Blockchain and Crypto

☞ Digital-Technology-Radar.net

	low	medium	high
Impact	▭	▭	▭
Complexity	○	●	◯

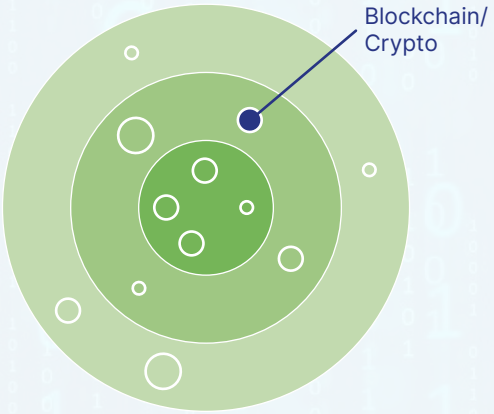
1 INTRODUCTION

Purpose

Blockchain is a decentralised technology that securely records transactions across multiple computers, ensuring transparency and immutability without intermediaries.

Key benefits

Blockchain enhances security through cryptographic hashing, offers transparency via a shared ledger, and guarantees immutability, making recorded data unchangeable. This fosters greater trust and efficiency in transactions.



2 KEY CONCEPTS

Fundamental principles:

Blockchain operates on decentralisation, distributing data and control across a network of nodes without a central authority. Its transparency allows transactions to be publicly verified, enhancing trust. Security is ensured through cryptography, making the system resistant to fraud and hacking. Immutability ensures that, once data is recorded, it cannot be altered, providing a permanent, tamper-proof record.

Terminology

- **Blocks:** data structures that store a list of transactions and are linked to previous blocks in a chain, forming a blockchain.
- **Hashing:** a cryptographic function that converts data into a fixed-size string of characters, which secures data by making it tamper-evident.
- Decentralisation: distribution of data across multiple nodes, eliminating a single point of failure and enhancing security.
- Ledger: a record-keeping system that maintains a continuously growing list of transactions or data.
- Consensus Mechanisms: algorithms that ensure all participants in the network agree on the validity of transactions, such as Proof of Work (PoW) and Proof of Stake (PoS).

3 POPULAR TOOLS AND FRAMEWORKS

Primary tools

- Ethereum: a decentralised platform that enables the creation and execution of smart contracts and decentralised applications (dApps).
- Hyperledger Fabric: a permissioned blockchain framework designed for enterprise solutions, offering modularity and flexibility.
- Bitcoin Core: the original implementation of the Bitcoin protocol, used for maintaining the Bitcoin blockchain.

Comparison

- **Ethereum vs Hyperledger Fabric:** Ethereum is public and focuses on smart contracts and dApps, while Hyperledger Fabric is permissioned, targeting enterprise use with modular and scalable features.
- **Bitcoin Core vs Ethereum:** Bitcoin Core is optimised for secure, peer-to-peer transactions with a focus on digital currency, whereas Ethereum supports a broader range of applications through its smart contract capabilities.

4 APPLICATIONS

Industry use cases

- **Finance:** facilitates secure, transparent transactions and enables the creation of decentralised financial (DeFi) applications. **> Best Practice:** Uniswap.
- **Supply chain:** enhances traceability and transparency in supply chains by recording every step of the process on a blockchain. **> Best Practice:** IBM Food Trust.
- **Tokenisation:** represents real-world assets like property or commodities as digital tokens on the blockchain. **> Best Practice:** RealT.

Practical examples

- Bitcoin: first and most well-known cryptocurrency, operating on a decentralised blockchain.
- Ethereum: a blockchain platform that enables the creation of decentralised applications and smart contracts.
- Chainlink: a decentralised oracle network that connects smart contracts with real-world data.

5 IMPLEMENTATION INSIGHTS

Best practices and tips

- **Security:** implement robust cryptographic practices and ensure secure key management. Consider using techniques like Zero-Knowledge Proofs (ZKPs) or multi-signature wallets.
- **Scalability:** designed with scalability in mind, considering techniques like sharding, sidechains or Layer 2 solutions to handle growing transaction volumes without sacrificing performance.
- **Conduct thorough testing and auditing:** before deployment, rigorously test your smart contracts and blockchain applications for vulnerabilities.

Common challenges

- Consensus Mechanism: needs to align with your specific use case and requirements, such as Proof of Work (PoW) for security or Proof of Stake (PoS) for energy efficiency. Each has its own trade-offs in terms of security, scalability and performance.
- **Scalability:** addressing issues related to transaction throughput and network congestion.
- **Interoperability:** ensuring seamless interaction between different blockchain networks and systems.

6 KEY TRENDS AND PREDICTIONS

Top milestones in Blockchain

- **2008:** Satoshi Nakamoto published the Bitcoin white paper, introducing the concept of blockchain technology.
- **2009:** Bitcoin started with creation of the first block, known as the 'Genesis Block' or 'Block 0'. In the first transaction Satoshi Nakamoto sent 10 Bitcoins to scientist Hal Finney.
- **2015:** Ethereum launch, expanding blockchain applications beyond currency to include smart contracts.
- **2021:** the rise of non-fungible tokens (NFTs) and the growing adoption of blockchain

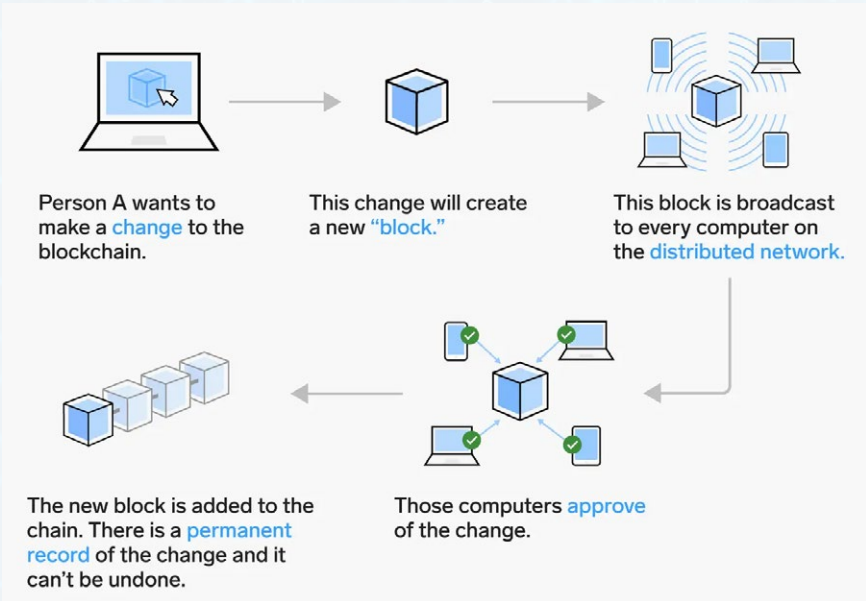
Current trends

- Decentralised Finance (DeFi): the growing use of blockchain technology to recreate and enhance traditional financial services.
- **Non-Fungible Tokens (NFT):** a unique digital asset representing ownership of a specific item, such as art, music or collectibles, verified using blockchain technology.
- Central Bank Digital Currencies (CBDCs): governments exploring digital currencies backed by central banks to modernise financial systems.

Future predictions

- **Interoperability Solutions:** development of technologies that enable different blockchains to communicate and work together.
- **Regulatory Frameworks:** creation of comprehensive regulations to guide the use and development of blockchain technology.
- **Mainstream Adoption of Decentralised Finance (DeFi):** DeFi platforms will provide decentralised alternatives to traditional banking, lending and insurance services.

The blockchain process can be broken down into simple steps.



Source: www.businessinsider.com

7 KEY RESOURCES AND MOST HELPFUL LINKS

Websites and blogs

- Bitcoin.org: a great starting point, offering a range of guides and explanations on how it works.
- CoinDesk: news and analysis on cryptocurrencies and blockchain technology.

Online courses

- Certified Enterprise Blockchain Professional by 101 Blockchains.
- Ethereum and Solidity: The Complete Developer's Guide by Udemy.
- Udacity: Blockchain Developer Nanodegree programme.

Communities and forums

- Bitcointalk: Q&A forum for blockchain-related questions.
- GitHub: repositories for blockchain projects and code.

8 GLOSSARY

Common terms and definitions

- Smart Contracts: self-executing contracts with the terms of the agreement directly written into code, automating and enforcing agreements without intermediaries.
- Nodes: individual computers or devices in a blockchain network that validate and relay transactions.
- Token: a digital asset issued on a blockchain, representing a unit of value or utility, often used in decentralised applications (dApps).
- Mining: the process of validating transactions and adding them to the blockchain, typically in exchange for a reward in cryptocurrency.
- Proof of Work (PoW): a consensus mechanism where nodes solve complex mathematical problems to validate transactions and create new blocks.
- Proof of Stake (PoS): a consensus mechanism where validators are chosen to create new blocks based on the number of coins they hold and are willing to 'stake' as collateral.
- Private Key: a secret key used to sign transactions and access one's cryptocurrency; it should be kept secure and never shared.
- Public Key: a cryptographic key that can be shared publicly and is used to receive cryptocurrency; it's derived from the private key.
- Wallet: a software or hardware tool that stores private and public keys, allowing users to send, receive and manage their cryptocurrency.
- Cold Wallet: an offline storage method for cryptocurrency, used to protect against hacking and theft.
- Hot Wallet: an online storage method for cryptocurrency that is connected to the internet, providing easier access but higher risk of cyberattacks.
- Stablecoin: a type of cryptocurrency that is pegged to a stable asset, like fiat currency, to reduce price volatility.
- ICO (Initial Coin Offering): a fundraising method where new cryptocurrencies or tokens are sold to investors in exchange for established cryptocurrencies or fiat money.
- DAO (Decentralised Autonomous Organisation): an organisation represented by rules encoded as a computer program, managed by its members without central leadership.
- dApp (Decentralised Application): an application that operates on a decentralised blockchain network rather than being hosted on centralised servers.

Authors

Dr Torsten Wingenter
Torsten established Digital Innovations at Lufthansa, founded the FlyingLab, and was responsible for the digital strategies of Austrian, Lufthansa and Swiss airlines. Today, as the "Inno Doc", he is digital advisor, coach and catalyst, interim manager and fire fighter for many organisations in their pursuit for digital innovations.
www.inno-doc.com

Prof Marc K Peter
Marc was an executive at eBay, E*TRADE (ANZ) and LexisNexis. Today, he is the "Digital Prof" at Rochester-Bern Executive Programs, the University of Rochester, at FHNW and at CSU in Australia. His research and teaching covers digital transformation, digital technology, digital leadership, cybersecurity and digital marketing.
www.digitalprof.com