which aims to achieve fully automated transactions. In the next iteration, Microgrid members can not only decide whom to buy/sell energy tokens based to or from on their price preferences, but also on other criteria that reflect their environmental or social values.

For instance, a consumer can specify the maximum price he is willing to spend on locally produced renewable energy, but he can also declare other preferences such as percentage of energy they are willing to purchase from local renewable energy or the main grid. Users can even prioritize selling/buying energy from friends, family, or a specific neighbor. The market clearance mechanism is supposed to work similarly to how stock markets work today:

1 The platform will record the interest of buyers and sellers (bids/offers) in an order book. Users will be able to change their price preferences in real-time.

2 The locally produced energy will be first allocated to the highest bidders.

3 The lowest allocated bid represents the market clearing price for each time slot, currently set 15 min intervals.

4 Users will be able in the future to collect historic information on prices, and therefore learn and adapt their bidding strategies.

Uncertainties & unanswered questions

The Brooklyn MicroGrid project says that it aims to serve as a testbed for exploring novel business models that promote consumer engagement in community projects. Localized energy trading opens the potential for energy cost savings, however, numerous research questions are open for debate. First and foremost, the importance and size of local energy trading markets need to be investigated. Only by implementing large-scale projects that represent diverse conditions in energy markets and social groups, will an accurate determination to participate in similar market architectures be made possible. Pricing in customer-sided markets is determined by the laws of demand and supply, resulting potentially in significant price volatility or even higher tariffs than the ones offered by the main grid. As a result, further work in engagement with and protection of the elderly, socially disadvantaged, and vulnerable from price volatility is required. In addition, equilibrium prices will not only be derived by simple cost functions but by social values and behavior. As a result, individual preferences and social behavior of market participants require further investigation to develop efficient market designs and pricing mechanisms. Other open research questions include the determination of most appropriate time frame for market clearance and data updates, which is increasingly dependent on the operating protocol rules and consensus. Another crucial issue is that of balancing demand to supply. Currently, existing network infrastructure is used not only to distribute and supply the energy traded in the marketplace, but also to resolve issues caused by RES (a large renewable energy company) intermittency and load balancing.

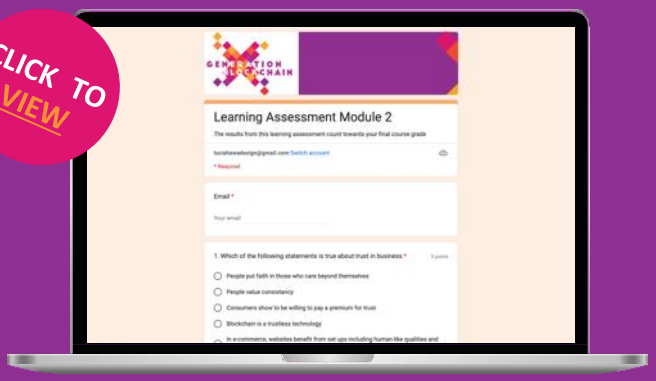
The future of Microgrid

In the future, the project aims to explore how blockchain could be used for active management of the distribution network. In principle, energy produced by local prosumers can provide additional flexibility for local substation balancing. This is currently not realized in the Brooklyn Microgrid case, although a number of projects have begun exploring the use of techniques from artificial intelligence, machine learning and big data analytics to achieve demand-side flexibility. What blockchains could contribute these solutions is the potential for decentralized matching between prosumers, enabling them to take real-time control of the own energy generation and supply. Please note that MicroGrid has been chosen for the sole purpose to display an existing industrial use case in the energy-sharing economy and is not an endorsement of the company or the project.

03

LEARNING ASSESSMENT FOR MODULE 2

To test your knowledge, finish this learning assessment as part of your overall grade for the course.
Click here.



01

MODULE 3

Cryptocurrencies

Co-funded by the European Union

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 National Agency. Neither the European Union nor National Agency can be held responsible for them.

contents module 3

Co-funded by the European Union

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 National Agency. Neither the European Union nor National Agency can be held responsible for them.

01| MODULE 3
Cryptocurrencies

Chapter Overview

In this module, Bitcoin transactions and its mining mechanism will be in focus. Additionally, you will be introduced to the basics of Ethereum, transactions on Ethereum and smart contracts. Finally, we will cover the principles of decentralized finance (DeFi) by drawing comparisons to the traditional financial system.

Learning Objectives

After the second module, you should be able to:

- Reiterate how a Bitcoin transaction works.
- Discuss scalability issues of Bitcoin.
- Have an understanding for the profitability of Bitcoin mining and the hardware and software
- requirements for miners.
- Understand what Ethereum is and what the differences between Ethereum and Bitcoin are.
- Assess the role of the Ethereum gas fee in transactions.
- Reiterate how an Ethereum transaction works.
- Understand the concept and use cases of smart contracts.
- Understand the different application layers of decentralized finance.
- Name and analyze the parallels and differences between decentralized finance & traditional finance.
- Identify current drawbacks with decentralized finance & traditional finance.

01| BITCOIN DEEP DIVE

1.1 Bitcoin Transactions

After having learned about Bitcoin transactions on a high-level overview before, we will now look at Bitcoin transactions in a more detailed manner.

There are No Bitcoins

It is important to note that there are no Bitcoins, only records of Bitcoin transactions. Bitcoins technically do not exist anywhere, not even on a hard drive. If you search for a specific Bitcoin address, you will not find any digital Bitcoins there. There is no physical object or a digital file that "is" Bitcoin. Instead, there are only records of transactions between different addresses with balances that have either increased or decreased. Every transaction that has ever been executed is stored in a public ledger (the blockchain). If you want to calculate the balance of any Bitcoin address, you must calculate it using the blockchain, because no information is stored in the address.

Any user on the Bitcoin network can view every transaction ever made via the Bitcoin Blockchain. As we already know, Bitcoin transactions are secured by digital signatures and are sent back and forth between Bitcoin wallets via their addresses.

Transaction Confirmation Time

Transaction confirmation can take minutes, hours, or days because a transaction needs to be confirmed by miners. Depending on the transaction fee that you paid, your transaction may remain in the transaction pool for a long period of time, simply because the provided incentive (i.e., the transaction fee) is not high enough for your transaction to be included in a block right away. Depending on the traffic on the Bitcoin network, this can delay the transaction by hours or days or can even lead to the rejection of the transaction.

The Bitcoin protocol is set so that each block takes about ten minutes to be mined. Some traders make the user wait until the block is confirmed. On the other hand, there are some traders who do not wait until the transaction is confirmed. They take the risk and assume that people will not try to spend their Bitcoins on other things before the transaction is confirmed. This is common for low transactions (micropayments) where the risk of fraud is not so high. Each recipient can decide for themselves how many confirmations they require. The principle is that more confirmations make the transaction more secure, but also slow it down.

The Logic of Bitcoin Transactions & Bitcoin Stored in Your Wallet

Since Bitcoins exist only as records of transactions, many different transactions may be tied to a specific Bitcoin address. Perhaps Jane sent Alice two Bitcoins, Chris sent her one Bitcoin, and Eve sent only one - all as separate transactions at separate times. They are not automatically converted to Alice's wallet to six existing bitcoins in one file, but they exist only as different transaction records. When Alice wants to send Bob bitcoins, her wallet will try to use transaction records with different amounts that add up to the amount of bitcoins she wanted to send Bob. Unlike on your bank account, amounts of Bitcoin accumulating in your wallet, on a technical level, do not add up to one mass but remain individual entities.

There is a possibility that Alice's wallet does not have the exact amount of addable transaction records that she wants to send to Bob. If Alice wants to send, say, 1.5 BTC to Bob and none of the transactions she has in her wallet match that amount or can be added to that amount, then the following happens: Alice sends the two Bitcoins she got from Jane to Bob. Jane is the input and Bob is the output. However, since Alice wants to send the amount of 1.5 BTC, her wallet automatically creates two outputs for her transaction: 1.5 BTC to Bob and 0.5 BTC to a new address created to hold the change from Bob for Alice.

Bitcoin transactions are divisible. One Satoshi is one hundred millionth of a Bitcoin. It is possible to send a Bitcoin transaction in the amount of 5,730 Satoshi.

Bitcoins (In)ability to Handle Transactions

Bitcoin is supposed to be an electronic money system where participants can send money directly to each other. A money system that is not controlled by a central office but is based on a computer protocol. Theoretically, this money system should be accessible to everyone in the world. This would provide a universal monetary standard; a common "language" for all mankind.

But theory does not translate so easily into reality. Even though Bitcoin is already an electronic money system without controlling middlemen, it cannot be used by everyone. The reason for this is the scalability it requires.

The problem becomes clear when you imagine how many transactions take place every day in the global economy. While Bitcoin technology can easily transfer gigantic sums, it reaches its limits when it comes to a high frequency of transactions. The reason for this is technical: the blockchain, on which all transactions are recorded, only offers limited space for transactions.

You can think of it a bit like a bus. This bus has a limited number of seats. When all the seats are full, no more people can ride. This is quite a similar mechanism to the blocks in the Bitcoin blockchain. These also only have a certain number of "seats" for transactions. When all the seats are taken, no more transactions can "ride" on the bus (i.e., be confirmed). An oft-recited metric when it comes to Bitcoin's functionality is transactions per second. A block in Bitcoin can be a maximum of 1 megabyte in size. An average transaction is 400 bytes in size. That means, on average, 2,500 transactions can fit in one block. A new block is found approximately every 10 minutes. Consequently, the Bitcoin system can process about 4 transactions per second.

However, the so-called "SegWit" upgrade now also allows blocks up to 4 MB but is not yet supported by all nodes. With the SegWit update for Bitcoin in 2017, an intelligent solution was found to circumvent this limit. This increased the possible number of transactions per second fourfold.

While the Bitcoin blockchain reaches its limit at more than four transactions per second, PayPal can process up to 115 transactions per second. The Visa payment network claims to be able to process up to 24,000 transactions per second. The SegWit update helps with scalability but does not achieve Visa payment network-like numbers.

One mechanism in Bitcoin is that transactions can secure a seat on the bus through their transaction fee. That is, if Alice wants to send an important transaction to Bob that should find a seat on the next bus, she can pay a higher-than-average fee. The "bus driver" (the miner) does not have to let the transaction ride, though he can earn a relatively high transaction fee if he does. As a result, he has an economic incentive to make room for the transaction on his bus.

The problem comes if everyone trying to send a transaction provided a higher-than-average fee. The space on the blockchain, the space on the next block, on the next bus, is fixed. As more and more people want to use the Bitcoin monetary system, as more and more transactions want to crowd onto the bus, the transaction fees go up. This is because transactions compete for a spot on the blockchain through their fees. In December 2017, you could see an example of this bidding up of transaction fees. The transaction fee is thus not dependent on how much Bitcoin you are trying to send but dependent on the competition in other unconfirmed transactions and how high of a transaction fee they are bidding.

However, two nuances must also be mentioned in the scalability discussion: The transaction size and the finality of a transaction.

In Bitcoin, it does not matter to the fees and the network whether an amount of 0.001 BTC or 10,000 BTC is sent. What matters is the number of inputs and outputs of the transaction. With alternative payment systems like Visa and PayPal, you usually pay a percentage fee on the transaction amount instead. Sending large amounts is accordingly more expensive.

The finality of the transaction describes the possibility that the transaction can be reversed. With Bitcoin, this is very difficult: once a transaction is sent and written to a block, it can hardly be undone. This is an advantage, because sellers can thus be sure that the supposedly friendly customer will not cheat them afterward. This is different with PayPal and Visa: here there is a period (usually 30 to 120 days) in which the payment can be revoked. This is possible because PayPal or Visa are the central authority in the monetary system. They determine the history of the transactions and can also change it in hindsight.

While Bitcoin is lagging in transaction frequency, the technology can already score massively in terms of transaction size and financial finality.

Solution Approaches for Scaling: On-chain vs. Off-chain

The transaction capacity question is also often called the scaling question. At its core, it has come to take on the same character as the Gretchen question in Goethe's Faust:

> “Now tell me, how are you at scaling?”

Basically, the answers can be divided into two camps: on-chain scaling and off-chain scaling.

The approach on-chain advocates, to go back to the bus example is to scale up the bus. That is to limit the blocks to 1 megabyte, a new upper limit is set for the block. This way, more transactions can fit on the bus, which still leaves every 10 minutes. Assuming the block size increases to 10 megabytes, the number of transactions per second also increases by a factor of 10. This means that it would then be possible to process about 40 transactions per second. The way to improve the capacity of the blockchain by increasing the block size is expressed in the Bitcoin hard fork Bitcoin Cash (BCH).

The alternative to this is off-chain scaling. Here, the aim is not to improve the transaction capacity of the blockchain itself, but to create a second layer for transactions that docks onto the first layer, the blockchain. This second layer would inherit the security aspects of Bitcoin and would also allow a magnitude more transactions. So instead of scaling linearly, as with the on-chain approach, the second layer could handle millions of transactions. And they could be done instantly, for very small amounts, and with similar security to the Bitcoin system itself. This method of scaling Bitcoin outside of the blockchain also goes by the name Lightning Network.

Lightning Network

The Lightning Network is a time-locked off-chain payment channel. This means that users can fix BTC off- chain, i.e., away from the Bitcoin blockchain, and send it to other users. Sending value is almost instantaneous and, similar to on-chain transactions, does not require a trusted third party. The Lightning Network is seen as a promising scaling solution for Bitcoin.
For many Bitcoin proponents, the Lightning Network (LN) is the logical next development of the Bitcoin payment system. You can imagine the architecture like a cake with several layers. The Bitcoin Blockchain is the bottom, or the so-called base layer. The Lightning Network would be built on top of that. Certain characteristics of the base layer could be inherited, such as security, while other limitations no longer apply, such as the limited number of transactions. The link between the base layer and the lightning network is achieved by a number of cryptographic mechanisms.

Payment Channels

The core of the Lightning Network is payment channels. A payment channel can be thought of as a tunnel between two parties, Alice, and Bob. It connects Alice and Bob directly. The difference between a payment channel and a transaction on the blockchain is that payments within the tunnel are not recorded on the blockchain. Instead, Alice and Bob can keep updating the state of the payment channel and only write the last state to the blockchain when they are "done." Updating the payment channel happens outside of the blockchain and is not bound by its limitations. Alice and Bob could refresh the state of their channel several times per second. In other words, micro-transactions become not only possible but plausible. Instead of sending multiple transactions, the amount owed is summed up after a certain amount of time only then is it settled on the main blockchain.

1.2 Bitcoin Mining Deep Dive

In Module 1, you have already gained an understanding of the purpose and working mechanism of the Bitcoin mining process. Now, you will dive into the details of mining such as hardware and energy requirements and the legality of mining in different countries in the Generation Blockchain Podcast on Bitcoin mining.

Click here to listen to the Generation Blockchain podcast on Bitcoin mining.

02

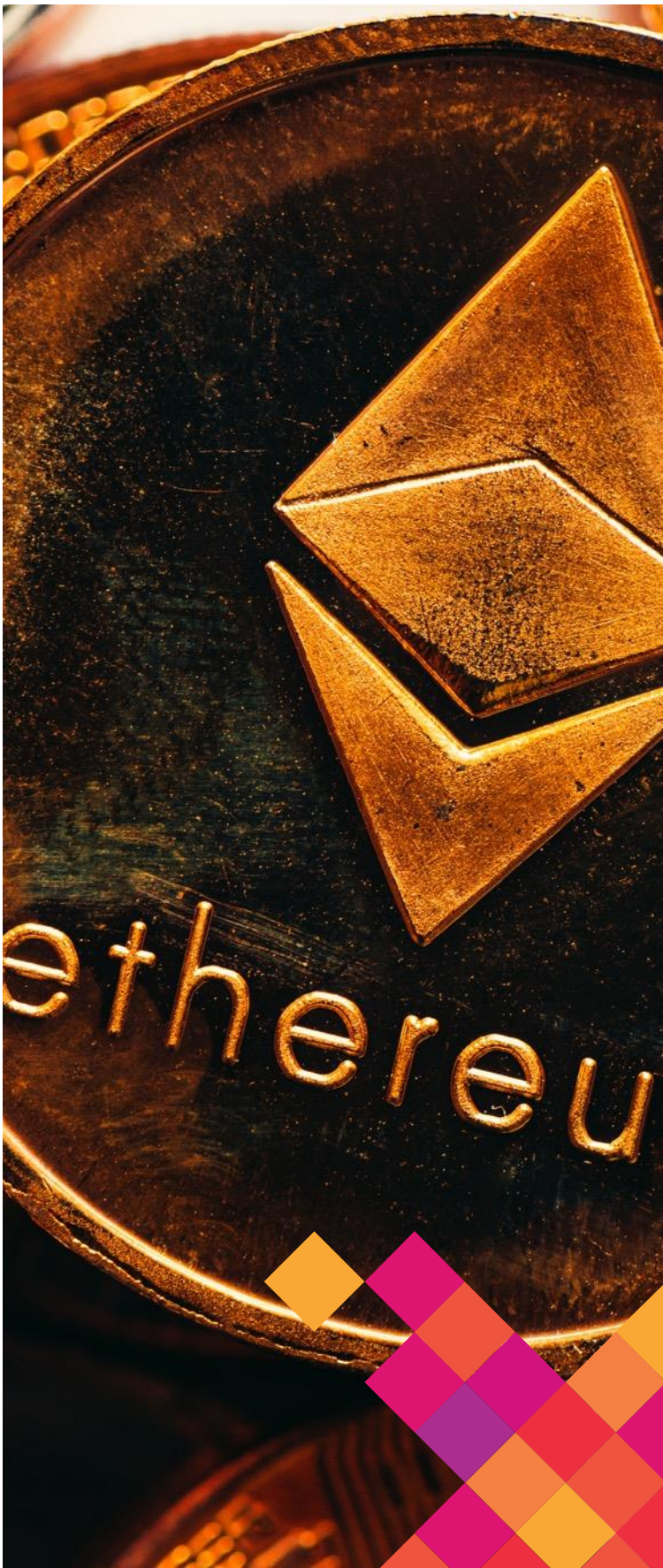
ETHEREUM

2.1 Introduction to Ethereum

Next to Bitcoin, Ethereum is the second largest cryptocurrency as measured by market capitalization. The Ethereum network is a blockchain-based platform focused on programmable contracts (smart contracts) and decentralized programs (dApps). The associated cryptocurrency is called Ether (ETH). Ethereum is also often referred to as a “world computer”. The term world computer comes from the fact that Ethereum does not just store the state of currency ownership like Bitcoin does, Ethereum can track the state of any kind of arbitrary data and execute all code that can be put into binary data format.

Ethereum (ETH) is a decentralized open-source platform based on blockchain technology. It allows any interested developer, individual or company to run and develop their own dApp or even a decentralized organization (DAO) using smart contracts. Ethereum has memory that stores both code and data and it uses the Ethereum blockchain to track how this memory changes over time like a general-purpose stored program computer Ethereum can load code into its state machine and run that code storing the resulting stage changes in its blockchain.

To understand the basics of Ethereum, watch this Generation Blockchain introduction video. Click here to watch the Generation Blockchain video on the Basics of Ethereum.



Inventors of Ethereum

Vitalik Buterin is the initial inventor and co-founder of Ethereum. In the early stages of Bitcoin's development, Buterin ran a magazine that was publishing on the topic of Bitcoin. Through this, he identified aspects that he saw as room for improvement. Vitalik Buterin then co-founded Ethereum with Anthony Di Iorio, Mihai Alisie and Charles Hoskinson. Buterin first explained the Ethereum Blockchain in a white paper in 2013. Ethereum was intended to unleash the full potential of Bitcoin. It combines a synthesis between radical openness and radical privacy. Buterin wanted to create a platform that is a mining system and provides a platform for developing one's own software applications.

Ether Currency Units

The cryptocurrency of the Ethereum blockchain is called Ether. Ether is a means of payment for every transaction or creation of smart contracts, as well as the use of various services on the Ethereum platform. All changes made on the world state of Ethereum cost Ether. To interact with the Ethereum Blockchain, one needs to buy Ether. Ether is the fuel of the entire platform. Ether is also distributed as a reward to Ethereum stakers and validators. Ether is subdivided into smaller units down to the smallest unit possible which is named wei 1 ether is 1 quintillion (1018) wei.

What are smart contracts?

Smart Contracts are digitized, determined contracts between two or more people or software programs. The code can either be the sole manifestation of the agreement between the parties or can also act as a complement to a traditional text-based contract and execute certain provisions, such as transferring funds from party A to party B. The code itself is replicated across multiple nodes of a blockchain and, therefore, benefits from the security, permanence, and immutability that a blockchain offers. It is possible to use smart contracts to develop a DAO or a dApp.

Smart contracts

1 are operated by a network of computers

2 execute agreed steps automatically when a specified event occurs

3 automatically track changes within the set terms of the contract

4 are stored on the blockchain

On the Ethereum network, smart contracts exist as independent users that can be interacted with, and thus, they have the same status as human users. This also means that they can be viewed and monitored by anyone in the network. Conditions are defined in the contracts, which anyone can check for correctness. Depending on whether the triggering event occurs, the smart contracts automatically execute the linked commands. These smart contracts are stored on the Ethereum Blockchain.

Smart Contract Example

For example, the smart contract includes the understanding that a person will receive their money for the package when it arrives three days after the order is placed. Moreover, such a smart contract is connected to software that is capable of checking on the status of the package (i.e., whether it has been delivered or not). Once the package has arrived, the smart contract automatically releases the recipient's Ether amount stored and locked up in the smart contract to the sender of the package. If the software would detect that the package has not been delivered. Here, the smart contract could override itself and the buyer will get their money back.

Smart Contracts and the Ethereum Blockchain

What makes Ethereum special, however, are the smart contracts that turn the Ethereum network into a decentralized computer. Smart contracts, as the name suggests, are smart contracts or small programs that run on the Ethereum network and can, for example, regulate Ethereum transaction conditions. Unlike the Bitcoin network, the nodes on the Ethereum network are also responsible for processing these contracts. Through smart contracts, it is possible to develop so-called decentralized Apps. DApps are publicly accessible decentralized applications. Since ultimately everyone can run an Ethereum node, all dApps have the same functionality and can offer services built on top of the infrastructure accordingly.

Ethereum dApps

Everywhere in the world, developers are building dApps on top of Ethereum and creating innovative dApps. There are almost no limits to dApp development. There are financial applications, decentralized exchanges (DEX), social media platforms, messenger services, games and others are just a couple of examples for dApps. Smart contracts can be seen as back-end APIs running in the blockchain while dApps are the front- end or UX. They represent the visible layer connecting users or other applications with the smart contracts running in the blockchain. You may think of app stores that we are already familiar with. Just like with dApps, there are countless apps in the app store today. These apps trust the app store with payment management and thus involve a third party and the need for established trust. Traditional developers are also dependent on the App Store's favor. App stores can remove apps from their stores as the ultimate authority. Accordingly, the consumer's choice also depends on the influence of third parties such as Google or Apple. Conclusively, this means that the content they generate is in the hands of third parties and influenced by unwritten rules of the industry. This is different with dApps which are built on Ethereum. Here, the data is in the hands of the users. Developers can offer dApps freely and independently of an app store provider, eliminating the pre-selection of an app store altogether. Running an Ethereum node is not a requirement for implementing DApps. Instead, there are private offerings in the cloud that can provide access to existing nodes.

Ether supply

As compared to Bitcoin which sets the maximum supply at 21 million, Ethereum does not have a limit. There will never be an end to Ether production. How many Ether exist has a direct impact on its price. Generally, the greater the number of coins that are publicly available, the lower its value. The total amount of Ether is still fluid, as the recent network upgrade to PoS have made an increase and decrease in both directions possibly in terms of Ether supply.

The differences of Ethereum and Bitcoin

Bitcoin and Ethereum differ in many aspects. While Bitcoin is a cryptocurrency, Ethereum is a platform. For this reason, Bitcoin is primarily a store of value and medium of exchange whereas Ethereum is seen as a general purpose blockchain. Ether is the native token on Ethereum's blockchain. Bitcoin is and always has been the largest cryptocurrency as measured by market capitalization and Ethereum is the second largest. Transactions are faster on the Ethereum network than on Bitcoin's due to the fact that the Ethereum blockchain is slightly faster than the Bitcoin blockchain. It is also important to note that Ethereum was created as a complement to Bitcoin and not as competition. While Bitcoin has been able to establish itself as a cryptocurrency, Ethereum aims to establish a decentralized world computer. In this sense, a comparison between the two cryptocurrencies is a difficult one.

2.2 Ethereum Transactions

To learn how Ethereum transactions work in accordance with smart contracts, listen to the Generation Blockchain podcast episode on the topic.

Click here to listen to the Generation Blockchain Podcast episode on Ethereum Transactions & Smart Contracts.

2.3 Ethereum Smart Contracts

In a previous section, you have already gained a high-level overview of smart contracts which will be deepened in the following.

As you already know, smart contracts are a type of Ethereum account. Thus, they have a balance and can be the target of transactions. Smart Contracts must not be controlled by a user, instead, they are deployed to the network and run as previously programmed. Actual user accounts can interact with a smart contract by submitting transactions that execute a function defined on the smart contract. Smart contracts can define rules, like a regular contract, and automatically enforce them via the code. Smart contracts cannot be deleted by default, and interactions with them are irreversible. They can only be overwritten by authorized parties. Smart contracts are simply programs stored on a blockchain that run when predetermined conditions are met.

They typically are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary's involvement or time loss. They can also automate a workflow, triggering the next action when conditions are met.

From an implementation standpoint, Vitalik and his co-founders designed the so-called Ethereum Virtual Machine (EVM) for running byte code in the blockchain. Every node in the network runs said EVM, and it is ready to execute any arbitrary code. Creating a new contract in the blockchain implies sending the program representation in byte code as part of the transaction data payload. Once the EVM runs the transaction and the block is added to the ledger, the programmer then receives the public address where it was published. From there, anyone that is given access to it can then start interacting with the contract at that address.

There are three important aspects of smart contracts. The execution context, the gas fee, and the immutability.

Execution context

Smart Contracts run in isolation meaning that they can only see data available on the Ethereum blockchain or call other smart contracts. Thus, they cannot make calls to any service or query data from outside the Ethereum blockchain. Some contracts in Ethereum act as oracles. External users or applications can feed these oracle contracts with external data so others can consume them.

Gas

Running code in the EMV cannot happen without a gas fee being paid since computing resources and storage are scarce and are not for free for the validators. The cost of using Ethereum services is expressed in a unit known as gas, which represents short fractions of Ether (denominated in WEI). For every transaction submitted one must pay gas, otherwise the code will not run. Gas is consumed by executing lines of code or allocating storage space. If a transaction runs out of it, it results in the cancellation of the transaction. In this case, the tokens or funds are spent anyway. Technically, gas represents a unit and not a price since the price for the transaction is assigned when it is created. Here, the higher the price that one pays or is willing to pay leads to a higher prioritization of the transaction in the execution queue. Validators have the incentive to execute transactions that pay more since they receive the gas fees. One can also set a gas limit on the transaction. This expresses how much one is willing to spend on the execution. If the transaction costs more, it is canceled, and the unused funds are returned to the sender.

Immutability

Smart contracts are immutable. Thus, by definition (byte code) they cannot be changed or updated once they are deployed on the Ethereum blockchain. In case an existing smart contract needs to be altered, one has to deploy a new version in a new address. Once bugs are introduced, they cannot be fixed.

03

DECENTRALIZED FINANCE

Before we will dive into decentralized finance (DeFi), we must first understand our current financial system on a base level to understand the parallels between traditional finance (TradFi) and DeFi.

3.1 Traditional Financial System

Any financial system that we know today is a highly interconnected network of intermediaries, facilitators, and markets serving the following purposes:

1 Allocating capital,

2 Sharing risks, and

3 Facilitating all types of trade, including intertemporal exchange.

On first glance, this might sound uninteresting, but it is one of the most crucial pillars to human welfare in a capitalistic system. Without this financial system, the technological progress of the last two centuries (e.g., invention of steam engines, cars, airplanes, land line telephones, computers, gene manipulation, and cell phones) would not have taken place, at least not at this pace.

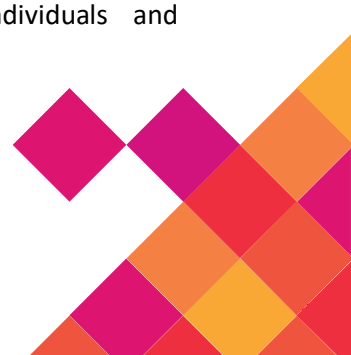
The purpose of the financial system

The main function of the system is to efficiently link money borrowers to lenders. Borrowers range from inventors, entrepreneurs, domestic households, governments, businesses, and startups with potentially profitable business ideas but limited financial resources where the expenditures are higher than the revenues. Lenders or savers also come in different calibrations and can take on the shape of domestic households, businesses, governments, and investors with excess funds where the revenues are higher than the expenditures. The financial system also helps to link risk-averse entities called hedgers to speculators.

It does happen that individuals and companies, especially small businesses or ones that sell into rapidly growing markets, have enough wealth (i.e., a stock) and income (i.e., a flow) to implement their ideas without outside financial support by plowing back profits which is also known as internal finance. The more usual case, however, is that people and firms that have good ideas do not have the funds needed to draw up blueprints, create prototypes, lease offices or production space, pay employees, obtain permits and licenses, or suffer the risks that come with bringing a good or service to market. Sufficient funds are vital to chasing and fulfilling our ideas from a professional and private standpoint. This course on blockchain for example is free because the EU deems education to be a necessity that should not be made available only for those students who have the means to pay for it.

The necessity of a financial system (?)

Why is it that individuals and companies do not simply borrow from other individuals and companies when they have to?



Lending, as goes for most other goods and services, is most efficient and cheap if done by specialists and companies that focus on doing only one thing (or a couple of related activities) very well. Firstly, through the practice, research that they have accrued over time and secondly, they also unlock economies of scale. For example, the fixed costs of making loans (i.e., advertising for borrowers, buying and maintaining computers, leasing suitable office space, and writing up contracts) are quite high. To make up for these fixed costs and make a large margin of profit, lenders must do a lot of business. Therefore, small businesses in a highly concentrated market cannot be profitable. This is not to say, however, that bigger is always better, only that to be efficient financial companies must exceed minimum efficient scale.

Asymmetric Information

Finance also suffers from another problem that is not easily overcome, namely the concept of opportunity costs (i.e., to obtain X you must give up Y). On top of this, we encounter an additional issue called asymmetric information. In the context of a financial system, when a seller (i.e., borrower, a seller of securities) knows more than the buyer (i.e., lender or investor, a buyer of securities), it is not long until the problems start to show. The two main issues with this are adverse selection before a contract is signed and moral hazard, which entails sinning after contract consummation.

Adverse selection

Ironically, the riskiest borrowers are also the ones who most strongly demand loans. If lenders are unaware of this selection bias, they will continuously become more and more reluctant to lend out their money. Unless recognized and effectively countered, moral hazard will lead to the same suboptimal outcome.

Moral hazard

Even if adverse selection bias did not cause a problem, borrowers that are good willed sometimes turn into thieves after signing because they realize that they can gamble with other people's money. This kind of embezzlement is common, and borrowers often end up unable to repay the loan.

The current financial system never kills the information asymmetry, but it reduces its influence, intermediaries by screening insurance and credit applicants and monitoring them thereafter, and markets by providing price information and analysis. Businesses and other borrowers can obtain funds and insurance cheaply enough to allow them to become more efficient, innovate, invent, and expand into new markets despite asymmetric information. Another way to look at it is to realize that the financial system makes it easy to trade intertemporally, or in other words across time. Instead of having to pay immediately for supplies, companies leverage the financial system to acquire what they require for operations today and pay for it at a defined time in the future, giving them time to produce and distribute their products.

Financial Instruments

Financial instruments are legally binding contracts that list the obligations of their makers, the individuals, governments, or businesses that issue them and promise to make payment, and the rights of their holders, the individuals, governments, or businesses that currently own them and expect to receive payment. They serve the purpose of specifying who owes what to whom, when or under what conditions payment is due, and how and where any payment should be made.

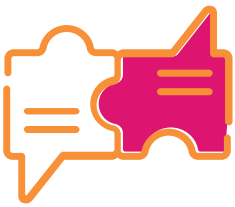
Financial instruments take mainly three shapes:

Debt

Debt instruments, such as bonds, are a lender–borrower relationship in which the borrower promises to pay a certain sum and interest to the lender at a specific date or over some period of time.

Equity

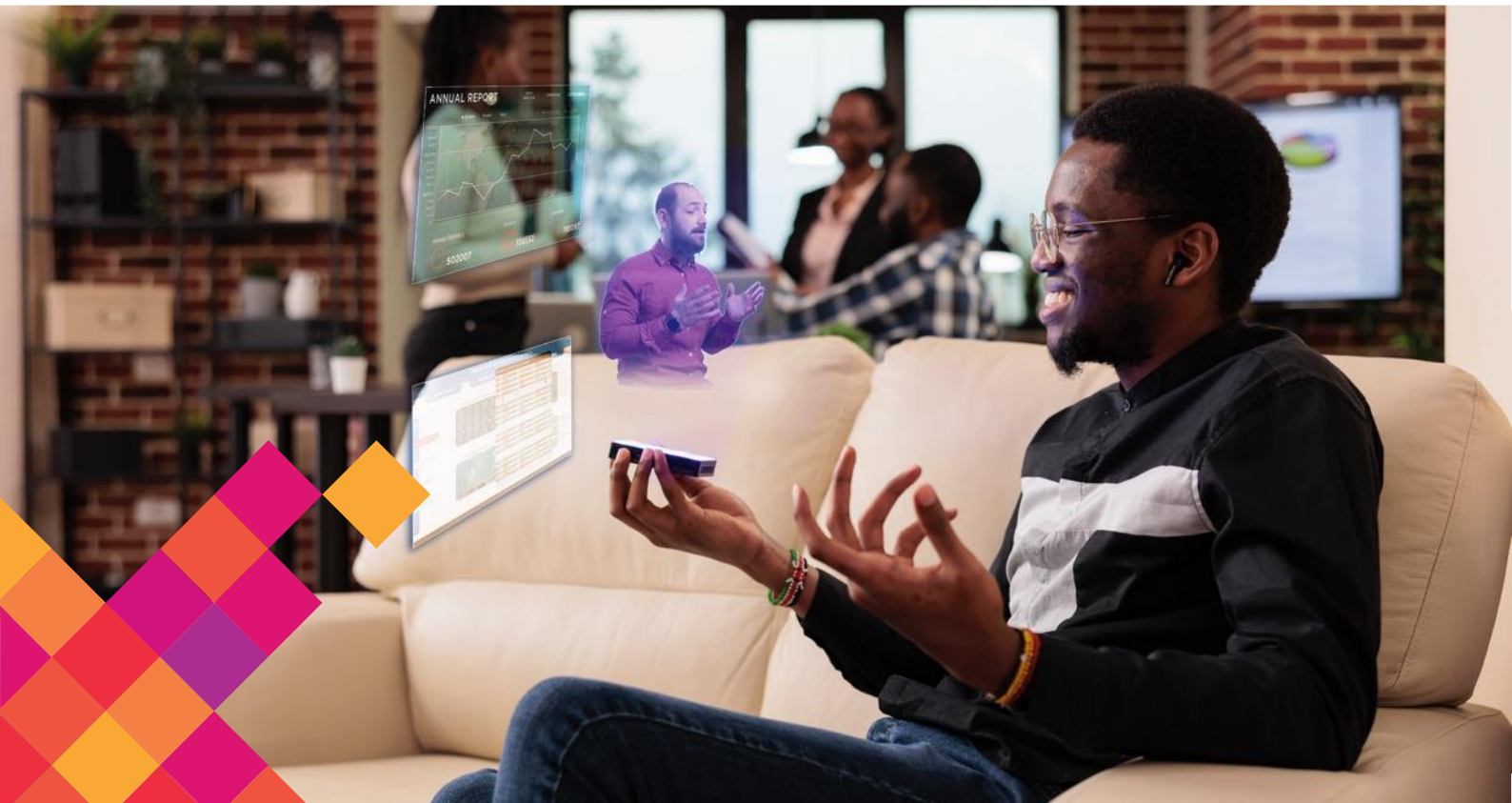
Equity instruments, such as stocks, represent an ownership stake in which the holder of the instrument receives some portion of the issuer's profits.



Hybrid

Hybrid instruments(e.g., preferred stock) have some of the characteristics of both debt and equity instruments. Like a bond, preferred stock instruments promise fixed payments on specific dates but, like common stock, only if the issuer's profits warrant. Convertible bonds, by contrast, are hybrid instruments because they provide holders with the option of converting debt instruments into equities.

Today, most financial instruments are held only as electronic accounting entries that are linked to a specific contract. Stocks used to be issued in paper form.



Financial Markets

The current financial system is not a direct financial system. There is always an intermediary needed to settle a transaction unless the transaction is made in physical cash. For example, brokers facilitate secondary markets by linking sellers to buyers of securities in exchange for a fee or a commission, a percentage of the sale price. Dealers “make a market” by buying and selling securities, profiting from the arbitrage, or the difference between the sale and purchase prices. Brokerages offer usually both – brokering and dealing and also consult their customers on investment decisions. Investment banks support primary markets by underwriting (i.e., buying for resale to investors) stock and bond offerings and by arranging direct placement of bonds. Investment banks can also be brokers by introducing securities issuers to investors.

As are financial markets, financial intermediaries are highly specialized. Financial intermediaries have very different functions from depositing money, giving advice, making use of different prices for the same asset at a certain time and many others. They are usually categorized according to their ownership structure. For example, depository institutions (i.e., commercial banks, savings banks, and credit unions) issue short-term deposits and buy long-term securities. Traditionally, commercial banks specialized in issuing demand, transaction, or checking deposits and making loans to businesses. Savings banks issued time or savings deposits and made mortgage loans to households and businesses, while credit unions issued time deposits and made consumer loans. Almost all commercial and many savings banks are joint-stock corporations. Some savings banks and all credit unions are mutual corporations and hence are owned by those who have made deposits with them. The current financial market is highly complex and is the result of years of developments.

Regulation

The financial system is relatively heavily regulated as compared to other sectors in capitalistic countries. Regulators serve four major functions:

1 Reduce asymmetric information

They try to do so by encouraging and claiming transparency. That usually means requiring both financial market participants and intermediaries to disclose accurate information to investors in a clear and timely manner.

2 Protect consumers

Regulators must protect consumers from scammers, and from the failure of honest but ill-fated or poorly run financial institutions. They do so by directly limiting the types of assets that financial institutions are allowed to do business with and by mandating minimum reserve and capitalization levels.

3 Strive to promote financial system competition and efficiency

Regulators promote competition by ensuring that the entry and exit of firms is as easy and cheap as possible.

4 Ensure soundness of the financial system

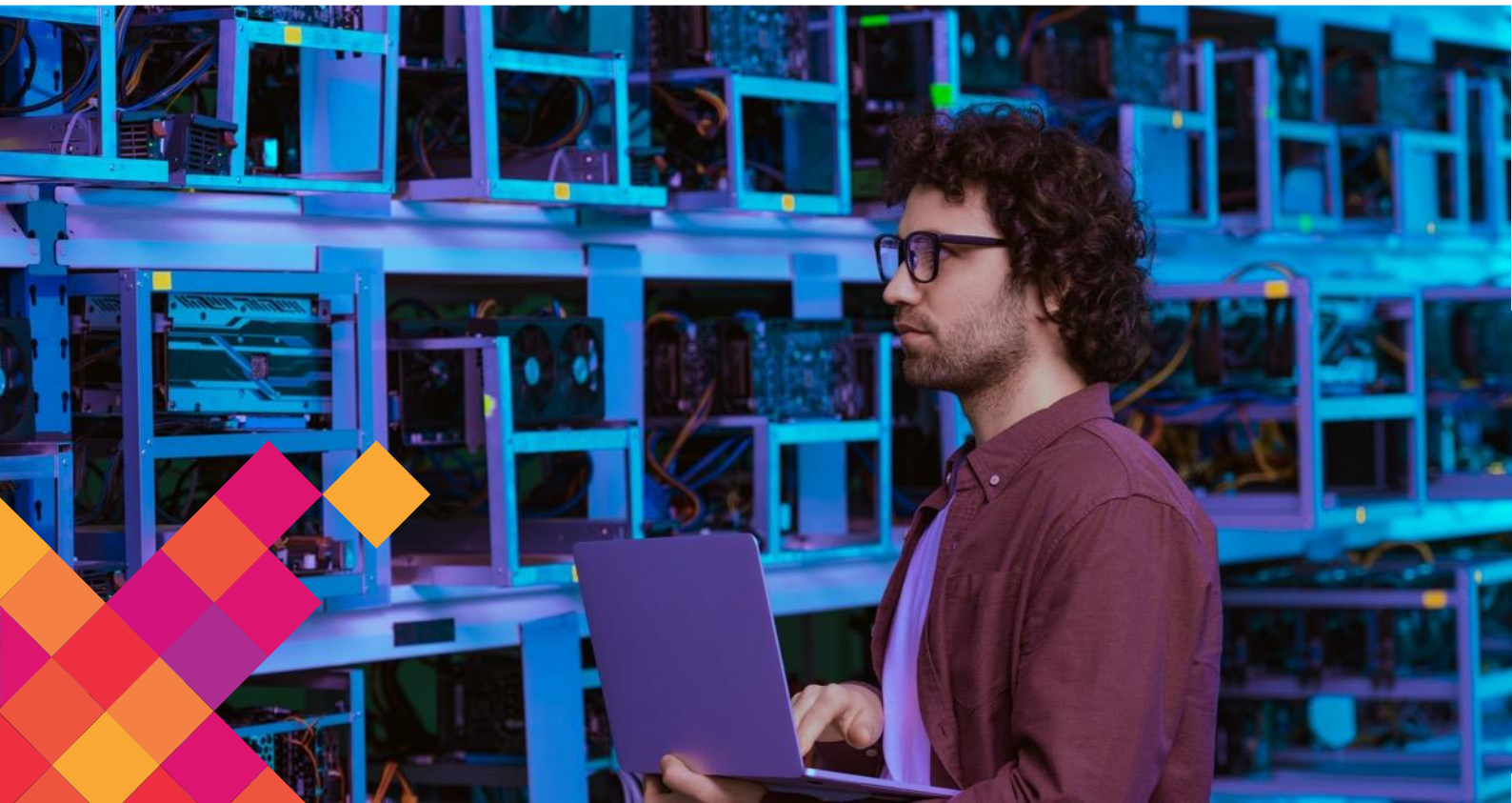
It is the goal of the regulator to ensure the soundness of the financial system by acting as a lender of last resort, mandating deposit insurance, and limiting competition through restrictions on entry and interest rates which is a controversial intervention in the market. Regulators are also capable of limiting competition in the market to ensure safety. However, this does extend privileges to existing institutions over new ones which is why existing companies are often proponents of regulation.

Depending on the jurisdiction, there is usually more than one local regulator that needs to be complied with. In the US for example, there is the Securities and Exchange Commission (SEC, which oversees exchanges and OTC markets), the New York Stock Exchange (NYSE, which oversees itself as an SRO or self-regulating organization), and the Commodities Futures Trading Commission (CFTC, which oversees futures market exchanges) monitor and regulate financial markets. Next to these three major ones, there are also other regulators, including the Office of the Comptroller of the Currency (which oversees federally chartered commercial banks), the Federal Deposit Insurance Corporation (FDIC, which oversees almost all depositories), and sundry state banking and insurance commissions which is monitoring financial intermediaries. Players that try to avoid regulatory scrutiny due to its high cost tend to use intermediaries instead of markets.

3.2 Decentralized Financial System

Promising to enhance access and efficiency within financial services, DeFi has gained significant attention (and some traction in the marketplace) in recent years. In essence, DeFi uses secure blockchain technology to facilitate peer-to-peer financial transactions, including borrowing, lending, and trading. DeFi seeks to disintermediate and decentralize the traditional financial services industry by automating complex financial processes. The functional roles of trusted third parties such as brokerage firms, banks, and other centralized financial institutions, are replaced by smart contracts. Although from a big-picture perspective DeFi is still a niche phenomenon whose long-term impact on the financial services industry is yet to be determined, that potential for disintermediation means it is important that established financial institutions understand how it might reshape the operational landscape and how they might themselves embrace the concept of decentralization. Certainly, a major market correction is underway in the digital assets space in 2022.

There is already a broad range of financial services or products available in the DeFi space including trading, lending, investing, deposits, and payments services. Furthermore, decentralized applications are highly modular. This means, that very often they can be combined and are interoperable to create new applications. DeFi's rise in popularity can be partly explained by real and perceived structural issues with the current financial services industry. DeFi arose out of a desire to free financial services from the control of centralized institutions and governments discussed in the previous section, thereby providing financial inclusion for more people. Proponents of DeFi argue that traditional financial services are dominated by large institutions and often characterized by tightly controlled access, leading to organically grown inefficiencies, high and opaque fees as well as financial exclusion. In addition, they point to the high level of regulation fostering an environment that is generally hostile to disruptive technologies or innovative business models in most of the world. While some industry commentators have cast doubt on the sustainability of fully decentralized financial services, others believe that DeFi has real potential as a disruptor of traditional financial services markets.



The layers of DeFi

A basic understanding of the different layers of technology used for DeFi applications will establish a mental map that is helpful in analyzing and evaluating specific DeFi implementations as shown below.

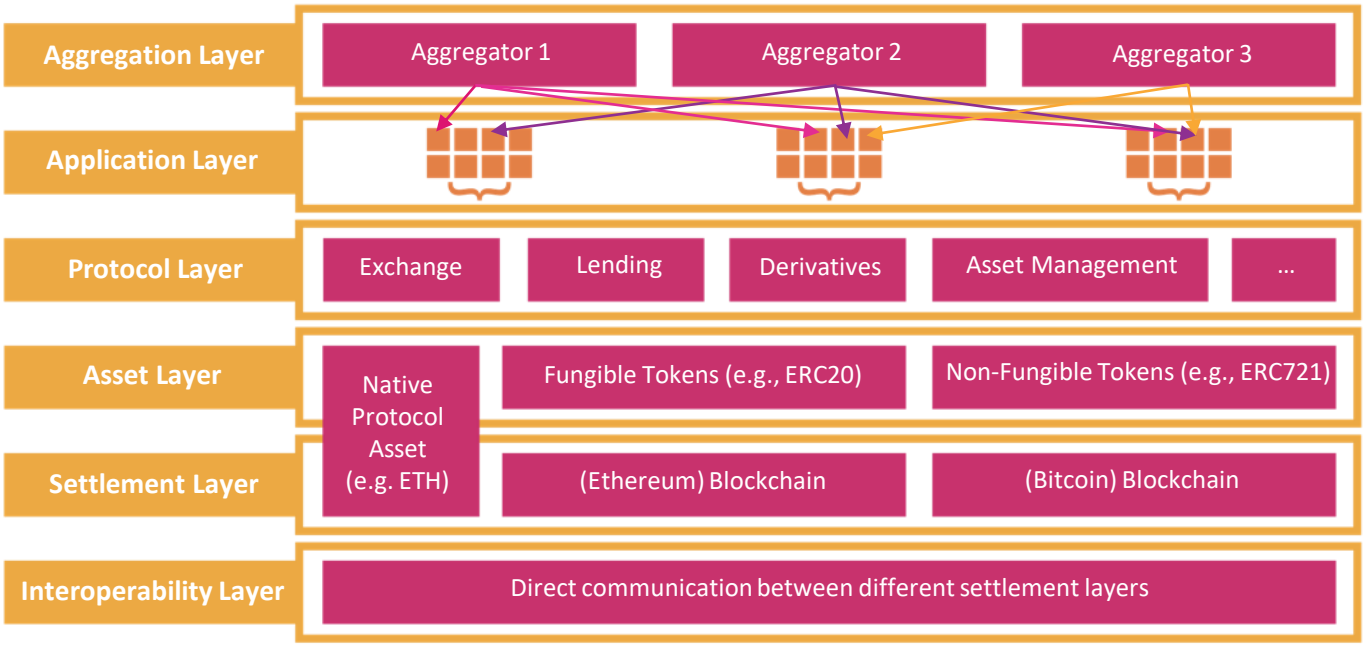


Figure 9: The DeFi Stack (based on IOSCO 2022 and Schär 2021)

Protocol, asset, and settlement layers form the core of the DeFi technology stack. The protocol layer consists of DeFi applications that offer some sort of financial service functionality such as trading or lending. The asset layer defines which digital assets can be processed by a DeFi protocol. It is important to keep in mind that normally a specific DeFi protocol is offering its services for only a few specific digital assets such as one fungible token or a pair of fungible tokens. Finally, the settlement layer forms the underlying infrastructure. DeFi applications as well as digital assets reside on Layer-1-protocols (e.g., Ethereum).

This Layer-1 protocol is of crucial importance, as it represents the execution and settlement layer for any transactions. In addition to these core layers, three additional layers can play a role. First, at the bottom of the stack, the interoperability layer allows different settlement layers to directly communicate with each other. It can be used to allow DeFi applications to incorporate different Layer-1-protocols into their functionality. At the top of the stack, an application layer normally provides user interfaces. Finally, an aggregation layer allows to aggregate the functionality of multiple DeFi applications.

DeFi solutions exist for major functions such trading, lending, investing, deposits, and payments more services being added on an ongoing basis. Below you see an overview of financial services, with examples of solutions across traditional finance (TradFi), Centralized Finance (CeFi) and DeFi. When comparing TradFi with CeFi and DeFi, it is important to distinguish infrastructures from assets. DeFi (and CeFi) solutions currently focus on the processing of digital assets such as cryptocurrencies, whereas TradFi handles traditional assets such as bonds or equities. However, it would also be conceivable that DeFi solutions process digitalized versions of traditional assets (e.g., tokenized bonds).

	Traditional Finance (TradFi)	Centralized Finance (CeFi)	Decentralized Finance
Trading	Exchanges / Brokers (e.g., Xetra)	Crypto Exchanges (e.g., Binance)	Decentralized Exchange (e.g., Uniswap)
Lending	Secured and unsecured (e.g., term loans)	Lending Platforms (e.g., BlockFi)	Lending Protocols (e.g., Aave)
Investing	Investment Funds (e.g., ETFs)	Crypto Funds (e.g., Grayscale)	Decentralized Asset Management (e.g., Cosmos)
Deposits	Saving Accounts (e.g., Commercial Banks)	Staking Pool (e.g., Coinbase)	dStaking Services (e.g., Cosmos)
Payments	Payment Platforms (e.g., SEPA, T2)	Centralized Stablecoins (e.g., USDC)	DeFi Stablecoins (e.g., DAI)

Figure 10: Main financial services categories in traditional finance, centralized finance, and decentralized finance.

As noted, DApps are currently available for users in financial services such as trading, lending, investing, deposit, and payment solutions.

Trading:
In DeFi, decentralized exchanges (DEXs) perform the function of centralized exchanges by using smart contracts. DEXs enable users to exchange digital assets without having to use or trust intermediaries or use custodians. Major DEX protocols include Uniswap and Sushiswap.

Lending:
DeFi lending protocols offer loan services. These solutions normally come in one of two varieties. With pool-based lending protocols, interested individuals provide liquidity or funds to a pool that others can borrow from.

Users putting their assets into the pool can earn interest-like income in return. With peer-to-peer based lending, individuals borrow directly from a particular lender. In this case, decentralized lending protocols enable borrowers to take out loans with minimum barriers. Major DeFi lending protocols include Aave, Maker and Compound.

Investing

DeFi DApps can also be used to execute automated trading strategies. For example, TokenSets is a DApp-based platform for portfolio management. Users provide the boundary conditions and investment objectives and then TokenSets trades, balances, and implements strategies to achieve the users' goals automatically. This enables users to gain exposure to a basket of digital assets, without the need to buy individual assets.

Deposits (Staking)

While there are no deposits in the traditional sense in the DeFi ecosystem, a very similar mechanism (called staking) exists. Staking is the process of locking up digital assets for a fee. It is thus comparable to depositing money at a regular bank. Just as a bank deposit represents a short-term loan that is given to the bank, staked cryptocurrencies can be seen as a short-term loan to a protocol. For the time that assets are staked, they earn a small income. However, they cannot be sold or otherwise used by their owners during this time. Digital assets that are locked up in this way are usually used for adjacent processes (e.g., supporting the transaction validation mechanism of the underlying blockchain network).

Payments and stablecoins

The high volatility of cryptocurrencies such as Bitcoin and Ether hampers their use for payment purposes. This is where stablecoins come in. Stablecoins are digital assets that are pegged to (a basket of) fiat currencies or some other stable asset. They aim to be a means of payment with a similar volatility as fiat currencies. As stablecoins are digital assets, they can be seamlessly integrated into other DeFi applications. Users can conduct on-chain transactions with these coins without the need for using traditional financial infrastructures within a matter of seconds. Stablecoins come in different varieties:

Asset-backed stablecoins are blockchain-based tokens that have their value pegged to a reserve asset such as another digital currency, fiat money, or a commodity. In contrast, algorithmic stablecoins try to keep a stable value by managing the supply of the coin based on demand from users. However, the recent collapse of Terra (Luna) has proven that algorithmic stablecoins have difficulty retaining their value and are rather unsuitable as a means of payment.

Also, the adequacy of reserves of asset-backed stablecoin projects have recently been publicly challenged. Some of the most popular stablecoins include USD Coin (USDC), Binance USD (BUSD) and Dai (DAI). In additon to these private sector-driven stablecoins, central banks around the world are looking into the opportunities of Central Bank Digital Currencies (CBDC) that can include the launch of a stablecoin. While the above examples represent the main solutions currently observed in the DeFi space, there are many other DeFi financial services that are tested (e.g., insurance services, derivatives, and prediction markets).

Decentralized Exchanges

One of the fastest growing areas in DeFi is Decentralized Exchanges (DEX). With the rise of cryptocurrencies and other digital assets after the financial crisis of 2008, users were looking for service offerings that enabled them to trade these new asset classes. Traditional financial service providers did not offer trading services for owners of digital assets. As a result, a new class of financial intermediaries emerged. In the beginning phase, this took shape in centralized exchanges (CEXs). CEXs replicate offers from TradFi in the CeFi world. To use the services of a CEX, a user undergoes registration at the CEX (i.e., KYC and AML processes) and then, before buying or selling digital assets, the user must fund their account using either cryptocurrencies (e.g., Bitcoin) or some traditional form of payment (e.g., bank transfer). This recentralized approach to DeFi means giving up control over any assets. Essentially, the CEX controls the user's account.

In the context of CEXs, users need to trust the exchange with their money. This makes them vulnerable to a certain degree of counterparty risk. At the beginning, this was especially problematic given most CEXs were newly established entities with untested operations and minimal to zero oversight from financial markets authorities. As a results, hacks, scams, and other illegal activities have been common in the early years of the CeFi space, often leading to a loss of capital for users of these services. You will learn more about the early phases of exchanges in a later module. To solving this issue, decentralized exchanges (DEX) emerged. The primary goal of a DEX is full disintermediation via the elimination of middlemen and allowing every user to deal directly with other users on a peer-to-peer basis. By migrating trading functionality directly onto the blockchain via smart contracts, a DEX serves as a trustless platform for the trading of digital assets. Much like traditional exchanges and CEX, these platforms coordinate supply and demand from many users. However, assets either remain in the custody of the user or (for a limited time) in an escrow account of the fully automated smart contract.

Main Types of DEXs

DEXs come in different forms. Over the years, several designs have been suggested and implemented, all to improve on previous projects and further streamline the functionality of the solution and its user experience. The following three major types of DEX exist:

Automated Market Makers-based DEXs (AMMs)

AMMs utilize pools of digital assets which are sourced from so-called 'liquidity providers' to enable trading services for their users. Prices are quoted automatically by the underlying smart contract, hence the name automated market maker. The main purpose of creating an AMM is to always ensure liquidity.

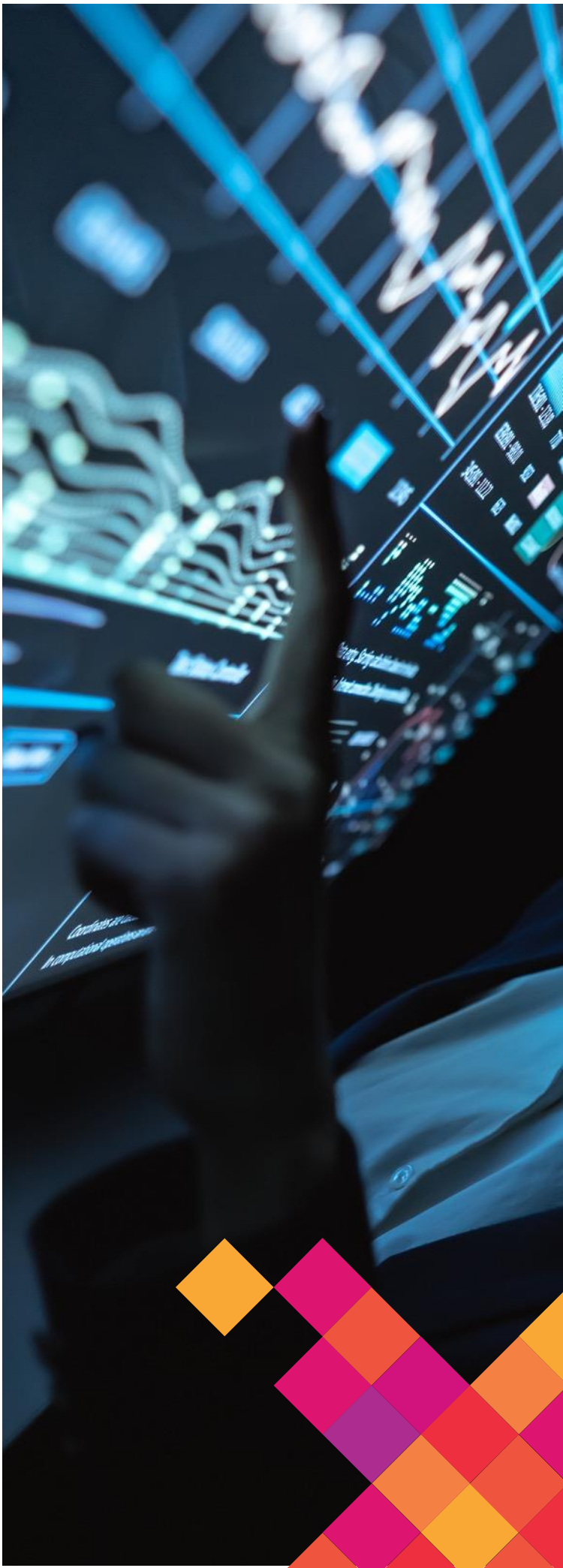
Order book-based DEXs

Order book DEXs compile the details of all open buy and sell orders for a particular pair of digital assets. A buy order implies that a trader desires to bid for an asset at a given price. A sell order on the other hand is an indication that a trader is willing to sell a specific asset at a particular price. Much like traditional exchanges, order book DEXs match these orders.

Hybrid / Alternative Platforms

While most DEXs can be classified as either AMM or order book-based, a growing number of platforms are beginning to merge the concepts of both these types to create new, hybrid DEXs. This is done to enable additional functionality (i.e., allowing users to seamlessly trade their assets across multiple blockchains).

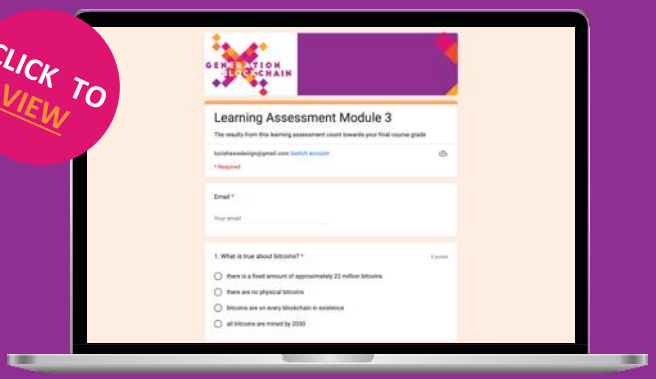
In addition, a noteworthy phenomenon has been the rise of DEX aggregators, which allow users to search for prices and liquidity across multiple DEXs. As the name implies, they aggregate liquidity from different DEXs to provide the users with the best execution price available within the shortest time, while lowering the level of slippage on large orders and optimizing fees.



04

LEARNING ASSESSMENT FOR MODULE 3

To test your knowledge, finish this learning assessment as part of your overall grade for the course.
Click here.



01

MODULE 4

Regulation & Policy

Co-funded by the European Union

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 National Agency. Neither the European Union nor National Agency can be held responsible for them.

contents module 4

Co-funded by the European Union

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 National Agency. Neither the European Union nor National Agency can be held responsible for them.

01| MODULE 4
Regulation & Policy

Chapter Overview

In this module, blockchain and crypto asset regulation (i.e., EU and non-EU regulation and law) will be examined.

Learning Objectives

After the first module, you should be able to:

- Explain the different types of risks in blockchain and crypto asset regulation.
- Reiterate how Liechtenstein's Token Container Model works.
- Understand the complexity of crypto regulation on a national and international level as well as the interests and rights of the stakeholders involved.
- Gain an overview of the current developmental phase of MiCAR in the EU.
- Understand how national and international law interoperates.
- Understand the importance of regulation as an innovation fostering or hindering factor.
- Explain the intricacies of tokenization right.
- Understand the three dimensions (financial regulatory treatment of cryptocurrencies, governance, and regulatory requirements for crypto service providers) of crypto asset regulation.
- Discuss the importance of collaboration and transparency in regulatory advancements.

01| BLOCKCHAIN & CRYPTO ASSET REGULATION

The international regulatory landscape is fragmented, with national legislations ranging from no regulation to explicit prohibitions, to comprehensive integration into the financial industry. In the following, you will learn about blockchain and crypto asset regulation in general and look at specific jurisdictional differences.

1.1 Blockchain & Crypto Asset Regulation in General

Risks connected to crypto regulation

The growth of the crypto market continues to be high despite the traditionally extreme price fluctuations, there is currently no flattening of this trend that can be observed at present. New, innovative developments are constantly observable in the market. Crypto assets are gaining importance for more and more jurisdictions. During this, regulators all around the world are trying to keep up with the developments, by gathering relevant information and gradually acquiring the necessary knowledge. In doing so, they encounter two inherent characteristics of crypto assets that continue to prove challenging:

1 The decentralized structure makes it difficult to identify a competent authority to take responsibility for any questions or responsibility for any questions or problems that arise.

2 Pseudonymity, i.e., the limited traceability of transactions and identities of sender and recipient, exacerbates this challenge in the case of further in the case of illegal activities.

The use of crypto assets is possible in many countries without or with few restrictions. In the case of particularly decentralized, globally operating blockchains, even restrictions on the part of state supervisory authorities are almost impossible to enforce. This results in risks, with which various challenges. These are analyzed in more detail below.

A significant risk, which traditionally has a cross-border character and requires a high degree of international cooperation, is compliance requirements in connection with:

1 Anti-Money Laundering (AML)

2 Countering the Financing of Terrorism (CFT)

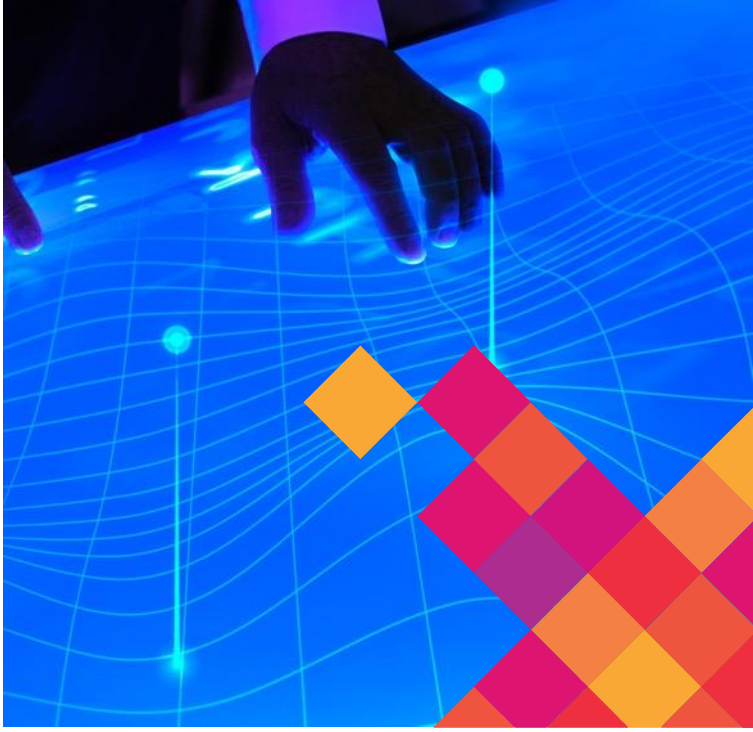
3 Identity verification (Know Your Customer, KYC).

The decentralized structure of cryptocurrencies enables users, transactions in the form of direct money transfers without the need for any regulated intermediaries, thereby bypassing (otherwise established) controls to be circumvented. For the exchange of crypto assets into official currencies, intermediaries such as crypto trading platforms, for example, are required. The peer-to-peer nature of crypto assets makes it difficult for the competent authorities to fulfill their regulatory obligations and to and to track suspicious activity.

Even though crypto assets are already regulated in some countries, the laws in force usually differ greatly. This heterogeneous regulatory landscape complicates international cooperation on money laundering, terrorist financing, and in enforcing sanctions or embargoes. It is also more difficult to detect the origin of funds to avoid tax payments.

Already today, there are global guidelines for the handling of crypto assets in the context of AML and CTF. These are driven in particular by the recommendations of the Financial Action Task Force (FATF), which is a state-independent body that sets international standards to prevent potentially illicit activities. Since the extension of global anti-money laundering and counterterrorist financing standards to crypto service providers in 2019, the FATF produces an annual report that tracks the progress of participating countries tracked in implementing the recommendations. In 2021, 27 of the 38 FATF members have already implemented or are working to implement required AML/CFT legislation for crypto service providers. But this initially high increase should be viewed in relation to the total cryptocurrency transaction volume, which grew by a full 567% compared to 2020. Overall, money laundering in 2021 accounted for just 0.05% of total crypto transaction volume-the lowest level in the past five years.

The fact that such statistics exist at all shows that, on the one hand, transactions on the blockchain are indeed well-tracked due to its transparency by companies such as Chainalysis. On the other hand, does not mean that it is easy to identify the parties involved. This is because pseudonymity means that flows of money cannot always be unambiguously assigned, in case of illegal activities, the responsible persons or organizations can be held accountable. But progress is being made here as well: Companies such as Chainalysis19 are specializing in transaction monitoring to detect and prevent illegal activity. Here, there is more talk about Know Your Transaction (KYT) and less about KYC, as transaction histories are continuously monitored in real-time to identify and detect patterns of illicit intent.



Operational risks

Another aspect that is relevant from a risk perspective is the operational risk in dealing with crypto assets and the associated use of blockchain infrastructures. In traditional payment transactions, in the event of an error, this can be reported to the central administrative body (e.g., in the case of an IBAN transfer, to one's own bank) and, depending on the rules, the transaction can be reversed or cancelled. This type of reversibility is generally not possible with blockchain-based transactions, since transactions are possible, as transactions are final and there is no centralized management point where errors can be reported and resolved. Thus, consumers generally have no claim to the reversibility of a transaction. In the event of errors, corresponding funds are thus lost unless no regulated intermediary in the form of a crypto service provider is used. In addition, consumers and investors using cryptocurrencies can lose portions or all their assets if they lose their private key or if it is stolen.

This risk exists with both custodial and non-custodial wallets. In the case of custodial wallets, the responsibility for the secure storage of the private keys is the responsibility of the third-party provider. Such a company can then be attacked, for example, by hackers using an insufficiently secure IT environment. Through such illegal access, investors may lose all or part of their crypto lose all or part of their crypto assets. The past few years have shown that such security vulnerabilities occur in the crypto market and the market and that the risk of hacking attacks continues to be present.

If the custodial wallet provider loses the private key of its customers, they can potentially claim compensation. This security does not exist with non-custodial wallets. Here, the responsibility for protecting the private key lies with the investor himself. The use of non-custodial wallets, therefore, entails greater responsibility for consumers and investors. For consumers and investors: If they lose their private key, all funds on the wallet are also irretrievably lost.

Consumer risks

Consumer and investor protection are two of the most important legislative priorities. With the emergence of innovative and lightly regulated business models, there is an increased risk for consumers to fall victim to unfair and fraudulent activities. This can also be observed in the crypto market. Consumers and investors are losing their assets time and again due to fraudulent schemes, market manipulation, hacker attacks, or lack of deposit insurance with crypto service providers. Two factors are highly relevant here: The first is a lack of knowledge about the crypto market on the part of consumers and non-professional investors. Many of them are not aware that they are trading in an environment that is not yet regulated. Mistakenly, the crypto market is compared to traditional financial services. In many cases, this leads to incorrect risk assessments.

Second, indirect risks arise for consumers and investors when dealing with regulated crypto service providers. It is true that the responsibility and risk for losses lie with the crypto service providers. Nevertheless, insufficient capital requirements for crypto service providers in the event of insolvency or similar financial crises for investors can lead to a partial or total loss of their assets (liquidity risk). In this context, the lack of deposit insurance may also be in the form of the separation of assets under management and assets under custody can also lead to similar consequences (credit and default risk). In addition, the protection of customer data is relevant. In many jurisdictions, there are already existing data protection regulations. Due to the transparent nature of blockchains, the question then arises to what extent existing regulations should be considered in blockchain-based and pseudonymized data transparency. In particular, the lack of accountability and accountability of cryptocurrencies can pose a challenge.

1.2 A Dive Into Non-EU Regulation & Law

In the following section, you will learn how nearly any right and therefore any asset be tokenized based on the Token Container Model from Liechtenstein.

Liechtenstein's token Act

In January 2020, new blockchain laws came into force in Liechtenstein. Based on these laws, companies and entrepreneurs can tokenize any right and therefore also any asset in a straightforward way. Then, complex workarounds or far-fetched interpretations of decade-old paragraphs are not needed anymore. This will provide legal certainty and inevitably lead to the emergence of the token economy. Standardized processes and registered service providers for tokenization will be emerging in Liechtenstein. This will significantly reduce the time and cost needed for tokenization processes. What exactly will be tokenized? Almost everything.

Figure 11: Milestones of the Liechtenstein Blockchain Act coming into force on January 1, 2020 (Source: NÄGELE Attorneys at Law LLC, 2019)

Precisely, the Liechtenstein Blockchain Act is actually called "Tokens and TT Service Providers Law" (TVTG) but we will, for the remainder of this article, use the former expression. Also, the new law uses the generic word "trustworthy technology" (TT) which can include blockchain and DLT systems.

The Liechtenstein Blockchain Act is a collection of new rules and changes of existing laws that allow rights and assets to become tokenized. Tokenization means that as of January 2020 nearly any right or asset can be "packaged" into a token according to the Token Container Model. Liechtenstein thereby acknowledges that — driven by digital transformation — the physical world as we know it for hundreds of years will sooner or later be augmented by a digital world. Often, we use paper documents to agree on a contract or for proofing evidence. This contracts then "creates" rights for the involved parties. Notaries are responsible to print, read and verify identities and documents — mostly all processes are conducted on paper.

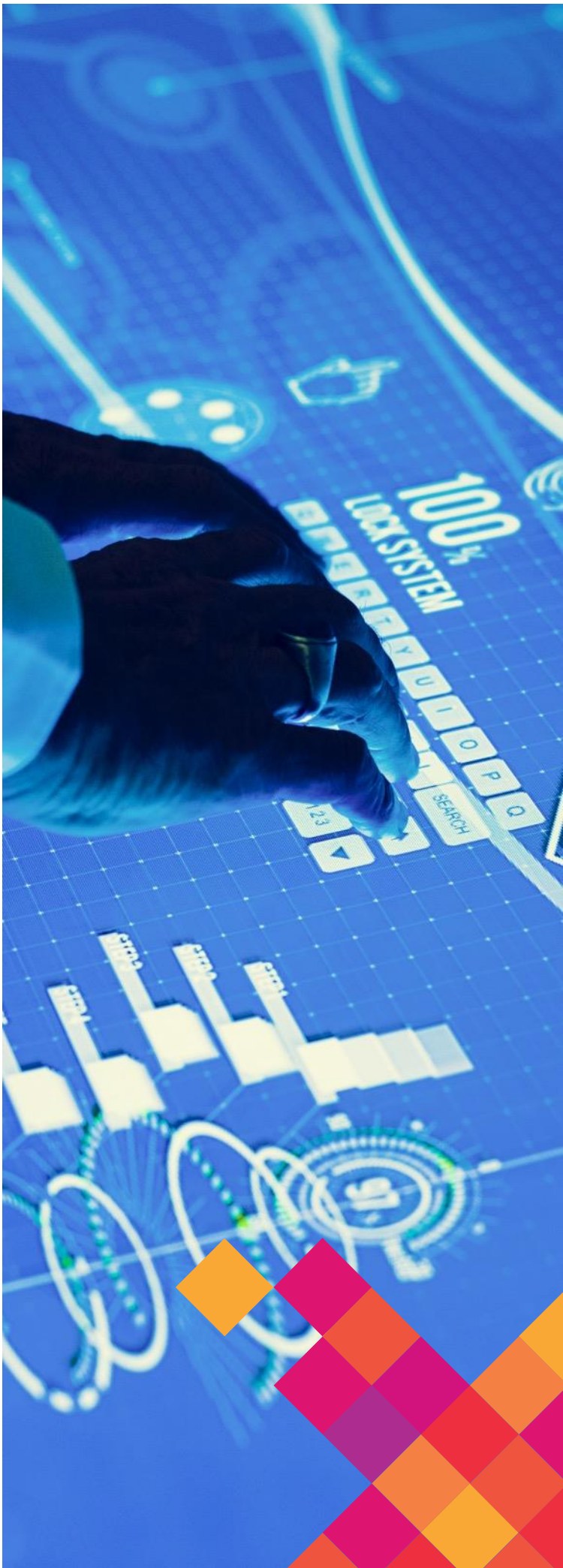
The Liechtenstein Blockchain Act now acknowledges that such paper-based rights and assets (yes, they can also be written on a PDF-document and signed digitally) can and will be brought to the digital world and will become tradeable easily: in the form of tokens. If thousands of rights and assets will be represented by digital tokens in a couple of years, we suddenly have two worlds: (1) the physical world as we know it and (2) the new digital world, which includes a subset of the rights and assets of the physical world. To become practical: But who is actually owning my house? The person in the real estate register? Or the person owning the token? What if the token is being stolen, or lost?

The Liechtenstein Blockchain Act also integrates the fact that the physical world always needs to be in perfect synchrony with the digital world of the tokens. This is very important because tokens can be, for example, lost or stolen. Also for this reason, Liechtenstein amended the civil law which is truly fascinating. This, by the way, is one fact that makes the Liechtenstein Blockchain Act really outstanding and, in our mind, a best-in-class framework.

The Token Container Model

One of the building blocks of the Liechtenstein Blockchain Act is the so-called Token Container Model (TCM). With this framework, a token serves as a container with the ability to hold rights of all kinds. The container can be "loaded" with a right that represents a real asset such as real estate, stocks, bonds, gold, access rights, money. But the container can also be empty. The latter case applies for example to digital code — the most notable example being Bitcoin.

This approach of loading a right or asset into a container (i.e., into a token) may sound trivial but allows a separation of (1) the right and the asset on the one hand side and (2) the token technically "running" on a blockchain-based system on the other hand side. In this manner, Liechtenstein differentiates between (1) law and (2) technology.



Therefore, this model is truly helpful to understand the process and the impact of tokenization. All rules governing the right and the asset basically stay as they are. But some specific rights are changed through the digital nature of the right packaged into a token. Here is an example: Some people think that security tokens (i.e., a stock on a blockchain system) are a new class of securities. But the Token Container Model makes it very clear that a security token is nothing else than a security (with all the rules, licenses, duties etc. applying to it) technically "packaged" into the token which loads the security like a container. The word "container" is meant literally. The token can now be transferred to new owners, can be managed in a portfolio, or can safely be stored by a custody provider — without the right and asset within the container changing.

To illustrate this for clarity: A right is virtually stored in a container representing the token and running on a blockchain-based system. The right could, for example, be the ownership right of a diamond. Whoever owns the token owns the diamond — exactly this relation is established by the Token Container Model. The diamond does not need to move its physical location; it can remain in a vault. But the ownership of the diamond can change by transferring the token to other persons. This would make sense for a private person storing value by owning a diamond but also for institutional investors who build entire portfolios of fractionally owned diamonds (think of 1.000 investments in fractions of a diamond for the purpose of risk diversification).

The Liechtenstein Blockchain Act

Liechtenstein did it! In the beginning of October 2019, the second hearing of the Liechtenstein Parliament on the new Liechtenstein Blockchain Act took place. No significant issues arose during this hearing. The result is that the Liechtenstein Blockchain Act will come into force in January 2020 and allows straightforward tokenization of all kinds of assets and rights without legal workarounds.

Figure 12: Token Container Model representing a right on a diamond in a container such that it can be transferred easily without moving the physical asset in custody
(Source: NÄGELE Attorneys at Law LLC, 2019)

This model is progressive and provides legal certainty for pre-existing rights that are tokenized as well as for the information stored on blockchain-based systems. Note that Liechtenstein amended its civil law to allow the token world to have priority over the physical world for the cases where tokens exist for rights and assets.

The physical validator has the duty to integrate the physical with the digital world

One guiding principle of the Liechtenstein Blockchain Act is that some new service providers that interact with the blockchain and the tokens need to be regulated. Some of these new formats of service providers need not only a registration with the Liechtenstein Financial Market Authority (FMA), but also a license to operate. One of these new roles is the so-called physical validator. Their role is to integrate the physical world into the digital world.

The physical validator has the duty to identify the holder of the tokens. In the previous example with the tokenized diamond, the physical validator knows who is owning the token and, with it, the diamond and has the duty to ensure the contractual enforcement of the represented rights and obligations, e.g., by storing the assets (or rights) of the real world in a vault. This is done by the physical validator. He also has the responsibility for having established correct business processes. If errors occur, if the physical assets are stolen or damaged, or if he does not comply with the rules, it is his responsibility to solve these issues. If he is not capable to do so, he risks his license as a service provider and therefore loses the right to operate. With this approach, the Liechtenstein Blockchain Act assigns the responsibility to guarantee perfect synchrony of the physical world and the digital world to the physical validator. Therefore, the newly defined role of the physical validator is highly important as it enables the token economy: providing certainty and allowing the tokenization of an existing right and its subsequent valid transfer onto a blockchain system.

Tokenization of any right and asset

According to the Token Container Model, any asset or right can basically be represented by a token. Some examples can be seen below. For example, a software license right or an access right can be put into the token container. In most jurisdictions, this would be classified as a utility token. If the token is sold to the market before the development of the product has actually been finished, this process is called Initial Coin Offering (ICO). Next, applying the European E-Money framework would allow to package traditional currencies such as the Euro or the Swiss Franc into a token. These tokens would be classified as payment tokens, more precisely, Euro tokens, digital Euro, Euro on blockchain, cash on ledger, etc. This is nothing else than putting a Euro into a token by applying E-Money rules for the content of the container.

Ultimately, a security can be packaged into the token. Then, all securities' laws apply, and the result is a security token. If sold to investors, we call this process a Security Token Offering (STO).

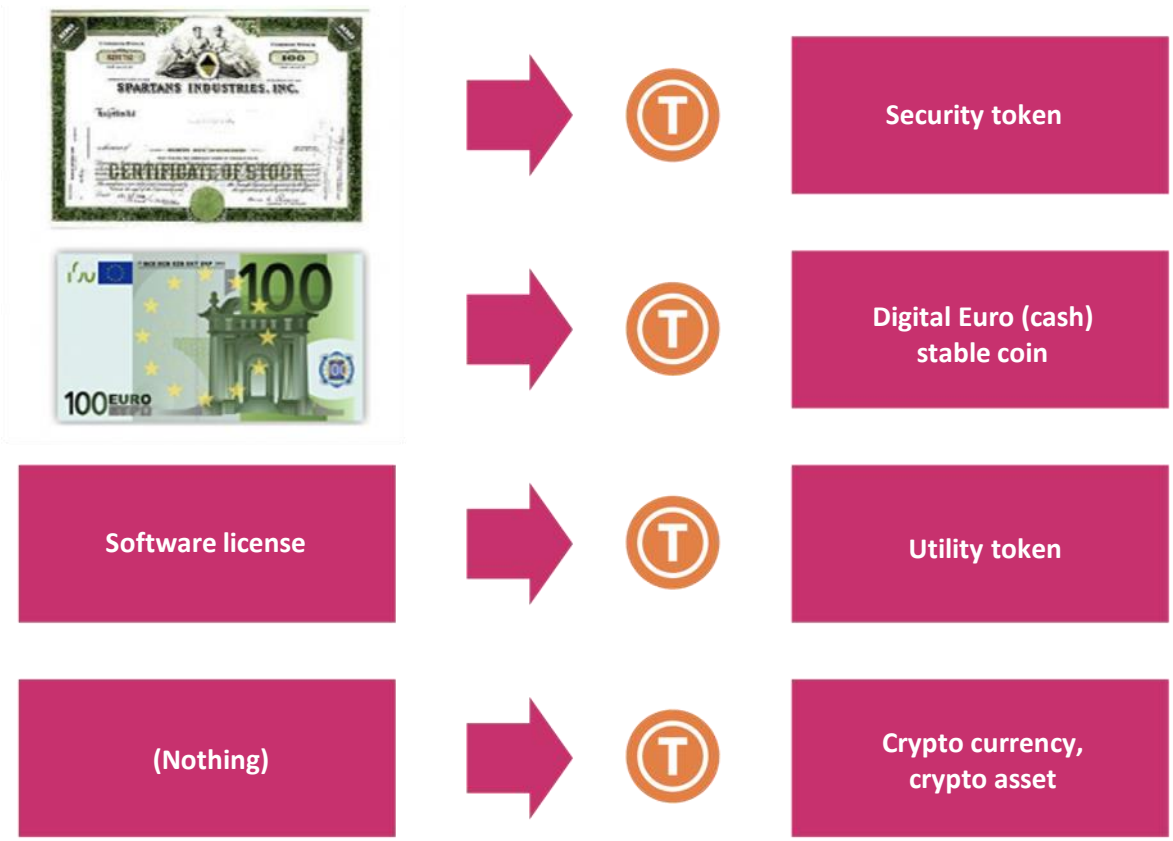


Figure 13: Examples for the Token Container Model (based on Dünser, 2018)

Tokenization follows a life cycle

When a right or an asset is tokenized, first, the tokens need to be generated technically. Then, the tokens need to be issued to the new holders. This can take place in a token sale (e.g., STO, IEO, ICO). Tokens then can be traded against other tokens and in most cases, they need to be custodied. Even more so, tokens — in the financial market — can be purchased and placed in a portfolio for investing purposes etc. To put it in a nutshell, tokens have a life cycle. Different events in the life cycle of the token indicate different requirements of the actors, e.g., token generator, token issuer, token depositary. The Liechtenstein Blockchain Act therefore provides multiple possibilities to register with the FMA such that companies can act along the life cycle of tokens. As Figure 4 points out, companies can soon apply for these registrations. There are multiple requirements for the applicant. And, of course, licenses are not for free. But comparing the fees and requirements for other registrations or licenses of financial authorities indicate that fees for licenses in Liechtenstein are reasonable. Once clearly defined registrations exist, as is the case in Liechtenstein, and once tokenization processes and smart contracts become standardized, ultimately costs for tokenization of any asset will be brought down.

	Token Generator	Token Issuer	TT Key Depositary	TT Token Depositary	Physical Validator
Registration Duty	✓	✓*	✓	✓	✓
REQUIREMENTS					
Personal Reliability (bankruptcy and criminal law)	✓	✓	✓	✓	✓
Organizational Suitable business structure and appropriate written internal proceedings and control mechanisms	✓	✓	✓	✓	✓
Minimum Capital	✗	Token <= 5 Mio = 50k Token > 5 Mio = 100k Issuance > 25 Mio = 250k	100k	100k	Varies depending on value of the property being guaranteed max. CHF 250'000
Special internal control mechanisms	✓	✓	✓	✓	✓
Licenced as Trustee	✗	✗	✗	✗	✗
SUPERVISORY FEES					
Minimum Fee		CHF 500	CHF 500	CHF 500	CHF 1'000
Fee	CHF 250	0.25% of CHF equivalent value of money recieved during issuance	0.25% gross revenue received from services provided.	0.25% gross revenue received from services provided.	0.25% gross revenue received from services provided.
Maximum Fee		CHF 100'000	max. CHF 100'000	max. CHF 100'000	max. CHF 100'000
DUE DILIGENCE ACT APPLICABLE					
	✗	✓	✓	✓	✓

Figure 14: Overview of 5 of the 10 registration requirements (source: NÄGELE Attorneys at Law LLC, 2019)

Liechtenstein and other countries

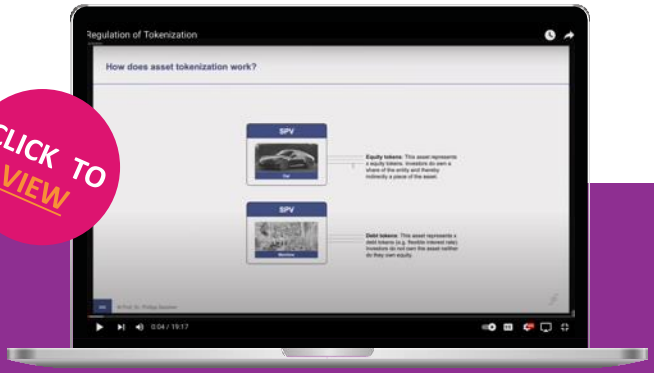
Liechtenstein sets forth a technologically neutral and all-encompassing framework designed to capture all aspects of tokenization. Due to Liechtenstein's status as a member of the European Economic Association (EEA), compliance with codified EU/EEA guidelines and regulations is required. These base line regulations create a floor that Liechtenstein legislators can build upon. The registrations and licenses issued under the foundational regulations and directives of the EU/EEA are passportable to other EU/EEA member states, while the Liechtenstein unique registrations under the Blockchain Act are not passportable. Of course, tax regulations in other countries and the upcoming "crypto license" in Germany might make business endeavors here and there more complex but not unfeasible.

At the core, the Liechtenstein Blockchain Act is focused on adapting pre-existing laws to foster legal certainty within the token economy. Drawing a clear line between what falls under civil law versus regulatory and supervisory law, the Liechtenstein Blockchain Act includes changes of the Liechtenstein Persons and Companies Act, Trade Act, Due Diligence Act, and Financial Market Authority Act. Probably the most important aspect are the changes in the civil right, to ensure that the underlying right represented by the token is effectively transferred from party A to party B. Besides this, the act provides regulatory and supervisory rules regarding those interacting with blockchain systems — including consumers, service providers, and intermediaries.

Liechtenstein: “straightforward tokenization” without workarounds

In case you try to tokenize rights and assets, this is typically difficult and challenging with local laws in place. In Germany for example, specific forms of debt can be tokenized but no shares or bonds up to now. A skilled lawyer is always necessary to try to find a workaround and — subsequently — convincing the regulatory bodies that the proposed workaround is complying with the local law by interpreting some paragraph of the law in a “new” way. The lawyer of course would never call this workaround a workaround. Nevertheless, it is often possible but not easy. Typically, such workarounds are also expensive since they are not yet subject to a standardized process. Therefore, Liechtenstein is an attractive destination for various tokenization efforts: Without time-consuming and costly efforts, rights and assets can be tokenized in a straightforward way. No workarounds are required as in other countries. This did not only standardized processes but also decreased the costs for tokenization processes significantly. However, since its introduction, the amount of goods tokenized with the TVTG was well below the expected numbers.

To dive into the regulation of asset tokenization specifically and the process of tokenizing, watch this Generation Blockchain video.

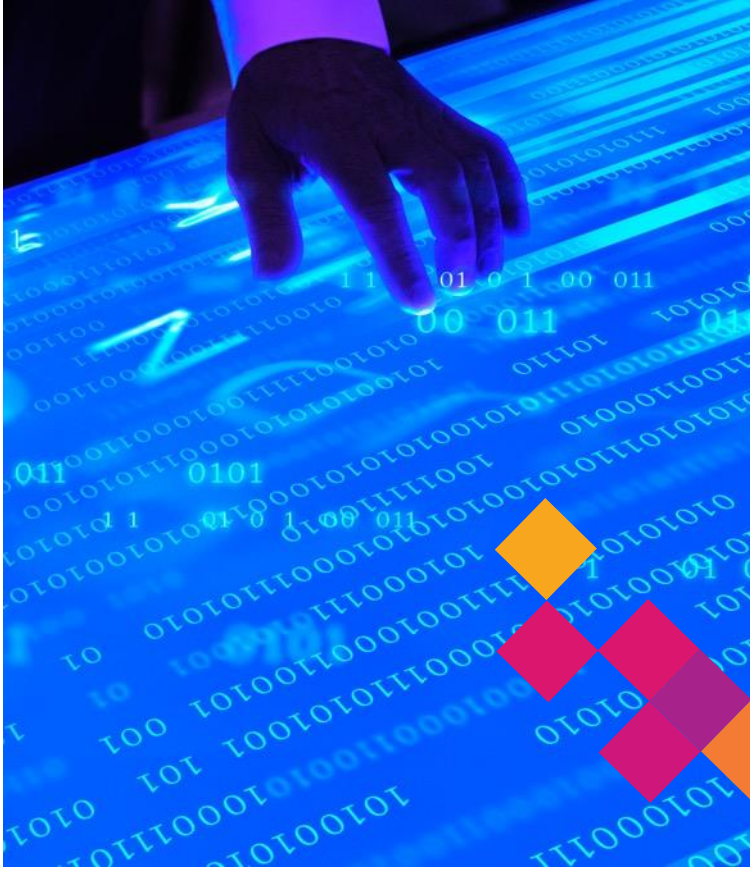


1.3 A Dive Into EU Regulation & Law

The current EU market around crypto assets is characterized by continued strong growth of a wide variety of use cases. Driven by the interest of private individuals, investors and companies from many industries, the industry continues to attract high demand despite extreme price fluctuations.

Definition of a cryptocurrency under the German Banking Act (KWG)

For a long time, there was no uniform definition of the term cryptocurrency. The term was used synonymously for different aspects of the blockchain ecosystem. Through the European Markets in Crypto Assets Regulation (MiCAR) as well as the German Banking Act (KWG), two definitions have now been established in the European area. In doing so, both definitions introduce the new term crypto value instead of cryptocurrency. The preliminary MiCAR definition for crypto assets is thereby broad and includes various subcategories. The KWG shows parallels to MiCAR, for example in digital mapping and transferability, but takes a different approach: In its definition, the KWG specifies the decentralization and corresponding governance of digital assets and thus clearly distinguishes crypto assets from existing monetary assets.



Thus, the definition according to section 1 para. 11 sentence 4 of the KWG: "For the purposes of this Act, crypto assets are digital representations of a value which has not been or guaranteed by any central bank or public authority and does not have the legal status of a currency or of money, but which may be used by natural or legal persons or legal persons on the basis of an agreement or actual means of exchange or payment, or for investment purposes, and which can be transmitted, stored, and traded electronically, stored, and traded by electronic means. " Crypto assets are thus a category of decentralized assets, such as Bitcoin and Ethereum. Building on the KWG definition, crypto assets are thus defined as follows:

1. A crypto-value is a digital asset that is created using a distributed ledger technology (DLT) and cryptographically secured.

2. Crypto assets have no existing central authority, for example in the form of a government agency or legal person/entity.

3. Crypto assets have no intrinsic value and no hedging by assets with intrinsic value.

Markets in Crypto Assets (MiCAR)

To understand crypto assets, it is important to establish some definitions and content boundaries. For this purpose, we use the existing legal texts from the European area as a basis. The law is set to create parameters for how each of the European Union's member nations regulates crypto. It is expected to create a common licensing regime, enabling companies operating in one member nation to launch in the others, as well as define rules for issues such as stablecoin issuance. The MiCAR's definition of crypto assets is not compatible with the term used in the German Banking Act (KWG), thus changes are also expected to the German market.

The MiCAR contains the following three sections:

1 The authorization procedure for issuers of crypto-assets and the corresponding obligations for the token types covered by the regulation (asset-referenced tokens, e-money tokens and, as a catch-all provision, crypto-assets).

2 The authorization procedure for crypto asset service providers.

3 The competent authorities and their competencies.

MiCAR has been created to introduce regulations on the licensing and supervision of crypto asset providers and their issuers. The focus is on issuers of asset-referenced tokens and e-money tokens. Thus, only legal entities that are established in the EU and have received a corresponding authorization from the competent authority may provide these services from 2024 onwards. An important component of the MiCAR is therefore the licensing regime established under it by the respective competent authorities.

Under the final deal, any crypto service provider with over 15 million active users would be subject to supervision at the European level tarting in 2022 when it comes into force. After an 18-month transition period, MiCAR will then become directly applicable in all member states. Thus, a harmonized set of rules for crypto assets in the European Union can be expected in 2024.

The text stems from the academic article "Liechtenstein Blockchain Act: How can nearly any right and therefore any asset be tokenized based on the Token Container Model" published on October 7th, 2019 by Prof. Dr. Philipp Sandner, Dr. Jonas Gross and Thomas Nägele. The authors consented to the use of the text for the purpose of the Generation Blockchain project.

1.4 A Framework conditions of appropriate regulation for crypto assets

The currently fragmented regulatory landscape is an impediment to international regulation. To create efficient and holistic regulations for the handling of crypto assets there is a need for cross-border initiatives. But to date, individual jurisdictions have taken their own approaches to regulating crypto assets, which consequently differ also differ in their level of development. To analyze the progress of different legislations across jurisdictions, a standardized framework was published based on the analyzed risks. It shows a holistic status of the regulation of a respective jurisdiction and thus enables comparisons and assessments. The framework serves as a tool to identify the regulatory risks relevant in the regulatory issues in the context of cryptocurrencies.

Before evaluating a particular jurisdiction against the framework, it is necessary to determine the extent to which the jurisdiction in question has an explicit or implicit prohibition on crypto assets. An implicit prohibition in this context would be, for example, that companies are prohibited from offering crypto services. In these cases, the application of the framework is not purposeful. The framework consists of two overarching categories, divided into twelve evaluation criteria. These can be evaluated using a rating scale.

In the first category, the financial regulatory treatment of cryptocurrencies in each jurisdiction is assessed based on the following factors:

Crypto values regulated as financial instruments
Classification of crypto assets as financial instruments recognized by regulators.

Fiscal regulation in place
Existing tax regulations for dealing with crypto values for both individuals and businesses.

Regulation of wallet infrastructures in place
Existing regulations on custodial and non-custodial wallets in the context of private keys and custody of crypto assets.

Regulatory responsibility settled
Clear mandating and delineation of responsibilities of authorities regarding supervisory duties in the dealing with crypto assets.

Since crypto service providers play an important role in the crypto ecosystem, the second category sets out the regulatory requirements for crypto service providers under governance and consumer and investor protection are assessed based on the following factors:

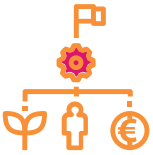
Capital requirements regulated
Obligations to hold of equity to mitigate credit and default risks.

Risk disclosure and profile for retail investors regulated
Obligations to inform customers about risks in dealing with crypto assets as well as categorization of customers according to risk classes.

Deposit security regulated
Regulations for the protection of customer deposits, e.g., by separating the assets of customers from the assets held for their own assets.

Protection of customer-relevant data regulated
Data protection regulations for crypto assets or possibility of applying existing regulations to crypto assets.

The third category regards governance of crypto assets and blockchain systems:



AML/CTF Compliance Regulated
Requirement to compliance with national and/or international regulations to combat money laundering and Terrorist Financing.

KYC Requirements regulated
Regulations governing the identification and verification of (prospective) customers on the basis of personal data.

Licenses in place
Existing licenses for the provision of crypto services or approvals as a provider of crypto services.

Requirements for IT security regulated
Requirements for the protection of IT systems incl. corresponding security precautions.

The individual factors are evaluated using a scale that represents the degree of fulfillment of the respective factor. It should be noted that the assessment is not dichotomous, consisting of "fulfilled" or "not fulfilled", but rather can take on different characteristics. The degree of fulfillment can therefore also be understood as a process. New developments in the market can thus result in modifications to the regulatory factors. In addition, the degree of fulfillment should not be understood normatively: A high degree of compliance is not per se "positive," and a low degree is not per se "negative". Rather, the goal of the framework is to provide an objective assessment that can separate the characteristics of an individual jurisdiction in accordance with its qualitative characteristics. In particular, depending on the perspective from which it is viewed, characteristics can be interpreted positively and negatively depending on the angle. For example, from the perspective of the investor, a regulation of crypto securities is to be evaluated positively. From an innovation perspective, on the other hand, regulation can be evaluated negatively, because it makes new business ideas in the crypto sector more difficult, prevents them or favors established companies. The valuation model must therefore always be viewed in the context of the individual consideration of the topic of crypto assets.

In order to create an appropriate regulation of crypto assets, the interests and ideas of all market participants and stakeholders should be understood and brought in. In case of conflicts of interest (e.g., between investor protection and innovation), a balance must be found. In doing so, the interests in the crypto market sometimes diverge strongly. It is a balancing act: on the one hand, legislators must ensure that consumers and investors are sufficiently protected from illegal activities as well as inherent risks. On the other hand, such an emerging market should be given the freedom to develop.

The following suggestions can serve as guard rails in this regard serve. First, there needs to be a concrete delineation between the user groups to ensure regulatory treatment that is appropriate for the target audience. Similarly relevant is the clear examination of the areas of application of crypto assets that are currently being used and will be used in the future. This is because the degree of risk of the user groups and areas varies greatly. Corresponding risks can then be better addressed on the part of the legislator if as many manifestations of risks as possible are considered.

The Travel Rule

The FATF's Travel Rule provides, among other things, that crypto service providers above a limit of 1000 euros are required to report information on senders and recipients of transactions to a government institution (Cf. Financial Action Task Force (FATF), 2021). The FATF's Travel Rule allows legislators to implement an approach that is risk-based and appropriate to the target group (in this case (here: investors). At the same time, this Travel Rule also leads to considerable requirements and efforts on the part of crypto service providers. These consequences should be discussed and weighed against each other. An elementary component and fundamental area of application of crypto assets is their safekeeping. It represents the starting point for other applications and increases security for users when dealing with crypto assets. In Germany, legal certainty was already ensured in 2020 through the crypto custody license, anchored in the KWG.

A collaborative approach to regulation

Furthermore, for a professionalized market, especially from the perspective of consumers and investors, trustworthy market participants and service providers are required. To this end, the institutionalization and supervisory control of crypto service providers is particularly useful, as these are usually the first points of contact between users and crypto with crypto assets. At the EU level, crypto service providers and their different roles are being acknowledged in the context of MiCAR are appreciated and comprehensively regulated. In the dynamic and complex crypto market, therefore, there is a need for ongoing collaboration between providers and legislators is strongly recommended. Legislators should permanently seek insights from the crypto industry, to gain a good penetration and up-to-date understanding of the market. As part of this process, regulatory approaches should always be questioned based on new developments and modified if necessary. Finally, due to the cross-border nature of cryptocurrencies, international cooperation is needed involving global bodies such as the FATF, the Bank for Bank for International Settlements (BIS) or the Financial Stability Board (FSB), as well as national organizations such as central banks and supervisory authorities. In addition to standardization of processes and optimized coordination between different jurisdictions, regulatory arbitrage can be kept low. Studies to date have shown that increasing regulation can reduce the overall market activity of crypto assets does not weaken. There is no significant migration of business activity from supposedly more regulated jurisdictions to less regulated jurisdictions observed.

Doesn’t decentralized equal unregulatable?

Various legal standards and rules of order create reliability and legal certainty in the analogous financial economy. An application of regulation in one world and a lack of access in the other world leads to a distortion of competition. The German financial supervisory authority has therefore already taken a clear stance on the principle of "same business, same rules” positioning. In the blockchain community, there are doubts that regulatory institutions will be able to enforce this mandate in the digital business world. This neglects several facts at once.

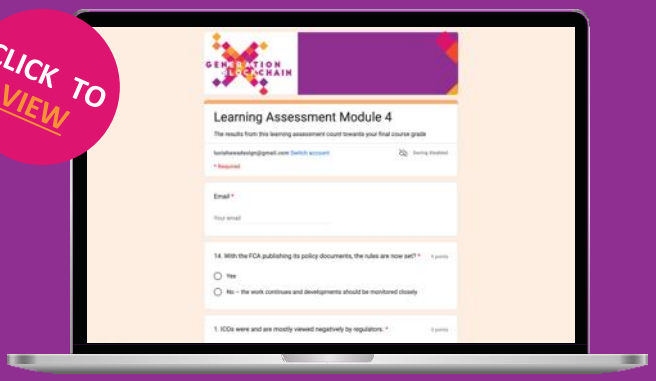
First, transactions of large amounts cannot be hidden. Second, the traces of Internet activities are much easier to find than the famous black money suitcase. Third, it is sufficient to prove actors and activity to take supervisory action. Decryption is not mandatory for the commencement of prosecution is not mandatory. Fourth, most market participants are interested in creating value within the legal order.

The institutions of banking and financial supervision are currently observing the scene closely and have set up corresponding divisions/departments, in which the necessary know-how for regulatory intervention is being gathered. In the ICO market, one can already see how regulatory interventions are being implemented and enforced. Many countries with different economies (e.g., Australia, China, Dubai, UK, Canada, South Korea, Russia), including previously ICO-friendly havens such as Gibraltar, are currently taking measures to put IPOs and ICOs on an equal footing or create a regulatory framework for blockchain applications. In the digital currency space, the responses from monetary regulators are also broad. There is no central bank that does not permanently track the artificial currency market. In authoritarian economies with high levels of state intervention, national coin currencies have already been announced. This reflects the attempt to bring the market for artificial money under control. In more liberal economies, people are following the cryptocurrency development with attention and are betting that cryptocurrencies will fail due to the difficulties of monetary control. Most independent central banks assume that the task of regulating cryptocurrency of regulation will therefore fall to them evolutionarily for the digital world as well. The real question is therefore not so much whether it is possible to carry out unregulated digital transactions, but whether it is possible to make the transactions legally secure and court-proof. The design of smart contracts and smart finance in terms of their compatibility with the private and public legal systems will be decisive for the mass suitability and thus the economic commercial success of blockchain applications. The regulatory authorities in the European Union so far see no reason to intervene in what is happening because the activities are too insignificant and because governmental interventions do not occur arbitrarily. The actions of regulators in other economic systems, however, give an impression of the possible options for action and potential consequences.

02

LEARNING ASSESSMENT FOR MODULE 4

To test your knowledge, finish this learning assessment as part of your overall grade for the course.
Click here.



01

MODULE 5

Fundamentals of Coding & Programming

Co-funded by the European Union

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 National Agency. Neither the European Union nor National Agency can be held responsible for them.

contents module 5

Co-funded by the European Union

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 National Agency. Neither the European Union nor National Agency can be held responsible for them.

01| MODULE 5 Fundamentals of Coding & Programming

Chapter Overview

In this module, you will be introduced to the programming language Solidity and the concept of building smart contracts and decentralized Apps.

Learning Objectives

After the first module, you should be able to:

- Learn how to program a game on Ethereum.
- Learn and use basic solidity concepts.
- Understand and deploy ERC721 & crypto collectibles.
- Understand and be able to program app front ends & web3.js.
- Understand how data feeds and computations work theoretically and in practice.
- Learn how to deploy dApps with Truffle.
- Learn how to build an Oracle.
- Test smart contracts with Truffle (e.g., using Chai to write more expressive assertions, testing against Loom).
- Learn how to deploy on TRON, one of the fastest-growing public blockchains.
- Understand the basics of zkSync.

01| INTRODUCTION TO SMART CONTRACT CODING

As programming is best learned through doing it, head over to the Solidity course “CryptoZombies” where you will be guided through deploying your own smart contracts once you have a good understanding for the basics. CryptoZombies is a free, open-source, interactive code school that teaches you to build games on Ethereum. The course is designed for beginners to Solidity and starts off with the absolute basics. Click here.

During the “Solidity: Beginner to Intermediate Smart Contracts” section, you will learn:

- How to build a game on Ethereum
- Basic solidity concepts
- ERC721 & crypto collectibles
- App front ends & web3.js

During the “Chainlink: Decentralized Oracles” section, you will learn:

- How data feeds and computations work

During the “Advanced Solidity: Get In-depth Knowledge” section, you will learn:

- Deploy dApps with Truffle
- How to build an Oracle
- Testing Smart Contracts with Truffle (e.g., using Chai to write more expressive assertions, testing against Loom)

During the “Beyond Ethereum: Explore the Blockchain Ecosystem” section, you will learn:

- The basics of zkSync

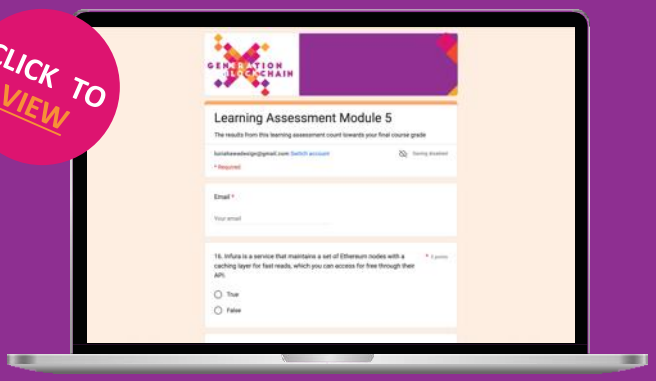
During the “Tron: Decentralize the Web” section, you will learn:

- How to deploy on TRON, one of the fastest-growing public blockchains

02

LEARNING ASSESSMENT FOR MODULE 5

To test your knowledge, finish this learning assessment as part of your overall grade for the course.
Click here.



01

MODULE 6

Financial Service Applications

Co-funded by the European Union

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 National Agency. Neither the European Union nor National Agency can be held responsible for them.

contents module 6

Co-funded by the European Union

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 National Agency. Neither the European Union nor National Agency can be held responsible for them.

01| MODULE 6 Financial Service Applications

Chapter Overview

In this module, the topics of crypto products and services (i.e., lending and borrowing and crypto exchanges) will be covered. Moreover, the tokenization of assets such as real estate, NFTs and items in the Web3 space and their role for the crypto ecosystem will be covered.

Learning Objectives

After the first module, you should be able to:

- Explain the concept of borrowing, lending, and tokenizing, staking and flash loans.
- Understand the differences between traditional lending and borrowing and decentralized lending and borrowing.
- Understand the concept of tokenization and their real-life applications and their use in the crypto ecosystem.
- Discuss the history of exchanges and understand their position in the crypto ecosystem.
- Understand web3 and their real-life applications and their use and role in the crypto ecosystem.
- Understand the potentials and risks in regards with web3 as compared to previous iterations of the internet.

01| CRYPTO PRODUCTS & SERVICES

In the following section, you will learn about the concept of lending, borrowing and staking.

1.1 Lending & Borrowing

Crypto lending refers to a function in DeFi that allows investors to lend their cryptocurrencies to different borrowers. This way, lenders receive interest payments in exchange, also referred as crypto dividends. Many platforms that specialize in lending crypto also accept stablecoins in addition to cryptocurrencies. Thus, cryptocurrencies go beyond being a payment method and can also act as an investment vehicle. When lending cryptocurrencies, it is important to note that one cannot access their cryptos while lending them out.

Example for lending

1 The lender owns 5 bitcoins and want to receive a steady passive income with them by depositing them into a crypto lending platform wallet.

2 Each month or week, the lender will receive interest (interest rates differ strongly based on the cryptocurrency and exchange).

Crypto lending works by taking crypto from one user and providing it to another for a fee. The exact method of managing the loan changes from platform to platform. There are crypto lending services on centralized and decentralized platforms, however, the core principles remain the same. In crypto lending, borrowers also have the chance to stake their cryptocurrency as guarantees of loan repayment or as security. Thus, the investors could sell the crypto assets in case the borrower does not pay off the loan anymore. In this way, they can recover their losses. Lending and borrowing platforms do not usually have the chance to recover their losses since they ask borrowers to stake between 25-50% of the loan in crypto. Having a certain percentage staked makes sense if borrowers do not pay off their loans anymore. This way, the staked amount can be redeemed by the exchange in the case of an outfall.

Staking

If a cryptocurrency you own allows staking (e.g., Ethereum, Tezos, Cosmos, Solana, and Cardano) you can stake some of your holdings and earn a percentage-rate reward over time. The reason why cryptocurrencies earn rewards while staked is that the blockchain puts it to work. Cryptocurrencies that allow staking use the consensus mechanism PoS. If you stake your cryptocurrency, it becomes part of someone else's share (or stake) in the network to increase the likeliness of validating the next block. While you can lend out all cryptocurrencies, staking is a concept exclusively for PoS-based cryptocurrencies.

How do crypto loans work?

Crypto lending usually involves three parties:

1 **the lender,**

2 **the borrower,**

3 **and a DeFi platform or crypto exchange.**

In most cases, the loan taker must provide collateral before being eligible for borrowing any crypto. An exception to this is flash loans which can be used without collateral. Lenders can then add their cryptocurrencies to a so-called pool that manages the whole process of lending for them and essentially forwards the lender their cut of the interest. Lending through centralized financial Fi platforms, as opposed to borrowing, works a little differently. Rather than lend all your money to just one individual, centralized exchanges use liquidity pools to lend your money out to multiple users at the same time. As a result, you are not informed whom your crypto is forwarded to, but the platform gives you a bond that underwrites your loans, making it a safe undertaking. Once such a loan expires, the bonds can be returned to recover the funds as well as any accrued interest.

Crypto lending rates

As mentioned, each platform has different rates for crypto lending. While there is a certain ROI for every crypto lending platform, there are also different risks depending on the platform of choice. Similar to investment strategies, crypto lenders tend to use several different platforms to spread the risks and diversify their investments.

When it comes to crypto lending, there is a yearly yield that can be expected

For crypto coins, it ranges from 3% to 8%,

For stablecoins, it ranges from 10% to 18%.

Different types of crypto loans

As mentioned, there are two types of crypto loans: flash loans and collateralized loans. We will focus on them in the next section.

Flash loans

Flash loans allow you to borrow crypto funds without the need for collateral. The name flash loan comes from the fact that the loan being granted, given, and repaid within a single block. If the loan amount cannot be returned including interest, the transaction is canceled before it can be validated in a block. From the outside, this looks like the loan never happened since it was never confirmed and added to the chain. A smart contract controls the whole process, making human intervention unnecessary.

With loans in traditional finance, the lender usually wants some kind of collateral to make sure they receive their money back. Setting up the contract often takes weeks or longer to get approved, and the borrower pays back the loan, with interest, over a period of weeks, months, or years. Flash loans work diametrical to that. They occur in an instant because the funds are both borrowed and returned within seconds.

How does a flash loan work?

To use a flash loan, the parties involved need to act fast. This requirement is where smart contracts come into play again. With smart contract logic, you can create a top-level transaction containing sub-transactions. If any sub-transactions fail, the top-level transaction will not go through.

For the sake of the example, a token is trading for $1,00 (USD) in liquidity pool A and $1,10 in liquidity pool B. To take advantage of this (arbitrage), you currently do not have sufficient funds to purchase tokens from the first pool to sell in the second. A flash loan could help you to complete this arbitrage within one block. For example, imagine that for your primary transaction, you will take out a 2.000 USDC flash loan from a DeFi platform and repay it.

We can then break this down into smaller sub-transactions:

1. **The borrowed funds are transferred to your wallet.**
2. **You purchase $2.000 of crypto from liquidity pool A (2.000 tokens).**
3. **You sell the 2.000 tokens for $1,10, giving you $2.200 in revenue.**
4. **You transfer the loan plus borrowing fee into the flash loan smart contract.**

If one or more of these sub-transactions cannot execute, the lender would cancel the loan before it takes place. The most common use cases for flash loans include collateral swaps and price arbitrage. However, flash loan can only ever be used on the same chain, as moving funds to a different chain would break the one transaction rule.

Collateralized loans

A collateralized loan gives a borrower more time to make use of their funds in return for providing collateral. This type of loan is the backbone of open lending protocols. Given that DeFi is a synonym for open, pseudo-anonymous finance, credit score and formal identity checks associated with the loan are not part of the equation. Like mortgages, most DeFi lending applications will require borrowers to collateralize their loan as an incentive to hold them accountable for repaying the debt. While there are parallels, the main difference between a traditional mortgage loan and a collateralized loan on MakerDAO or Compound is that it requires the borrower to over-collateralize the loan.

MakerDAO is one example for a collateralized loan provider. Since cryptocurrencies are volatile, the loan-to-value ratio (LTV) reflects this volatility (the LTV is often only around 50%). This indicates that the loan will only be 50% the value of your collateral. This discrepancy is what provides wiggle room for collateral's value in case it decreases. Once the collateral of the loanee falls below the loan's value or some other given value, the funds are automatically sold or transferred to the lender. It is necessary to top up the collateral if there is a change in price to avoid liquidation. If the LTF ratio becomes too high, there are fees to be paid. This monitoring is done by a smart contract. When the loan is repaid (plus interest) the loaner regains their collateral.

Example

A 50% LTV loan of $10.000 USDC will require you to deposit $20.000 (USD) of ether (ETH) as collateral. If the value drops below $20.000, you will need to add more funds. If it falls below $12.000 you will be liquidated, and the lender will receive their funds back.

When someone takes out a loan, they will most likely receive newly minted stablecoins (such as DAI) or cryptocurrency someone has lent. Lenders will deposit their assets in a smart contract that may also lock up their funds for a specific time. Once the borrower receives the funds, they can utilize them for their purpose.

Advantages and disadvantages of crypto loans

Crypto loans have been commonly used tools in the DeFi space for years for various operations. In this section, you will look at the advantages and disadvantages of crypto loans:

Advantages		Disadvantages	
Easily accessible capital	Crypto loans are given to anyone who can provide collateral or return the funds in a flash loan. This quality makes them easier to acquire than a loan from a traditional financial institution, and there's no credit check needed.	**High risk of liquidation**	Even with highly over-collateralized loans, crypto prices can drop suddenly and lead to liquidation.
Smart contracts manage loans	A smart contract automates the whole process, making lending and borrowing more efficient and scalable.	**Smart contract attack risk**	Poorly written code and back-door exploits can lead to the loss of the loaned funds or collateral. Smart contracts and projects can be the targets of scams and attacks which could result in partial or complete loss of coins as well as the freezing of accounts, making withdrawal impossible.
Passive investment through vaults	Investors can place their crypto in a vault and earn annual percentage yield (APY) without managing the loan themselves.	**Risk through borrowing & lending**	The risks of lending and borrowing include the risks connected to handing over custody of crypto coins. What happens in which scenarios is usually part of the loan terms and conditions which should be studied in depth before loaning out crypto coins. Depending on the loan, the lock up period of the crypto coins can interfere with one's ability to react to crypto market crashes and other market conditions.

1.2 Exchanges

When Bitcoin was first launched in 2099, the only way to acquire bitcoin was by trading on forums or Internet Relay Chats, requiring a great deal of trust.

In March 2010, the first cryptocurrency exchange called bitcoinmarket.com went live. A user of the Bitcointalk forum named “dwdollar” proposed to create the first real market for people to buy and sell bitcoins with each other. The need for a useful pricing system as a starting point arose which was supposed to be based on the energy requirement for mining. In 2010, Bitcoinmarket.com, started with a price at launch of around $0,003 per Bitcoin. Bitcoinmarket.com used PayPal to exchange fiat money to Bitcoin but was removed after increasing fraudulent trades in June 2011 when Bitcoins price hit $23,99. Bitcoinmarket.com was certainly an improvement from exchanging Bitcoin on forums but started to see competing exchanges gain popularity.

Mt. Gox & Early Platforms

In 2010, Jed McCaleb developed Mt. Gox. The initial name of the exchange was mtgox.com which is a reference to the digital collectible card game “Magic: The Gathering Online eXchange”. Within the next three years, 70% of all bitcoin trades were being handled via the Mt. Gox platform. McCaleb started to use the site to exchange USD for Bitcoin. Soon after the successful initiation period, he sold Mt. Gox off to another active executive. Regarding Mt. Gox there are several different records of fraudulent business operations. Missing funds, hacks and legal disputes were just the tip of the iceberg.

Examples for fraudulent business operations

According to court documents dating back to the time that Mt. Gox was sold off, 80.000 bitcoins were already missing which was followed by the first of several hacks where a total of 2.650 BTC were stolen. Nonetheless, the site gained traction and become the world’s largest bitcoin exchange by 2013. Mt. Gox proved to have severe website coding issues and poor security measures which facilitated attacks. The US Department of Homeland Security accused them of acting as an unregistered money transmitter which resulted in over $5 million USD seized by the US government from the company’s bank accounts. In turn, this leaded to the suspension of USD withdrawals and long delays for customers of Mt. Gox. In 2024 the situation faltered. A few weeks later, Mt. Gox suspended all trading for customers, the website went offline, and it filed for bankruptcy protection. The reason was an ongoing hack for years which amounted to 844.408 Bitcoins stolen from the hot wallets of customers that could not be recuperated.

The Mt. Gox management claimed to have been unknowledgeable about the missing funds. Karpelès, McCaleb's successor, was indeed charged with fraud and embezzlement however, the aftermath (such as lawsuits) of the hack is yet to come to an end. Users can expect a certain return of their lost funds in the form of USD, however, the lost profit on their bitcoins since purchase will not be reimbursed.

The example of Mt. Gox highlights the risk landscape of centralized exchanges being reintroduced into a decentralized money vision perfectly. Mt. Gox is only the most notable example of crypto exchanges that later were sued for various reasons of business misconduct. Regulation only grew from negative examples such as Mt. Gox. Equivalent measures, laws and code of conduct that already exist for traditional finance had and still must be introduced for DeFi. Mt. Gox has served as a painful lesson that gives origin to the credo of Bitcoiners preaching "not your keys, not your coins". The credo has also proven wise in more recent development around one of the biggest crypto exchanges worldwide, namely FTX, until they too filed for bankruptcy due to fraudulent business operations involving customer funds.

Current Developments

In 2018 and 2019, the rest of the crypto exchange market worldwide tried to catch up and regain market share. As a general trend, some exchanges such as Binance have given out their own their own utility token called BNB. It acts primarily as a discount token to pay for trading fees on the Binance exchange and to pay for goods and services. Similar loyalty-based incentives, so-called IEOs (Initial Exchange Offering), were introduced by projects to try and gain and retain customers. They have taken precedence over the ICO launches of prior years. Through IEOs, successful projects then received instant availability on a large exchange from day one, the exchange were able to determine the future exchange fees right away and also benefited from the IEO raise being denominated in their own exchange token. Crypto exchanges offer altcoins to their offering and some offer NFT capabilities or separate wallet apps. Exemplarily, Coinbase has added several altcoins to its 2017 offering, and other exchanges like Huobi and Bitfinex have followed since. Recent crisis related to crypto exchanges and the subsequent bankruptcy of FTX as one of the biggest crypto exchanges is taking a toll on the entire crypto exchange market and the consumer protection in these cases. As by the beginning of 2023, the liquidation of the Bahamas-based cryptocurrency exchange FTX is still ongoing. The collapse of FTX was caused by a liquidity crisis of the company's token (FTT) and unlawful use of customer funds in the background. The contagion effects within the crypto world and specifically amongst exchanges cannot be denied and have been observed in different bear markets and crisis.

Exchanges around the world

According to CoinMarketCap, there are more than 13.000 exchanges listed with a growth trend. Jurisdictions are beginning to regulate and establish specific rules for the operations of the exchanges. South Korea and Japan are rather progressive and most open to these platforms as long as they comply with certain rules focused on transparency and avoiding money laundering. Switzerland, Estonia, and Malta are the ones that provide the most facilities when it comes to establishing exchanges and other projects based on cryptocurrencies, because they have clear laws that must be complied with and that seek to protect users. The United States supports and controls the exchanges, although it does not have clear rules in favor or against it, and the position is quite ambiguous despite exchanges being allowed to operate.

Exchanges in Europe

Bitstamp is the first exchange developed and based in Europe and located in Luxembourg and was founded by Nejc Kodric in 2011. It is highly valued and operates globally. LocationBitcoins is the most reputed European crypto exchange today and one that moves the highest funds in their business operations on a European level. It was founded by brothers Nicholas and Jeremias Kangas in Helsinki, Finland in 2012. CEX.io is a UK based exchange bureau and was founded in 2013 by Oleksandr Lutskevych. CEX.io are known for adding new cryptocurrencies to their product portfolio frequently.

Exchanges in the United States

In the US, the crypto exchange Kraken, based in San Francisco, was the first US-American crypto exchange founded in 2011 by Jesse Powell. It has great prestige and as compared to other US exchanges, it moves the largest volumes of Bitcoin every day. Coinbase is also a San Francisco -based exchange founded in June 2012 by Brian Armstrong. The exchange Bittrex is based in Seattle and was founded in 2013. It offers option pairs with US dollars. Poloniex in Delaware, United States and founded by Tristan D'Agosta in January 2014, is one of the most demanding when it comes to adding cryptocurrencies and offers high-security measures to protect users.

Exchanges in Asia

In the Asian market, there is Bitfinex which is Hong Kong-based and was founded in 2012 by Raphael Nicolle and Giancarlo Devasini. It is characterized by being reliable and safe, benefitting from first mover advantage. It is the second largest in terms of volume of Bitcoin movements. Huobi is a Singapore-based exchange founded in 2013 by Leon Li and has the largest volume of Bitcoin and other cryptocurrencies in the market. Okex is an exchange house founded in 2013 by Star Xu based in Beijing, China. It is the third in volume of exchange of BTC and the first in Ethereum and EOS, among others. Binance was founded in 2017 by Chanpeng Zhao and is based in Shanghai, China. It is the one with the largest volume of Bitcoin today.

02

TOKENIZATION OF ASSETS

In the next section, we will cover the process of tokenization of real-life assets, the concept of NFTs and web3.

2.1 Tokenization of Real-Life Assets

Asset tokenization is a process that essentially converts an asset (such as real estate) into tokens that can be distributed, traded, transferred, fragmented, and stored on a distributed ledger technology. Specifically, tokenization is the process of transforming ownerships and rights of assets into a digital form. By tokenization, you can transform indivisible assets into token forms. Such a process is transforming the way how assets can be financed, allowing asset owners to place them on blockchain and distribute in a more technologically advanced and cost-effective way. Tokenization as a blockchain term can be defined as the process of issuing a token on blockchain that represents various real assets (i.e., real estate, company bonds, luxury items etc.).

After the boom of unregulated Initial Coin Offerings (ICOs) in 2018, Security Token Offerings (STO) emerged as a new, more regulated way of raising liquidity for various projects by tokenizing them. This is one such example for tokenization. Tokenized assets can take shape in different forms though. They can be security tokens, platform tokens, utility tokens, fungible, or non-fungible tokens.

Real estate is viewed as one of the main assets that can be tokenized. Traditionally, it was an illiquid asset that was accessible only to a small pool of wealthy individuals, while smaller investors could benefit only from investing in Real Estate Investment Trust (REIT) stocks. However, this is changing rapidly, and more investors will have access to single-asset real estate investments which they can trade as tokens within decentralized exchanges (DEXes). Concretely, this would mean that someone can be 1/25 owner of a house without needing to own the funds to buy the entire house. Asset divisibility, faster and cheaper transactions, higher liquidity in rather illiquid markets and transparency are some of the benefits of tokenization.

To learn more about tokenization, listen to the Generation Blockchain podcast episode on asset tokenization.

Click here to listen to the Generation Blockchain Podcast on Asset Tokenization.

2.2 NFTs

Nonfungible tokens are a blockchain-based, programmable proof of ownership to an asset. This digital proof gives its holder the exclusive ability to use, sell and transfer the asset's ownership rights, as dictated by their private key signature.

These rights could take different shapes. They can pertain to resale, physical redemption, contain digital functions, financial benefits, or other intangible rights. The NFT does not necessarily "contain" the asset purchased but rather is a programmable record of ownership with an inbuilt pointer to the asset location. For example, if you buy NFT art in the form of a picture, the picture itself is not stored on the blockchain but rather, the link leading to the NFT is stored on chain.

Fungibility refers to the interchangeability of the asset. Bitcoin, Ether (ETH) and fiat currencies are fungible since there is no difference between each unit. One 20€ bill is exactly the same in terms of its value and purchasing power as another 20€ bill despite the fact that they have different serial numbers. "Nonfungible" assets on the other hand are unique and cannot be interchanged seamlessly (e.g., houses or rare art). Nonfungible tokens represent unique assets on the blockchain.

Semi-fungibility is a relatively new term and refers to interchangeability between specific classes of assets. While football tickets can be interchangeable if they are for the same game and same booth or seating area. Note that these types of assets can change in fungibility over their lifetime. For instance, after the semi-fungible concert ticket is used, it becomes a unique, so-called clipped ticket" and is thereafter nonfungible.

Artist Beeple and his $69 million NFT

The biggest NFT media attention to date was given to the artist Beeple. His digital artwork was sold for $69 million US dollars at an auction at the Christie's auction house in March 2021.

Behind the artist's name Beeple is the US American Mike Winkelmann. The NFT artwork in question is called "EVERYDAYS: THE FIRST 5000 DAYS" and is a digital collage of a total of 5000 individual artworks created in just as many days. Accordingly, there are over 10 years of work behind the overall artwork, with the actual effort being the creation of a 319-megabyte JPEG file with a resolution of 21,069 x 21,069 pixels. But the entire story behind it is unique: the most expensive NFT work by a modern artist to date, the first NFT auction of its kind at Christie's, and thus the worldwide breakthrough on the art market.

Figure 15: NFT: „EVERYDAYS: THE FIRST 5000 DAYS“ (Source: Beeple)

Origin and development

NFTs have become much more present in the media in recent months. For example, Jack Dorsey's $2.9 million NFT tweet or the sale of the Beeple NFT for $69 million make the headlines of non-crypto-specific magazines and media bringing NFTs closer to a much wider audience. Though NFTS seem to be a completely new phenomenon, the history of blockchain-based NFTs already dates several years back. The first NFT project was in 2012, namely the colored coins on the Bitcoin blockchain. The so-called colored coins are a concept designed to be layered on top of Bitcoin. Coins can be given additional information before being exchanged. "Coloring" in this context means giving coins specific attributes which turn them into tokens. These tokens can be used to represent anything. Due to lack of monetization of the concept on the Bitcoin blockchain, colored coins did not take flight until today. It was not until the Ethereum Blockchain that NFT gained momentum. In the summer of 2017, the first Ethereum-based NFTs appeared as CryptoPunks.

CryptoPunks

Crypto Punks are 10.000 unique digital 8-bit-style punks, all with unique features created by Larvalabs. Their digital property credentials are stored in the form of ERC20 tokens on the Ethereum blockchain. Each CryptoPunk is distinguished by individual visual characteristics, so no two are alike. The punks were initially available and distributed for free. All you had to do to get one was pay the associated Ethereum transaction fee.

Figure 16: CryptoPunks by Larvalabs

Because of their hard-cap supply and cult status among early adopters, they are already considered digital antiques. They are still tradable and interoperable with most NFT applications on Ethereum though they have been wrapped into ERC-721 tokens to make them tradable on NFT marketplaces. Technically, the wrapped CryptoPunks are a bit different from the others, but they can be unwrapped back into ERC20 standard once they are purchased from OpenSea, a leading NFT marketplace on Ethereum.

CryptoKitties

In 2017, CryptoKitties became the first mainstream application of NFTs that is also the most remembered NFT in history. CryptoKitties are digital representations of cartoon cats created by Dapper Labs for a blockchain computer game. Each of the cats is unique and thus exists only once on the blockchain. Players could own, breed, and trade kitties.

Figure 17: Example of CryptoKitties (Source: CryptoKitties, 2022)

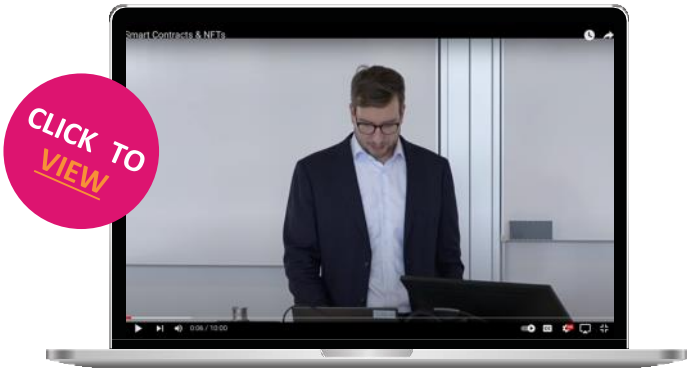
The allure to the on-chain computer game is that new unique CryptoKitties could be bred by uniting different cats. These newly cats could breed cats could then be auctioned off or sold on the open market similar to how the private pet market works in real life.

The CryptoKitties bubble

The breeding activity attracted speculation and hype. At its peak in 2017, trading volume was around 5.000 ETH and sales of a single CryptoKittie reached amounts of $100.000. This sudden increase of traffic on Ethereum's network caused the digestion of the network. Ethereum's network capacity at the time was not up to this demand. Trading and breeding CryptoKitties incurred high transaction fees and hours of waiting.

The CryptoKitties bubble had formed from a mixture of hype, speculation, and viral story. The bubble burst soon after in mid-December 2017, when the demand and prices for CryptoKitties dropped drastically. The entire crypto bubble began to burst thereafter, and a several-year-long bear market was ushered in in the entire crypto market.

To learn more about NFTs and their technical set-ups, watch this Generation Blockchain video. Click here to watch the Generation Blockchain video on Smart Contracts & NFTs.



2.3 Web3

In this section, we will dive into the previous and current developmental phases of the internet (web 1.0 and web 2.0) and finally into the often-proclaimed next phase of the internet – called web 3.0.

Web 1.0 – The internet of information

Though it is hard to imagine, the internet is only about 30 years old (as per 2023). Originally, the internet allowed to share research among academics and governments. Its main function was to act as a big library. In the 90s, the internet was also referred to as the "information web" since it allowed users to access research materials. It even enabled us to contact anyone through email.

Web 1.0 allowed users to browse information and send emails but did not support publishing content for the average user. A group of developers acted as the gatekeepers to the information on the internet. The key offering of Web 1.0 was to share information and contact anyone throughout the world with an internet connection.

Web 2.0 – The internet of interaction

In 2004, Facebook and YouTube revolutionized the web with the concept of user-generated content. From then on, everyone with an internet connection could actively publish their own web content. The internet became democratized with web 2.0. Web 2.0 enabled users to form communities around a central idea, and then mobilize themselves for a common cause.

The Arab Spring movement is a good example of this scenario. Social media played a significant role in facilitating communication among the participants of this movement and allowed them to form a large community. Individuals created something big enough to challenge large power structures with web 2.0 as the tool.

Problems with Web 2.0

The structure of web 2.0 is inherently centralized by hardware and software providers that often hold monopoles or have a few competitors of equal footing. Users only have a choice of which applications to use for social media, banking and dating within a narrow frame. These applications in turn rely on a handful of internet servers causing another layer of centralization.

Centralization & monopolies

We can imagine the internet as a few huge suns (i.e., the servers) that have thousands of smaller planets orbiting around them (i.e., our day-to-day apps). The complete authority or control over the applications and data is centralized at one point (the server). The underlying problem with this architecture here is the lack of ownership of data and power to control and decision making. Our entire experience on Web 2.0 is reliant on central entities granting us access to their applications which can be cut off at any time. Pictures in a cloud, social media account access, banking access are just some examples to name. Essentially, if the control of a user's content is defined by someone else, it is not really their content anymore. We know this to be true with posting picture on social media to which we lose the rights of ownership once they are uploaded on the platform and the control over what happens to it and where it is stored.

Data as a commodity

What is even more concerning is the fact that the content and personal data posted online can be monetized by companies to make money and influence democratic processes. The bottom line is that the current internet allows users to publish but owns and monetizes everything the users create. User data is a commodity in web2.0.

Honey pots and information silos

When signing up for online banking, the user must trust that service with their personal data. Online banking is especially sensitive since it requires sharing personal information such as identity cards, addresses and the data of your finances. This big amount of personal information stored in central databases gives a huge incentive for hackers to target those storage servers that act as honey pots. Despite security efforts, centralized databases are vulnerable to digital crimes and security threats.

The role of the servers

Inernet servers as the base layer are among the most powerful entities of the web2.0 infrastructure. Whether you use the internet for social media, dating, business, education or banking, there is only a handful of huge entities that gather our information and have absolute control over the collected data. This is a dangerous amount of power, no matter whose hands it is in, and which regulation is in place to avoid fraudulence.

Value transfer

Additionally, in web 2.0 users cannot autonomously transfer value without a third party involved. This is especially true for cross-border transactions. Despite advancements in digitalization and digitization of online banking, an intermediary or third-party provider is needed, nonetheless.

While web 2.0 allowed users to publish content, build communities, and social movements, it also concentrated the right and control of personal data in the hands of big digital entities. In web2.0 we are not the owners of any content we publish, and users also do not exert “self-sovereignty.”

Web 3.0 – Internet of Ownership

Web 3.0 answers the questions:

1 What if we could access all services without sharing any of your data, and without handing over the ownership of the content you create ?

2 What if we could own our digital life and manage our assets autonomously?

Web 3.0 (or also referred to as web3) is the proclaimed next generation of internet after web 2.0. The name was created by Gavin Wood, the co-founder of Ethereum and Polkadot's founder. It is also important to note that there is no uniform definition for the term web 3.0 yet. While web 2.0 focuses on user-created content hosted on centralized websites, web 3.0 will give users more control over their online data. To do so, web 3.0 makes use of machine learning, artificial intelligence (AI), and blockchain technology. Web 3.0 proponents aim to create open, connected, intelligent websites and web applications with the help of an improved machine-based understanding of data. The aspects of decentralization and digital economies also play an important role in web 3.0 which is where blockchain technology steps in. That being said, web 3.0 is still far from mass adoption.

Security

A blockchain is essentially an infinite digital storage space that is open to everyone. Blockchain does not compromise on security meaning that it is a safe locker for your digital assets. Blockchain-based assets allow the user to "own" their own data and safeguard it themselves. Blockchain also eliminates the current centralized infrastructure of the internet, data, and assets.

Autonomous value transfers

Since blockchain is a digital ledger that keeps track of value and ownership as it is transferred, users can send and receive value digitally without an intermediary. This allows the next iteration of the web to break out of its current centralized structure and become a safer, fairer, and more efficient space, resulting in financial freedom for users.

The technical side of web 3.0

Just like different programming stacks defined web1 and web2, there is a new software stack that defines web3 to make decentralized internet happen. Web3 is in many aspects an iteration of Web2 in terms of interactivity. The big difference between them is that at the core of the stack there is a blockchain protocol.
On top of the blockchain protocol, there are four layers that bind blockchain to the end-user experience:

1

Smart contracts

Smart contracts are embedded into each data block and tie in NFTs and cryptocurrencies into the web3 concept. While Ethereum is the leading platform for deploying smart contracts written in Solidity there are other blockchains, such as Cardano that use other programming languages such as Haskell.

2

Web3.0 libraries

Web3.0 libraries provide access to helper methods on how blockchains link to web3 provider dApp interfaces (e.g., ethers.js, web3.js, or web3.py). The web3.0 libraries enable you to build frontends that can communicate with the blockchain (including smart contracts deployed on the blockchain).

3

Nodes

It is the role of nodes to link web3 libraries to smart contracts as blockchain's decentralization cornerstones. Instead of relying on a centralized server, blockchain networks are dispersed across thousands of computer nodes worldwide.

4

Wallets

Wallets connect to blockchain networks and individual dApps on them. Wallets should not be seen as containers. Rather, crypto wallets like MetaMask unlock access to blockchains and their dApps, via the user's private keys.

With these four web3 layers in play, it is possible to replicate every web2 platform that exists today. They offer the same functionality but are improved in the sense of offering decentralized monetization, funds/data ownership, and censorship-resistant content. In web3.0, 3D visualization and interaction presentation are a big part of the user experience. The fields of UI and UX also work towards presenting information in more intuitive ways for web users. In connection with blockchain, AI can both present data to us and sort it, making it a versatile tool for Web 3.0. This also reduces the work needed for human development in the future.

The edge of web3.0 over web1.0 and web2.0

The combination of Web 3.0's key features (in theory) can lead to many benefits and differ depending on the exact blockchain calibration:

1

No central point of control

Since intermediaries are removed from the web3.0 equation, users are controlling their user data. The lack of centralization reduces the risk of censorship by governments or corporations and cuts down the effectiveness of Denial-of-Service (DoS) attacks.

2

Increased information interconnectivity

As more products become connected to the internet, larger data sets provide algorithms with more information to analyze. This can help them deliver more accurate information that accommodates the individual user's specific needs.

3

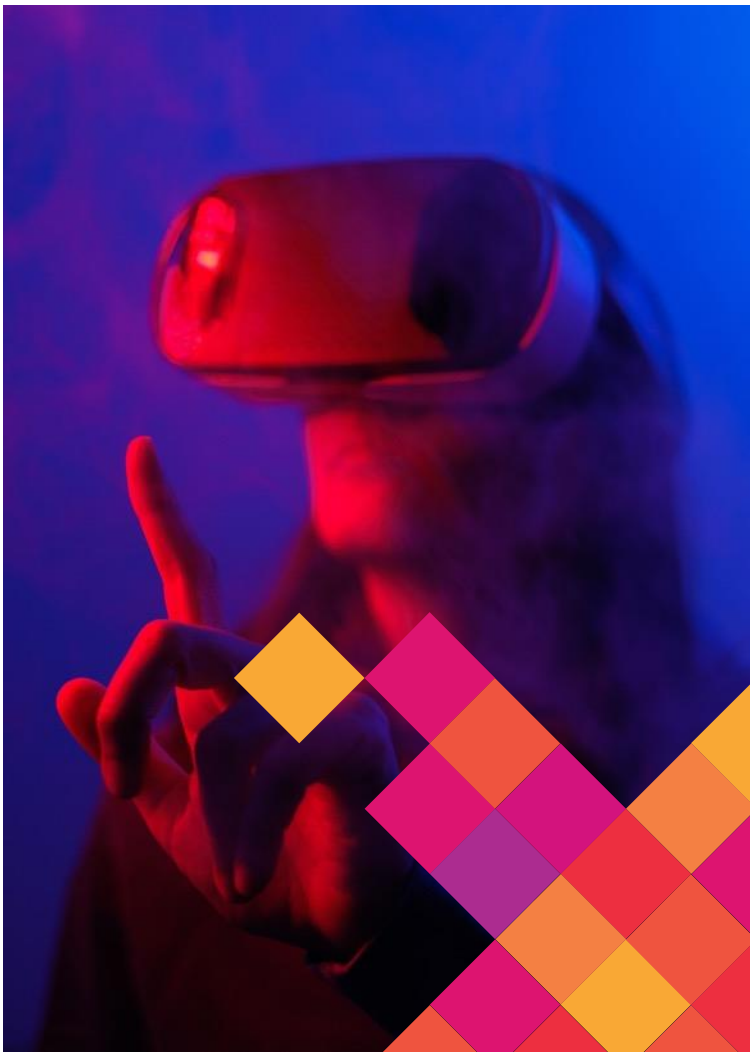
Increased browsing efficiency

When using search engines, finding the best results have sometimes posed a challenge. However, they have become better at finding semantically relevant results based on search context and metadata over the years. This results in a more convenient web browsing experience that can help anyone find the exact information they need with ease.

4

Improved advertising and marketing

Web 3.0 aims to improve advertising by leveraging smarter AI systems and targeting specific audiences based on consumer data.



How does crypto fit into web3.0?

Blockchain and crypto play a crucial role in web3.0 since decentralized networks successfully create incentives for more responsible data ownership, governance, and content creation as compared to web2.0. Some of its most relevant aspects for Web 3.0 include the following:

1

Digital wallets

Anyone can create a wallet that allows you to make transactions and acts as a digital identity. There is no need to store your details or create an account with a centralized service provider. The user has total control over their wallet, and often the same wallet can be used across multiple blockchains.

2

Decentralization

The transparent spread of information and power across a vast collection of people is simple with blockchain. This contrasts with web2.0 where large tech giants dominate huge areas of our online lives.

3

Digital economies

The ability to own data on a blockchain and use decentralized transactions creates new digital economies. These allow us to easily value and trade online goods, services, and content without the need for banking or personal details. This openness helps improve access to financial services and empowers users to begin earning with their own data and content.

4

Interoperability

On-chain dApps and data are increasingly becoming more compatible. Blockchains built using the Ethereum Virtual Machine can support each other's DApps, wallets, and tokens. This helps improve the ubiquity needed for a connected web3.0 experience.

Web3.0 use cases

Although web3.0 projects are still in development, we do have some examples that are already in use today:

Decentralized autonomous organizations (DAOs)

As well as owning your data in web 3.0, web3.0 users can own the platform as a collective, using tokens that act like shares in a company. DAOs coordinate decentralized ownership of a platform and make decisions about its future in a democratic way. DAOs are defined technically as agreed-upon smart contracts that automate decentralized decision-making over a pool of resources (i.e., tokens). Users with tokens vote on how resources get spent, and the code automatically performs the voting outcome. However, people wrongfully define many web3.0 communities as DAOs. These communities all have different levels of decentralization and automation by code.

Connected smart homes

One key feature of web3.0 is its ubiquity. This means that we can access our data and online services across multiple devices. Systems that control heating, air conditioning, and other utilities can now do so in a smart and connected manner.

Siri & Alexa virtual assistants

Both Apple's Siri and Amazon's Alexa offer virtual assistants that are interoperable with web3.0. AI and natural language processing help these assistants to get better at understanding human voice commands. The more people use Siri and Alexa, the more their AI improves its recommendations and interactions. This makes it a perfect example of a semantically intelligent web app for web3.0.

Web3 limitations

Despite the numerous benefits of web3.0 in its current form, there are certain limitations that the ecosystem must address for it to flourish:

Accessibility

Web3.0 is less likely to be utilized in less-wealthy, developing nations due to the required high transaction fees. On Ethereum, these challenges are being solved through network upgrades and layer 2 scaling solutions. The technology is underway but is still in need of higher levels of adoption on layer 2 to make web3.0 accessible to everyone.

User experience

The technical barrier to entry to using web3.0 is currently quite high as users must comprehend security concerns, understand complex technical documentation, and navigate unintuitive user interfaces. Wallet providers are working to solve this, but more progress is needed.

Education

Web3.0 introduces new paradigms that require learning different mental models than the ones used in web2.0. A similar education drive happened as web1.0 was gaining popularity in the late 1990s. Proponents of the internet used a slew of educational techniques to educate the public from simple metaphors (the information highway, browsers, surfing the web) to television broadcasts. Web3.0 is not inherently more difficult, but it is different. Educational initiatives informing web2.0 users of these web3.0 paradigms are vital for its success.

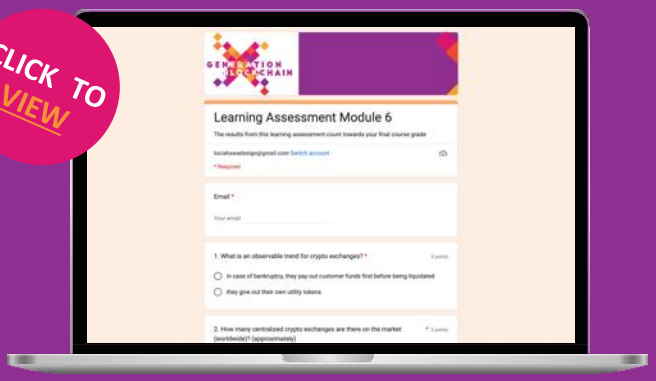
Centralized infrastructure

The web3.0 ecosystem is young and quickly evolving. As a result, it currently depends mainly on centralized infrastructure (GitHub, Twitter, Discord, etc.). Many web3.0 companies are rushing to fill these gaps, but building high-quality, reliable infrastructure takes time.

03

LEARNING ASSESSMENT FOR MODULE 6

To test your knowledge, finish this learning assessment as part of your overall grade for the course.
Click here.



01

MODULE 7

Industry Applications

Co-funded by the European Union

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 National Agency. Neither the European Union nor National Agency can be held responsible for them.

contents module 7

Co-funded by the European Union

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 National Agency. Neither the European Union nor National Agency can be held responsible for them.

01| MODULE 7
Industry Applications

Chapter Overview

In this module, blockchain technology in the context of manufacturing (i.e., supply chain management and resource responsibility) will be examined. Furthermore, blockchain technology in the energy sector (i.e., the energy-sharing economy and exemplary use cases) will be subject of this module.

Learning Objectives

After the first module, you should be able to:

- Explain how blockchain technology can be used in synergy with other technologies for data management (i.e., IoT, AI).
- Understand how blockchain technology can enable resource responsibility through tokenization.
- Argue concrete ways in which blockchain can improve the energy-sharing economy.
- Explain exemplarily how the roles of stakeholders involved in the energy-sharing economy will change from a legal and task-distribution standpoint with blockchain-based systems.
- Detect potential risks regarding the introduction of blockchain technology in industry applications.
- Reiterate one specific use case for a blockchain industry application in the energy sector.
- Gain a critical view of the Bitcoin energy consumption.

01| BLOCKCHAIN TECHNOLOGY AND OTHER TECHNOLOGIES

Today, blockchain technology, internet of things (IoT), and artificial intelligence (AI) are remarkable innovations, which will improve business processes, bring new business models into existence, and disrupt whole industries:

1 Blockchain, for example, can increase trust, transparency, security, and privacy of business processes by providing a shared, decentralized distributed ledger. Precisely, blockchain technology or, in general, distributed ledger technology can store all kinds of assets similar to a register.

2 IoT drives the automatization of industries and user-friendliness of business processes, which is essential for the German and the European industry.

3 AI improves processes by detecting patterns and optimizing the outcomes of these processes.

Currently, the interconnection between these innovations is mainly neglected. However, these innovations can and should be applied jointly and will converge in the future. A possible connection between these technologies could be that IoT collects and provides data, blockchain offers the infrastructure and sets up the rules of engagement while AI optimizes processes and rules. By design, blockchain, IoT and AI are complements and can exploit their full potential if applied combined.

In the following, you will learn about the added value, which blockchain, IoT and AI can provide for companies. The convergence of these technologies can be particularly beneficial for data management, identity management and the automatisation of business processes.

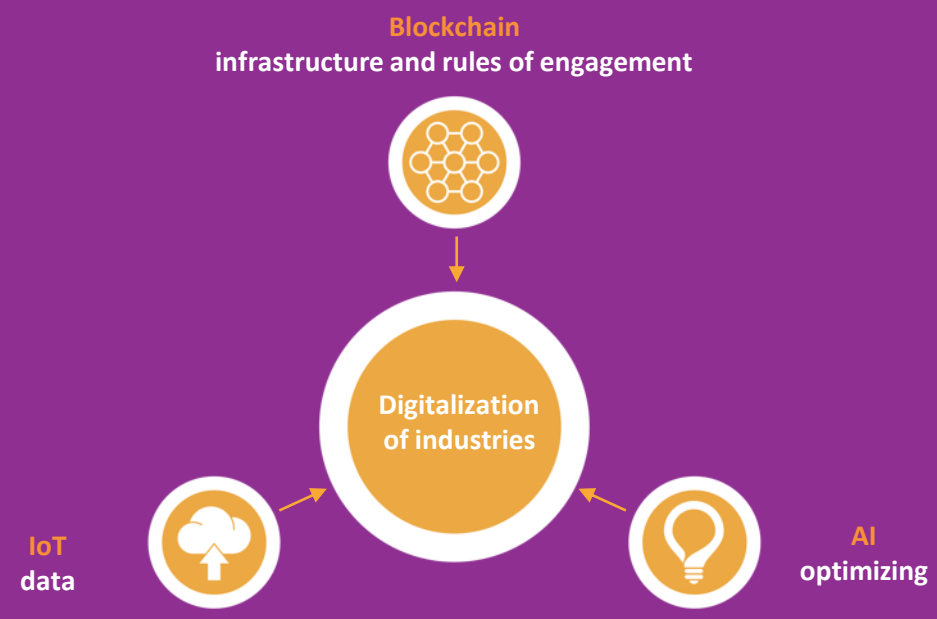


Figure 18: Convergence of technologies

1.1 Data management

Standardization of data

IoT devices, such as sensors, machines, cars, or smart grids, collect a high amount of data. This data is often stored in a centralized database. Typically, these data lack standardization since different legacy systems for collecting and storing data are being used. Blockchain technology could support the standardization of data by setting up a harmonized digital platform for IoT data accessible for multiple parties. On blockchain systems, data is stored in one data format due to the use of hash functions. Therefore, data would be highly standardized. Moreover, the size of the stored data would be heavily reduced since hash functions transform the obtained data into a string of a specific length. Consequently, data management could be optimized by increased standardization of data.

Data privacy and security

In blockchain systems, the underlying cryptography enables a high degree of privacy. On most blockchains, e.g., the blockchain used for Bitcoin or Ethereum, transactions are conducted pseudonymous. However, it is also possible to enable completely anonymous transactions which is for example the case with Monero or Zcash. The architecture of blockchain systems i.e., private/public key infrastructure also allows full encryption of stored and transmitted data such that, if desired, only the device itself can read and write its own data.

The privacy of data is especially beneficial in the context of IoT. In IoT, machines, and devices store a high amount of sensitive data. It is essential to ensure privacy and security of stored data. It is common practice to send IoT data directly from the machine to the respective database for collection purposes.

However, there is a trade-off between a high level of privacy and control for illicit activities. In case transactions are anonymous, it is not possible to infer the name and the address of the transaction sender. This anonymity features illicit activities such as money laundering or terror financing. In this case, AI can be helpful and can increase security by detecting illicit activities. Certain research proposes to use AI, leveraging data analytics, to reduce the risk of illicit activities on the blockchain, which results from the anonymity of transactions. Note that AI technologies benefit from the high amount of provided IoT data as AI algorithms learn from data.

Scalability

A key limitation of IoT is the management of the massive amount of collected data. To improve scalability, the use of blockchain technology and AI can be highly beneficial. Opponents of blockchain technology argue that blockchain systems are per se not scalable because consensus mechanisms such as proof-of-work are very energy consuming. However, there are alternative consensus mechanisms such as proof-of-stake or proof-of-authority, which are more energy efficient and are scalable. Of course, consensus mechanisms will be and must be further improved. To reach a higher level of scalability on a blockchain, AI can be helpful. In academia, there is a suggestion for the use of a performance optimization framework for blockchain-enabled IoT systems. This system could be based on machine learning in the form of a DRL-based algorithm to dynamically select/adjust the block producers, consensus algorithm, block size, and block interval to improve the performance.

Authentication via a blockchain-based identity

Furthermore, blockchain technology can be applied for authentication purposes and is able to increase trust in network participants by managing the identity of IoT devices. In general, identity management typically refers to individuals and companies but can also refer to IoT devices and machines. Blockchain-based identities will make sure that transaction parties will receive a digital identity, which is based on their actual "real" physical identity: for individuals' identity cards and for companies it would be commercial register entry. Based on such identities, transactions between individuals and companies (e.g., car sharing) but also between individuals and machines (e.g., passenger transport of an autonomous car) or between two machines (e.g., autonomous car pays for parking) can be conducted and processed in an efficient way with low transaction costs and a high transaction speed.

IoT Analytics estimates that more than 20 billion devices will be connected to the internet by 2025. These devices will partly be connected to a payment network requiring a new payment infrastructure. Individuals, companies, and machines must be registered with their digital identities in order to participate in this new payment network. Blockchain technology is a perfect fit to provide a system for installing and managing digital identities in a secure and efficient manner. Therefore, identity management on the blockchain will be of major importance in the future. As with conventional centralized systems also the blockchain identity system has to comply with data protection laws. In fact, blockchain technology with its inherent access systems and encryption processes is even better than non-blockchain-based systems able to, first, protect data by design, second, organize the ownership of data and, third, facilitate the monetization of data. Blockchain also enables security of identity as the records are immutable and difficult to forge.

Automatization via smart contracts

Another field that highly benefits from applying blockchain, IoT and AI jointly is the automatization of business processes. Smart contracts have tremendous potential to yield efficiency gains in various sectors but are currently not heavily adopted in the industry. This is due to the fact that classical smart contracts require crypto assets. However, companies are typically reluctant to use crypto assets because of regulatory and economic limitations. The main drawback of crypto assets is their price fluctuations. If a smart contract is denominated in crypto assets, the receiving party is exposed to a high exchange rate risk due to the volatile price. Even if coins exert a high level of price stability (stablecoins), they might not be adopted by the majority of industrial companies due to several drawbacks: First, stablecoins are currently unregulated. Hence, risk-averse companies do not seek to use these assets. Second, the IT and accounting systems of companies are not denominated in crypto assets but in fiat currencies like the Euro or the US dollar. Converting stable coins into fiat currencies for accounting purposes is an operational burden as it costs both personnel and financial resources.

The blockchain euro

There is only one way how smart contracts can unfold their full potential. A blockchain-based fiat currency is necessary to "flow-through" the smart contract. Only a blockchain-based digital Euro would enable Euro-denominated smart contracts, such that IoT devices can directly offer services on their own like pay-per-use, leasing, and factoring. Due to a digital blockchain-based Euro such new business models could become reality: fully automated devices making decisions on their own while leveraging AI and "economically surviving" by using blockchain for financial transactions while implementing a profit center logic on the device-level.

With such a digital blockchain-based currency, micropayments for IoT devices could be conducted easily and cost-effectively. All transactions denominated in the blockchain-based currency would be directly included in internal accounting and IT systems and would not have to be converted. A further advantage would be that such a blockchain-based Euro would comply with current regulation. First startups like CashOnLedger and Monerium have developed such currencies in 2019. They use e-money licenses for the tokenization of fiat currencies. In contrast to crypto assets, and stablecoins in particular, companies demanding such payment solutions do not have to fear regulatory uncertainty since all players act under existing regulation.

Central bank digital currencies

As previously described, a blockchain-based Euro is currently issued by banks and e-money institutes. Also, the central bank could launch such a digital currency. In the literature, this is called "central bank digital currency" (CBDC). According to a recent study by the Bank for International Settlements more than 70 central banks worldwide analyze implications of CBDCs. However, only a hand full of central banks has introduced such a currency. Nevertheless, central banks are starting to engage with digital currencies e.g., the ECB announced the project "EUROchain", which will be a CBDC prototype developed on the Corda DLT framework.

An ECB-issued blockchain-based CBDC would enable the use of central bank money for smart contracts.

Why is this necessary? What are the advantages of a digital Euro issued by a central bank compared to a digital Euro issued by e-money institutes? E-money counts as commercial bank money while money provided by the central bank is central bank money. Even if both kinds of money represent a digital version of the Euro, in the case of bankruptcy, commercial bank money could default, whereas central bank money is a claim to the central bank and cannot default. This difference gets highly relevant in case of financial turmoil when banks and e-money institutions potentially face bankruptcy.

Monetization of IoT devices via tokenization

Besides improving data management, supporting the authentication of network participants, and facilitating the automatization of business processes, blockchain technology can unlock new business models for the monetization of IoT devices. Blockchain technology enables the dematerialization of assets ("tokenization").

An example: Think about a lamp (e.g., a streetlight), which has its own (blockchain-based) identity and operates with a blockchain-based Euro. The use of blockchain technology makes the lamp an autonomous entity, operating "on its own". Via smart contracts, direct payments to the lamp are possible. If a respective payment is received the lamp will turn on. Such payments can be, provided by individuals, companies or even the public administration. As a consequence, pay-per-use payment schemes become feasible.

These lamps can further be tokenized so that investors can invest into them in the form of digital assets. Investors would have an incentive to build and maintain the lamps on a full scale as investors receive a share of the lamp's profits. By providing incentives for investors to invest into building and maintaining the lamps, a new wave of investments could be generated. Tokenization is not only beneficial in the case of lamps but also for all kinds of IoT devices, such as sensors, cars, machines, or cameras. The only requirement for tokenization is a connection to the internet and to a blockchain network.

	Blockchain	IoT	AI
Car	Providing secure and immutable database featuring data privacy of car data; enables tokenization of car	Collect high quality data from different cars	Optimizing fuel consumption of car
Machine	Providing secure and immutable database featuring data privacy of machine data; enables tokenization of machine	Collect high quality data from different machines	Optimizing production and maintenance processes of machine

Figure 19: Examples of convergence of Blockchain, IoT and AI

Conclusion

Blockchain, IoT and AI are innovations providing tremendous benefits for security, transparency, immutability, privacy, and the automatization of business processes. However, the impact of these innovations is even higher when blockchain, IoT and AI are combined. We argue that these innovations will converge in the future, driving the digitization of the industry. This convergence will increase the quality of data management by reaching a higher degree of standardization, privacy, and security of data. Further, new business models are enabled such that autonomous agents (e.g., sensors, cars, machines, trucks, cameras, and other IoT devices) can be set up as profit centers that autonomously send and receive money. We recommend executives to engage with these technologies in order to realize efficiency gains. Blockchain technology, combined with IoT and AI, will pave the way to a new age of digitization.

To dive deeper into success factors for the use of blockchain technology in all fields of business, listen to this Generation Blockchain podcast episode.

Click here to listen to this Generation Blockchain Podcast episode on Success Factors for Blockchain Projects.

1.2 Resource Responsibility

Climate change is one the most pressing issues of our times

Climate change is one of the most pressing issues of our times. Global warming has come to dominate the discussions in industrialized nations, and renewable energies and CO2 avoidance have come to the fore, as each report published by the Intergovernmental Panel on Climate Change (IPCC) demonstrates increasing urgency to act: ocean acidification, sea-level rise, and ecosystem extinction are at record levels. According to the International Energy Agency (IEA), carbon dioxide emissions have risen to their highest level ever, and according to NASA, 2022 is going to be the year with the hottest average temperature in the last 2000 years. The current trajectory is making the aim of the 2015 Paris Agreement to limit global warming to 1.5°C to avoid the worst impacts of climate change an increasingly ambitious target.

The carbon cycle, part of a complex system

Most carbon is stored in rocks such as limestone, with much of the rest being found in the ocean's sediment, soil carbon, fossil carbon, plant biomass and atmosphere. As with everything else in nature, the carbon flow is a cycle: Carbon, mainly in the form of carbon dioxide and methane, cycles through the earth, the ocean, living organisms (plants, animals, micro-organisms), the atmosphere, through the land, the earth's interior, and the ocean.

Man-made climate change and its impact results from the interruption of the natural carbon cycle. Specifically, carbon is released back into the cycle quicker than it can be absorbed by the natural system, mainly due to the combustion of fossil fuels.

This is happening as — despite urgent efforts — our modern lives are still mainly powered by fossil fuels that constitute around 84.3% (2019) of global primary energy consumption. This includes the industrial production of goods such as cement and steel, transportation, energy use in buildings, as feedstock for petrochemical products, etc. Other energy sources like renewables (such as wind and solar) and other non-fossil fuels (such as nuclear) represent 5.0% and 10.7% of global energy respectively.

At this stage it is clear to see that fueling our economy by burning huge amounts of fossil fuel is pushing the natural carbon cycle out of balance, as nearly ¾ of greenhouse gas emissions result from energy use, amplifying the greenhouse gas effect and resulting in a significant increase of global average temperatures.

The energy transition

The energy transition refers to a shift in the energy sector towards net-zero carbon. To achieve this, the energy system will need to move away from fossil fuels toward renewables. The predictions of the potential of renewables as a primary energy source vary between 70% International Energy Agency (IEA) and 75% International Renewable Energy Agency (IRENA) by 2050. A push of clean technology is needed (i.e., energy efficiency, circular economy approaches, green transportation, alternative energy carriers like green hydrogen, etc.). Such a massive transformation in the global energy system implies major shifts, also in geopolitical power structures, as an energy system powered by renewables will differ profoundly from the energy current one.

The trilemma

The war in the Ukraine made the vulnerability of the energy system and the challenge of balancing energy security, affordability, and environmental sustainability, also known as the energy trilemma, painfully apparent. Sustainability has the following facets:

1 **Security**
The ability to meet future demand and the resilience of the energy system to bounce back from interruptions.

2 **Affordability**
The ability to keep energy universally affordable.

3 **Sustainability**
The transition towards a "clean" energy system.

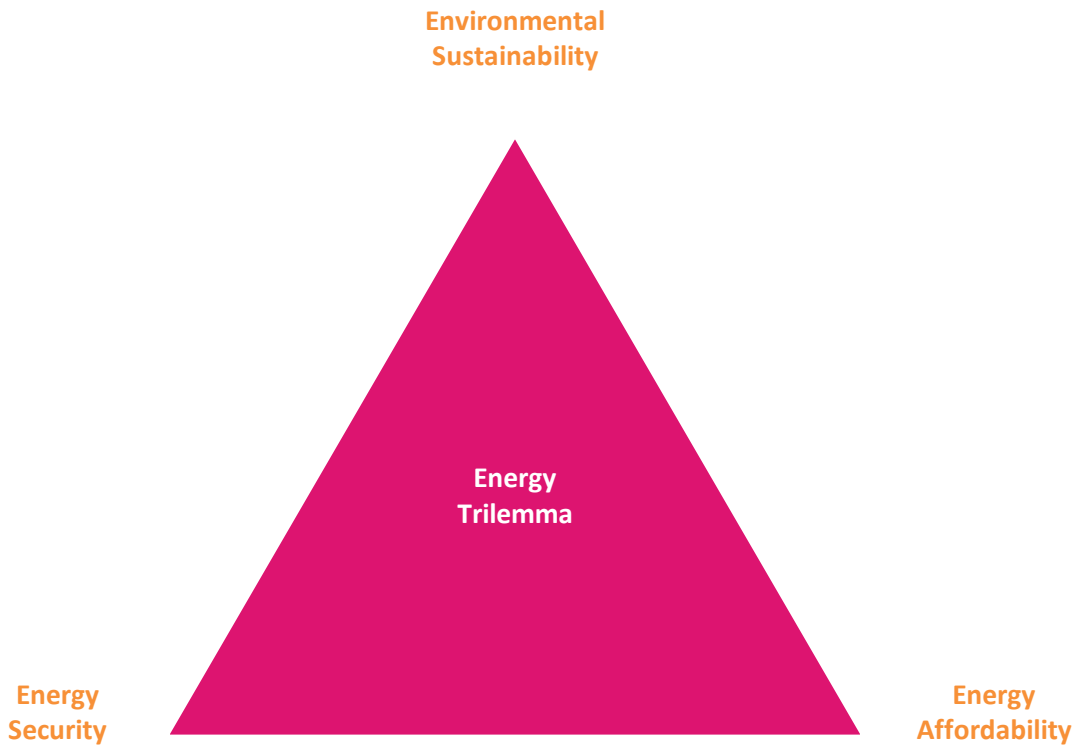


Figure 20: The energy trilemma

With Russia covering a high percentage of the global energy supply, energy security and affordability are greatly challenged, especially in Europe. For example, Germany is already preparing to ration gas during the coming winter. Furthermore, investments in big oil firms and an increase of coal-based power plants have been increased, challenging the sustainability component. While national energy strategies were greatly disrupted by the war in the Ukraine, there is a clear hope that the situation has created a sense of urgency to improve energy security through cleaner alternatives. That means, diversifying in terms of energy source and type, and a decoupling from Russia. The EU, for example, with its REPowerEU plan, has the target to accelerate the green transition to reduce Russian dependencies through, e.g., increasing hydrogen targets for industry and transport, as well as through increased investments.

The energy transition is complex and balancing the energy triangle will stay a challenging task, and energy strategies can be expected to continue being interrupted by unexpected events. Hence, the resilience for energy security and accessibility is critical for economic development and will be at the core of future strategies.

The financing question — mobilizing investments

One of the main questions in the energy transition remains who is financing this shift. Dynamically driving innovation requires the mobilization of a lot of capital. Not to forget that the rise of the fossil fuel industry was and still is highly subsidized by government spending. Governments still put several 100 billion USD into fossil fuels each year, whereas only a fraction of that is spent on renewables.

According to McKinsey, “USD 9.2 billion capital spending on physical assets for energy and land-use systems will need to rise by USD 3.5 trillion per year for the next 30 years and USD 1 trillion will need to be reallocated from high to low emissions assets.” (McKinsey, 2022)

To achieve the necessary mobilization of capital for the energy transition to occur it is necessary to focus not only on public funds, but to also tap into the trillions held by private actors. Thus, financial vehicles need to be created.
Securitization that

1. split the high initial investment risks of those technologies’ developments while keeping capital sufficiently concentrated to push innovation,
2. sends demand-side signals,

3 supports additional finance streams at various risk levels, and

4 creates vehicles make real ESG efforts investable and create vehicles to re-pay for the green premium, may prove necessary.

Such financial instruments are not just crucial to further advance the energy transition in developed countries, but also to facilitate global development and push the transition in developing countries where financial markets are not as mature, and the cost of capital remains high.

The positive aspects a crypto-assets-based infrastructure could bring

In its 6th Assessment Report, the IPCC calculated a remaining carbon budget of around 400 Gt of CO_2 that would still allow our world to comply with the 1.5 °C target. The current emission level is around 56 Gt CO_2 per year and the average polluting country will run out of "emission budget" in around 8 to 9 years. This shows that a lot of capital will be necessary: Efficient capital allocation into green tech, ecosystem restoration and minimizing waste through circular economy approaches. These approaches, to just name a few, will be decisive for minimizing adverse climate change effects.

Markets that provide full transparency in terms of impact and accurate measurement along the value chain, that are scalable to many market participants, could use the proven mechanisms of our economic system and help drive the system towards a net-zero economy. But externalities and stakeholders need to be adequately represented and accounted for.

Smart contract platforms as trusted record-keeping tool for ESG criteria

Smart contract platforms such as Ethereum, in combination with other technologies like IoT, AI, and machine learning, establish a great basis for data recording in a trusted and transparent way. Through smart contracts, real-time data can be gathered along the entire value chain and automated, through programming business logic and regulatory insights into the ledger, pre-and post-trade. Standardized processes and integration with measurement systems streamline and optimize this, allowing for a high automation rate reducing time and resources needed.

Algorithms allow input data to be checked and verified instantaneously with the blockchain record serving as the ultimate truth in the long term. With this, verification and validation processes can be integrated using signing agreements, as well as proven and established methods from the 'off-chain' world to ensure data integrity. Once the right mechanisms for record-keeping are established, data can be stored and handled with minimal risk of error and across many individual parties, with reduced risk of manipulation. This could facilitate the transition from trust in traditional paper-based processes towards having real traceable data, along the entire value chain.

Tokenization and smart contracts as an efficient tool to incentivize and allocate capital for ESG efforts along the value chain

The standardization and rules for accounting units' alignment process is an ongoing and highly complex topic. This also includes the effort to integrate those into a system with the right incentive structures. The result is a structure that allocates capital for 'true ESG' efforts. The basis for such a system is data integrity and mutual benefit along the entire value chain. As discussed above, this has been highly challenging in the past decades. A DLT-based infrastructure can improve the situation, as data can be efficiently gathered in real-time pre- and post-trade, and mechanisms for verification can be integrated therein. In turn, this creates a highly trusted, and immutable audit trail. Token contracts provide a tool to create assets from data gathered along the entire value chain so that each participant in the system can monetize their actual ESG contribution without the need for intermediaries.

Future proof infrastructure for an evolving system

Smart contract platforms such as Ethereum have the unique capability to cater to the above-described requirements in terms of flexibility within a dynamic system, promoting innovation by enabling collaboration. Such infrastructure provides the possibility of integrating participants in an evolving market efficiently into the system on a trusted partner level. This allows data sovereignty and adaptation to locally differing and evolving requirements and standards. Through standardization and publicly accessible code, a high level of efficiency can be achieved.

Tokenization, an efficient tool to create financial instruments

As described above, data gathered along the value chain is documented in an immutable and trustworthy way on a distributed ledger. This highly trusted data can in turn be securitized in a standardized and highly efficient manner. It also allows programming business logic and applying regulatory insights in tandem with governance rules directly on the ledger, by use of smart contracts. This can support many of the needed mechanics, making this entire transition process scalable and improving what in today's infrastructure is a time-consuming and cost-intensive process.

First benefit of tokenization: Split the high initial investment risks of those technologies' developments, while keeping capital sufficiently concentrated to push innovation, and send demand side signals. Tokenization makes fractionalization of investments possible which may prove useful in the energy transition in many ways.

One example of this would be a solar farm in the initial building phase. Investment and returns of those projects can be efficiently managed through smart contract platforms and their end-to-end integration — automated in combination with AIoT along the chain of custody. Once the project enters the production phase, returns can be allocated according to initial agreements. This would also have a positive effect on capital aggregation and avoidance of too fragmented developments.

Efficient and automated processes pre- and post-trade generate massive gains in efficiencies and allow many investors to be included in a market that is otherwise accessible to institutional investors only due to its cost intensity. Hence, making more capital available while allowing retail investors a greater level of control over their portfolios.

While supporting the initial project development phase, financial instruments may be created at various stages of the project. At a later stage, once the technology is ready and the project is operational, a fractionalized investment could be used as a refinancing tool for developers leading to capital being available for new projects while facilitating the same mechanics along the way.

The second benefit of tokenization is the support of additional finance streams at various risk levels.

Conclusion

New possibilities around trust and transparency made possible through digitization and tokenization allows for new forms of decentralized documentation and securitization. This enables the realization of technological potential to transact and own assets in an unprecedentedly scalable manner, as many participants can be cost-efficiently integrated into the system.

This can open new worlds in terms of efficient capital allocation through transparent markets, enabled through: (1) an accurate and transparent lifecycle "track & trace", (2) economic incentives to act sustainably for the many, and (3) a dynamic system that pushes innovation while allowing for collaboration in a trusted way within a growing system. This way, markets for all kinds of assets will be able to mobilize the vast amount of funds necessary for the energy transition at scale and speed.

The text stems from the academic article "Blockchain, IoT and AI – A perfect fit" published on March 25th, 2010 by Prof. Dr. Philipp Sandner, Dr. Jonas Gross and Ricarda Joas. The authors consented to the use of the text for the purpose of the Generation Blockchain project.

02

BLOCKCHAIN TECHNOLOGY IN THE ENERGY SECTOR

The sharing economy is one of the fastest-growing segments in blockchain as well as in business. The sharing economy enables people to rent out their own property for use by others. Airbnb, for example, allows travelers to rent out part of an apartment or house instead of leaving it empty when on vacation. Uber and Lyft are a proxy for taxi cabs where the car of the owner is used to provide the service that normally a taxi would provide. The traditional sharing economy also has certain issues. There can be high fees for using the platform, bad working conditions and unfair revenue sharing that hurt individual users but benefit the underlying corporation. Some companies have abused their power, for example, by receiving access to private data without customers' consent. Sharing economy has also taken over in several blockchain related projects. One of the most promising use cases for blockchain in the sharing economy is the energy-sharing sector which the next section.

2.1 Energy-Sharing Economy

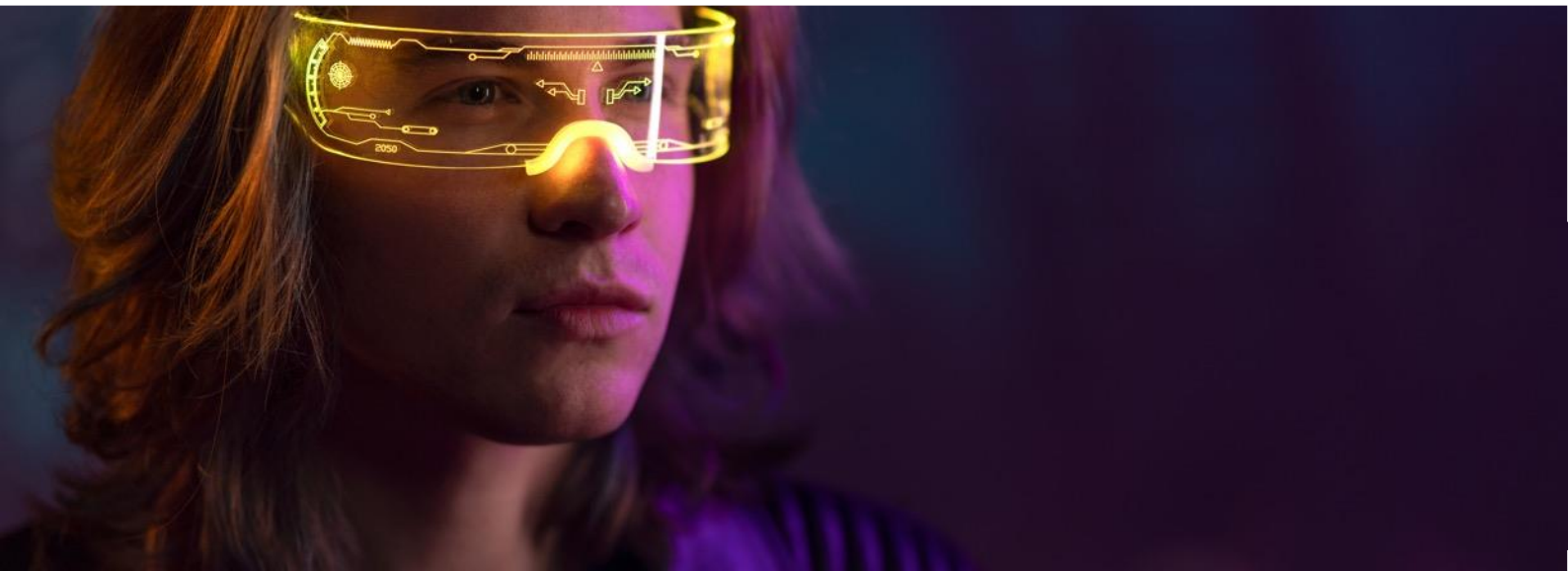
Blockchain technologies could be applied to a variety of use cases related to the operations and business processes of energy companies. Some of the potential applications and affected parts of business (models) are:

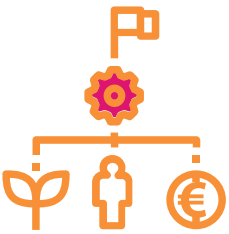
Billing

Blockchains, smart contracts and smart metering can execute automated billing for consumers and distributed generators. Utility companies might benefit from the potential for energy micro-payments, pay-as-you-go solutions, or payment platforms for pre-paid meters.

Sales & Marketing

Sales practices may change according to consumers' energy profile, individual preferences and environmental concerns. Blockchains, in combination with artificial intelligence (AI) techniques such as machine learning (ML), can identify consumer energy patterns and therefore enable tailored and value-added energy products provision.





Trading and markets

Blockchain-enabled distributed trading platforms might disrupt market operations such as wholesale market management commodity trading transactions and risk management. Blockchain systems are currently being developed also for green certificate trading.

Automation

Blockchains could improve control of decentralized energy systems and microgrids. Adoption of local energy marketplaces enabled by localized P2P energy trading or distributed platforms can significantly increase energy self-production and self-consumption, also known as behind the meter activities, which can potentially affect revenues and tariffs.

Smart grid applications

Blockchains can potentially be used for communication of smart devices, data transmission or storage. Intelligent devices in the smart grid include smart meters, advanced sensors, network monitoring equipment, control, and energy management systems, but also smart home energy controllers and building monitoring systems. In addition to providing secure data transfer, smart grid applications can further benefit from data standardization enabled by blockchain technology.

Grid management

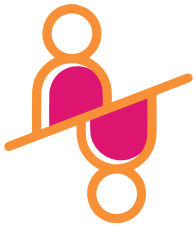
Blockchains could assist in network management of decentralized networks, flexibility services or asset management. Blockchains could achieve integrated flexibility trading platforms and optimize flexible resources, which might otherwise lead to expensive network upgrades. As a result, blockchains might also affect revenues and tariffs for network use.

Security & identity management

Protection of transactions and security can benefit from cryptographic techniques. Blockchain could safeguard privacy, data confidentiality, and identity management.

Sharing of resources

Blockchains could offer charging solutions for sharing resources between multiple users, such as sharing EV charging infrastructure, data, or common centralized community storage.



Competition

Smart contracts could potentially simplify and speed up switching of energy suppliers. Enhanced mobility in the market could increase competition and potentially reduce energy tariffs.

Transparency

Immutable records and transparent processes can significantly improve auditing and regulatory compliance. Blockchains can enable and potentially disrupt established business models and traditional roles of energy utility companies.

Blockchain use cases can thus be distributed into the following eight larger groups according to their purpose and field of activity:

1. **metering/billing and security**
2. **cryptocurrencies, tokens, and investment**
3. **decentralized energy trading**
4. **green certificates and carbon trading**
5. **grid management**
6. **IoT, smart devices, automation, and asset management**
7. **electric e-mobility**
8. **and general-purpose initiatives and consortia**

The most popular category is decentralized energy trading (including wholesale, retail, and peer-to-peer) energy trading initiatives. The second most popular category is cryptocurrencies, tokens, and investment accounting. The third most popular use case is IoT, smart devices, automation and asset management, and metering, billing, security, and accounting.

Regulation of the blockchain energy sharing sector

If a decentralized transaction model were to be implemented based on blockchain technology, it would cause a transformation of current market roles. These changes would also be reflected in regulation. All energy consumers would have to manage their own energy balances and meter operators would no longer need to collect data themselves since all transaction data would be recorded automatically on the blockchain.

As of present, the regulatory unbundling provisions require energy companies to separate their network activities (regulated business) from the supply of energy to customers (competitive activity). Customers have the right to freely choose their energy supplier (i.e., electricity or gas supplier) in a liberalized energy market. In order to ensure that customers can smoothly transfer between suppliers, so-called balancing groups were introduced. This made it possible for each customer to be assigned to a supplier in a simple way. Another significant area of regulation is the so-called clearing process, which is run to reconcile planned consumption against customers' actual consumption as recorded by their meters. The difference between these is referred to as balancing energy and the costs incurred in relation to this are charged to each electricity supplier according to causation.

A key prerequisite for the regulatory regime to function is that each customer is accounted for as part of a balancing group. This is done by clearly assigning customers to balancing groups and their suppliers to the responsible balancing group managers (which may or may not be the same entity). The meter operators obtain readings of the verified meter data relevant for billing and transportation charging purposes and pass them on to the other players involved:

- to the relevant electricity supplier for billing purposes
- to the relevant transmission system operator (TSO) for clearing and settlement purposes. The TSO collects all data for each balancing group and aggregates it to determine the balancing energy costs to be allocated to the balancing group.
- to the relevant distribution system operator (DSO)
- to the relevant balancing group manager, who in turn charges the balancing energy (cost-generating) it has been allocated to the suppliers using its balancing group.

This shows that the delivery of electricity entails complex settlement processes across the entire electricity market and that the corresponding meter readings are required for various purposes.

Role transformations through blockchain

One major benefit of a blockchain-based transaction model is that all electricity delivered to the networks can be clearly attributed to individual customers in small time units (near real-time). Thus, electricity produced and consumed can be settled very precisely at variable prices. Interestingly, the physical electricity would continue to flow to the end user directly from the closest generator as is the case today. A simplified clearing process through blockchain would lead to less balancing energy being charged to market participants.

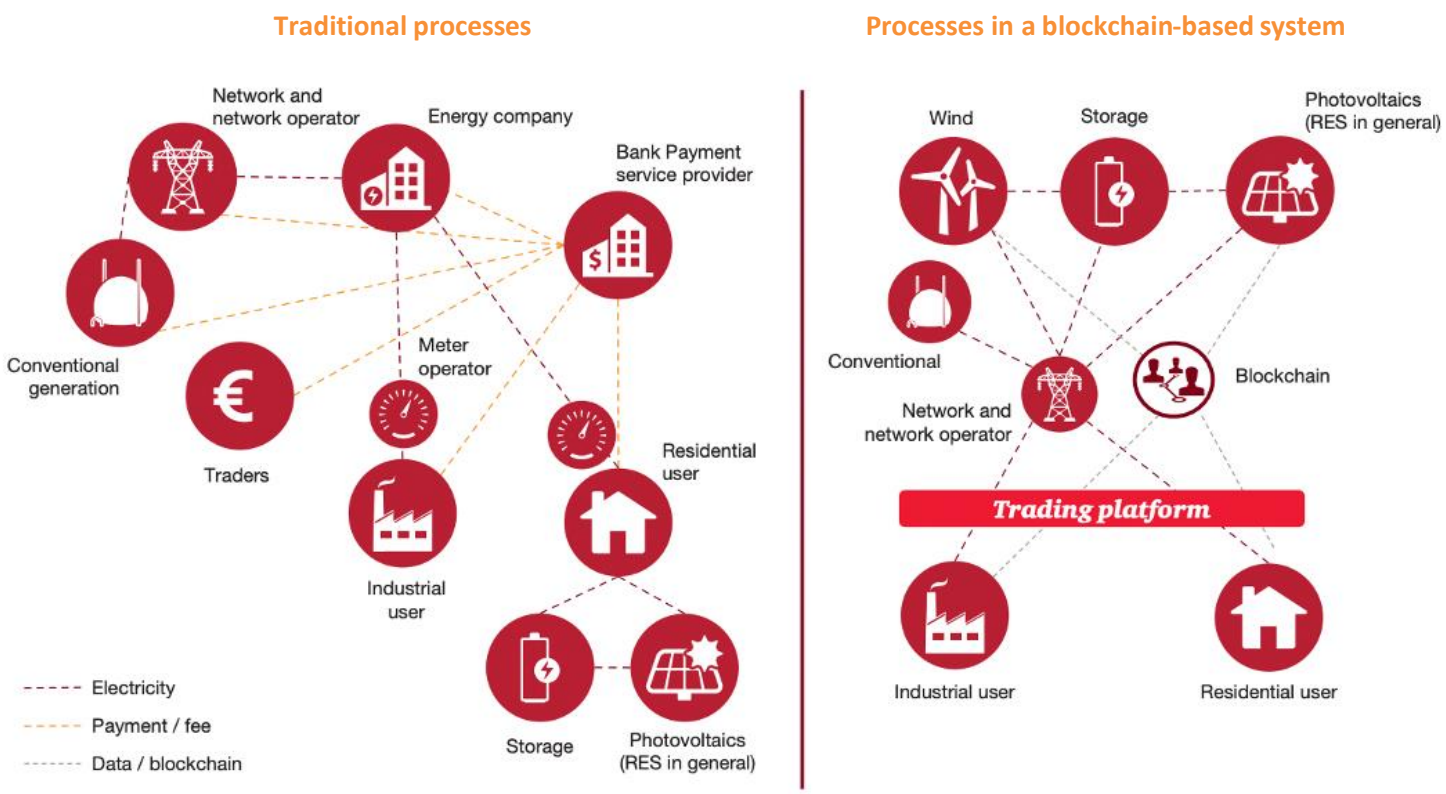


Figure 21: Figure 12: Transformation of market structures on introduction of decentralized transaction model (source: PwC study "Blockchain – An opportunity for energy producers and consumers?")

As is shown, blockchain technology allows for direct contractual relationships between energy consumers and producers. Both energy consumers and energy producers could act as prosumers. This would result in the following changes:

Energy consumers

Energy consumers would have to become balancing group managers and to comply with the provision of security and risk management requirements of this market role. For example, energy consumers would have to submit their own demand forecasts to the relevant network operator.

The role of meter operators

Meter operators would no longer have to collect and record data themselves. The consumption and transaction data would be exchanged automatically and accurately. The transaction data necessary to determine network tariffs would be provided to meter operators (and thus also to network operators) by oracles. The responsibility of meter operators could be limited to providing reliable and tamperproof meters and oracles.

Distribution system operators

Distribution system operators would also receive the information on transactions they require to charge their network costs to customers from the blockchain.

Transmission system operators

If the decentralized transaction model is fully implemented, transmission system operators would no longer require receiving data for clearing purposes, as all transactions would be executed in real-time and settled only on the basis of actual consumption.

Financial market regulation

If financial transactions are no longer handled by energy companies or banks but by a peer-to-peer system, the responsibility for ensuring that financial transactions are properly settled also shifts. While it would not be possible to impose such an obligation on the energy consumers this could cause unbearable administrative overhead work. Instead, an actual responsible entity, e.g., a platform operator, would be needed that would meet the requirements to be satisfied by a financial service provider of the respective legislation.

Looking at the regulatory transformation of blockchain technology in the energy sector shows that blockchain business models and the overhaul of existing customer and provider relationships in the context of law are far more complex than one might think. The idealistic blockchain model without a responsible central authority is not a feasible option, as this would require clear and transparent liability rules and compliance with local regulations to ensure that such a platform can be operated properly and securely. Without such, the liability of the parties involved in the case of payment defaults, technical failures or intentional tampering would not be covered. As the energy supply business involves the use of critical infrastructure, the event of a complete or partial failure of the system must be prevented by emergency plans.

Opportunities for blockchain technology in the energy sector

Blockchain technology could lower energy bills for consumers since these systems operate on the assumption that all providers transact directly with their customers. One consequence of this would be that the intermediaries previously operating in the market, among them trading platforms, traders, banks, or energy companies, might no longer be needed or that their number and importance would be reduced. This could lead to a significant decrease in system costs. The reduced or eliminated types of system costs include the following:

- no or lower costs to account for the costs (including personnel and other operating costs, infrastructure etc.) and profit margins of the above companies that are currently active in the market but will have no or only a reduced role in the future system
- no or lower operating costs for meter reading, billing etc.
- no expenditure required for payment reminder and debt collection processes
- no costs for bank payments (especially direct debits for payments by customers)
- possibly lower transportation charges
- no certification costs for renewable electricity

The above cost reductions would lower the energy bills of consumers, whether directly or indirectly. There are operating costs of blockchain systems, which include transaction fees for blockchain transactions. Here, the required computing power and related energy use also belong to the operating costs. As of today, the actual costs of blockchain applications cannot be projected.

Set up of a blockchain as an operation cost factor

What is definitive is that private blockchains usually involve lower transaction costs and usually operate on the basis of simplified verification processes leading to lowered costs. These cost considerations must also factor in the investment required to make the electricity networks flexible. Blockchains can only be used effectively if the power grid can cope with a larger number of individual energy producers and of managing greater flexibility, all of which is also essential to ensure supply security.

Network effects

Another point to be considered is that maximum cost benefits can only be achieved via network effects in which as many providers and customers as possible agree to use blockchain applications that are based on common standards and rules. This would prevent the parallel emergence of incompatible applications and the need for bridges between different systems.

Energy consumer benefits

Additionally, energy consumers would also have greater flexibility in choosing their supplier. In blockchain-based transaction systems customers almost constantly switch supplier, as they can find new transaction partners and contract with them within extremely short timeframes

Transparency

The use of blockchain technology would ensure greater transparency for consumers, for example in tracking exactly where the electricity they purchase was produced. Direct transactions between energy providers and energy consumers would allow the parties to define the “contractual counterparty” (i.e., the wind or solar farm delivering the energy). The source of the electricity supplied could be tracked exactly as well as the exact percentage share of renewable energy. Each energy consumer could specify these aspects individually and to an unprecedented level of granularity.

The transaction history stored on the blockchain (energy consumed and payments made) would also become transparent. The availability of a full transaction history and the possibility of conducting analyses on this basis would bring customers a yet unrivalled level of clarity. The monetization of such data which is owned by and at the disposal of commercial and large customers would be inhibited but at the same time probably reveal more details on which they could base their analyses. This level of transparency would clearly also cause new difficulties, as all transactions are publicly accessible. Though pseudonymous aliases can be used, it is theoretically possible to “decrypt” a certain number of aliases without authorization.

Local value creation and prosumers

Blockchain technology could also boost to a current trend: the rise of the role of the prosumer that we have already looked into when talking about web 3.0. In the context of energy sharing, lower transaction costs and simplified billing processes could enable small providers or energy consumers to participate in the market not only as consumers but rather as providers. If consumers operate their own solar systems, they could more easily sell the produced electricity to their neighbors or feed it into the network. This would lead to improved viability of solar systems, small-scale wind turbines or customer-owned CHP plants. This in turn would increase the number of prosumers again. In the energy sharing economy, consumers also benefit from a more diverse product offering and lower prices.

In addition, blockchain models could facilitate the realization of community-funded energy projects. Simplified routes to market for distributed energy generators would further boost the growth of renewables. Indirectly this might also have a positive effect on the economic structures in the region of production. Distributed generation can provide economic stimulus through services, for example in the fields of maintenance or operations. Increased deployment of wind power could be a particular benefit in areas with little infrastructure and slow economic growth.

Risks in the energy sector

Blockchain risks in the energy sector blockchain technology are still largely unexplored, which means that it comes with a range of uncertainties and risks since there is no long-term experience available. Many experts also suspect that blockchain technology might not be as scalable as needed for certain uses. Given the extremely fast rate of data growth, the sheer data volumes accumulating after several years of operating a blockchain place high demands in terms of security, speed, and costs. As a new technology operating on the basis of a completely new transaction model, it is to be expected that blockchain technology will at least to some extent be rejected by some energy players, among energy consumers, and in part by the general public. Blockchain technology is a rather clunky database system that requires many copies of the same data to be stored, communicated, and added to at all times. The anonymity underlying the blockchain concept also entails the risk of the system being used for the purpose of illegal activities (e.g., organized crime). A decentralized blockchain system without any superior authority might also turn out to entail drawbacks for consumers, as at least under the models discussed today there is no responsible entity that could intervene in a regulatory capacity, provide simple services, or revise previously executed transactions. What would happen when a user forgot their personal access details needed to access their own account? In this case, users are irrevocably locked out of their accounts and lose their settings, information and assets stored in them.

Security risks

Non-cryptocurrency use cases of blockchain technology are more complex and require the direct participation of end users. They must be secure but user-friendly at the same time. Still, there will always be a risk of tampering (e.g., attacks by hackers) and technical faults (e.g., system failures). Just how realistic the hacking scenario is was proven by the attack on the application “DAO” (Decentralized Autonomous Organization).

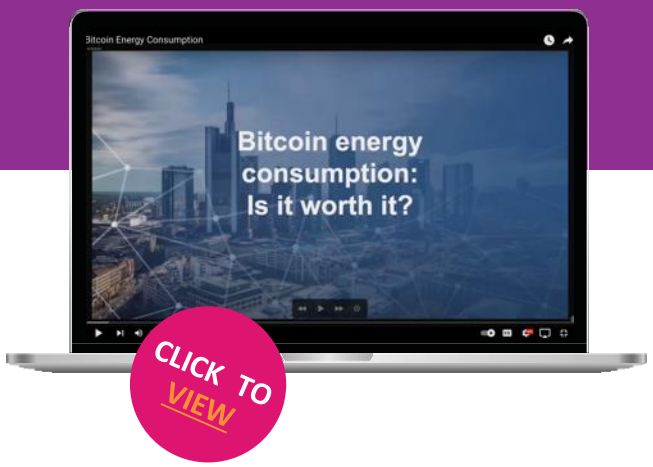
Common problems specific to blockchain in the energy-sharing economy

A technical challenge of P2P electricity trading systems from a grid's management perspective is that every node needs to respond to grid conditions, prices, local supply, and demand. This could result in the need for individual consumers to provide demand forecasts for use by the system operator, similar to current electricity market operations.

Machine learning techniques can be used to predict future behavior of large sets of prosumers and electricity consumers, but it is argued that the aggregation of multiple blockchain users to comply with grid reliability requirements forms a technical challenge, as it might increase uncertainty and costs of balancing services. Here, the deployment of distributed storage systems and the adoption of electric vehicles could help to overcome these challenges. Another looming consequence is that if energy systems evolve to being more local and decentralized, the traditional roles in the energy system (i.e., energy retailers or grid operators) could be disrupted. Increasing energy self-sufficiency could bring reduced revenues, while at the same time costs related to the operation and maintenance of the power grid could increase, as grid asset utilization deteriorates.

While blockchain technology can contribute to meet ESG goals and turn economies greener, Bitcoin certainly poses a threat to sustainability efforts. To learn more about Bitcoin’s energy consumption, watch this Generation Blockchain video.

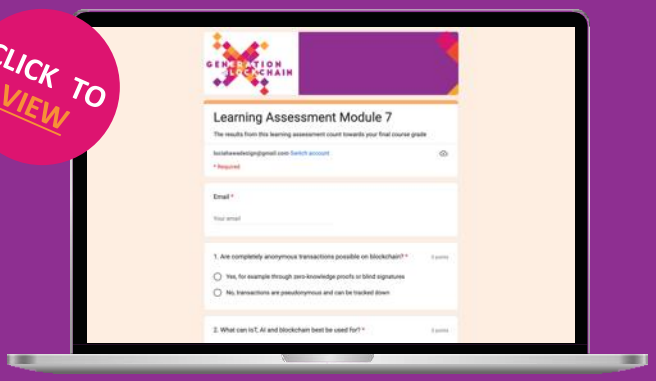
Click here to watch the Generation Blockchain video on Bitcoin Energy Consumption.

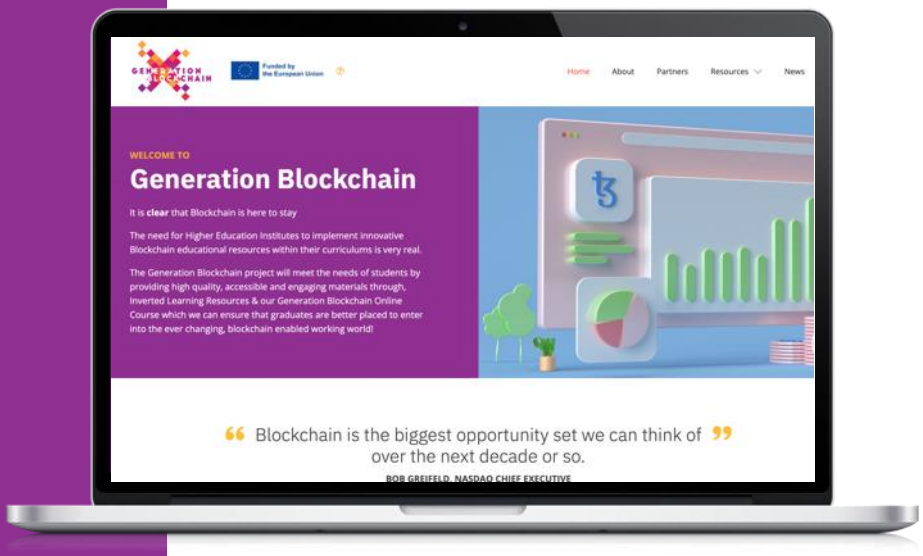


03

LEARNING ASSESSMENT FOR MODULE 7

To test your knowledge, finish this learning assessment as part of your overall grade for the course.
Click here.





follow your journey

www.**generationblockchain**.eu

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 National Agency. Neither the European Union nor National Agency can be held responsible for them.

Co-funded by the European Union

Frankfurt School Blockchain Center · momentum [educate + innovate] · European E-Learning Institute · Amsterdam University of Applied Sciences · U.PORTO