## What is blockchain?

A blockchain is a type of **distributed ledger** or decentralized database that keeps continuously updated digital records of who owns what.

Rather than having a central administrator like a traditional database, a distributed ledger has a network of replicated databases, synchronized via the internet and visible to anyone within the network.

What is the Blockchain?

Blockchain is a shared, digital ledger that all users can see but no single user can control.
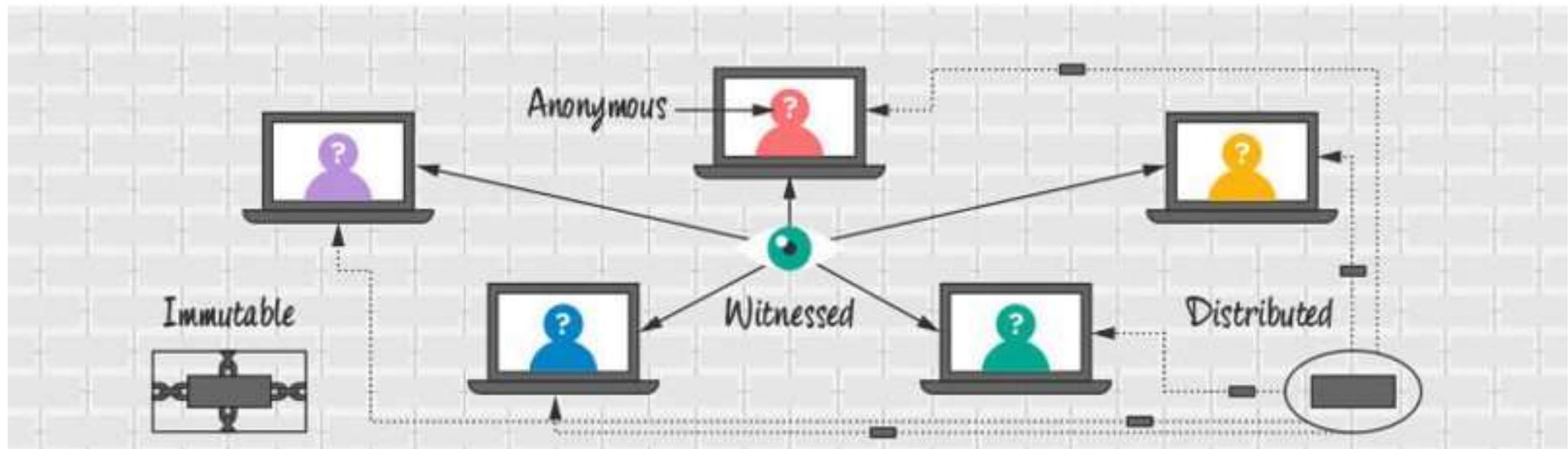
What will Blockchain Technology help us achieve?

- Greater transparency leads to greater accountability and higher integrity.

- Decentralization leads to increased efficiency through automation and increased trust.

- Better security increases confidence.

- Improved traceability improves security and prevents fraud.

Blockchains vs centralized databases

Blockchains are ideal for shared databases in which every user can read everything, but no single user controls who can write what in traditional databases, a single entity exerts control over all read and write operations, while other users are entirely subject to that entity's whims.

Blockchains represent a trade-off in which disintermediation is gained at the cost of confidentiality.

Types of Blockchain

	Public (eg. Bitcoin)	Private	Consortium/Permissioned (eg. EHRs)
Network Type	Decentralized	Partially decentralized	Partially decentralized- hybrid between public and private blockchains.
What is it?	Anyone anywhere in the world can read and write on the network. Data is validated by every participant ('node') in the network, thus making it very secure.	Permissions to read and write data onto the Blockchain are controlled by a single highly "trusted" organization-the owner of the blockchain.	Permissions to verify, read and write on the blockchain are controlled by a few predetermined nodes. The choice of predetermined nodes can be different for every entity on the blockchain.
Benefits	Secure as the entire network verifies transactions – transparent as all transactions are made public with individual anonymity.	Efficient as verification is done just by owner of the blockchain. Private as the owner can control who has access to read or write on the blockchain.	Efficient as relatively lesser nodes verify transactions. Private as read and write access can be controlled by the predetermined nodes. No consolidation of controlling power.
Challenges	Inefficient as all nodes need to verify the transaction.	Controlling power is consolidated to a single organisation. Difficult to align many organizations to use the same blockchain.	Controlling power is consolidated to a few organisations.

What are smart contracts

A smart contract is a specialized program that encodes business logic and runs on a dedicated virtual machine integrated into a blockchain or distributed ledger.

Terms and conditions are agreed by all parties involved.
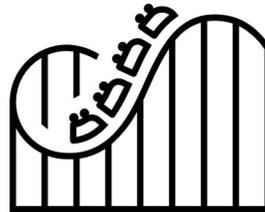
Execution of the contract is triggered by an event.
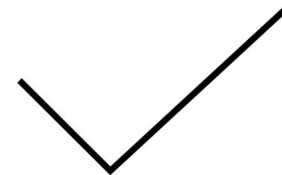
The smart contract is executed automatically.

Blockchain & Crypto Assets
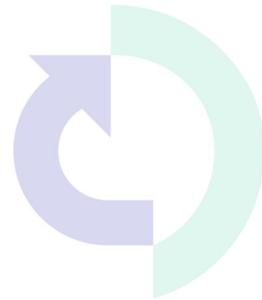
Central Bank Digital Currencies (CBDCs)

Supporting competition, efficiency and innovation in payments

Meeting future payment needs in a digital economy

Improving the availability and usability of central bank money

Avoiding the risks of new forms of private money creation

Addressing the consequences of a decline in cash

Supporting a resilient payments landscape

As a building block for better cross-border payments

CBDC

Source: Bank of England

What are NFTs?

Non-fungible tokens (or NFTs) are a new class of digital assets stored and handled on a blockchain. These assets are characterized as unique, irreplaceable and non-interchangeable. Non-fungible tokens are not cryptocurrencies. They are not traded on exchanges like any other tokens. They are not built on the same technical standards (ERC-721 on Ethereum).

Non-Fungible tokens allow anyone to digitalize ownership of any arbitrary data, while drastically increasing the design space and usability aspects of blockchain solutions. The biggest differentiator of Non-Fungible tokens versus "regular" tokens is that each one is tied to a different identifier, making each token unique to its owner.

Blockchain for digital asset (NFTs) Management?

- Digital assets (NFTs) enable the creation of rare & unique items that can't be destroyed, replicated or forged

- NFTs can be tracked on the blockchain, providing an immutable history of the assets

- NFTs cannot deteriorate over time. So, when utilized in applications such as digital collectibles they do not deteriorate like their physical counterpart

- Peer-to-peer, secure trading enabled by blockchain technology

- NFTs can be sold and traded/exchanged back into Fiat

NFTs and Asset Tokenization

Asset tokenization refers to the process of creating digital tokens that represent ownership of a real-life asset, commonly known as NFTs. The token creation process uses blockchain technology, allowing you to store and trade the tokens freely and securely as you would with other cryptocurrencies and blockchain-based assets.

After generating a non-fungible token of an asset, you can list it on an NFT exchange (if you wish to sell ownership of it). It is possible to tokenize assets directly with well-understood market value, like artwork or digital trading cards. However, tokenizing real estate or artwork will require assessment and auditing by a bank, accountant, or law firm.

What are Crypto Assets?

Crypto assets are digital representations of value or rights that can be transferred or stored electronically using distributed ledger technology, such as blockchain. They utilize cryptography, peer-to-peer networks, and public ledgers over the internet to validate ownership. These assets include cryptocurrencies like Bitcoin and Ethereum, as well as digital tokens issued on blockchain platforms.

Categories of Crypto Assets

- A wide range of crypto assets exist.

- The use of Crypto Assets has evolved rapidly since the 2017 market cycle. Today their use extends well beyond tokens for payment-type purposes.

- At present there is no common taxonomy of crypto assets in use by international standard setting bodies.

  However, a basic taxonomy comprises of 3 main categories of Crypto Assets:

Payment, Exchange Tokens – Cryptocurrencies	Investment – Security Tokens	Utility Tokens

Classification of Crypto Assets
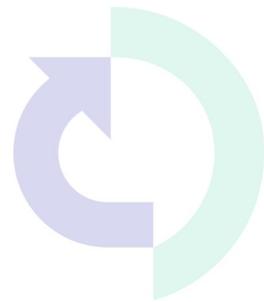
Classifying Cryptocurrencies

- All cryptocurrencies and tokens will not share many of the same key characteristics.

- First, we should classify the most notable examples based on a variety of criteria.

- We will use the Blockchain Research Institute Taxonomy of Cryptoassets. (link: https://www.blockchainresearchinstitute.org/wp-content/uploads/2020/02/Tapscott_Token-Economy_Blockchain-Research-Institute.pdf)

- This should provide the background to understand whether a given cryptocurrency or token falls within the purview of national and/or international regulations.

Classifying Crypto Assets

Cryptocurrencies

Platforms

Utility Tokens

Security Tokens

Natural Asset Tokens

Crypto-Collectibles

Crypto-fiat currencies & stablecoins

Cryptocurrencies
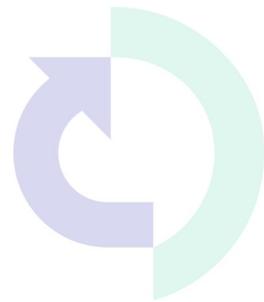
Cryptocurrencies

Bitcoin

Cryptocurrencies (in the taxonomy, 'payment tokens') are the native cryptographic asset of a particular blockchain protocol, designed and intended to 'serve as a general-purpose store of value or medium of exchange.'

Bitcoin (BTC) is the leading example in this category.
- Genesis Block: 3 January 2009
- Consensus Mechanism: Proof-of-Work
- Average Block Time: 10 minutes
- Total Supply Limit: 21 million bitcoin

Cryptocurrencies

Litecoin

- 13 Oct 2011: Litecoin (LTC) went live.

- Maximum supply: 84 million compared to Bitcoin's 21 million.

- Average block time: 2.5 minutes compared to Bitcoin's 10 minutes.

- Litecoin was often referred to as the 'silver' to Bitcoin's digital 'gold.'

Cryptocurrencies

Monero

Monero, a leading privacy coin, obscures transaction history, unlike Bitcoin's transparent blockchain. It employs three techniques:

•Ring Signatures: Group signatures that link transaction inputs to multiple equally valid outputs, hiding the sender's identity.

•Stealth Addresses: Generate unique, one-time recipient addresses, ensuring transaction unlinkability.

•RingCT (Ring Confidential Transactions): Enhances privacy by concealing transaction amounts.

Platform Tokens

Platform Tokens

Ethereum

Platform tokens (in the taxonomy, 'consumer tokens') are designed to support blockchain platforms on which decentralized applications may be built. These "DApps" will have tokens of their own that can be used in the application.

- Ethereum and Ether (ETH) are the leading example in this category.
- Genesis Block: 30 July 2015
- Consensus Mechanism: Proof-of-Work; shifted to Proof-of-Stake in 2022
- Average Block Time: 13 seconds
- Total Supply Limit: None

Platform Tokens

Binance Coin

Binance Smart Chain (BSC) also supports smart contracts, is now the biggest platform chain after Ethereum.

- Binance Coin (BNB) is the native token powering the Binance ecosystem.
- Genesis Block: 18 April 2019
- Average Block Time: 1 second
- Total Supply Limit: 200 million BNB

Utility Tokens
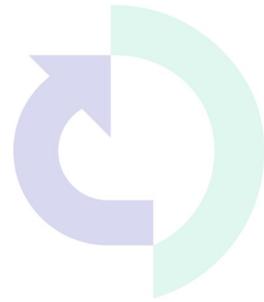
Utility Tokens

Utility tokens are intended to provide digital access to an application or service. After the application is completed, utility tokens may give holders perks such as access to the network or voting rights.

Examples include:
- Brave Software's Basic Attention Token (BAT), for a digital advertising exchange ecosystem.
- Golem Network Token (GLM), facilitating a decentralized market for computing power.
- FunFair Token (FUN), an online gaming and casino platform using smart contracts.
- Filecoin (FIL), for a decentralized storage system.

Security Tokens
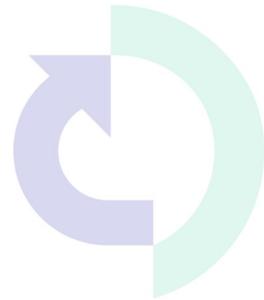
Security Tokens

A classic security is a fungible (identical cannot be distinguished from another), negotiable (can be owned and traded) financial instrument that holds some type of monetary value.

- Security Tokens introduced the important concepts of 'Tokenization' or 'Digitization' or 'Fractional Ownership', meaning that an asset (tangible or intangible) can be divided into fungible (identical) tokens, which can be issued, tracked and transferred via the blockchain. This allows for an investor to have 'fractional' ownership of an underlying asset.

- Following the Howey Test (a test created by the US Supreme Court for determining whether certain transactions qualify as "investment contracts" or securities), a token will be an investment contract (and therefore subject to securities registration requirements) if:

  - It is an investment of money;

  - There is an expectation of profits from the investment;

  - The investment of money is in a common enterprise; and

  - Any profit comes from the efforts of a promoter or third party.

Natural Asset Tokens
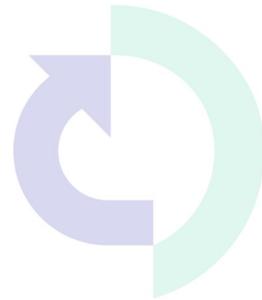
Natural Asset Tokens

- Natural Asset Tokens represent tangible goods in established markets (like gold, oil, natural gas, base metals) or in frontier markets (like carbon, water, air).

- Earth Token is a decentralized Natural Asset Exchange blockchain platform with accompanying Earth Token (EARTH).

- Power Ledger is a blockchain-based, peer-to-peer energy platform that lets users buy and sell electricity, using Power Ledger Token (POWR) ERC-20 tokens.

- SunContract is a similar blockchain platform for trading energy, using the Sun Token (SUN).

- Note: the boundaries in classifying Natural Asset Tokens are not completely clear. Depending on the details of how it is structured, it could be seen as a Security token or a 'Stablecoin'.

Crypto Collectibles
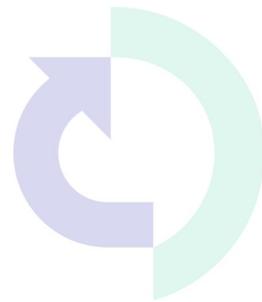
Crypto Collectibles

- Non-Fungible Tokens (NFTs) have unique properties, meaning they can be distinguished from another and cannot be duplicated.

- The ERC721 standard on Ethereum is fundamental for non-fungible tokens.

- "CryptoKitties" are unique virtual cats that people can purchase, trade, raise, and even breed with other CryptoKitties.

- Non-Fungible Tokens can also be used in gaming to create unique gaming characters.

- They may also be linked to unique real-world assets such as art or rare cars and can allow investors to own a fractional interest in such a unique asset.

- Link: https://nftvaluations.com/

Crypto-Fiat Currencies & Stablecoins
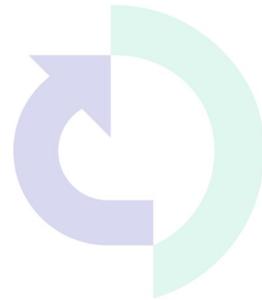
Crypto-fiat currencies & Stablecoins

- Stablecoins (as the term indicates) were introduced to address the high price volatility of Bitcoin, Ethereum and other altcoins and designed to maintain a relatively stable value (at least short-time).

- A stable coin is tied or 'pegged' to an underlying asset or currency, can take many forms and can reference the following assets:
    - Fiat currencies. A crypto-asset can be related to one or more fiat currencies.
    - Other real-world assets such as securities, commodities, real-estate, financial instruments and/or other assets.
    - Other crypto-assets. A crypto-asset can be related to one or more other crypto-assets.
    - Algorithmically controlled. A crypto-asset can use an algorithm that attempts to mimic monetary policy and adjust the supply of tokens to match demand.

- Regarding how stablecoins are implemented we may classify two broad categories:
    - Centralized custodial stablecoins: the underlying asset(s) are hold by a centralized custodian.
    - Decentralized non-custodial stablecoins: managed in a decentralized fashion, operated through smart contracts, that has reserves in cryptocurrency, rather than fiat.

Conclusions

- Blockchain is a transformative innovation with wide-ranging applications.

- Key blockchain features: transparency, security, immutability.

- Understanding blockchain components: nodes, blocks, consensus mechanisms.

- Taxonomy: cryptocurrencies vs. tokens (utility, security, NFTs).

- Stay updated on evolving regulations, collaborate across disciplines.

- Continuous learning is crucial for professional growth.

- Blockchain offers exciting opportunities in professional services.