EU Blockchain
Observatory and Forum

Blockchain for beginners- basic guiding principles

About this guide

This guide is designed to provide novice learners with an introductory understanding of blockchain technology. As we release this guide, it's important to acknowledge the ever-evolving landscape of the blockchain ecosystem. Blockchain is a field characterized by rapid advancements, continuous innovation, and shifting regulatory landscapes. This guide, as comprehensive as it is at the time of publication (April 2024), represents a snapshot of a dynamic and fast-paced domain.

This guide has been produced by the EU Blockchain Observatory and Forum team:

- Marianna Charalambous, University of Nicosia, and
- Tonia Damvakeraki, Netcompany-Intrasoft.

Note

All mistakes and omissions are the sole responsibility of the authors of this guide.

Disclaimer

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the European Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for any use which may be made of the information contained herein.

Blockchain for beginners

Table of Contents

Table of Figures

A-Z Glossary of Blockchain Terms

Bitcoin: A cryptocurrency, the first and most renowned application (use case) of blockchain technology, specifically within financial services.

Blockchain: A tamper-proof, shared digital ledger that records transactions in a decentralized peer-to-peer network. The permanent recording of transactions in the blockchain permanently stores the history of asset exchanges between the peers (participants) in the network.

CBDC: A Central Bank Digital Currency is a form of digital money, issued by a central bank.

Centralization: When a single entity, such as a bank or land registry, maintains control over transaction records and data.

Consensus Mechanism: A consensus mechanism is a way to achieve agreement on a single data value among distributed processes or systems. In the context of blockchain, it's a set of rules or protocols that decide on the validity of the information added to the ledger.

Consortium Blockchain: It is used by organizations to enable private transactions among a circle of trusted participants, often spanning different corporate entities and geographical locations.

Cryptography: A set of techniques and algorithms that ensure the security and integrity of data stored and transmitted on a blockchain network. Cryptography plays a crucial role in maintaining the decentralized, transparent, and tamper-proof nature of blockchain systems.

Decentralization: Eliminates the need for gatekeepers and the vulnerabilities of single points of failure

DeFi: Decentralized Finance

Digital Signatures: Digital signatures are used to authenticate valid transactions.

dPoS: Delegated Proof of Stake, a type of consensus mechanism that is a democratic version of PoS. Stakeholders vote for a few delegates who manage the blockchain on their behalf.

Hash Function: A mathematical function commonly used to verify the integrity of data, by transforming identical data to a unique, representative, fixed-size digest.

Hybrid Blockchain: It combines elements of both private and public blockchains. It attempts to use the best features of both worlds to cater to specific business needs.

Interoperability: The ability of blockchain networks to communicate with each other, sending and receiving messages, data, and tokens

Ledger: A ledger is a distributed, tamper-proof record, of all transactions that have ever taken place on the blockchain. It is a shared, synchronized database that is maintained by several computers (nodes). This means that no single entity has control over the ledger, and it is extremely difficult to alter or forge entries. The ledger is a crucial component of blockchain technology because it allows for secure and transparent transactions. Anyone with access to the ledger can view the entire history of transactions, which makes it impossible for any participant to cheat or double-spend. This transparency is essential for building trust in the system.

Virtual Worlds (Metaverse): The product of a technology-driven shift with generalized impact through persistent and adaptable digital experiences.

Mining: The trust system in Bitcoin relies on computing power. Transactions are grouped into blocks, and it takes a lot of computing effort to prove (or "confirm") these blocks. However, once confirmed, they require only a little effort to verify as “proven”. This validation process is known as mining. Mining generates new bitcoins in each block, in the same way that a central bank prints new money.

MiCA: Markets in Crypto-Assets (MiCA) is a regulation in EU law, designed to bring clarity to the crypto-assets market. It is intended to help streamline distributed ledger technology (DLT) and virtual asset regulation in the EU whilst protecting users and investors. With MiCA, the EU has become the first leading jurisdiction globally to roll out a detailed regulation framework for the sector.

Nick Szabo: A computer scientist, who conceptualized 'bit gold', a decentralized digital currency that, although it was never realized, foreshadowed the structure of Bitcoin.

NFTs: Non-Fungible Token, is a type of digital asset distinct in its uniqueness and non-interchangeability with other digital tokens.

Node: A node is a device, typically a computer, which runs the blockchain's software and maintains a copy of the blockchain's transaction history. Nodes are responsible for validating transactions, ensuring their authenticity and adherence to the blockchain's rules. They also play a crucial role in broadcasting new transactions to the network and ensuring the integrity and consistency of the blockchain's data.

Permissioned Blockchain: In permissioned blockchains not anyone can join the network. Permission is provided to certain identifiable participants to join the network. They often have a level of privacy and control that is not present in permissionless systems. This can be particularly useful for consortia of businesses that wish to transact privately.

Permissionless Blockchain: In permissionless blockchains, there are no gatekeepers, and all transactions are public. This type of blockchain supports an environment where anyone can create an address and begin interacting with the network.

PoW: Proof of Work, a type of consensus mechanism used by Bitcoin, where miners solve complex mathematical puzzles to validate transactions and create new blocks. The first one to solve the puzzle gets to add the block to the blockchain and is rewarded with cryptocurrency.

PoS: Proof of Stake, a type of consensus mechanism where participants 'stake' their cryptocurrency as a form of security. Validators are chosen to create a new block based on the amount they stake and other factors. It is more energy efficient than PoW.

PoA: Proof of Authority, a type of consensus mechanism where transactions and blocks are validated by approved accounts, known as validators. It is faster and more energy-efficient but less decentralized.

Private Blockchain: Private blockchains are not open to the public and participation requires an invitation or permission. They provide more control over the participants and transactions.

Public Blockchain: Public blockchains such as Bitcoin and Ethereal are decentralized platforms that anyone can access and participate in. They are open for anyone to join, transact on, and participate in the consensus process.

Satoshi Nakamoto: A pseudonym for the individual or group of individuals that created Bitcoin in 2009.

1 Introduction to Blockchain

1.1 What is Blockchain: Definition and Basics

Centralization is a fundamental aspect of today's record-keeping systems, where a single entity, such as a bank or land registry, can control transaction records and data. This centralized structure is so ingrained in our societal operations that it often goes unquestioned, managing everything from financial transactions and property ownership to personal medical records and national IDs. However, reliance on a central authority raises concerns about trustworthiness, given the risks of corruption, hacking, and business failures. Central record-keepers also function as gatekeepers, deciding who can access and transact within these systems, thus wielding considerable power over participation and data accessibility.

In contrast, **decentralized systems** eliminate the need for gatekeepers and the vulnerabilities of single points of failure. Such systems offer a robust alternative by allowing parties to interact peer-to-peer without an intermediary. Notable examples include the Internet, which enables global, decentralized communication, and **blockchain networks** like Bitcoin, which eases trustless financial transactions. These decentralized platforms demonstrate the potential for secure, peer-to-peer interactions, even among parties who do not know or inherently trust one another, marking a significant shift from the traditional, centralized paradigms.

The Internet fundamentally reshaped our world by creating a new foundational infrastructure that democratized the exchange of information. This shift led to two transformative processes: disintermediation, which phased out players that failed to adapt, and cybermediation, giving rise to innovative business models that were previously inconceivable, like Instagram, Netflix, and Airbnb.

Similarly, blockchain is poised to revolutionize our world by democratizing the exchange of value and trust. While it may start with transitioning existing e-commerce to blockchain-enabled commerce, it can lead to the elimination of redundant intermediaries and the emergence of new business models and industries that leverage the unique properties of blockchain.

In terms of what can be built on blockchain, there are native blockchain applications that couldn't have existed without this technology, promising exponential advancements, and the potential to disrupt existing industries significantly. As we stand on the cusp of this innovation wave, the full potential of blockchain applications is only beginning to be realized.

Blockchain is a technology that has the potential to create new foundations for our economic and social systems. It is a shared, immutable ledger (a complete record of a business's economic activities, usually used to keep track of the transfer of money and asset ownership) for recording the history of transactions. The technology is used to record transactions and track assets in a business network. An asset can be tangible (like a house, car, cash, or land) or intangible (intellectual property, patents, copyrights, branding).

A blockchain is essentially a tamper-proof, shared digital ledger that records transactions in a decentralized peer-to-peer network. The permanent recording of transactions in the blockchain stores permanently the history of asset exchanges that take place between the peers (participants) in the network.

1.2 Historical Background

The roots of blockchain technology go back much further than its current link to digital currencies. The groundwork for blockchain was laid in the early '90s by researchers Stuart Haber and W. Scott Stornetta. They

developed an early prototype for a system that would securely timestamp digital documents, preventing any possibility of backdating or alteration, effectively setting the stage for later blockchain frameworks. In 1998, a computer scientist, Nick Szabo conceptualized 'bit gold', a decentralized digital currency that, although never realized, foreshadowed the structure of Bitcoin.

It wasn't until 2009 that blockchain found its first significant application with the creation of Bitcoin by the pseudonymous Satoshi Nakamoto. Bitcoin was groundbreaking; it was the first technology to prevent the issue of double spending in a digital currency without relying on any central authority, due to its transparent and immutable ledger system.

In the years following Bitcoin's debut, blockchain applications have proliferated far beyond the realm of cryptocurrency. Today, it's being used to create impenetrable voting systems, enhance supply chain transparency, and even verify identities and property ownership. Through this evolution, blockchain has transitioned from an abstract idea to a transformative technology, fundamentally altering the landscape of digital transactions and data management.

1.3 Why Blockchain Matters: Key Advantages

Blockchain technology marks a transformative shift in the digital landscape, introducing a multitude of benefits that highlight its importance. Its foremost feature is its decentralized nature. In contrast to the centralized governance of traditional databases, blockchain spreads its data across a vast array of computers. This distribution fortifies the system against failures and attempts at centralized manipulation, ensuring that no individual or group can wield unilateral power over the data, thereby making the process of data management more democratic and secure.

Additionally, the fundamental structure of blockchain promotes both transparency and an enduring record of data. Altering recorded data on a blockchain is highly challenging, providing a durable and trustworthy ledger of transactions that is critical for areas like financial services and supply chain operations, where the accuracy of historical records is non-negotiable. This transparency gives every network participant equal insight, fostering trust where it is often difficult to secure. The distinctive benefits offered by blockchain technology not only revolutionize safeguarding data and upholding its integrity but also open doors to groundbreaking uses across various sectors, including but not limited to finance and healthcare.

A summary of the key advantages of blockchain technology, demonstrating how blockchain can offer unique benefits over traditional centralized systems:

- **Peer-to-Peer Transactions:** Blockchain enables transactions directly between participants without the need for intermediaries, streamlining processes and potentially reducing costs.
- **Distributed Network:** The blockchain network consists of its participants, distributing data across multiple nodes, which enhances data integrity and resilience against failures or attacks.
- **Reliability:** The significant amount of replication in blockchain networks ensures a high degree of data accuracy and consistency.
- **Censorship Resistance:** No single party has control over the data flow in a blockchain, making it resistant to censorship and unilateral alterations.
- **Public Verification:** In many blockchains, transactions are publicly available and verifiable, promoting transparency.
- **Open/Permissionless Access:** Many blockchain networks are open, allowing anyone to participate, which fosters inclusivity and broadens access.

- **Immutability:** Once recorded, transactions on a blockchain may become permanent and unalterable, ensuring the longevity and unchangeability of records.

1.4 The case of Bitcoin

There is a common misconception that Bitcoin and blockchain are synonymous, but this is not the case. Bitcoin represents the first and most renowned application of blockchain technology, specifically within the realm of financial services.

Bitcoin's emergence mirrors a pattern of technological revolutions that Marc Andreessen eloquently described. Initially perceived as a mysterious novelty, Bitcoin, much like personal computers in 1975 and the Internet in 1993, was the culmination of two decades of rigorous research by nearly anonymous individuals. Initially met with scepticism by some and perceived as a tool for liberation by others, Bitcoin captivated technologists and innovators who recognized and nurtured its potential. Over time, it evolved into a technology with profound mainstream impact, leading many to retrospectively acknowledge its transformative promise.

The trust system in Bitcoin relies on computing power. Transactions are grouped into blocks, and it takes a lot of computing effort to prove (or "confirm") these blocks. However, once confirmed, they require only a little effort to verify as “proven”. This validation process is known as mining.

Mining generates new bitcoins in each block, the same way that a central bank prints new money. The quantity of new bitcoins created is predetermined and decreases over time. Mining builds trust by ensuring that transactions are only confirmed if a significant amount of computational work has been put into the block containing them. The more blocks added, the more computing work is required, which in turn strengthens the trust in the system.

> “[...] Bitcoin gives us, for the first time, a way for one Internet user to transfer a unique piece of digital property to another Internet user, such that the transfer is guaranteed to be safe and secure, everyone knows that the transfer has taken place, and nobody can challenge the legitimacy of the transfer. The consequences of this breakthrough are hard to overstate.”
>
> Marc Andreessen, Why Bitcoin Matters, The New York Times, 2014

The evolution of Bitcoin, the first decentralized cryptocurrency, is a testament to the evolution of blockchain technology:

- 2008: The journey began with the registration of bitcoin.org by Satoshi Nakamoto and Martti Malmi. Nakamoto released the seminal Bitcoin white paper later that year, laying the foundation for a decentralized currency.
- 2009: Bitcoin officially came into existence as Nakamoto mined the first block, known as the genesis block, and released Bitcoin software. The first Bitcoin transaction occurred this year, marking a new era in digital transactions.
- 2010: Bitcoin's first commercial transaction took place, famously involving the purchase of two pizzas for 10,000 BTC. At that time, the value of those Bitcoins was about $41. This year also witnessed the launch of the first Bitcoin exchange and the start of pooled mining.
- 2011-2013: The Bitcoin Foundation was established. Bitcoin underwent its first halving, where the reward for mining a new block was halved from 50 Bitcoins per block to 25 Bitcoins per block. The cryptocurrency's popularity surged, with significant growth in mining difficulty and market capitalization. The University of Nicosia became the first university in the world to accept Bitcoin for tuition payment.

- 2014-2015: The Court of Justice of the European Union issued its first-ever ruling on Bitcoin, stating that it was indeed a currency and a means of payment, not a commodity or an asset (as some argued). Bitcoin was also exempt from VAT. Regulatory advancements included the issuance of the 'BitLicense' in New York. NASDAQ adopted blockchain technology for securities, reflecting growing mainstream interest.
- 2016-2017: The second halving event occurred where the reward for mining a block was halved from 25 to 12.5 Bitcoins. Bitcoin's value skyrocketed to nearly $20,000. Bitcoin Cash (BCH) emerged from a hard fork, as a result of debates and disagreements about how to scale Bitcoin.
- 2018-2019: Bitcoin experienced volatility, with notable endorsements and incidents such as the collapse of a major cryptocurrency exchange, emphasizing the importance of secure key management.
- 2020-2021: The third halving took place amidst economic uncertainty, with Bitcoin proving its resilience. Tesla's investment in Bitcoin and El Salvador's adoption of it as legal tender were major highlights. Bitcoin reached its all-time high of $69,000 in November 2021 before falling below $16,000 a year later.
- 2022-2023: The cryptocurrency's price dropped and then saw a resurgence, displaying both its volatility and enduring appeal.

As the most prominent application of blockchain technology, Bitcoin's evolution has been instrumental in demonstrating blockchain's potential beyond a mere digital ledger. Tracing its roots from an innovative idea to a globally recognized cryptocurrency, Bitcoin exemplifies the transformative power of blockchain.

2 Understanding the Fundamentals

2.1 How does Blockchain work

2.1.1. Decentralization

Blockchain decentralization is a “paradigm shift” from centralized systems. It distributes power and control across a network, enhances security, and promotes transparency. This technology has far-reaching implications beyond cryptocurrencies, including supply chain, healthcare, and more, where trust and security are paramount.

The key concepts of decentralization include:

Distributed Ledger
Traditional System: In a traditional, centralized system, e.g., a bank, all records are stored in one place. If this central point fails or is attached, the entire system is compromised. Blockchain System: In a blockchain, the ledger is spread across many computers – called “nodes”. Each node has a full copy of the ledger, ensuring no single point of failure.
Consensus Mechanism
Decision Making: Instead of a central authority (e.g., a bank manager), deciding on transactions to be made, in blockchain the transactions are agreed upon by consensus among the nodes.

Process: When a new transaction is made, it is broadcast to the entire network. The nodes verify the transaction based on preset/pre-agreed rules and add it to their ledger copy if it is valid (approved).
Security and Trust
Cryptography: Each block in the blockchain is secured using complex mathematical algorithms, making it extremely difficult to alter previously created records. Trust: As every node has the same version of the ledger and follows strict rules for validation, trust is established -not through a central authority, but through the network's collective agreement.
Transparency and Immutability
Transparency: every transaction on the (public) blockchain is visible to anyone who accesses it, promoting transparency. Immutability: once a transaction is added to the blockchain, it is not possible to have it altered or deleted, thus ensuring the integrity of the ledger.

Figure 1: The Key concepts of decentralization

A practical example of how decentralization works on blockchain is Bitcoin (see previous section). Bitcoin is a digital currency built on blockchain. There is no central bank controlling it; instead, transactions are verified by a global network of nodes, making it decentralized.

2.1.2. Cryptography

To grasp what Cryptography entails, think of it as a tamper-proof seal on a jar. If the seal is broken (akin to the cryptographic rules being violated), the contents of the jar might have been tampered with. Just like how the seal protects the jar, cryptography protects the information on the blockchain.

When we discuss blockchain cryptography, this entails the following components:

Digital Signatures: the purpose of digital signatures is to ensure security and authenticity. To achieve this, when a user makes a transaction, they sign it with their private key (a secret code known only to them, also known as Privkey). Others can use the sender's public key (a code that everyone can see, also known as Pubkey) to verify that the transaction was indeed created by the rightful owner of the private key. Imagine the public key as something like a bank account number, and the private key as a secret PIN or a signature on a check, which gives you control over the account.

Hash Functions are used to maintain the integrity and the order of the blockchain. In practice, a hash function is like a digital fingerprint for data. It takes any input (like a block of transactions) and produces a fixed-size string of characters, which is unique to that specific input. Any small change in the input data changes this hash drastically. Each block in the blockchain contains the hash of the previous block, creating a secure link.

Blockchain Cryptography is important because it provides **security** using private keys, i.e., ensures that only the owner of the key can authorize transactions. It also provides **integrity**, as the hash functions make it extremely difficult to alter any information on the blockchain without being detected. As previously mentioned, we also get **decentralization**, as the same cryptographic rules apply to every copy of the blockchain, thus ensuring consistency across the network, without the need for a central authority.

It is still important to note that although blockchain cryptography is highly secure, it's not completely foolproof. It depends on the robustness of the algorithms used and the secrecy of the private keys.

2.1.3. Consensus Mechanisms

A consensus mechanism is a way to achieve agreement on a single data value among distributed processes or systems. In the context of blockchain, it's a set of rules or protocols that decide on the validity of the information added to the ledger. This is crucial because it ensures that all participants in the network agree on the current state of the ledger.

Types of Consensus Mechanisms:

Proof of Work (PoW):

- Used by Bitcoin.
- Miners solve complex mathematical puzzles to validate transactions and create new blocks.
- The first one to solve the puzzle gets to add the block to the blockchain and is rewarded with cryptocurrency.
- Very secure but requires a lot of energy.

Proof of Stake (PoS):

- Participants 'stake' their cryptocurrency as a form of security.
- Validators are chosen to create a new block based on the amount they stake and other factors.
- More energy efficient than PoW.

Delegated Proof of Stake (dPoS):

- A democratic version of PoS.
- Stakeholders vote for a few delegates who manage the blockchain on their behalf.

Proof of Authority (PoA):

- Transactions and blocks are validated by approved accounts, known as validators.
- Faster and more energy-efficient but less decentralized.

To better understand the concept of Consensus Mechanisms, picture a group of stakeholders who share a notebook. Each time one of the stakeholders wishes to add one note, they should follow specific rules:

- In PoW, they need to solve a difficult puzzle to earn the right to add the note.
- In PoS, they need to show they have a certain number of pages in the notebook (their stake) to be chosen randomly to add the note.
- In DPoS, everyone votes on a few people who will have the right to add notes.
- In PoA, only a few trusted people have the pen to write in the notebook.

Regardless of the type of the Consensus Mechanism, this ensures that everyone agrees on what is written and no one can cheat. The consensus mechanism makes sure that all the notes (transactions) are valid and agreed upon by everyone.

2.2 Blockchain vs Traditional Databases

Traditional databases

When discussing traditional databases, we acknowledge that there is management and control over all the data by a single entity or organization. Regarding data structure, data is typically stored in tables or in a structured format, which can be easily modified or deleted by those with access. Access and security to the database are controlled by the administrator, and security is maintained through passwords, firewalls, and other security measures. In such databases, data can be easily added, modified, or deleted, while at the same time, it is not possible to trace the original data unless there are specific audit trails.

Traditional databases are used for storing, retrieving, and managing data in various applications like banking systems, inventory systems, websites, etc.

Blockchain

Blockchain is a decentralized system that doesn't have a single point of control. Instead, it is maintained by a network of nodes (computers), each holding a copy of the ledger. The data is stored in blocks, and each block is connected to the previous one, forming a chain. This makes it extremely difficult to alter records. Every transaction taking place on the blockchain is transparent and can be seen by everyone in the network. The use of cryptographic techniques ensures that data is secure and tamper-proof. Once data (or a transaction) is added to the blockchain, it cannot be altered or deleted. This ensures a high level of data integrity and trust.

Blockchain is widely used for cryptocurrency transactions like Bitcoin and Ether. Still, there are several other uses, in areas like supply chain management, voting systems, and anywhere where transparency and security are crucial.

Key Differences in Simple Terms

Control: Traditional databases are like a personal diary kept and managed by one person. Blockchain is like a shared ledger where entries made by anyone are visible to everyone and cannot be erased.

Security: Think of traditional databases as a bank vault that is secure but managed by the bank itself. Blockchain is like a transparent safe where everyone can see what's inside, but no one can change or remove anything once it's put in.

Data Modification: In a traditional database, you can easily change past entries (like editing a Word document). In blockchain, once something is written, it's more like writing in pen on a piece of paper – it cannot be erased.

For selecting the technology that would best serve the user needs or application, it is essential to understand the above differences.

When to Use Blockchain

As elaborated in the previous sections, Blockchain and traditional databases serve different purposes and have distinct characteristics; therefore, the selection between them depends on the specific requirements of your application.

Blockchain would be a better option for the following cases:

- **Immutable and tamper-proof records:** Blockchain is designed to provide an immutable and tamper-proof ledger. If your application requires a trustless and transparent record-keeping system where data once written cannot be altered, blockchain is a better choice.
- **Decentralization and trustlessness:** If you need a system that operates without a central authority or intermediary, blockchain's decentralized nature can be advantageous. It allows multiple parties to participate in a network without relying on a central entity to maintain and validate data.
- **Transparency and auditability:** Blockchains are transparent, and every transaction or change to the data is recorded in a public ledger. This transparency can be crucial in industries like supply chain management, where stakeholders want to trace the origins of products or verify the authenticity of records.
- **Smart contracts:** Blockchain platforms like Ethereum enable the use of smart contracts, self-executing contracts with predefined rules and conditions. If your application relies on automation and trust in contract execution, blockchain-based smart contracts can be valuable.
- **Cryptographic security:** Blockchain technology leverages cryptographic techniques for securing data and transactions. This can be advantageous when dealing with sensitive information or when strong security guarantees are required.
- **Cross-organizational trust:** In situations where multiple organizations or parties need to collaborate and share data while maintaining trust, a blockchain can be a suitable solution. It ensures that all participants have equal access to the same data and can independently verify its integrity.
- **Cryptocurrency or token management**: If your application involves managing digital assets like cryptocurrencies or tokens, blockchain is essential as it provides the infrastructure needed for their creation, transfer, and security.
- **Use cases requiring consensus:** In applications where achieving consensus among multiple parties is crucial, blockchain's consensus algorithms can be beneficial. These algorithms ensure that all participants agree on the state of the system.

Blockchain may be a useful technology, but it is important to bear in mind the limitations, including scalability, performance, and cost considerations. Traditional databases may be more suitable for applications that require high-speed data processing, and low latency, or do not require the features provided by blockchain. In certain cases, there is also a possibility for a hybrid approach, combining both technologies to leverage the strengths provided by each of them.

3 Types of Blockchain

Blockchains have transcended their initial role as platforms for peer-to-peer payments, expanding into a diverse ecosystem that supports a wide range of organizational functions. This evolution has transformed them from a simple 'internet of money' to a robust 'internet of value.' Beyond the well-known open, public, and permissionless blockchains like Bitcoin and Ethereum, there exists a variety of blockchains including public, private, permissioned, permissionless, and hybrid models. Each type is designed to fulfill specific needs, adhere to rules, and utilise distinct protocols, offering a spectrum of advantages and challenges tailored to various use cases.

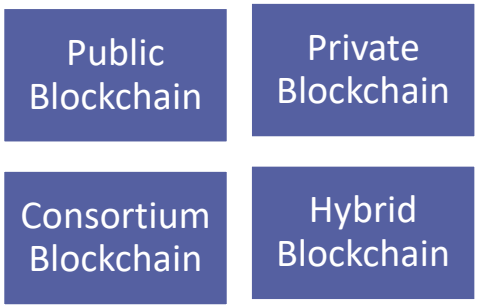

Figure 2: Four main types of blockchain technology

3.1 Public vs Private Blockchains

Public blockchains are decentralized platforms that anyone can access and participate in. Unlike private blockchains that are restricted and often managed by single organizations, public blockchains like Bitcoin and Ethereum are open for anyone to join, transact on, and participate in the consensus process. This openness, however, comes with trade-offs in terms of scalability and privacy. *Private blockchains*, on the other hand, are not open to the public and participation requires an invitation or permission. These blockchains provide more control over the participants and transactions, which can be beneficial for businesses with privacy concerns or for those needing to comply with specific regulatory standards.

3.2 Permissionless vs Permissioned Blockchains

In *permissionless blockchains*, there are no gatekeepers, and all transactions are public. This type of blockchain supports an environment where anyone can create an address and begin interacting with the network. Permissionless blockchains are generally public, though not all public blockchains are necessarily permissionless. In public and permissionless blockchains any individual has the liberty to join or exit the network, partake in transaction validation, or engage in the mining process. Participants can independently maintain a full copy of the blockchain, ensuring total transparency and public verification of all transactions. These networks avoid the conventional barriers of credentials or identity verifications, allowing anyone to become a part of the network simply by downloading the necessary software. In such an ecosystem, the trust is placed in the blockchain protocol itself rather than in any individual operator, fostering a truly decentralized environment. The most well-known examples of public and permissionless blockchains include Bitcoin (2009) and Ethereum (2015). These public and permissionless networks have their own native currency/asset: bitcoin for the Bitcoin blockchain, and ether for the Ethereum blockchain.

In *permissioned blockchains* not anyone can join the network. Permission is provided to certain identifiable participants to join the network. They often have a level of privacy and control that is not present in permissionless systems. This can be particularly useful for consortia of businesses that wish to transact privately. They designate who is authorized to operate a node, validate new transactions, and gain access to, or exert influence over, various segments of the blockchain. Additionally, these blockchains restrict the ability to implement changes to the system, ensuring that only approved individuals or entities can modify the protocol. Two well-known examples of Permissioned blockchain are Hyperledger Fabric and Ripple.

3.3 Consortium Blockchains

Consortium blockchains are used by organizations to enable private transactions among a circle of trusted participants, often spanning different corporate entities and geographical locations. Notable examples include R3 Corda and Quorum. The Enterprise Ethereum Alliance furthers this concept by working towards a standardized Ethereum-based framework tailored for varied enterprise applications like finance and supply chain, boasting a robust membership of over 450 businesses, including prominent names like Microsoft and Intel.

3.4 Hybrid Blockchains

Hybrid blockchains combine elements of both private and public blockchains. They attempt to use the best features of both worlds to cater to specific business needs. For example, a hybrid blockchain might allow control over who can participate in the blockchain network while still allowing certain transactions to be visible on a public blockchain system. These hybrid systems are not as open as public blockchains but offer more transparency than private blockchains. This type of blockchain is particularly appealing to businesses that require transaction privacy but still need to maintain a level of transparency with regulators or the public. Some well-known examples of hybrid blockchains are Dragonchain and Kadena.

4 Blockchain Use Cases

4.1 Finance and Cryptocurrency

Finance is a broad field that deals with managing money, investments, and financial resources. It encompasses various activities and concepts, including personal finance, investing, banking, insurance and financial markets.

- Personal finance involves managing one's own money, budgeting, saving, and making financial decisions to achieve financial goals. It includes concepts like saving for retirement, paying off debt, and creating an emergency fund.
- Investing involves using money to buy assets like stocks, bonds, real estate, or mutual funds with the expectation of earning a profit. Investors typically aim to grow their wealth over time through smart investment choices.
- Banking services include opening and managing bank accounts, using credit cards, and accessing loans. Banks provide a safe place to store money, facilitate transactions, and offer various financial products and services.
- Insurance protects individuals and businesses against financial losses due to unexpected events, such as accidents, illnesses, or disasters. Common types of insurance include health insurance, auto insurance, and home insurance.

- Financial markets are platforms where various financial instruments are bought and sold. Stock exchanges, bond markets, and commodity markets are examples. They play a crucial role in the global economy.

Cryptocurrency is a relatively new and quite disruptive development within the financial world. It is a type of digital or virtual currency that uses cryptography for security. Some of the main characteristics of cryptocurrencies are:

- Cryptocurrencies exist only in digital form, and they are not physically tangible like traditional money (e.g., cash or coins). They are stored in digital wallets, which can be software-based or hardware-based.
- They operate on blockchain technology, which is a decentralized and distributed ledger (see previous sections for details). This technology ensures transparency, security, and immutability of transactions.
- Contrary to what we know about traditional currencies controlled by governments and central banks, cryptocurrencies are decentralized. This means that there is no single entity that has control over the currency, and transactions are verified by a network of participants (nodes).
- Some cryptocurrencies, like Bitcoin, use a process called mining to validate and add transactions to the blockchain. Miners use powerful computers to solve complex mathematical puzzles, and in return, they are rewarded with new cryptocurrency coins (see previous sections for details).
- Cryptocurrencies can be used for various purposes, including online purchases, and investment, as well as a means of transferring value across borders quickly and with lower fees compared to traditional banking methods.
- Cryptocurrency prices can be highly volatile, with significant fluctuations in value over short periods. This presents both opportunities and risks for investors and users.

Finance and cryptocurrency share a connection while also maintaining their identities within the realm of monetary matters and investment. They each present a range of prospects and hurdles.

4.2 Supply Chain Management

We meet blockchain technology as part of the supply chain management process more and more these days, especially as the technology is key for enhancing transparency, traceability, and security throughout the entire supply chain.

Blockchain allows for the creation of a tamper-proof, immutable ledger that records every transaction or event in the supply chain. This enables **end-to-end visibility**, making it easier to **track the origin**, production, and movement of products. This is particularly useful for industries where traceability is critical, such as in the food and pharmaceutical industries.

Through blockchain, companies can ensure the **authenticity** of products and components. Products are assigned unique digital identifiers (e.g., a serial number or QR code) that are recorded on the blockchain. Consumers and other involved stakeholders can verify the authenticity of a product by scanning the code.

Smart contracts are self-executing agreements with the terms of the contract written into code. In supply chains, smart contracts can automate various processes such as payment, quality control, and delivery when predefined conditions are met, thus reducing the need for intermediaries. In addition, the transparency and security of blockchain can help in decreasing counterfeiting allowing both companies and consumers to verify the authenticity of products at any point in the supply chain.

Other benefits of blockchain include:

- the optimization of inventory levels and the facilitation of supply-chain financing, through real-time data monitoring of goods.
- Data recorded on the blockchain can also include information about the products and materials' quality, thus ensuring that only high-quality resources are used in manufacturing, reducing defects and potential recalls. This is essential for industries that need to comply with strict regulatory requirements.
- Tracking of environmental and sustainability performance and impact through supply chain operations, i.e., carbon emissions, water usage, etc.
- Management and verification of suppliers' performance and credentials/ qualifications. This is useful for making responsible selection of ethical and reliable partners.

4.3 Healthcare

Blockchain technology is currently used by the healthcare industry in various applications, from sharing clinical trial data to managing patients' records. Some of the most common and highly effective applications include:

Electronic Health Records (EHRs) are both secure and interoperable, providing a secure and standardized way to store and share electronic health records, ensuring that patient data is both protected and easily accessible to any authorized parties. This allows patients to have more control over who can access their health and insurance data.

Medical data sharing, for example, research and clinical trials results can be shared in a secure and transparent manner. Data is anonymised but both integrity and patient privacy are secured.

Medical supply chain management, i.e., drug traceability for the entire pharmaceuticals supply chain is made possible, by ensuring authenticity and quality of drugs, reducing counterfeits, and improving safety.

Patient consent management is maintained through smart contracts on a blockchain, allowing patients to have better control of their data and how they are used.

Telemedicine and remote monitoring through **secure communication**, facilitated by blockchain. The technology can ensure secure and private communication between healthcare providers and patients in telemedicine consultations and remote monitoring.

Management of healthcare providers' credentials. Blockchain can store and verify credentials of healthcare professionals, ensuring that practitioners have all necessary qualifications.

Processing of health insurance claims through blockchain, to help streamline and automate verification, reducing fraud.

Authentication of drug prescriptions for both patients and healthcare providers, by checking the origin and supply chain on a blockchain.

Patient-managed health records, giving them control over their medical history and allowing them to share with any healthcare providers as needed.

Encryption and access control to help enhance data security of patient information and to allow granular access control, thus reducing the risk of data breaches.

Access to a diverse range of healthcare data on a blockchain for population health studies and analytics for research and analysis purposes, while respecting privacy and security concerns.

4.4 Voting and Governance

As discussed in the use cases presented earlier, blockchain is used for enhancing transparency, security, and efficiency. Blockchain can be used for

- **Secure Voting Systems** to:
  - securely verify the identity of voters, reducing the risk of fraudulent votes.
  - record votes in an immutable and tamper-resistant manner, ensuring the integrity of the voting process.
  - enhance transparency and auditability for the entire voting process, including the counting of votes.
- **Secure and verifiable remote voting**, i.e., enabling people to vote from the comfort of their homes or remote locations.
- **Proxy voting** for shareholders in corporations or members of organizations to securely cast their votes, reducing the need for intermediaries.
- **Creating Decentralized Autonomous Organisations (DAOs),** i.e., self-governing entities that make decisions through smart contracts and voting mechanisms encoded on the blockchain.
- **Maintaining transparent and tamper-proof records** of decisions, pieces of legislation or regulations, and government processes.
- **Verifying the identities of individuals** participating in voting and governance activities, reducing the risk of identity fraud.
- **Token-based voting**, i.e., allowing stakeholders to vote in proportion to their holdings (tokens), as seen in some blockchain-based governance models.
- **Enabling decentralized decision-making,** where participants have a say in governance decisions without relying on centralized authorities.
- **Performing immutable audits** of voting and governance processes, ensuring compliance and transparency.
- **Enhancing the security** of voting and governance systems, as the immutability and decentralized nature of blockchain makes it resistant to hacking or manipulation.

4.5 Intellectual Property

Blockchain is currently used in Intellectual Property management in a number of ways:

- Blockchain can be used to establish and verify the **ownership and origin of digital assets** such as creative works, patents, trademarks, and digital media. Each IP asset can be recorded on the blockchain with a timestamp, creating an immutable and transparent record of its creation and ownership history.
- Content creators can timestamp their work on a blockchain, providing indisputable evidence of the creation date. This can be used to **establish copyright and prove ownership** in case of disputes.
- In IP management, **smart contracts can automate royalty payments, licensing agreements, and other contractual obligations.** For instance, when a piece of content is used, the blockchain can automatically trigger the payment of royalties to the creator.
- Blockchain can streamline the process of **licensing IP assets**. Smart contracts can enforce the terms of licensing agreements, ensuring that royalties are automatically and fairly distributed to creators and rights-holders based on predefined conditions and usage data.
- For physical products, blockchain can be used to **create digital certificates of authenticity**. This helps in preventing counterfeit goods and ensuring that consumers are purchasing genuine products with the associated IP rights.

- In industries like fashion and luxury goods, blockchain can **track the entire supply chain of products**, from creation to distribution. This helps in **ensuring the authenticity of products** and helps in identifying and addressing IP infringements.
- **Managing patent information**, including filing, prosecution, and maintenance, can be made more efficient using blockchain technology. This can help inventors and organizations keep a **secure and transparent record of their patents.**
- Blockchain can facilitate decentralized **marketplaces for buying and selling IP rights**, making it easier for creators and companies to monetize their intellectual property directly with others without the need for intermediaries.
- Blockchain's cryptographic and decentralized nature enhances the **security and protection of sensitive IP data**, reducing the risk of data breaches and unauthorized access.
- The transparency of blockchain allows for **easy auditing of IP transactions and rights**. This can help organizations and creators ensure that their IP assets are being used in compliance with agreements.

5 Emerging Topics in Blockchain

5.1 NFTs (Non-Fungible Tokens)

An NFT, short for Non-Fungible Token, is a type of digital asset distinct in its uniqueness and non-interchangeability with other digital tokens. Unlike fungible tokens, each NFT is cryptographically verified for its singularity and stored on a blockchain or distributed ledger, visible to all. While this isn't always the case, NFTs represent more than just digital records of an asset; they are unique digital assets. This concept is akin to how blockchain technology has enabled the creation of an" internet of value".

The history of NFTs has evolved from basic digital collectibles to complex asset ownership models. Originating with "colored coins" on the Bitcoin network in 2012, these early NFTs added specific utility to Bitcoins. The first major NFT project, CryptoPunks, launched in mid-2017 on Ethereum, featuring 10,000 unique digital characters. CryptoKitties soon followed, popularizing NFTs with a game that allowed users to breed digital cats. Today, NFTs have expanded into the realms of art, sports, and music, with platforms like SuperRare and OpenSea facilitating the trading and creation of a wide range of digital assets. Ethereum's ERC-721 is the most popular blockchain for NFTs and it serves as the basis for determining specific characteristics of NFTs:

- **Uniqueness:** NFTs are individually identifiable, with a limited number issued, like the 10,000 unique CryptoPunks.
- **Rarity:** NFT rarity takes various forms:
  - Artificial Rarity: Determined by code or specifics of issuance, like CryptoPunks' rare traits.
  - Numerical Rarity: Linked to limited issuance, like a limited number of digital art pieces.
  - Historical Rarity: Based on the NFT's historical significance or past ownership.
- **Ownership:** NFTs provide proof of ownership, potential for fractional ownership, and provenance tracking, especially for assets tied to the real world.
- **Immutability:** NFTs on blockchain are resistant to tampering, ensuring trust and transparency.
- **Programmability:** NFTs can be programmed for various purposes, including ensuring ongoing artist royalties or use as collateral in decentralized finance (DeFi) applications.

The European Union Blockchain Observatory & Forum (EUBOF) Demystifying Non-Fungible Tokens (NFTs) report provides an in-depth explanation of how NFTs work.

5.2 DeFi (Decentralized Finance)

To grasp the essence of Decentralized Finance (DeFi), it's crucial to first explore its counterpart in the financial world: Traditional Finance, or TradFi. The term 'TradFi' refers to the conventional financial services industry, covering a broad spectrum of activities like money management, credit, banking, and investment. At the heart of TradFi are centralized institutions, often termed as CeFi (Centralized Finance), which function as intermediaries in various financial transactions. This sector is typified by two primary characteristics: a custodial approach where assets are entrusted to CeFi entities for management and safekeeping, and a permissioned nature requiring verified identity for participation. Despite its long-standing role in economic growth, TradFi has significant drawbacks. Financial exclusion remains a major issue, with approximately 1.7 billion people worldwide lacking access to a bank account. This scenario is prevalent even in developed regions, including Europe and the United States. Additionally, TradFi is plagued by high transaction costs and slow processing times, particularly in remittances, currency manipulation, capital controls, lack of transparency, and systemic risks like financial crises and bank runs.

In contrast, DeFi represents a paradigm shift. Operating on decentralized, open, and peer-to-peer models through smart contracts on blockchains, DeFi bypasses traditional intermediaries. It's not just a fintech evolution but a radical reimagining of financial services, offering lending, borrowing, and trading of assets in a P2P manner. DeFi can not only replicate traditional financial services but also foster novel business models unfeasible in the realm of TradFi.

Figure 3: Functional differences of TradFi and DeFi (Source: EUBOF DeFi report)

Feature	TradFi	DeFi
Accounting	Double-entry accounting bookkeeping.	Triple-entry accounting bookkeeping.
Trust	Trusted. Identity-based systems.	Mostly trustless.
Data availability	Transaction history is private. User is known.	History of financial transactions is publicly open. User is (pseudo)anonymous.
History and characteristics	Established. Slow and rigid in terms of innovation.	Nascent. Incrementally/radically innovative. Constantly changing, often faster than regulation can keep up with.
User experience	Easy to use. Embedded in everyday life.	Often difficult to use. More technical competency is required.
Risk	Risks are managed and thoroughly regulated.	Requires an individual understanding of the underlying risks.
Reversibility	Reversible transactions. Amend permissions.	(Mostly) irreversible transactions. Append only.

DeFi, running on public blockchains, is distinguished from the private networks of TradFi by several key features. It is open, permissionless, and resistant to censorship, allowing anyone to participate without identity verification or authorization, and preventing any single entity from blocking valid transactions. DeFi operates on a peer-to-peer basis, eliminating the need for intermediaries. Its decentralized nature means multiple independent network participants validate transactions, ensuring enhanced security and reliability.

Additionally, DeFi is characterized by its public, verifiable transactions, immutable transaction history, and lack of geographical constraints, making it a truly global financial solution.

DeFi, while offering revolutionary financial services, carries inherent risks. These include technology risks, such as failures in the DeFi protocols due to issues with their technological infrastructure. Project risks are also prevalent, originating from the unique characteristics of each DeFi application while economic and governance risks arise from the management styles of these apps. DeFi has seen considerable growth, yet it still is an emerging field marked by distinct risks and a regulatory landscape that is still developing.

The European Union Blockchain Observatory & Forum (EUBOF) Decentralized Finance (DeFi) report provides an in-depth explanation of DeFi.

5.3 Virtual Worlds

Defining Virtual Worlds (or Metaverse) is challenging; hence, a lot of different definitions exist.

- *"The metaverse seems to be whatever people's imaginations dream it to be." - McKinsey*
- *"It's partly a dream for the future of the internet." – The Verge*
- *"A seamless convergence of our physical and digital lives" – Onyx, JP Morgan*
- *"A massively scaled and interoperable network of real-time rendered 3D virtual worlds which can be experienced synchronously and persistently by an effectively unlimited number of users with an individual sense of presence, and with continuity of data" – Matthew Ball*
- *"But the metaverse is not 3D or 2D, or even necessarily graphical; it is about the inexorable dematerialization of physical space, distance, and objects." –Jon Radoff*
- *"The metaverse is the moment in time where our digital life is worth more than our physical life." –Shaan Puri*

The European Commission (EC) has recently provided a concrete definition on the metaverse – or virtual world as it is now widely referred to:

"Virtual worlds are persistent, immersive environments, based on technologies including 3D and extended reality (XR), which make it possible to blend physical and digital worlds in real-time, for a variety of purposes such as designing, making simulations, collaborating, learning, socializing, carrying out transactions or providing entertainment."

In a report published in 2022, the EU Blockchain Observatory and Forum defined the Virtual Worlds (Metaverse) as **"the product of a technology-driven shift with generalized impact through persistent and adaptable digital experiences."**

According to the EUBOF report,, *"it is still too early to draw definitive conclusions on the desirable, let alone the commercially successful or the socially optimal characteristics of metaverses. Even the very definition of the term we have offered, as well as similar definitions found in the scientific or business literatures, cannot be considered definitive – the technology, its applications, and its use cases are rudimentary and are still evolving. Attempting to conclude the metaverse today is as risky as it would have been in the early 1990s to attempt to predict the future path of the internet".*

The essence of the definitions mentioned above, highlights several core themes. Firstly, there's a broad and profound transition occurring across various norms, fields, and cultural divides, which is opening unprecedented opportunities. Secondly, the creation of continuous, unified, and collective experiences is fostering the emergence of what feels like a new 'world.' Lastly, while Virtual Worlds offer immersive and

interactive environments, they also accommodate more restrained forms of user interaction, making it an adaptable and flexible experience.

The exploration of Virtual Worlds leads us to two different visions: a closed Virtual World and an open Virtual World. The closed version, akin to today's digital realm dominated by tech giants, would see the Virtual World controlled by a few powerful entities. Proponents argue that these entities have the resources and experience to facilitate this shift. However, this model risks siloed experiences within proprietary domains. Conversely, advocates for an open Virtual World emphasize the need to reimagine web infrastructure, advocating for a return to interoperable, open systems enhanced by modern digital applications.

	Closed Virtual Worlds	Open Virtual Worlds
Infrastructure	Platforms Serve as the basis for deploying applications and tools	Networks and platforms Serve as the basis for deploying applications and tools, as well as other platforms (platform for other platforms)
Governance	Centrally governed by identifiable entity or entities	Provides the ability for decentralized community-based governance, as well as algorithmic governance.
Values	Decisions are based mainly on adding shareholder value	Decisions are based mainly on adding stakeholder value
Business models/ revenues, sources	Advertisements, subscriptions, digital items, and services Business models must account for intermediation	Advertisements, subscriptions, digital items, and services Disintermediation will introduce new business models
Privacy, data, ownership, identity	Stored in centralized databases and managed by authorized private and public providers. Limited user control over information enforceable by law. Digital content is managed and controlled by providers.	Stored in decentralized and centralized databases and managed by authorized private and public providers as well as smart contracts. User control over information ranges from limited to complete and is enforceable by law, and/ or algorithmically. Some digital content cannot be managed or controlled by providers.
Assets and financial services	Proprietary asset registries and financial interoperability necessitate intermediation and are subject to fees and inefficiencies.	Possibility for universally shared registries of digital and physical assets (NFTs or Blockchain).

		Intermediated and efficient financial services that can interoperate with legacy finance.

Figure 4: Open vs Closed Virtual Worlds (Source: EUBOF Metaverse report,2022)

This debate mirrors the evolution of the web from Web 1.0 (Read-only) to Web 2.0 (Read-write) and now to Web 3.0 (Read-write-own), where blockchain and cryptocurrencies are pivotal in transitioning from centralized to decentralized web models.

Open, permissionless blockchains are crucial in shaping the open Virtual Worlds, offering the most viable solution for establishing versatile systems for the internet's future. In the open Virtual Worlds, key operations and decision-making processes are decentralized, potentially leading to self-regulated cities or districts with their specific policies, rules, and access criteria. Blockchains offer the flexibility to integrate with current Web 2.0 applications, whether financial or otherwise, and can support the launch of centralized apps or those with centralized elements, like user interfaces. This integration emphasizes the enhancement of user choice.

The European Union Blockchain Observatory & Forum (EUBOF) Metaverse report provides an in-depth explanation.

5.4 CBDCs (Central Bank Digital Currencies)

Currently, the broader population, which includes individuals and businesses, can possess money in **two primary ways**:

- In *physical form*, such as coins and banknotes. These are issued by central banks and represent the sole type of central bank currency accessible to the public.
- *Electronically*, as seen in accounts maintained with commercial banks and similar regulated entities. These entities can then keep a portion of their funds (referred to as reserves) in accounts with the central bank.

*"{..} the public cannot open accounts directly with the central bank today or hold any form of central-bank-issued eMoney. A **Central Bank Digital Currency (CBDC)** would change that." (Giaglis G. 2020)*

"A Central Bank Digital Currency, as the name suggests, is a form of digital money that is issued by a central bank. For a value medium to be considered a CBDC it must fulfil both requirements simultaneously (Cœuré et al., 2020). By this definition, CBDCs are not an entirely novel concept. Commercial banks in Europe, the US, and most of the developed world are required to hold a minimum amount of cash, as well as deposits with the central bank in the form of reserves. These reserve accounts fulfil the definition of a CBDC presented above, as they are digital representations of value, recorded as a liability of the central bank and an asset for the commercial bank. "

EUBOF (2021), Central Bank Digital Currencies and a Euro for the Future

CBDCs differ fundamentally from decentralized cryptocurrencies such as Bitcoin or Ethereum. Unlike these cryptocurrencies that operate on decentralized networks without centralized control, CBDCs are centralized digital currencies issued by central banks. They represent a claim against the issuing central bank. This interest in CBDCs by various central banks globally is driven by factors like the increasing popularity of digital

payments, a decline in cash usage in certain regions, and the rise of private digital currencies, such as the initially proposed Diem (formerly Libra) by Facebook (now Meta).

Central Bank Digital Currencies (CBDCs) may come in two distinct models.

Wholesale CBDCs	Retail CBDCs
• Expansion of reserve model to include entities beyond commercial banks. • Used by commercial banks and central bank-appointed institutions. • Facilitates payments, remittances, and settlement of financial instruments.	• Form of legal tender in national currency. • Fulfils functions of money: medium of exchange, store of value, unit of account. • Liability of the central bank. • Asset of the private sector: individuals, households, and businesses.

Figure 5: Wholesale vs Retail CBDCs

CBDCs are also poised to modernize existing financial practices into a digital format. Issued and backed by Central Banks, CBDC holders have a claim against these institutions without exposure to credit or liquidity risks. This digital currency system can help central banks maintain control over monetary policy in a tokenized asset market, provide new tools for regulatory oversight, and lead to more efficient cross-border remittances. Moreover, CBDCs could revolutionize the interbank payment infrastructure and serve as an alternative to physical cash, potentially transforming the relationship between central banks, commercial banks, and depositors.

CBDCs also attract criticism and concern. Financial stability is at risk, as rapid conversion from bank deposits to CBDCs during crises could trigger bank runs. Privacy issues arise with the fear of increased surveillance and central banks' access to transaction data, leading to potential privacy infringements. CBDCs could become magnets for cyberattacks, threatening individual savings and financial stability. They may also limit the effectiveness of certain economic policies, such as those involving negative interest rates. If CBDCs gain excessive popularity, they could marginalize traditional banking institutions, undermining their role and profitability. The implementation of CBDCs presents its own challenges, requiring extensive resources to navigate the technical, regulatory, and logistical hurdles. Moreover, inequality concerns persist, as a CBDC system that isn't inclusively designed may fail to reach segments of the population lacking digital access.

Many nations are exploring and establishing their own iterations of central bank digital currencies (CBDC). The European Central Bank (ECB) is exploring a potential implementation of the "digital euro" and has conducted various experiments and projects to study the feasibility, benefits, and challenges of launching a digital euro. According to the Atlantic Council, 105 countries are now (2023) engaged in CBDC development, which is three times the number of countries identified as active in this area in 2020.

The European Union Blockchain Observatory & Forum (EUBOF) Central Bank Digital Currencies and a Euro for the Future report provides an in-depth explanation.

5.5 Interoperability

Blockchain interoperability is defined as ***'the ability of blockchain networks to communicate with each other, sending and receiving messages, data, and tokens'*** (Chainlink, 2023). It is an emerging requirement for the continuity of blockchain technology, but it comes with certain challenges as each blockchain system differs in various aspects such as governance models, confirmation speed, consensus robustness, levels of permissibility, anonymity, and the security and reliability of its nodes. These variations make network coordination complex and create difficulties in achieving standardization.

The blockchain landscape is currently fragmented, with thousands of networks like Bitcoin, Ethereum, Cardano, and Ripple operating in isolation due to distinct protocols and mechanisms. This lack of interoperability confines their effectiveness and limits their broader application. Interoperability is vital for linking a fragmented ecosystem, allowing each network to contribute its unique advantages and preventing a new form of centralization where certain blockchains dominate, thereby maintaining blockchain's ethos of decentralization. For the widespread adoption of blockchain, interoperability is key. Different industries adopting blockchain will need systems capable of exchanging information across various chains. For example, a logistics company using one blockchain should be able to validate transactions with a financial institution on another blockchain. Without this capability, the full commercial potential of blockchain remains unrealized.

In a report published in 2023, the EU Blockchain Observatory and Forum, identified interoperability complexities as below indicated:

1. ensuring transaction finality across different chains
2. managing cross-chain smart contract execution
3. maintaining data integrity during cross-chain communication

It's important to recognize that the regulatory and legal frameworks governing cross-chain interactions are currently in a state of flux. As the blockchain landscape evolves, these frameworks are continuously adapting to new technological advancements and challenges. Despite the considerable obstacles that need to be overcome, the progress in developing cross-chain protocols, bridges, and standardizations of blockchain technology indicates a positive trajectory toward an increasingly interconnected blockchain ecosystem.

The potential of blockchain interoperability extends across various technological realms, shaping a transformative landscape. This interoperability enables technologies like 6G networks, satellite internet, digital twins, and quantum computing to converge, enhancing efficiency, security, and transparency. In the realm of Web 3.0, interoperability is vital for the success of a decentralized internet, allowing diverse blockchain networks to communicate and create efficient applications and services. It also plays a crucial role in developing smart global ecosystems, fostering seamless data and value exchange across industries and regions. In the creator economy, blockchain interoperability enhances cross-chain transaction capabilities, paving the way for new revenue streams and improved transparency and accountability for creators. Moreover, it accelerates the transition to a net-zero economy by enabling decentralized energy marketplaces and carbon offset trading, contributing to sustainable and resilient energy systems. Lastly, in the burgeoning realms of the Virtual Worlds and omniverse, blockchain interoperability is key to ensuring data security and enabling the integration of various technologies like IoT, digital twins, and AI. This interconnectedness not only fosters a more equitable and sustainable future but also propels continuous evolution and adaptation of blockchain solutions in these expansive digital ecosystems.

The European Union Blockchain Observatory & Forum (EUBOF) The current state of interoperability between blockchain networks report provides an in-depth explanation.

5.6 Environmental Concerns and Solutions

The environmental impact of blockchain technology has been the topic of discussion for quite some time now, particularly regarding public proof-of-work (PoW) blockchains like Bitcoin and Ethereum (before the merge), where there has been severe criticism of the high energy consumption and carbon footprint imposed by the application of the technology. Below, we explain the above concerns:

- Blockchain networks, especially those utilizing PoW consensus mechanisms, require substantial computational power to validate transactions and add new blocks to the chain. This energy-intensive process has raised concerns about the environmental impact, as it often relies on fossil fuels for electricity generation:
- The energy consumption of PoW blockchains directly contributes to their carbon footprint. As miners compete to solve complex mathematical puzzles, they consume vast amounts of electricity, resulting in a significant release of greenhouse gases.
- The rapid advancement of blockchain technology can lead to a high turnover of hardware components, such as ASIC miners and GPUs, which become obsolete relatively quickly. The disposal of these electronic devices contributes to electronic waste and its associated environmental issues.

The above concerns may be addressed by exploring alternative consensus mechanisms. Proof-of-Stake (PoS) and Proof-of-Authority (PoA) are examples of more energy-efficient alternatives. These consensus mechanisms require validators to stake cryptocurrency as collateral instead of solving resource-intensive puzzles (that require high computational power).

Furthermore, there are some environment-friendly solutions to support the crypto-mining activity that can help reduce the carbon footprint, including renewable energy sources such as solar, wind, or hydroelectric power. There are options that allow the optimisation of smart contracts and applications for minimizing energy consumption and the use of resources, which can be beneficial both for the environment and for cutting down operational costs. Newer ASIC (application-specific integrated circuit) miners are designed to be more energy-efficient than their predecessors, and miners can choose locations with access to renewable energy sources to reduce their carbon footprint.

Several blockchain projects and mining pools have implemented carbon offset programs. These initiatives involve investing in projects that reduce greenhouse gas emissions to balance out the carbon footprint created by blockchain operations.

We have seen blockchain communities becoming actively engaged in discussions and initiatives to raise awareness and promote sustainability (e.g. Positive Blockchain, BC100+). Raising awareness about environmental concerns and supporting sustainable and eco-friendly blockchain projects, can significantly promote change and enhance the technology adaption.

Blockchain technology has the potential to bring about transformative changes in various industries. Still, it is essential to be aware of its environmental impact and try to contribute to more sustainable solutions that will help the broader adoption and scalability of the technology, reducing environmental concerns as much as possible.

6 Regulation of Blockchain and Cryptocurrencies

As blockchain and cryptocurrencies gain prominence, regions worldwide are grappling with regulatory approaches for the industry. The European Union has emerged as a frontrunner, establishing the first

comprehensive regulatory framework on a global scale (MiCA). Meanwhile, in the United States, the Securities and Exchange Commission (SEC) is aggressively engaging with crypto companies, with various lawsuits while the federal government has introduced a proposed regulation on digital assets. Similarly, Asian countries like Singapore, previously known for their tolerant stance, are now introducing more strict regulations, reflecting a global trend towards tighter oversight of the cryptocurrency market.

6.1 Europe

Markets in Crypto-Assets (MiCA) is a regulation in EU law, designed to bring clarity to the crypto-assets market.

MiCA's proposals included regulations on crypto-asset issuance and service providers, stablecoins, and measures to prevent market abuse. It is intended to help streamline distributed ledger technology (DLT) and virtual asset regulation in the EU whilst protecting users and investors. MiCA was approved on 20 April 2023 by the EU Parliament and will become law in 2024. **With MiCA, the EU has become the first leading jurisdiction globally to roll out a detailed regulation framework for the sector.**

The European Union is advancing towards a unified approach to crypto-asset regulation. Historically, EU nations have had their own set of regulations, often disparate and sometimes conflicting, leading to complexity and uncertainty. The new directive aims to replace these varied regulations with a single, comprehensive framework. This harmonization is expected to diminish confusion, establish the same level for all member states, and facilitate smoother cross-border cryptocurrency transactions within the EU. Such a framework will enhance consistency and predictability, bolstering investor confidence and positioning the EU as a prime destination for digital finance innovation.

MiCA aims to establish clear, unified regulations for service providers and token issuers. This approach aims to create standardized guidelines that ensure fairness and protect investors, fostering a more consistent and secure environment for the growth of crypto services and tokens.

MiCA also offers explicit regulatory guidance for crypto assets where traditional financial regulations fall short. As the variety and popularity of crypto services and tokens continue to grow, there's a pressing need for specific guidelines that can adapt to the unique nature of these digital assets. Clear regulations will help reduce uncertainty, allowing for innovation and participation in the market while maintaining robust consumer protection measures. This clarity is intended to support the fair treatment of investors and users in the dynamic crypto landscape.

According to the European Securities and Markets Authority (ESMA), EU-level safeguards and complaint mechanisms specific to MiCA will not be in effect until December 2024. Post-implementation, states are expected to enter an 18-month transitional period, during which some protections may not be enforceable until 1st July 2026. Furthermore, National Competent Authorities may face constraints on their supervisory powers over entities that utilize the "grandfathering clause." This clause allows certain operations to continue under pre-existing regulations before the new rules take full effect.

6.2 United States of America

The U.S. Securities and Exchange Commission (SEC) generally has regulatory authority over the issuance or resale of any token or other digital asset that constitutes a security. Under U.S. law, a security includes “an investment contract,” which has been defined by the U.S. Supreme Court as an investment of money in a common enterprise with a reasonable expectation of profits to be derived from the entrepreneurial or managerial efforts of others. SEC v. W.J. Howey Co., 328 U.S. 293, 301 (1946).

In 2023, the Biden-Harris Administration has released proposed regulations on the sale and exchange of digital assets by brokers *'in an effort to crack down on tax cheats while helping law-abiding taxpayers know how much they owe on the sale or exchange of digital assets'*. According to the press release, the proposed regulations outline the necessity for digital asset brokers to report specific sales and exchanges. They aim to provide clarity and alignment with tax reporting standards, ensuring that digital asset brokers adhere to the same information reporting rules as brokers dealing with securities and other financial instruments. Numerous well-known crypto experts expressed their concerns that these regulations could further discourage crypto companies from doing business within the United States.

The United States government has also announced in 2023 the **National Standards Strategy for Critical and Emerging Technology**. According to the document, the US will prioritise standards development in eight areas, including 'digital identity infrastructure and distributed ledger technologies, which increasingly affect a range of key economic sectors'.

In May 2023, NY Attorney General James proposed 'landmark legislation to tighten regulations on the cryptocurrency industry to protect investors, consumers, and the broader economy'. The bill called the Crypto Regulation, Protection, Transparency and Oversight Act (CRPTO) would grant New York officials the authority to shut down businesses suspected of engaging in fraud or illegal activity, issue subpoenas, and apply penalties to crypto firms breaking state law. CRPTO must still be passed by NYC lawmakers for it to become state law.

Throughout 2022 and 2023, the United States has seen an increased regulatory focus on the cryptocurrency industry. The SEC has intensified its oversight and enforcement, particularly examining the crypto market's compliance with securities laws, and has entered multiple legal battles with various crypto companies such as Binance and Ripple. For a comprehensive overview of the SEC's enforcement actions in the cryptocurrency space, please refer to the official SEC press releases and statements on their website.

6.3 Asia: Singapore and Hong Kong

Every Asian nation follows a different strategy toward regulating blockchain and cryptocurrencies, varying from strict consumer protection measures to more liberal policies. As crypto regulations are inconsistent in Asian countries and regions, we will focus on Singapore and Hong Kong.

Singapore:

Singapore is a leading nation in blockchain technology, not only in Asia but globally, as it endeavours to balance fostering innovation in blockchain and cryptocurrency with implementing regulatory measures to ensure market stability and consumer protection.

In 2023, Singapore updated and introduced new legislation to enhance the regulation of blockchain-based services. These changes involve revisions to the Payment Services Act (PS Act) from 2020 and the new Financial Services and Markets Act. Singapore has recently adopted more stringent rules for cryptocurrencies, aiming to both encourage innovation in this field and maintain effective regulatory control.

Singapore is set to introduce more regulations for closer monitoring of crypto-asset companies, planned to be rolled out progressively from the end of 2023. The aim is to create a more regulated and safer environment for digital assets. The Monetary Authority of Singapore (MAS) has played a key role in developing and refining regulations for providers of digital payment tokens (DPT). This initiative is critical in creating a more regulated and secure cryptocurrency market in Singapore.

Regarding the Stablecoin Regulatory Framework, in August 2023, the MAS completed a regulatory framework for stablecoins, which marks a further step in strengthening Singapore's regulatory approach to digital currencies. The MAS has previously released new guidelines that require cryptocurrency service providers to retain client funds in a statutory trust by the end of 2023. The guidelines urge consumers to be vigilant and not deal with unregulated entities, 'as they risk losing all their assets'.

Hong-Kong

Hong Kong adopts an open stance towards cryptocurrencies, permitting unrestricted trading and usage of digital assets without levying taxes or implementing constraints. The Hong Kong Monetary Authority (HKMA) is adopting a *"same risk, same regulation"* approach to crypto. The Hong Kong government recognizes the advantages that blockchain technology can bring to various industries, especially in terms of transparency and cost-efficiency, and has even established a Task Force on Promoting Web3 Development.

A 'Licensing Handbook for Virtual Asset Trading Platform Operators' was published by the Securities and Futures Commission (SFC) of Hong Kong in 2023. The Handbook provides general information about licensing matters concerning virtual asset trading platform operators and warns that 'It is a serious offence to carry on a regulated activity and/ or VA service in Hong Kong or actively market to the investing public of Hong Kong any services which constitute a regulated activity and/or VA service without the required licence(s)'

In 2023, the HKMA issued a warning to users reminding them 'to beware of firms engaged in crypto business purporting to be "banks" or describing their products as "deposits"'. The central bank emphasised that, according to Hong Kong's banking laws, only licensed institutions are permitted to engage in banking or deposit-taking activities within the region.

7 Additional Resources

For more insights and in-depth information on various blockchain topics, readers are encouraged to visit the EU Blockchain Observatory and Forum website. An extensive list of comprehensive reports and studies can be accessed at the EU Blockchain Observatory and Forum.

References

IBM. Blockchain defined: Blockchain is a shared, immutable ledger for recording transactions, tracking assets, and building trust. Available at: https://www.ibm.com/topics/blockchain (Accessed: [date]).

Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available at: https://bitcoin.org/bitcoin.pdf (Accessed: 30/11/2023).

How the Byzantine General Sacked the Castle: A Look Into Blockchain. Medium. Available at: https://medium.com/@DebrajG/how-the-byzantine-general-sacked-the-castle-a-look-into-blockchain-370fe637502c (Accessed: 30/11/2023).

Bitcoin Mining. Buy Bitcoin Worldwide. Available at: https://www.buybitcoinworldwide.com/mining/ (Accessed: 30/11/2023).

Lamport, L., Shostak, R., and Pease, M. (1982). The Byzantine Generals' Problem. Available at: https://www.andrew.cmu.edu/course/15-749/READINGS/required/resilience/lamport82.pdf (Accessed: 30/11/2023).

The Byzantine Generals' Problem. SpringerLink. Available at: https://link.springer.com/article/10.1007/BF00196791 (Accessed: 30/11/2023).

ICAEW. A brief history of blockchain: A timeline from the 1970s to today, plus ideas for implementation 2008. Available at: https://www.icaew.com/technical/technology/blockchain-and-cryptoassets/blockchain-articles/what-is-blockchain/history (Accessed: 30/11/2023).

TechTarget., A timeline and history of blockchain technology. Available at: https://www.techtarget.com/whatis/feature/A-timeline-and-history-of-blockchain-technology (Accessed: 30/11/2023).

On public and private blockchains. Ethereum Blog. Available at: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/ (Accessed: 30/11/2023).

IBM Blockchain Blog. (2017). The difference between public and private blockchain. Available at: https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/ (Accessed: 30/11/2023).

Andreessen, M. (2014). Why Bitcoin Matters. The New York Times. Available at: https://archive.nytimes.com/dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/ (Accessed: 29/11/2023).

EU Blockchain, Observatory and Forum. (2021). Decentralized Finance (DeFi). Available at: https://www.eublockchainforum.eu/sites/default/files/reports/DeFi%20Report%20EUBOF%20-%20Final_0.pdf (Accessed: 29/11/2023).

EC (2020) 'The Retail Payments Strategy'. EC and TNS Opinion & Social. (2016) Financial products and services: report. LU: Publications Office. Available at: https://data.europa.eu/doi/10.2874/863808 (Accessed: 19/10/2023).

ECB (2019) Goodbye EONIA, welcome €STR!, European Central Bank. Available at: https://www.ecb.europa.eu/pub/economicbulletin/focus/2019/html/ecb.ebbox201907_01~b4d59ec4ee.en.html (Accessed: 19/10/2023).

ECB (2020a) 'Payments in a digital world'. Available at: https://www.ecb.europa.eu/press/key/date/2020/html/ecb.sp200910~31e6ae9835.en.html (Accessed: 19/10/2023).

ECB (2020b) 'Report on a digital euro', p. 55. European Central Bank. (2023). Eurosystem proceeds to next phase of digital euro project. Available at: https://www.ecb.europa.eu/press/pr/date/2023/html/ecb.pr231018~111a014ae7.en.html (Accessed: 19/10/2023).

EU Blockchain Observatory and Forum (2021), Central Bank Digital Currencies and a Euro for the Future, Available at: https://www.eublockchainforum.eu/sites/default/files/reports/EUBOF-report-on-a-Digital-Euro-2906.pdf (Accessed: 19/10/2023)

Kumhof, M., & Noone, C. (2018). Central bank digital currencies—design principles and balance sheet implications. Bank of England Staff Working Paper No. 725.

Mersch, Y. (2017). Digital Base Money: an assessment from the ECB's perspective. European Central Bank.

Meaning, J., Dyson, B., Barker, J., & Clayton, E. (2018). Broadening narrow money: monetary policy with a central bank digital currency. Bank of England Staff Working Paper No. 724.

Giaglis, G. (2020). Everything You Always Wanted to Know About CBDCs (But Were Afraid to Ask). Medium. Available at: https://medium.com/the-capital/everything-you-always-wanted-to-know-about-cbdcs-but-were-afraid-to-ask-c7b11fe67aba {Accessed on 19/10/2023}

Central Banks and Digital Currencies by Professor George Giaglis: https://www.youtube.com/watch?v=mitdNXqza98 {Accessed on 19/10/2023}

Schickler, J. (2022), Europe's CBDC Designers Wrestle with Privacy Issues', CoinDesk. Available at: https://www.coindesk.com/policy/2022/04/04/europes-cbdc-designers-wrestle-with-privacy-issues/ {Accessed on 19/10/2023}

Jenkinson, G. (2023), 'CBDC frameworks must guard user privacy, monetary freedom of choice: BIS Chief', CoinTelegraph. Available at: https://cointelegraph.com/news/cbdc-frameworks-must-guard-user-privacy-monetary-freedom-of-choice-bis-chief {Accessed on 19/10/2023}

Monetary Authority of Singapore. (2023). MAS Finalises Stablecoin Regulatory Framework. Available at: https://www.mas.gov.sg/news/media-releases/2023/mas-finalises-stablecoin-regulatory-framework (Accessed: 3/12/2023).

Chambers and Partners. (2023). Blockchain 2023 – Singapore. Available at: https://practiceguides.chambers.com/practice-guides/blockchain-2023/singapore (Accessed: 3/12/2023).

Monetary Authority of Singapore. (2023). MAS Publishes Investor Protection Measures for Digital Payment Token Services. Available at: https://www.mas.gov.sg/news/media-releases/2023/mas-publishes-investor-protection-measures-for-digital-payment-token-services (Accessed: 3/12/2023).

Securities and Futures Commission. (2023). Licensing Handbook for Virtual Asset Trading Platform Operators, June 2023. Available at: https://www.sfc.hk/-/media/EN/assets/components/Guidelines/File-current/Licensing-Handbook-for-VATPs-31-05-2023.pdf?rev=88121998f25d480191abefb35b140a2e (Accessed: [date]).

Hong Kong Monetary Authority. (2023). Alert: Misrepresentation by crypto firms using the word "bank", 15 September 2023. Available at: https://www.hkma.gov.hk/eng/news-and-media/press-releases/2023/09/20230915-5/ (Accessed: 3/12/2023).

Securities and Futures Commission., Warning statement on unregulated virtual asset trading platform. Available at: https://www.sfc.hk/en/News-and-announcements/Policy-statements-and-announcements/Warning-statement-on-unregulated-virtual-asset-trading-platform (Accessed: 3/12/2023).

Government of Hong Kong. (2023). Task Force on Promoting Web3 Development established. Available at: https://www.info.gov.hk/gia/general/202306/30/P2023063000579.htm (Accessed: 3/12/2023).

Chainlink. (2023) What Is Blockchain Interoperability? Available at: https://chain.link/education-hub/blockchain-interoperability (Accessed: 7/12/2023).