FUTMOFIN
OKP – Part B
Chapter 1
First version: 31.1.2025
Latest version: 31.1.2025

FUTMOFIN

Open Knowledge Platform

A project curated and edited by Tiziano Bussani*

Part B

The Future of Money and Finance: Blockchain Transformation

Chapter 1

Fundamentals of Blockchain and Distributed Ledger Technologies

Authored by Tiziano Bussani

The release of Bitcoin in 2009 introduced blockchain technology: a decentralized, public ledger enabling peer-to-peer transactions without intermediaries. This innovation laid the foundation for applications such as decentralized payment systems (e.g., Bitcoin) and smart contract platforms (e.g., Ethereum). Smart contracts enable the creation of digital objects like fungible tokens (such as cryptocurrencies and stablecoins) and non-fungible tokens (or NFTs) and support the development of decentralized applications (dApps), empowering inter alia *decentralized financial services (DeFi) and decentralized autonomous organizations (DAOs). These technological advancements marked a major shift in the digitalization of monetary, financial, and business interactions, positioning blockchain and distributed ledger technology as a transformative evolution of the Internet, where users can exchange and store value in decentralized and distributed digital environments.*

* Tiziano Bussani, University of Milan (tiziano.bussani@unimi.it), Post-doc Research Fellow of Fondazione Fratelli Confalonieri, Ph.D. in International Law, Lawyer in Italy. He is a member of the Scientific Committee of the Chair FUTMOFIN and Curator, Editor, and Author of the Open Knowledge Platform (https://futmofin.unimi.it/openknowledgeplatform/). The supervisor of the Project is the Chair Leader Prof. Giulio Peroni.

The Project is funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the EU nor EACEA can be held responsible for them.

1. General overview

1.1 **The release of the Bitcoin protocol in 2009 introduced the world to a disruptive technology: blockchain and the broader universe of distributed ledger technologies**. The underlying fundamental innovation consists of an open and public **distributed ledger** – composed of a unique chain of chronologically ordered blocks of verified data transactions – that is managed algorithmically by a peer-to-peer network of Internet-connected nodes. Without relying on trusted intermediaries or authorities, the network verifies and executes transactions based on advanced cryptographic protocols and specific consensus algorithms, while each node stores the same copy of the ledger, which is continually updated as new blocks of transactions are validated by the network and added to the chain forming the ledger. **The possibility for peer-to-peer networks to operate distributed ledgers in which transaction data are verified and stored securely opens infinite opportunities for innovation in the realms of money, finance, and business**.

1.2 More specifically, distributed ledger technologies allow the creation of a **decentralized electronic payment system** like **Bitcoin**, where users can send value denominated in bitcoin (BTC, the native cryptocurrency of the protocol) in a fully peer-to-peer digital mode without trusted intermediaries, as well as more sophisticated **blockchain platforms for smart contracts** like **Ethereum**.
Smart contracts are self-executing agreements encoded in software and stored on the blockchain, allowing any blockchain user to create **fungible tokens** (digital representation of value, including cryptocurrencies and stablecoins, granting holders various rights versus the issuer), **non-fungible tokens** (NFT, non-interchangeable digital certificates of authenticity, property, or rights over a digital or a physical object), **decentralized applications** (dApps, software applications deployed on blockchain, including decentralized finance or De-Fi), **decentralized autonomous organizations** (DAO, digital entities operating on blockchain and governed by voting), and other blockchain applications. Thanks to smart contracts, blockchain protocols and cryptocurrencies have gained global interest, marking a **new phase in digitalization of monetary, financial, and business relations**.

1.3 The rise of blockchain has profoundly influenced the evolution of the Internet, allowing users to hold and exchange value on the Internet directly, that is to say, in **decentralized and distributed environments, without any trusted intermediary or authority**. In this regard, the evolution of the Internet can be described through three paradigms: **Web 1.0**, which allowed users only to read data stored on centralized databases; **Web 2.0**, which enabled users to read and write data, making it possible to communicate; and **Web 3.0**, which empowers users to read, write, and own on the Internet, exchanging value without intermediaries. The blockchain-driven transformation of monetary, financial, and business relations is a result of the ongoing shift from an Internet relying solely on centralized databases to one that integrates both centralized databases and distributed ledgers.

2. The Bitcoin protocol: the first blockchain and its native currency

2.1 In 2008, someone under the pseudonym **Satoshi Nakamoto** published a **whitepaper** entitled "***Bitcoin: A Peer-to-Peer Electronic Cash System***" (in short: the "Bitcoin Whitepaper") proposing an innovative cryptographic protocol operating a distributed ledger of transactions (Bitcoin, the blockchain protocol), that allows creating a decentralized digital currency (bitcoin or BTC, the native currency) that operates without the need for trusted intermediaries. In this regard, it is essential to distinguish *B*itcoin (the first blockchain protocol and the network running its code) from *b*itcoin (the first cryptocurrency and unit of account of the Bitcoin protocol).

At the core of the Bitcoin protocol is the blockchain, a **distributed ledger** consisting of a unique **chain of consecutive and chronologically ordered blocks of verified transactions,** that allows the immutable recording of the latter, enabling trust and transparency without the need for intermediaries.

On January 3, 2009, the first block – the "Genesis block" or "Block 0" – of the Bitcoin blockchain was created, marking the birth of a new disruptive technology, the blockchain, and a revolutionary currency, bitcoin.

⇒ SATOSHI NAKAMOTO, Bitcoin: A Peer-to-Peer Electronic Cash System. Whitepaper, 2008

⇒ Bitcoin Genesis Block

2.2 *Bitcoin's Rationale*. To appreciate the functioning of Bitcoin and blockchain technology, it is crucial to understand what a distributed ledger is and how it works (§ 2.3), including how transactions are verified and executed (§ 2.4) and how blockchain accounts operate (§ 2.5). Before delving into the functioning of Bitcoin, however, it is necessary to first focus on its **rationale**. As clearly stated in the Bitcoin whitepaper, the protocol's aim is to **create "*a purely peer-to-peer version of electronic cash*" that "*would allow online payments to be sent directly from one party to another without going through a financial institution*"**. The motivation behind this goal is expressed in the Bitcoin Whitepaper as follows:

> *"Commerce on the Internet has come to rely almost exclusively on financial institutions acting as trusted third parties to process electronic payments. While this system works well for most transactions, it is still plagued by the inherent weaknesses of the trust-based model.*
>
> *Truly non-reversible transactions are not feasible, as financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, which limits the practical minimum transaction size and excludes small, casual transactions. There is also a broader cost in the inability to make non-reversible payments for non-reversible services. With the possibility of transaction reversal, the need for trust grows, and merchants must be cautious of their customers, often asking for more information than necessary. A certain level of fraud is accepted as inevitable, and these costs, along with payment uncertainties, could be avoided in*

> *person by using physical currency, but no mechanism exists to enable payments over a communication channel without relying on a trusted third party.*
> ***What is needed, then, is an electronic payment system based on cryptographic proof rather than trust, allowing two willing parties to transact directly with each other without requiring a trusted intermediary**. Transactions that are computationally impractical to reverse would protect sellers from fraud, while routine escrow mechanisms could easily be used to safeguard buyers.*
> *In this paper, we propose a solution to the double-spending problem through a peer-to-peer distributed timestamp server that generates cryptographic proof of the chronological order of transactions. The system remains secure as long as honest nodes collectively control more computing power than any group of attacker nodes".*

Therefore, the invention of blockchain by Satoshi Nakamoto was based on the **idea of creating an electronic payment system using algorithms to verify transactions instead of trusting third-party intermediaries**, thereby enabling disintermediated, peer-to-peer digital transactions. Building on this core feature of blockchain, innumerable applications can be developed.

⇒ SATOSHI NAKAMOTO, Bitcoin: A Peer-to-Peer Electronic Cash System. Whitepaper, 2008

2.3 *Understanding Distributed Ledger Technology*. Technologically speaking, the Bitcoin blockchain enables the participants of a **peer-to-peer network**, called the "nodes" of the network, to manage directly, without relying on trusted intermediaries, a **"distributed ledger" of transactions organized in "blocks", i.e. the "blockchain"**. **All network nodes store the same copy of the distributed ledger (or the blockchain), which is constantly updated as subsequent blocks of transactions are verified and executed by the network and added to the chain of blocks forming the ledger**.
When a user node initiates a transaction, the instruction to send a certain amount of bitcoin from the sender's address to that of the receiver is broadcast to the network, whose nodes collaborate to ensure that every transaction follows the protocol rules. In particular, they verify that the sender has the required funds to complete the transaction and prevent the double spending of money. **A new block of transactions is added to the chain of blocks upon cryptographic verification: when verified and executed, a transaction cannot be modified**. Indeed, as all nodes in the network store the last updated version of the blockchain ledger, every node can easily detect fraudulent transactions when they are broadcast to the network for verification and execution.
Distributed ledger technology overcomes the limits of centralized ledgers. While centralized ledgers exist electronically in centralized digital storages and are managed by a single controlling entity, a distributed ledger exists simultaneously on all nodes storing the blockchain and is collectively managed by the entire network of nodes running the protocol's code.

A **distributed ledger** operated by a **decentralized network** is highly resistant to destruction or falsification. This makes blockchain technology **secure and tamper-resistant**. Beyond being distributed and decentralized, the Bitcoin blockchain is also **public and permissionless**: anyone with an Internet connection can consult the transaction ledger and, without requiring authorization, become a network node by running the Bitcoin code on their computer and storing the blockchain.

2.4 *Transaction Verification and Execution*. **The process by which any subsequent block of transactions is verified, executed, and added to the ledger is known as "mining"**. This process can be carried out, without permission, only by specific nodes of the network, known as **"miners"** or **"validating nodes"**.

Mining a block involves solving a complex mathematical puzzle generated by the protocol known as **"proof-of-work"**. This involves finding a specific value, called a "nonce", that, when combined with the data in the block of transactions to validate, produces a hash (a unique cryptographic fingerprint) that meets certain predefined criteria. Specifically, the hash must start with a certain number of leading zeros, making it possible to find only by trial and error. When a miner solves the proof-of-work problem generated by the protocol to add a new block of transactions, the solution is broadcast to the network. If the solution and transactions are validated, the new block is executed and added to the chain, allowing the next block to be mined.

The miner who solved the proof-of-work puzzle is rewarded with newly minted bitcoins and earns transaction fees included in the block and paid by the senders. This incentive structure motivates miners to participate in the network and secure the system.

The process of mining a block is **computationally intensive and highly energy-consuming**, requiring miners to perform millions or even billions of computations. To maintain system stability, the difficulty of the puzzle is dynamically adjusted so that, on average, a new block is mined approximately every ten minutes. This adjustment helps regulate the rate at which new blocks are added to the blockchain, maintaining the system's stability despite changes in the total computing power (or "hashrate") of the network.

Once a block is mined, it is linked to the previous block of the blockchain via a cryptographic hash, making it computationally infeasible to alter any data in previous blocks without redoing the proof-of-work for the modified block and all subsequent blocks, a process that is economically unsustainable. This makes it **extremely difficult for any malicious actor to tamper with the blockchain, ensuring that once transactions are confirmed, they are permanent and irreversible**. Thus, the process of mining not only serves to verify transactions algorithmically but also plays a **critical role in maintaining the decentralized nature of Bitcoin by ensuring that no single entity can control the ledger or alter the transaction history**. The combination of proof-of-work and decentralized consensus guarantees the integrity of the Bitcoin blockchain, allowing users to trust the system without relying on any central authority.

2.5 *Core Features of Blockchain Accounts*. Thanks to mining and the other core features explained above, the Bitcoin protocol has been able to create an **electronic payment system** enabling users to send and receive value expressed in bitcoin, the native (crypto)currency of the blockchain and unit of account, in a distributed and decentralized fashion with a high level of security and reliability. To further understand the functioning of the Bitcoin protocol, it is necessary to examine how this payment system operates from the user's perspective.

By interacting with the Bitcoin blockchain, **anyone can create freely, without permission and without providing any identity data, a "Bitcoin account"**. The latter consists of a **public key** (an alphanumeric string) derived from a **private key** (an series of randomly generated words) released to the user by the Bitcoin code when creating a new Bitcoin account. Similarly to the IBAN code – which however is tied to the user's identity data – the public key is used to receive bitcoin from other users. To send bitcoin, instead, users must sign transactions with their private key. **The private key must remain secret and securely stored as it is the sole and only way to dispose of the bitcoins held at the related public key**. Private keys can be securely stored in a **wallet**. The latter are software tools that allow users to manage their private keys, enabling them to sign, encrypt, and broadcast transactions to the Bitcoin network.

Bitcoin transactions and accounts are pseudonymous: while they are recorded on a public ledger, the identity of users is not tied to their Bitcoin addresses, as **the sole information visible on the blockchain concerning the sender and receiver are their respective public keys**. However, it is crucial to note that while Bitcoin offers pseudonymity, it does not guarantee complete anonymity, as blockchain transactions are publicly visible and traceable, and the transaction history of any Bitcoin account can be easily explored by accessing the blockchain.

2.6 *Bitcoin Issuance and Distribution*. The final step to understanding the Bitcoin protocol is to appreciate how bitcoins are generated and distributed within the network, that is, **the Bitcoin monetary policy, encoded in the Bitcoin code**. As illustrated above, new bitcoins are created after a new block is mined and are awarded only to the miner who successfully solved the proof-of-work puzzle allowing to add a block to the blockchain. The distribution of new bitcoins through mining ensures a decentralized issuance process, where the control over the network remains with its participants rather than a central authority.

Bitcoin can be created only through mining. Initially, the block reward consisted of 50 bitcoins per block, but it is halved every 210.000 blocks (approximately every four years, since, on average, a block is mined every 10 minutes) in an event known as the "**halving**". This reduction continues until the total supply of bitcoins reaches its **maximum cap of 21 million bitcoins**. The current reward is 3,125 bitcoins per block and, to date, approximately 19.9 million of the maximum cap of 21 million bitcoins have already been mined. The next halving will take place in 2028.

The maximum cap creates scarcity in Bitcoin, similar to precious metals like gold. This is why it is often viewed as "**digital gold**". This means that as demand for bitcoin increases its limited supply would drive its value higher. Moreover, its **deflationary nature** (or, more accurately, its programmed decreasing inflation) makes bitcoin appealing as a store of value in the long run. These two features combined explain the growing interest in Bitcoin and the increasing price of bitcoins.

2.7 *Bitcoin today.* **All the above features were designed by Satoshi Nakamoto and encrypted into the Bitcoin protocol for the aim stated in the Whitepaper**. After the release of the protocol through the mining of the Genesis block, the Bitcoin blockchain has been operated by a growing number of miners (interested in achieving block rewards) and used by a growing number of users (interested in spending and holding bitcoin). Nowadays, there are around 20.000 running nodes of Bitcoin and 800.000 active addresses worldwide.
In April 2011, **Satoshi Nakamoto published his last message and vanished**; all bitcoins he had mined (around 1 million) remained stored in the relevant accounts and have not moved. Afterward, the network further updated the Bitcoin protocol to increase efficiency, but without modifying its core features. The last protocol upgrade, known as "Taproot", was implemented in November 2021.
The **history of bitcoin price** is stunning.
In 2009 (the same year as the Genesis Block) bitcoin was listed for the first time on a marketplace, with an initial price of **USD 0,00099**. The first known commercial transaction took place in May 2010, when 10.000 BTC were exchanged for two pizzas.
In 2011, the price of bitcoin reached USD 1 and spiked to **USD 31**.
In 2013, it hit a high of over **USD 1.000**.
In 2017, it jumped to nearly **USD 20.000** and fell to around USD 6.000 some months after the spike.
In 2021, **El Salvador adopted bitcoin as legal tender**. In the same year, its price surpassed **USD 69.000**. The next year, it hovered around USD 16.000.
In 2024, the first **ETF on bitcoin** was approved, thus facilitating investing in this asset. By the end of 2024, the price of a single bitcoin surpassed the target of **USD 100.000**, after the newly elected **US President Donald Trump** promised to make the USA the leading crypto industry hub in the world and accumulate bitcoin as a part of the US federal budget.

2.8 Finally, it is important to recall that **the Bitcoin protocol introduced blockchain as a revolutionary digital technology**, that is now being used worldwide at impressive growth rates to create electronic payment systems, issue cryptocurrencies, and provide innumerable advanced technological applications using transactions and data stored in distributed digital ledgers. To understand this ongoing revolution, a closer examination of the functioning of the Ethereum blockchain is needed.

3. The Ethereum blockchain: a decentralized platform for smart contracts

3.1 In 2013, Vitalik Buterin, a young Russian-Canadian programmer, proposed in the "**Ethereum Whitepaper**" the idea of Ethereum, a decentralized blockchain platform designed to support not only digital payments but also decentralized applications based on **"smart contracts"**.

The concept of smart contracts was theorized in 1996 by Nick Szabo, an American computer scientist, legal scholar, and cryptographer, who described smart contracts as "*a set of promises, specified in digital form, including protocols within which the parties perform on these promises*". In other words, they are **self-executing agreements encoded in software**. More specifically, they are transaction protocols (computer programs) stored on blockchain that are automatically executed when predetermined conditions are met. As such, smart contracts allow the parties to automatically execute an agreement by encoding the relevant terms and conditions on the blockchain. Smart contracts also allow users to create and interact with sophisticated decentralized applications (dApps), such as decentralized exchanges for cryptocurrencies or decentralized financial services (De-Fi). Smart contract applications will be explored in section §4.

Ethereum was officially launched in July 2015, bringing a **revolutionary shift in blockchain technology by extending its use case far beyond purely monetary transactions**. While Bitcoin operates as a digital currency for peer-to-peer payments, Ethereum introduces a broader scope by providing a platform for the creation and execution of smart contracts that are operationalized thanks to **Ether (ETH)**, the native unit of account of the Ethereum blockchain and the second cryptocurrency in the world by market capitalization.

⇒ Nick Szabo, Smart Contracts: Building Blocks for Digital Markets, 1996
⇒ Vitalik Buterin, Ethereum Whitepaper, 2013
⇒ Ethereum – Website

3.2 Ethereum is, first of all, a blockchain, a distributed ledger of verified transactions organized in a series of blocks linked together in chronological order and operated by a decentralized network of nodes. Like Bitcoin, it allows users to exchange value expressed in Ether (ETH), the protocol's native cryptocurrency, in a secure, reliable, and peer-to-peer manner.

But beyond payment transactions, Ethereum also supports the deployment of smart contracts (i.e. the transaction by which a smart contract is recorded on the blockchain ledger) and their execution (i.e. the transaction operating a function of a smart contract). Ethereum smart contracts are written in **Solidity**, the native scripting language of the platform.

When a smart contract is deployed on the blockchain, it can be executed when conditions are met. In this case, the user interacts with the smart contract, calling the *ad hoc* function of the program and broadcasting the resulting data transaction to the network for its verification and execution.

Acting as a decentralized virtual machine (EVM, the **Ethereum Virtual Machine**), the nodes of the network work together to verify that the execution of the contract is legitimate, similar to how they collaborate to verify pure payment transactions. When validated, all kinds of transactions (payments, contract deployments, contract executions) are recorded on the ledger.

⇒ Ethereum – Website – Documentation
⇒ Ethereum – Website – Guide

3.3 With the Ethereum 2.0 update, the Ethereum protocol was upgraded in 2022 to increase scalability, energy efficiency, and capability of supporting a broader range of decentralized applications and services. In particular, the **consensus algorithm** was changed, **shifting from the original proof-of-work (PoW) model to proof-of-stake (PoS)**. While in PoW validators have to compete to solve complex mathematical puzzles in order to validate transactions and earn rewards, requiring significant computational power and energy consumption, in **PoS validators have to "stake" or lock up a certain amount of cryptocurrencies to be eligible for validating transactions and earn rewards**, but they are subject to significant penalties if a fraudulent transaction is included in the block they validate.
Proof-of-stake is far more energy-efficient, as it does not rely on computational power but instead on the stake of validators. However, PoS offers fewer guarantees for long-term reliability and decentralization compared to PoW, as the concentration of power and wealth in a small number of validators can undermine the network security and resilience and may result in a greater susceptibility to collusion, governance manipulation, and 51% attacks, especially if large validators or staking pools dominate the network.

⇒ Ethereum – Website – Documentation

4. Smart contract applications: fungible and non-fungible tokens, dApps, De-Fi, DAO

4.1 Smart contracts allow users to create **fungible tokens**, that is, digital objects that are interchangeable, divisible, and identical in value. On Ethereum, ERC-20 is the reference smart contract standard for the creation of fungible tokens.
This category includes many different sub-categories of tokens, such as:

- **Cryptocurrencies**: a broad category of digital currencies issued on a blockchain, further divided into "coins" and "tokens" (in a narrower sense). While the former includes the native cryptocurrencies of a blockchain protocol, like BTC and ETH, the latter groups all cryptocurrencies issued on other blockchains, such as ERC-20 tokens on Ethereum. Examples include LINK, an ERC-20 token from Chainlink, a decentralized network designed to provide real-world data to smart contracts, bridging blockchains and the outside world through complex software applications called "oracles";

- **Stablecoins**: a specific type of cryptocurrency designed to maintain a stable value by being pegged to a reserve asset, such as a fiat currency or a commodity. Examples include Tether (USDT) and USD Coin (USDC), which are fiat-collateralized stablecoins issued by private companies on Ethereum (as ERC-20 tokens) and other blockchains and are pegged at 1:1 to the US Dollar;
- **Security tokens**: a sub-category of tokens representing ownership or a stake in a real-world asset, such as shares, bonds, real estate, and other assets;
- **Utility tokens**: a sub-category of tokens used within a specific ecosystem or platform to access certain services or products;
- **Governance tokens**: a sub-category of tokens granting holders the right to participate in the governance of a decentralized project or protocol.

⇒ Ethereum – Website – ERC-20
⇒ Chainlink – Website
⇒ Tether – Website
⇒ USDC – Website

4.2 Smart contracts also allow users to create **non-fungible tokens (NFT)**, that is, non-interchangeable digital objects representing a certificate of authenticity, property, or rights over other digital or physical objects as identified by the metadata encrypted in the NFT. NFTs can be easily created on Ethereum using standard ERC-721 or ERC-1155. The most common use cases for NFTs include digital art, collectibles, and gaming.

⇒ Ethereum – Website – ERC-721
⇒ Ethereum – Website – ERC-1155

4.3 Smart contracts make it possible to develop complex **decentralized software applications (dApps)**. Compared to other software applications, which are hosted on centralized servers controlled by a single entity, dApps are deployed on blockchains and operate without any intermediation. As they are encrypted on public blockchains, the software code of dApps is public and transparent and can be audited, improved, and verified by any user.
Complex dApps have been developed in the field of finance to offer blockchain users **decentralized financial services (De-Fi)**, which are reshaping finance by providing decentralized alternatives to banking, trading, lending, and investing. Examples include:

- **decentralized cryptocurrency marketplaces** such as Uniswap (built on Ethereum for ERC-20 token swaps) and SushiSwap (built on Ethereum and available on other blockchain platforms);
- **decentralized NFT marketplaces**, such as Opensea and SuperRare (Ethereum);
- **decentralized platforms for borrowing and lending**, such as Aave and Compound (both built on Ethereum but also available on other blockchains);
- **decentralized staking platforms**, such as Lido (Ethereum and other blockchains);

and much more.

The growing phenomenon of De-Fi and its impact on traditional finance will be examined in OKP, Part B, Chapter 4.

⇒ Uniswap – Website
⇒ SushiSwap – Website
⇒ Opensea – Website
⇒ SuperRare – Website
⇒ Aave – Website
⇒ Compound – Website
⇒ Lido – Website

4.4 Another application of smart contracts is the creation of **decentralized autonomous organizations (DAOs)**. These are digital entities run and governed by software code encoded on the blockchain, whose decisions are made through a voting process that takes place on the blockchain and involves the holders of specific fungible or non-fungible tokens as voters. Typically, the decisions to be voted on are **self-executing programs**: once approved, the decision is automatically executed by a smart contract.

The governance model of DAOs is often used in De-Fi to manage decentralized protocols.

DAOs represent a revolutionary shift in how organizations are governed and managed, allowing for decentralized, transparent, trustless, and self-executing decision-making. While they offer many benefits, including greater efficiency, community involvement, and accessibility, DAOs are still evolving and face challenges related to security, governance, and scalability. Nonetheless, DAOs have the potential to transform industries and redefine the concept of organizational governance, especially in the field of finance, as **DAO smart contracts can be used to raise funds and collectively manage any kind of asset that is represented by tokens on the blockchain**.