DUY TAN UNIVERSITY

GRADUATES DEPARTAMENT

BLOCK-CHAIN

PERSOPNAL ASSIGMENT

QUESTION 5

ELABORATE NFT TOKENS? EXPLAIN DEFI AND ALSO ILLUSTRATE HOW BLOCKCHAIN CAN SUPPORT CYBER SECURITY IN REAL TIME WORLD

Instructor: **Ph.Dr. Anand Nayyar**

Create : Eng**. Ngô Thanh Lợi**

Code: 30311570108

DA NANG, SEP-2025

ACKNOWLEDGEMENTS

The author would like to express his deepest gratitude to Prof.Dr. Anand Nayyar the lecuter from Duy Tan University, Vietnam, for his invaluable guidance, insightful lectures and constant encouragement throughout the Blockchain course. This has motivated me to pay special attention and explore the outstanding application features of NFT, DeFi and Blockchain-based cybersecurity applications.

I would also like to sincerely thank the support and resources from the university, which has created a wonderful learning and research environment. I look forward to receiving comments and suggestions from teachers and readers to improve my research in the future.

CONTENTS

ACKNOWLEDGEMENTS ---------- *ii*

List of figures and table ---------- *i*

Chapter 1. Introduction ---------- *1*

1.1 Background and motivation for report ---------- **1**

1.2 Subject of the report ---------- **1**

1.3 Scope of report ---------- **1**

Chapter 2. NFT (Non-Fungible Tokens) and Applications ---------- *2*

2.1 Concept, characteristics ---------- **2**

2.2 Technical NFT components ---------- **3**

2.2.1 Blockchain ---------- 3

2.2.2 Smart Contracts ---------- 3

2.2.3 Metadata, Data Encoding and Storage ---------- 4

2.2.4 NFT Activity Lifecycle (Operational Phases) ---------- 5

2.3 NFT Market from Marketplace and Ecosystem Perspective ---------- **6**

2.4 Challenges of NFT ---------- **7**

Chapter 3. DeFi Expectations and Challenges ---------- *8*

3.1 Concept and operating ---------- **8**

3.2 Traditional Finance vs. Decentralized Finance (DeFi) ---------- **9**

3.3 Market and typical applications ---------- **9**

3.4 NFT-Fi and its combination with digital assets ---------- **10**

Chapter 4. Blockchain Applications in Real-Time Cybersecurity ---------- *11*

4.1 Overview: Why blockchain is suitable for cybersecurity ---------- **11**

4.2 Illustrative application in practice ---------- **12**

4.3 Blockchain in real-time monitoring and response ---------- **13**

4.4 Threats and limitations ---------- **15**

Chapter 5. Question from 1-4 ---------- *16*

5.1 Question 1: Blockchain & Related topic ---------- **16**

5.1.1 What is blockchain? ---------- 16

5.1.2 Types of Blockchains ---------- 16

5.1.3 Additional for blockchain: How it Works (high level flow) ---------- 16

5.1.4 Four Real-Time Use Cases (with concrete scenarios) ---------- 17

5.2 Question 2: Bitcoin & Crypto and related topic ---- 18
5.2.1 What is Bitcoin? ---- 18
5.2.2 Why is Bitcoin the most traded cryptocurrency? ---- 18
5.2.3 Explain the concept of Digital Wallet: ---- 18
5.2.4 Major issues in cryptocurrency ---- 19
5.3 Consensus and related technology ---- 20
5.3.1 What is "Consensus"? ---- 20
5.3.2 Explain Proof of work and Proof of Stake ---- 20
5.3.3 PoW vs PoS — key differences ---- 22
5.4 Ethereum & Hyperledger Related ---- 22
5.4.1 What is Ethereum? ---- 22
5.4.2 System & Network Architecture ---- 23
5.4.3 What's Hyperledger ---- 25
5.4.4 Ten differences across Ethereum, Hyperledger (Fabric/Besu), Bitcoin, and Dogecoin ---- 25
References* ---- *27

List of figures and table

FIGURE 2-1 THE CONTRACT INFORMATION, HANDLE DECENTRALIZED METADATA URIS 4
FIGURE 2-2 NFT IMPLEMENTATION WORKFLOW 5
FIGURE 2-3 HORSE NFT FOR GAMING SELL ON VVV MMARKETPLACE 6
FIGURE 3-1 THE DEFI WITH AMM MODEL WORKS IN DEX 8
FIGURE 4-1 BLOCKCHAIN DEPLOYMENT WORKFLOW FOR ENHANCED CYBERSECURITY 13
FIGURE 4-2 INTEGARED THE BLOCKCHAIN INTO CYBERSECURITY IN IOT – DRIVEN SMART CITIES 14
FIGURE 5-1 THE CYCLE TRANSACTION ON BLOCKCHAIN 17
FIGURE 5-2 ETHERIUM WORKFLOW 24

TABLE 2-1 THE NFT CHARACTERIZATION 3
TABLE 2-2 THE MAJOR NFT STANDARDS PROTOCAL 3
TABLE 3-1 COMPARISON OF TRADFI AND DEFI 9
TABLE 4-1 COMPARISON OF PUBLIC VS PRIVATE VS CONSORTIUM BLOCKCHAIN 11
TABLE 4-2 COMPARISON OF TRADITIONAL CYBERSECURITY AND BLOCKCHAIN-BASED CYBERSECURITY 13
TABLE 5-2 MAJOR ISSUES IN CRYPTOCURRENCY 19
TABLE 5-3 POW VS POS — KEY DIFFERENCES 22
TABLE 5-4 ETHEREUM ARCHITECTURE — EXPLORING NODE STRUCTURES AND CONSENSUS MECHANISMS 23

Chapter 1. Introduction

1.1 Background and motivation for report

Over 10 year ago, blockchain technology has become one of the most far-reaching innovations in the economic, social, and technological arenas. Blockchain initially emerged as a way to facilitate cryptocurrency transactions like Bitcoin, but has quickly expanded into a variety of areas, including Non-Fungible Tokens (NFTs), Decentralized Finance (DeFi), and cybersecurity-related applications (Consensus in Bitcoin, n.d.).

This report to investigate to answer for question "**Elaborate nft tokens? Explain defi and also illustrate how blockchain can support cyber security in real time world**". By examining the mechanics, applications, and challenges of each area, this document aims to demonstrate how blockchain is not merely a tool for digital currency but a foundational infrastructure for a new, digitally-native economy

1.2 Subject of the report

The report focuses on three main applications of blockchian that including:

- **NFTs**: Characteristics and survey of applications in digital assets in industries such as art, games and music.
- **DeFi**: Components of decentralized finance and survey of decentralized exchanges (DEXs), stablecoins.
- **Blockchain for Cybersecurity**: Application of blockchain to ensure data integrity and security.

1.3 Scope of report

This report is limited to an overview analysis and illustrated with practical examples from prominent projects. This report does not cover code development or testing, but focuses on synthesizing and evaluating available information and upcoming trends in the three main topics of the report.

For other question from 1 to 4, i will provide the short information at chapter 5.

Chapter 2. NFT (Non-Fungible Tokens) and Applications

2.1 Concept, characteristics

NFT stands for Non-Fungible Token; it is a Non-Fungible Token and is a cryptographic digital asset stored on the blockchain with a unique identifier and separating the Metadata to differentify them from each other. Unlike cryptocurrencies (Bitcoin or Ether) which are fungible at par, NFT cannot be traded or exchanged at par and is a non-fungible unit of data stored on the blockchain.

Characteristics of NFT:

- **Uniqueness**: Each NFT is uniquely identifiable and cannot be replicated, making it one of a kind
- **Indivisibility**: NFTs cannot be divided into small units like traditional currencies. They are either owned in full or not at all
- **Immutability**: Once an NFT is created, it cannot be modified or altered, ensuring the authenticity of the asset
- **Verifiability**: The ownership & authenticity of an NFT can be verified on a public blockchain ledger
- **Value**: The value of an NFT determined by the market based on factors such as scarcity, demand & perceived value.

NFTs stored on the blockchain are provided with public certificates of authenticity that provide metadata and proof of ownership. No one can modify the metadata, the ownership record for a given NFT. However, they do not restrict sharing or copying of the underlying digital files, and do not prevent the creation of NFTs with identical associated files; this creates challenges for managing NFTs across platforms.

Keypoint	Description	Note
Indivisible	ERC-721 has **no decimals** field; tokens are inherently whole units. **Fractional ownership** is possible via wrappers or newer standards (eg, EIP-7651).	If you plan revenue sharing, mention fractionalization or ERC-1155/other mechanisms.
Indestructible	Ledger entries are durable, but NFTs can be **burned** ; and **metadata** may be mutable if hosted off-chain unless frozen/pinned.	Prefer IPFS/Arweave + "freeze metadata" for immutability guarantees.
Ownership (two-way encryption)	Ownership = **who controls the private key** ; transfers rely on **digital signatures** and contract's ownerOf() —not "two-way encryption." Creators ≠ owners after transfer.	Use wallet key management best practices; show ownerOf(tokenId) in demos.
Traceability	Public chains are **auditable in real time** via explorers; addresses are **pseudonymous** (not real-name).	Add a note about privacy and on-/off-chain linkability.

Table 2-1 The NFT Characterization

2.2 Technical NFT components

This section summarizes the core building blocks that make non-fungible token (NFT) systems work in practice: the blockchain runtime, smart contracts, accounts and transactions, data/metadata handling, and the typical NFT activity lifecycle

2.2.1 Blockchain

A blockchain is an append-only, distributed ledger that links records (blocks) using cryptographic hashes and reaches consensus over their order. Public networks tolerate malicious or faulty nodes (a variant of the Byzantine Generals problem) by using consensus protocols. While Bitcoin pioneered this model with Proof-of-Work, most contemporary NFT activity occurs on Ethereum and EVM-compatible chains (e.g., Ethereum mainnet, Polygon, BNB Chain), which now use Proof-of-Stake for economic finality and energy efficiency. Alternative NFT platforms (e.g., Flow, Solana, Tezos, and enterprise frameworks such as Hyperledger Fabric) provide different performance, fee, and programming trade-offs. The blockchain's key contributions for NFTs are: globally ordered state transitions, tamper-evident history, and a neutral settlement layer shared by many applications.

2.2.2 Smart Contracts

On-chain programs managing NFT state and logic. The structure of NFTs is based on specific technical standards, notably ERC-721 and ERC-1155 on the Ethereum platform [1][2]. ERC-721 is the first standard dedicated to NFTs, defining how a single token can be issued, transferred, and ownership verified – a single contract can manage multiple NFTs with separate IDs. Meanwhile, ERC-1155 is an improved standard, allowing the issuance of both fungible and non-fungible tokens in the same smart contract, thereby reducing costs and increasing operational efficiency. The most important point of NFT is the smart contract; Smart contract not only manages the issuance and transfer of NFT, but also automates the terms attached to the digital asset. In addition to ERC-721 and ERC-1155, there are other standards, the main standards include:

Standard	Blockchain	Description	Key Features
ERC-721	Ethereum	First widely adopted NFT standard	Unique tokens, transfer functions, owner verification
ERC-721A	Ethereum	Optimized ERC-721	Reduced gas costs for multiple mint operations
ERC-1155	Ethereum	Multi-token standard	Supports both fungible and non-fungible tokens in one contract
SPL-NFT	Solana	Solana Program Library	High-speed, low-cost NFTs with native wallet integration
Bitcoin	Bitcoin	NFTs on Bitcoin	Inscriptions directly on Bitcoin blocks

Table 2-2 The Major NFT Standards protocal

2.2.3 Metadata, Data Encoding and Storage

The metadata is the next component that makes each NFT unique. On EVM chains, contract calls and events are ABI-encoded (hex) for deterministic parsing by all nodes. For NFTs, **on-chain state** stores canonical ownership (which address owns which tokenId) and a pointer—usually a URI—to metadata describing the asset. That metadata is a small JSON document (per ERC-721/1155 conventions) containing fields like name, description, and an image link.

Because media files (images, video, 3D, audio) are large, they are commonly **stored off-chain** on decentralized storage (IPFS, Arweave) or centralized storage (cloud/CDN) [8]. Storing hashes or content-addressed links (*e.g., ipfs://...*) provides verifiability. Importantly, owning an NFT does not automatically confer copyright or commercial rights to the underlying media; any license terms must be expressed explicitly (on-chain or off-chain).

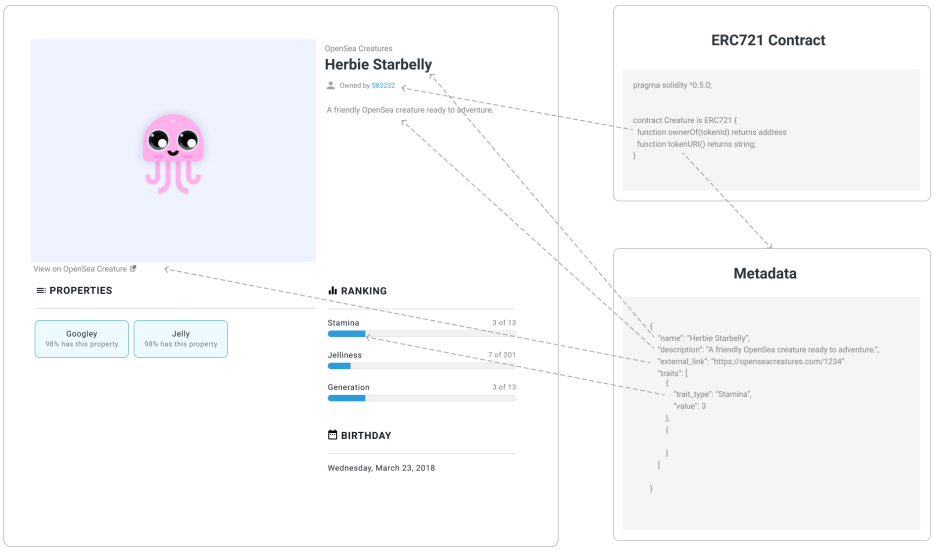


Figure 2-1 The Contract information, handle decentralized metadata URIs

Implementing token URI: For OpenSea to pull in off-chain metadata for ERC721 and ERC1155 assets, your contract will need to return a URI where we can find the metadata. To find this URI, we use the tokenURI method in ERC721 and d sERC1155.

```
function tokenURI(uint256 _tokenId) public view returns (string) {
  return string.concat(
     baseTokenURI(),
     Strings.uint2str(_tokenId)
  );
}
```

- **Metadata structure** is the factor that makes NFT unique. Metadata usually includes the following information:

```
{ "name": "CryptoPunk #3100",
"description": "An NFT in the CryptoPunks collection",
"image": "ipfs://Qm...",
"attributes": [
{ "trait_type": "Headband", "value": "Blue" },
{ "trait_type": "Background", "value": "Gray" } ] }
```

2.2.4 NFT Activity Lifecycle (Operational Phases)

NFT-related activities generally follow four operational phases:

- **Mint** (Creation): A contract creates new tokens (mint), assigning each a unique tokenId and setting initial metadata/URI and owner. Optionally, the contract records royalty info (ERC-2981) and freezes metadata to signal immutability.
- **Approve** (Delegation for Market Ops):The owner grants permissions (approve/ setApprovalForAll) so a marketplace or escrow contract can transfer the NFT upon sale. This minimizes trust in intermediaries while enabling flexible listing flows.
- Update / Burn (Curation and Lifecycle End)
- Transfer / Trade / Settle (Exchange): A sale or swap settles when a validated transaction updates contract state: the buyer pays (in native coin or ERC-20), fees/royalties are distributed per marketplace logic, and Transfer events finalize new ownership.

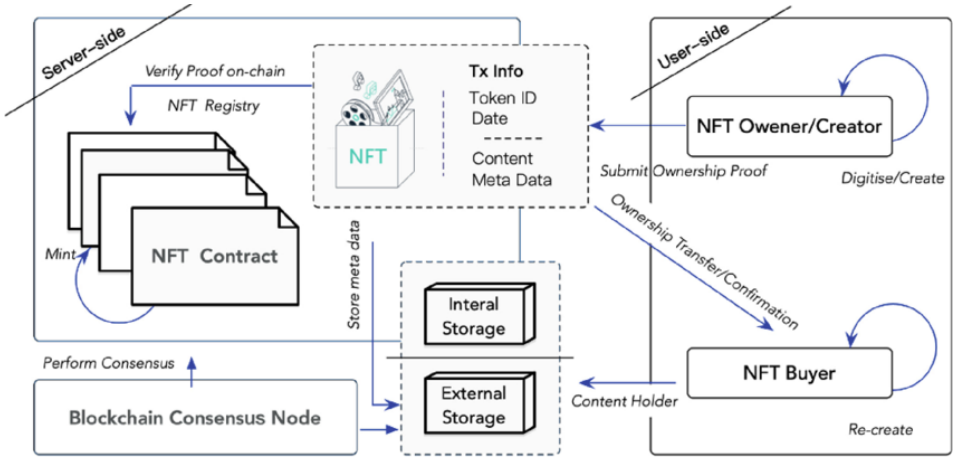


Figure 2-2 NFT Implementation Workflow

The combination of standardized structure, metadata and smart contracts, NFTs are both transparent (anyone can verify transaction history), unique (each token is attached to its own metadata), and have the ability to operate automatically financially (distribute royalties, manage benefits). This is the technical foundation that has brought NFTs far beyond the role of a "passing trend", becoming an indispensable part of the modern blockchain ecosystem. However, buying/selling an NFT usually only transfers the ownership of the token/certificate; copyright is still subject to a legal contract and does not automatically transfer with the token unless explicitly stated in the smart contract[9].

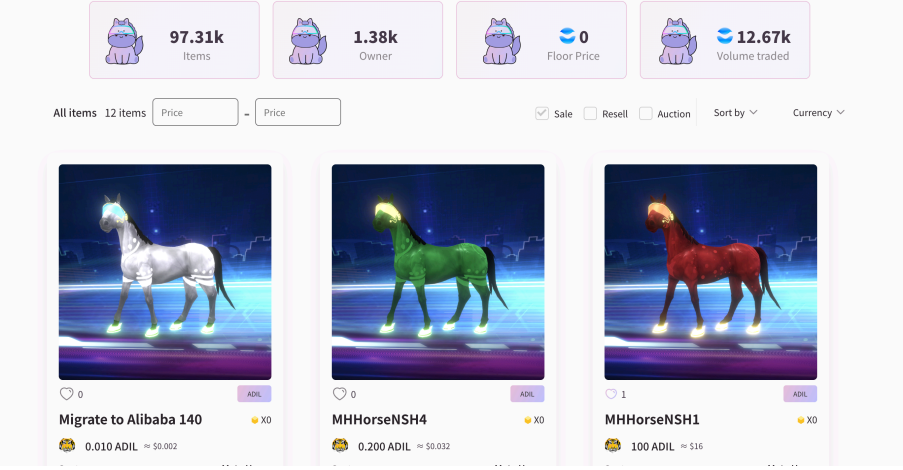


Figure 2-3 Horse NFT for Gaming sell on VVV Mmarketplace

2.3 NFT Market from Marketplace and Ecosystem Perspective

The NFT market reached $17 billion in transactions in 2021 (NonFungible.com), but has contracted significantly since then: from around $683.9 million in 2024, it is expected to decline by 11.01% in 2025 to around $504.3 million, shifting from speculation to utility-driven applications (down 70% volume from the 2021 peak) [3].

Marketplace: are online platforms that play a central role in the NFT ecosystem, where users can publicly buy, sell, and exchange digital assets. Their main functions and tasks include:

- **Minting (NFT Minting)**: Provides tools for artists and creators to convert artwork, videos, music, or any digital asset into NFTs on the blockchain. Some platforms also support "lazy minting" (minting NFTs without initial gas fees), only charging fees when the work is sold.
- Buying and Trading:
  - Provide a secondary market for minted NFTs.
  - Supports various transaction methods such as fixed price, auction, or offers.
  - Facilitate the transfer of ownership in a secure and transparent manner.
- Transaction Fees and Royalti (Royalty Fees): Collect fees to maintain the platform and return them to the original creators:
  - Marketplace Fee: Platform fee charged on each successful transaction
  - Gas Fee: Blockchain network fee (Ethereum, Solana,…) paid by users to perform transactions. This fee is not controlled by the marketplace.
  - Royalty Fee: Automatically transfers a portion of revenue from secondary sales back to the original creator, helping them earn a sustainable income.
- Marketplace Classification:
  - General Marketplaces: A place to trade a variety of NFTs (eg OpenSea, Blur).

- Niche Marketplaces: Focus on a specific niche (e.g. Foundation focuses on high-end art, NBA Top Shot for sports).
- Curated Marketplaces: Require artist approval before allowing minting and listing, ensuring quality and exclusivity.

Current NFT Ecosystems and Marketplaces: - Art: CryptoPunks and BAYC become cultural icons, NFT ownership means joining exclusive communities.

- Sports: NBA Top Shot sells “basketball moments” as digital assets.
- Education: MIT Blockcerts issues NFT diplomas, anti-counterfeiting.
- Finance (NFT-Fi): collateralize NFTs to borrow stablecoins, fragment NFTs to increase liquidity.
- Metaverse: Decentraland, The Sandbox use NFTs for virtual land, items, identities.

2.4 Challenges of NFT

As above, NFTs have many practical applications and can thrive; but NFTs also face many problems that need to be solved to become a sustainable part of the digital economy.

- First, strong price fluctuations make it easy to fall into a state of speculation and bubbles. Many types of NFTs that have no real value and are difficult to quantify are sold at very high prices during the "fever" period.
- Second, copyright issues are another core issue: there have been many cases where users mint NFTs from artwork they don't own, causing complex legal disputes.
- Third, the legal framework in most countries has not kept pace with the development of NFTs, leading to a legal vacuum that puts investors and artists at risk in protecting.

NFTs have long-term promise in use-cases such as education, utility NFTs, and the metaverse, but NFT adoption for digital assets has plateaued (see 2021–2025 transaction data [3]). The decentralized finance (DeFi) model described below opens up a new service layer where NFTs are used as collateral or combined with DeFi to create new products. In the metaverse, NFTs serve as a foundation for asset ownership and identity, bringing users into virtual spaces that operate like the real economy. NFTs have the potential to become **the fundamental infrastructure of the digital economy** , where every asset is digitized, transparently traded, and integrated with DeFi.

Chapter 3. DeFi Expectations and Challenges

3.1 Concept and operating

DeFi, short for Decentralized Finance, is an ecosystem of financial services built on a public blockchain, in which smart contracts replace the role of traditional banks and financial institutions. Instead of needing an intermediary such as a commercial bank to validate transactions, DeFi allows people to interact directly through decentralized applications (dApps), where terms are automatically enforced by code in many different programming languages such as RUST, SOLIDITY. The operating principle of DeFi is based on several core elements:

- First, decentralization: transactions are confirmed by a network of nodes using a consensus mechanism instead of a single authority.
- Second, transparency: all transactions and contract states are publicly stored on the blockchain, anyone can check.
- Third, immutability: once a transaction has been recorded in a block, it cannot be modified, ensuring data integrity.
- Fourth, programmability: smart contracts allow the construction of complex financial instruments, from lending, borrowing, issuing stablecoins, to secondary products.

To illustrate, we can consider the operating mechanism of a DEX (Decentralized Exchange) like Uniswap. Instead of using an order book like a traditional exchange, Uniswap uses an Automated Market Maker (AMM) model, where the price of an asset is determined by the formula (xy = k), where (x) and (y) are the quantities of two tokens in the liquidity pool.

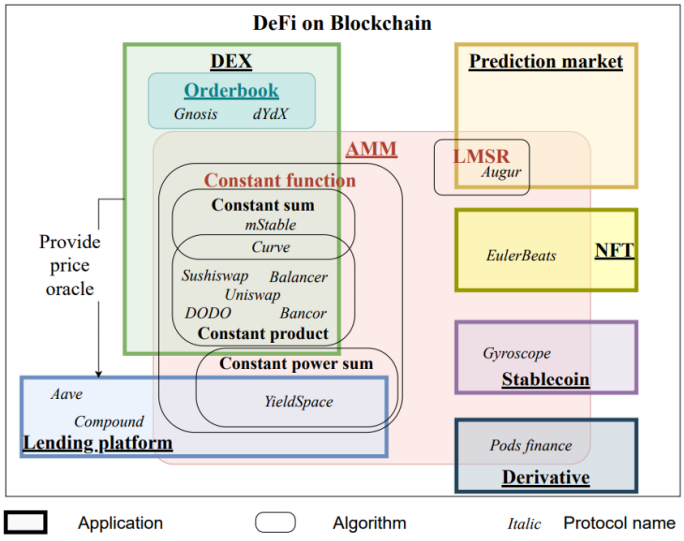


Figure 3-1 The Defi with AMM model works in DEX

Wtith this mechanism, anyone can become a liquidity provider by depositing tokens into the pool and receiving transaction fees, while users can trade instantly without relying on a centralized order book. This clearly demonstrates the fundamental difference between DeFi and traditional finance.

3.2 Traditional Finance vs. Decentralized Finance (DeFi)

TradFi relies on licensed intermediaries (banks,brokers) under national regulation; DeFi replaces institutions with smart contracts on public blockchains, aiming for open, programmable finance.

Dimension	Traditional Finance (TradFi)	Decentralized Finance (DeFi)
Access & onboarding	Account opening with KYC/AML, jurisdiction-based access	Permissionless access with a wallet; pseudonymous; compliance often pushed to gateways (exchanges, fiat ramps)
Intermediation & custody	Banks/brokers/custodians hold assets; user has legal claim	Self-custody (user controls keys) or smart-contract custody; code enforces rules
Governance	Corporate boards + regulators	On-chain/off-chain governance (token voting, multisig); varying decentralization
Market hours	Banking hours; exchanges may have sessions	24/7/365 programmatic markets
Settlement	Netting & delayed finality (e.g., T+2); reconciliation across ledgers	Atomic on-chain settlement (block finality) subject to network conditions
Transparency	Proprietary ledgers; disclosures via reports	Public ledgers; state and code are auditable
Pricing & liquidity	Order books & market makers; central bank rates	AMMs (constant product, etc.), algorithmic rate curves; oracle-fed prices
Risk model	Credit, liquidity, operational, conduct risks in firms	Code risk, oracle/manipulation, governance capture, liquidity/leverage feedbacks
Consumer protection	Deposit insurance, best-execution, dispute mechanisms	Limited recourse; audits, bug bounties, insurance pools are emergent
Compliance perimeter	Mature & harmonized (Basel, FATF)	Evolving: FATF VA/VASP, travel rule; accountability debates
Composability	Low; bilateral integrations via contracts/APIs	High; “money legos” enable protocol stacking but increase contagion
Throughput & cost	High off-chain capacity; fees vary by rails	L1 constrained; L2 improves cost/throughput; fees vary with congestion
Privacy	Account privacy protected by law; bank secrecy (varies)	Transparent by default; privacy via mixers/L2s is contested
Resilience	Institutional backstops (lender of last resort)	Protocol-level risk buffers; no central backstop

Table 3-1 Comparison of TradFi and DeFi

3.3 Market and typical applications

The DeFi market has exploded since 2020, with the Total Value Locked (TVL) reaching over $100 billion in 2021, according to DefiLlama data [3]. This figure fluctuated sharply due to the 2022 incidents (Terra/Luna, FTX), dropping sharply but gradually recovering: by September

2025, TVL reached around $156,939 billion, with Aave leading the way ($40,496 billion on 17 chains) and Lido ($38,071 billion on 5 chains), up 1.95% in the last 24 hours [3].
Some typical applications in DeFi include:

- Decentralized Exchanges (DEXs): Uniswap, SushiSwap, Curve Finance. These are platforms that allow users to swap tokens without the need for an intermediary.
- Lending and borrowing platforms: Aave, Compound. Users can deposit digital assets to earn interest, or use assets as collateral to borrow other tokens.
- Stablecoin: MakerDAO issues DAI – a decentralized stablecoin pegged to the USD, which helps minimize the risk of price fluctuations in transactions.
- Secondary Markets and Insurance: Synthetix enables the creation of secondary assets that simulate stocks, gold, or fiat currencies; Nexus Mutual provides decentralized insurance for smart contract risks or cyberattacks.

Specific case studies illustrate the potential of DeFi:

- **MakerDAO and DAI**: Allows anyone to collateralize ETH or other digital assets to create the DAI stablecoin. This model has maintained stability even during periods of high market volatility, proving the viability of decentralized stablecoins.
- **Aave**: Implemented flash loans – instant loans that require no collateral, as long as they are repaid in the same transaction. Despite the flexibility they offer, flash loans have also been used to manipulate the market, that DeFi opens up both opportunities and challenges
- **Uniswap**: Become the largest DEX with tens of billions of USD in monthly trading volume, proving that the AMM model can replace traditional in many situations.

3.4 NFT-Fi and its combination with digital assets

A recent prominent trend is NFT-Fi, which is a combination of NFT and DeFi. In which, NFT is considered as an asset that can participate in financial transactions:

- Collateralize NFTs to Borrow Stablecoins: For example, a collector who owns a valuable Bored Ape NFT can collateralize that NFT to borrow USDC without selling the asset.
- Fractionalization of NFTs: A valuable NFT can be divided into multiple ERC-20 tokens for multiple people to own and trade, increasing liquidity.
- NFT Trading on DEXs: Combining decentralized exchanges (DEXs) and centralized exchanges (CEXs) to expand trading scope and provide more access channels for investors.

The above direction raises an important question: for NFTs to have real financial value, is it necessary to have real assets as collateral? Many experts believe that NFTs need to be attached to tangible assets (such as real estate or goods) and verified by an independent entity. This is the development direction that helps NFT-Fi no longer be a virtual asset but an identifier for digital assets, becoming a useful tool in the digital economy.

Chapter 4. Blockchain Applications in Real-Time Cybersecurity

4.1 Overview: Why blockchain is suitable for cybersecurity

In the context of digital transformation, data and information are strongly digitized, so cybersecurity becomes a vital factor for every organization. Attacks are increasingly sophisticated: from ransomware that encrypts all data, attacks on software supply chains, to digital identity fraud. Traditional security systems, which are based on a centralized model, are increasingly exposed to weaknesses when attackers only need to penetrate one central point to gain complete control.

Blockchain emerges as a distributed security infrastructure layer where data is no longer dependent on a central server but distributed across multiple nodes. Basic characteristics such as immutability, transparency, consensus, and cryptography make blockchain an ideal candidate for cybersecurity reinforcement.

At a principle level, blockchain can play a role in four core attributes of information security according to the CIA- AAA model:

- Confidentiality: data can be encrypted before being written to the blockchain, only the person with the key can decrypt it.
- Integrity: data is hashed and distributed across multiple nodes, no one can change it without being detected.
- Authentication and Non-repudiation: the digital signature of an organization or individual helps ensure that the creator of the data is real, and cannot be denied later.
- Access control: decentralized applications (dApps) allow owners to decide who can see data and to what extent.

To compare the types of blockchains suitable for cybersecurity:

Type	Throughput	Privacy	Governance	Cost
Public	Low (eg, Bitcoin 7 TPS)	Low (public data)	Decentralized, community	Low (network fee)
Private	High (thousands of TPS)	High (members only)	Focus, business	High (custom built)
Consortium	Medium	Average (group members)	Sharing between parties	Medium

Table 4-1 Comparison of Public vs Private vs Consortium Blockchain

For cybersecurity use-cases like log audits, private/consortium is often used with hash anchoring on the public chain to balance immutability and privacy. Highlights of blockchain in Cybersecurity:

- **Resist cyber attacks**: Blockchain can help counter cyber attacks thanks to its decentralized architecture and immutability.
  - **DDoS Attack**s: Distributed denial of service (DDoS) attacks can cripple an organization. However, these attacks are difficult to carry out on a blockchain network because it has no single point of failure. Instead of relying on a vulnerable centralized

server, blockchain-based systems can use decentralized solutions like IPFS (Interplanetary File System) to replace the centralized DNS system, helping to protect against DDoS attacks.

- **Phishing and Changing Wallet Addresses**: Attackers often target weak points, such as phishing for personal information or changing an Ether wallet address on a website to transfer funds to another account. Blockchain can solve this problem by using a distributed public key infrastructure to authenticate devices and users instead of very weak passwords. This makes the use of fake certificates almost impossible.

- **Data and Personal Information Protection**: One of the biggest problems is that personal data (valuable data and a target for hackers) is stored by many different organizations, leading to attacks like Equifax and Uber causing huge damage. Blockchain can be used to allow individuals to store and control their own information. An example is Civic , built on the Bitcoin blockchain, which gives individuals control over their data.
  - **Reduced costs**: When combined with digital identity solution providers (like Civic), blockchain can significantly reduce the costs of processes like KYC/AML (know your customer/anti-money laundering) and reduce the need for organizations to store and protect customers' personal data
  - **Encryption**: Information on the blockchain can be encrypted, even on a public blockchain, so that only the owner of the private key can read it. This ensures that even if an attacker breaks into the system, they cannot read the encrypted information.

4.2 Illustrative application in practice

To see more clearly the potential of blockchain in cybersecurity, we can analyze some specific application areas:

- **Digital Identity Management**: Estonia is a pioneer in e-Residency, which gives citizens digital identities on the blockchain. This makes identity forgery almost impossible.
- **Education**: MIT is launching Blockcerts, a blockchain-based diploma that employers can authenticate with just a few taps. This is especially important in the digital education environment, where counterfeiting of diplomas is a global problem.
- **Supply Chain**: IBM Food Trust uses blockchain to track food from farm to supermarket. This not only increases trust but also reduces the risk of fraud, an issue directly related to data security and product quality.
- **IoT Security**: US-based company Xage has applied blockchain to secure IoT devices in the energy industry, ensuring that no single node can be hijacked to cause a system crash.
- **Secure Domain Names**: Ethereum Name Service (ENS) provides a decentralized domain name system, avoiding spoofing or censorship from a centralized authority.

Additionally, in the cybersecurity space, smart contracts can be used to automate security processes. For example, a contract can be set up to automatically lock an account or pause a transaction if suspicious activity is detected, speeding up response to threats. Smart contracts can

also be used to conduct transparent and automated security audits of systems, alerting to vulnerabilities before they are exploited.[13]

Characteristic	Traditional System	Blockchain-based system
Architecture	Centralized, data is stored on a single server	Decentralized, data is distributed across multiple network nodes
Weaknesses	Vulnerable to single point of failure attacks, such as DDoS attacks on servers	Resistant to DDoS attacks due to lack of centralized targeting; however other vulnerabilities still exist
Data integrity	Data can be edited and changed in ways that are difficult to detect	Immutable data, any change breaks the chain and is rejected in real time
Accessibility	Traceability can be complex and time consuming due to the lack of a common ledger	Provide instant and transparent traceability
Authentication mechanism	Rely on trusted intermediaries (e.g. Certification Authorities) and humans	Based on consensus algorithm and cryptographic encryption between network nodes
Automation	Dependent on humans and manual processes	Can be automated through smart contracts, minimizing human intervention

Table 4-2 Comparison of Traditional Cybersecurity and Blockchain-Based Cybersecurity

These examples show that blockchain is not just a theoretical concept, but has been deployed in many real-world scenarios, from government to business, from education to industry.

4.3 Blockchain in real-time monitoring and response

One of the highlights of blockchain is its ability to support real-time network security monitoring. In a traditional system, log data from servers is sent to an analysis center (SIEM). The weakness of this model is that if the center is attacked or modified, the entire system becomes unreliable.

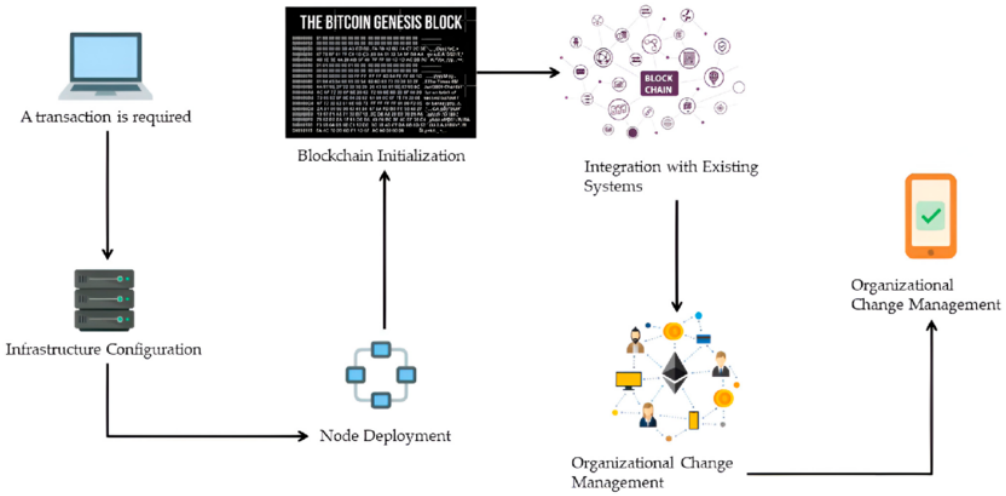


Figure 4-1 Blockchain deployment workflow for enhanced cybersecurity

When integrating blockchain, logs or hashes of logs can be written directly to the chain, ensuring that every event has immutable evidence. Additionally, smart contracts can be programmed to automatically react when anomalies are detected, such as temporarily locking accounts, alerting administrators, or pausing transactions. However, writing entire logs to the public chain is not recommended due to high costs and privacy tradeoffs; instead, use off-chain SIEM + on-chain hash anchoring (or Merkle root) to balance [9]. This model helps build an automatic detection and response mechanism, significantly reducing the time from detection to prevention, which many traditional systems find difficult to meet.

In addition, the increasingly popular Internet of Things (IoT) systems are also facing serious security vulnerabilities due to their dependence on central servers. If they are integrated with blockchain, it will enable the transformation of the IoT model from "centralized" to "decentralized autonomous". IoT devices must communicate and send data to a central server for processing. This creates an attractive target for hackers and causes network congestion as the number of devices increases.[15].

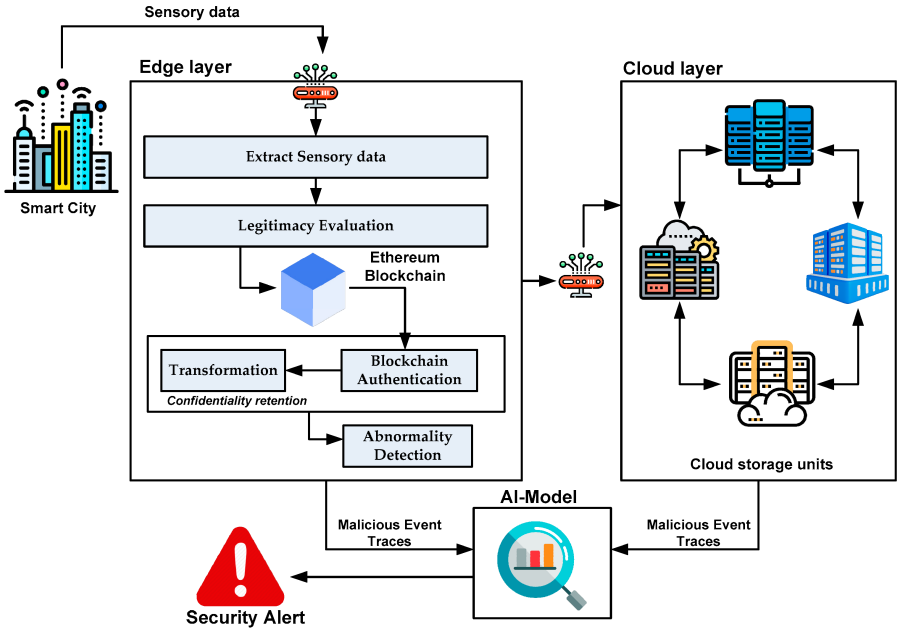


Figure 4-2 Integared the blockchain into Cybersecurity in IOT – Driven smart Cities

By integrating blockchain, each IoT device can be assigned a unique identifier on the blockchain. Data is only transmitted between verified devices, ensuring authenticity in real time. Information collected from sensors, such as temperature or location, can be stored directly on the immutable ledger, preventing data tampering. Furthermore, blockchain allows IoT devices to act as nodes in a peer-to-peer network, allowing them to communicate and transact directly with each other via smart contracts without the need for an intermediary. This creates a decentralized autonomous organization (DAO) of IoT devices, which operates independently and is more secure against attacks on a central server, while reducing costs and latency.

4.4 Threats and limitations

While blockchain has security advantages, it is not completely immune to issues. Blockchain's practical security vulnerabilities often stem not from the fundamental nature of the technology, but from problems in its implementation.

- **User Wallet Attacks**: These attacks target how humans interact with the blockchain, with vulnerabilities including buggy software, mining malware, and hash function vulnerabilities.
- **Attack 51%**: An attacker who controls more than 50% of the network nodes (in networks with a small and fixed number of nodes) can control the hash rate and create an alternative fork to gain dominance and make fraudulent transactions. A situation similar to a double-spending attack. And another such attack on Ethereum Classic in August 2020 resulted in a loss of about $5.6 million in ETC.
- **Smart Contract Attacks**: Vulnerabilities in the source code of smart contracts can pose a huge risk. For example, a bug in an Ethereum contract caused a loss of $80 million in 2016. One of the most common vulnerabilities is a reentrancy attack , where a malicious contract can repeatedly call a function in another contract to withdraw funds multiple times.

Chapter 5. Question from 1-4

5.1 Question 1: Blockchain & Related topic

5.1.1 What is blockchain?

A **blockchain** is a distributed, append-only ledger where data (transactions, state updates) are grouped into **blocks**, cryptographically linked (via block hashes), timestamped, and replicated across a **peer-to-peer (P2P) network**. Immutability arises from hash chaining + consensus; tampering one block changes its hash and breaks all successors, so honest nodes reject it.

Key properties: decentralization, transparency/auditability, fault tolerance, tamper-resistance, programmable logic via **smart contracts**.

5.1.2 Types of Blockchains

We have 5 types of blockchain network base one the Pros:

- Public (permissionless): Anyone can read/write/validate. Examples: Bitcoin, Ethereum.
  Pros: openness, censorship resistance. Cons: lower TPS, probabilistic finality (varies).
- Private (permissioned, single org): One owner controls participation.
  Pros: performance, privacy, governance clarity. Cons: trust anchored in operator.
- Consortium (federated): Multiple known organizations co-govern (e.g., Hyperledger Fabric, R3 Corda).
  Pros: shared control, compliance, privacy channels. Cons: coordination overhead.
- Hybrid: Mix of public anchoring + private data/logic (L2 rollups posting proofs on L1).
- Layering (by scalability role):
  - L1 base chain (security + data availability)
  - L2 (rollups/channels for scalable execution).

5.1.3 Additional for blockchain: How it Works (high level flow)

- Transaction creation: Users sign transactions with private keys.
- Gossip to network: Nodes propagate txs over P2P.
- Validation: Nodes check signatures, balances, nonce, and smart-contract rules.
- Block proposal:
  - PoW (Proof of Work): Miners compete to find a nonce making block hash < target.
  - PoS (Proof of Stake): Validators are selected (stake-weighted) to propose/attest.
- Consensus & Finality: Network agrees on the canonical block sequence (e.g., Nakamoto consensus for PoW, BFT-style finality layers for PoS).
- State update: Transactions are executed; global state (account balances, contract storage) is updated; blocks appended.

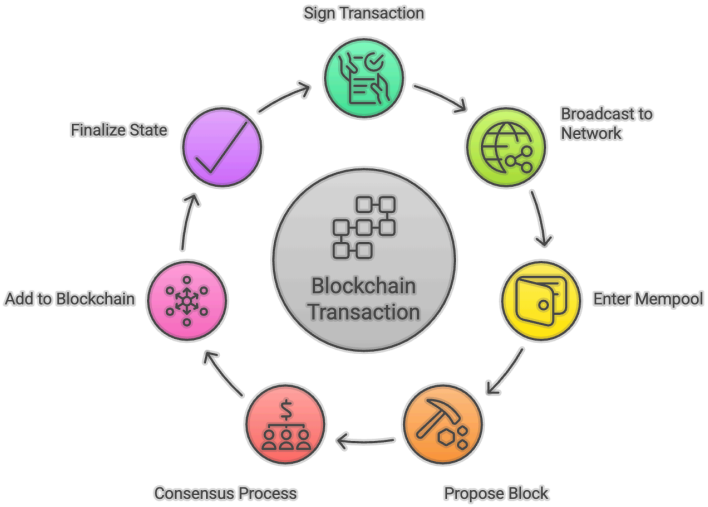


Figure 5-1 The Cycle Transaction on Blockchain

5.1.4 Four Real-Time Use Cases (with concrete scenarios)

- **1. Cross-Border Payments & Stablecoins**
  - Problem: Slow, costly remittances with many intermediaries.
  - Blockchain solution: On-chain stablecoins (e.g., USD-pegged) enable near-instant settlement, 24/7, with transparent fees.
  - Impact: Faster payroll/remittance rails for SMEs, improved treasury flows.
- **2. Supply Chain Provenance & Traceability**:
  - Problem: Counterfeits and opaque sourcing.
  - Blockchain solution: Each custody handoff (farm → shipper → processor → retailer) is recorded; tokenized lots or NFT batch IDs bind physical to digital.
  - Impact: Auditable trails, recall efficiency, ESG reporting (e.g., coffee/cocoa, pharma cold-chain).
- **3. DeFi (Decentralized Finance) & Tokenization**:
  - Problem: Fragmented access to financial products.
  - Blockchain solution: Smart contracts for lending/borrowing, DEX AMMs, on-chain collateral; tokenization of real-world assets (RWA) like T-bills or invoices.
  - Impact: Programmable liquidity, global access, composability; transparent risk (on-chain metrics).
- **4. Digital Identity & Verifiable Credentials (DID/VC):**
  - Problem: Repeated KYC, data silos, privacy leakage.
  - Blockchain solution: Decentralized Identifiers anchored on-chain; Verifiable Credentials issued off-chain, selectively disclosed by users; on-chain revocation registries.

- Impact: Reusable identity, privacy-preserving verification for onboarding, healthcare, and education.

5.2 Question 2: Bitcoin & Crypto and related topic

5.2.1 What is Bitcoin?

Bitcoin (BTC) is a peer-to-peer electronic cash system (Nakamoto, 2008) that maintains a **public, append-only ledger (**blockchain) secured by **Proof-of-Work (PoW)**. Transactions consume and create UTXOs (unspent transaction outputs); miners group transactions into blocks, compete by hashing, and the longest valid chain becomes canonical. **Scarcity is encoded**: a hard **cap of 21 million BTC** with block-subsity halving ~every 4 years.

Purpose: censorship-resistant value transfer and store-of-value ("**digital gold**").

5.2.2 Why is Bitcoin the most traded cryptocurrency?

- **First-mover & Lindy effects**: earliest network, strongest brand, deep developer/tooling and educational base.
- **Liquidity & market microstructure**: tight spreads, deepest spot books, largest derivatives (futures/options) open interest → easier hedging and price discovery.
- **Institutional access**: widest availability on exchanges, custodians, ETFs/ETPs in multiple jurisdictions → larger capital base.
- **Narrative clarity**: simple, credibly-scarce monetary asset with predictable issuance → macro hedge thesis.
- **Regulatory familiarity**: compared to many altcoins, BTC often has clearer treatment → lower perceived compliance risk.
- **Infrastructure resilience**: most battle-tested PoW hash rate and node count → higher perceived security.

5.2.3 Explain the concept of Digital Wallet:

A **digital (crypto) wallet** is software/hardware that **manages keys** to authorize blockchain transactions.

- **Keys & addresses**:
  - Private key: proves control; must be kept secret.
  - Public key / Address: shared to receive funds.
  - HD wallets (BIP-32/39/44): derive many keys from a seed phrase (12–24 words).
- **Types**:
  - Custodial: a third party holds keys (e.g., exchanges). Pros: easy recovery; Cons: counterparty risk.
  - Non-custodial: you hold keys (self-custody). Pros: sovereignty; Cons: you bear security/recovery.
  - Hot vs Cold: internet-connected apps vs offline devices (hardware wallets, air-gapped).

- Multisig / MPC: split control across devices/people to reduce single-point failure.

❖ What a wallet does:

- Tracks your UTXOs,
- Builds a transaction
- Sgns it locally with your private key
- Broadcasts to the P2P network
- Updates balance after confirmations.

5.2.4 Major issues in cryptocurrency

Table 5-1 Major issues in cryptocurrency

Issue	Why it matters	Typical mitigations
Volatility & leverage cycles	Sharp drawdowns/liquidations harm users and adoption	Risk controls, derivatives for hedging, stablecoin use for cash needs
Security & key management	Exchange hacks, phishing, seed loss	Hardware wallets, multisig/MPC, passkeys, better UX/recovery schemes
Scams & market manipulation	Rug pulls, wash trading erode trust	KYC/AML on ramps, audits, on-chain analytics, consumer education
Regulatory uncertainty	Differing rules across countries	Clearer classifications, disclosures, licensed custodians
Scalability & fees	L1 congestion → high fees/slow tx	L2s (e.g., Lightning for BTC; rollups for EVM), batching, better fee markets
Privacy vs compliance	Transparent ledgers vs data protection	Selective disclosure, zero-knowledge proofs, regulated privacy tools
Energy (PoW)	Environmental concerns, jurisdictional pushback	Migration to renewables, efficiency gains, demand-response participation
Custody concentration	Centralized exchanges/ custodians pose systemic risk	Self-custody, proof-of-reserves, distributed validators/miners
Interoperability & UX	Chain silos, complex signing → user errors	Safer bridges, account abstraction, human-readable intents

5.3 Consensus and related technology

5.3.1 What is "Consensus"?

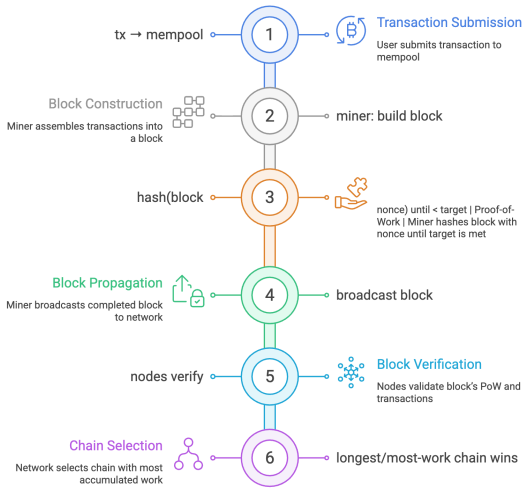
Consensus is the protocol a decentralized **network uses to agree on a singl**e, valid history of transactions (the canonical chain/state) despite faults or adversaries. It solves:

- **Sybil resistance**: prevent fake identities from controlling the network.
- **Fork choice & finality**: pick one chain when multiple candidates exist and know when it's "final enough."
- **Incentive alignment**: reward honest participation; penalize misbehavior.

5.3.2 Explain Proof of work and Proof of Stake

- **Proof of Work (PoW):**
  - **Idea**: Security comes from **scarce external work** (electricity + hardware). Miners find a nonce so the block hash < difficulty target.
  - Flow (Bitcoin-style)

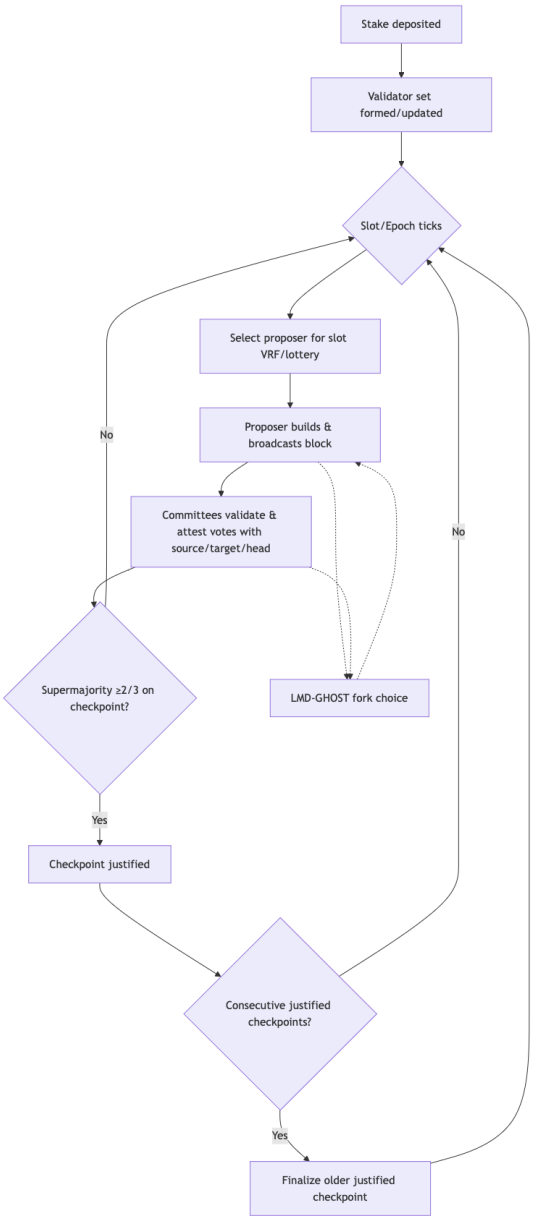
Image 5-1 Bitcoin PoW: Creation and Consensus Process



  - **Properties**:
    - Sybil resistance: costly hashing makes attacks expensive.
    - Probabilistic finality: confidence grows with confirmations (more blocks on top).
    - Costs: high energy use; specialized hardware (ASICs).
    - Attacks & mitigations: 51% reorgs (mitigate via hash diversity, pool decentralization), selfish mining (protocol/relay tweaks), fee sniping.
- **Proof of Stake (PoS)**:
  - Idea: Security comes from **economic stake** locked in the protocol. Validators are pseudo-randomly selected to **propose blocks;** others **attest/vote**. Misbehavior can be **slashed** (stake destroyed)

- Flow (modern PoS with BFT)

Image 5-2 Ethereum PoS: Creation and Consensus Mechanism



- **Properties**:
  - **Sybil resistance**: weight = staked coins, not identities.
  - **Finality**: can achieve economic finality within minutes via supermajority votes.
  - **Capital costs**: requires capital lockup + operational uptime.
  - **Attacks & mitigations**: long-range attacks (mitigate with weak subjectivity checkpoints), nothing-at-stake (slashing), censorship (inclusion lists/CR-lists), stake centralization (delegation designs, permissionless entry).

5.3.3 PoW vs PoS — key differences

Table 5-2 PoW vs PoS — key differences

Dimension	Proof of Work (PoW)	Proof of Stake (PoS)
Sybil resistance resource	External: electricity + hardware (hashpower)	Internal: native token stake
Who proposes/validates	Miners with highest hashpower	Stakers/validators proportional to stake
Security cost to attack	Buy/commandeer majority hashpower + energy	Acquire/control ≥1/3–1/2 of stake (model-dependent)
Finality	Probabilistic; grows with depth (confirmations)	Economic/BFT finality in epochs (minutes)
Energy profile	High, tied to difficulty	Low, mainly server operations
Hardware	Specialized (ASIC/GPUs), logistics-heavy	Commodity servers; HSM/TEE optional
Penalties	Lost OPEX if attack fails	**Slashing** burns stake; inactivity penalties
Reorg characteristics	Deep reorgs possible with enough hashpower	Deep finalized reorgs economically/cryptographically deterred
Bootstrapping	Needs miners to invest pre-fees	Needs initial distribution & anti-cartel design
Centralization pressures	Pooling by variance/ASIC supply chains	Large staking providers/delegation; liquidity derivatives
Censorship resistance	High if hashpower geographically diverse	Varies; mitigations via inclusion lists, PBS/mev-boost-like designs
Environmental debate	Significant	Reduced

5.4 Ethereum & Hyperledger Related

5.4.1 What is Ethereum?

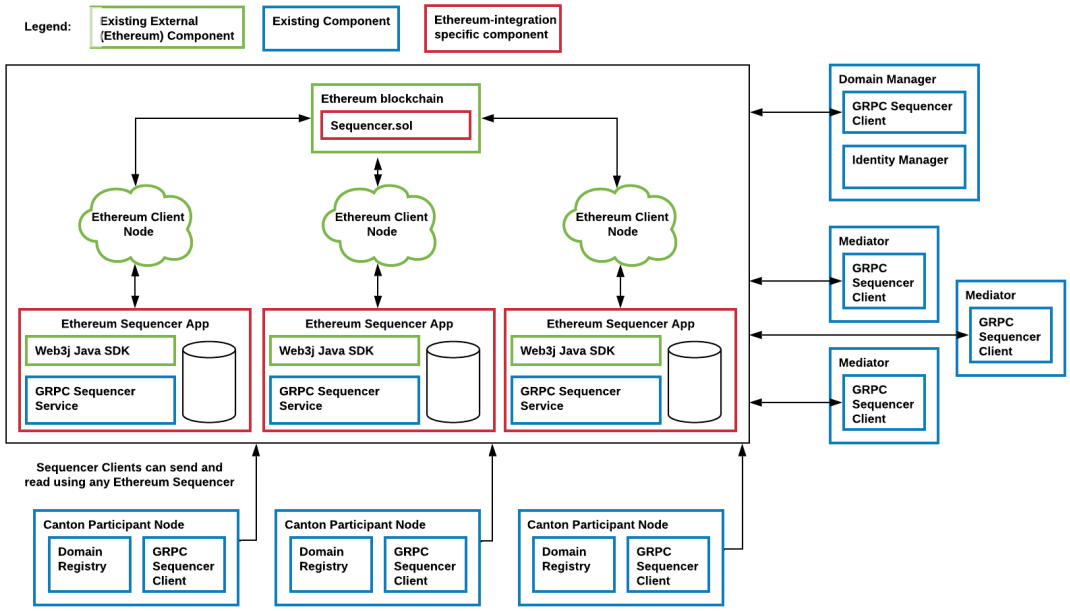
Ethereum is a general-purpose**, public blockchain for programmable trust**. It maintains an account-based global state and runs smart contracts in the **Ethereum Virtual Machine (EVM).** Since the Merge (2022), Ethereum secures blocks via **Proof of Stake**: validators propose/attest to

blocks; finality occurs in epochs. The base layer emphasizes neutrality and security, while **scalability is achieved via Layer-2 rollups (optimistic/zk).**

5.4.2 System & Network Architecture

- **Logical layers**:
  - **Application layer**: dApps, wallets, RPC gateways, indexers (TheGraph), oracles.
  - **Execution Layer (EL):** client implementations (e.g., Geth, Nethermind, Erigon, Besu). Executes EVM bytecode, manages mempool, state trie (**Merkle-Patricia**), gas accounting, and exposes JSON-RPC.
  - **Consensus Layer (CL)**: Beacon chain clients (e.g., Prysm, Lighthouse, Teku, Nimbus). Runs PoS duties: validator registry, proposer/committee selection, attestations, **LMD-GHOST** fork choice, and **Casper FFG** finality.
  - **Data Availability**: L1 calldata + **EIP-4844 blobs** (proto-danksharding) improving L2 data costs (full sharding is the longer-term roadmap).

Table 5-3 Ethereum Architecture — Exploring Node Structures and Consensus Mechanisms

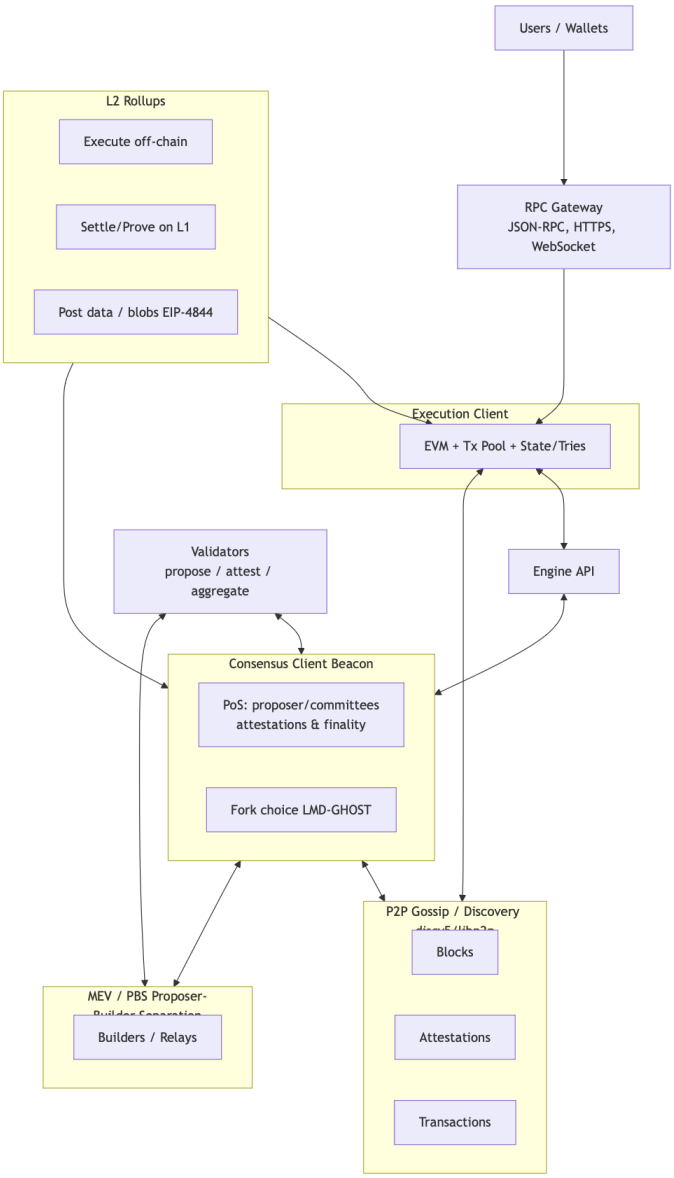


- **Validator workflow (PoS):**
  - Stake 32 ETH → enter validator set.
  - Per slot (~12s): one validator proposes a block; committees attest.
  - Epochs (~6.4 min): checkpoints can be justified, and with two consecutive justifications, the older is finalized.
  - Misbehavior (equivocation, surround votes) → slashing; downtime → inactivity leak.
- **Networking**:

- devp2p + libp2p gossip for blocks/attestations/txs; discovery (Discv5).
- **Engine API** bridges EL↔CL for safe block building.
- **MEV-Boost / PBS** (Proposer-Builder Separation) in practice for better MEV handling.

- **Data structures**: Accounts (EOA, Contract), **state trie, storage tries,** receipts/logs; gas-metered EVM execution.
- **Scalability**: **Rollups (L2)** execute off-chain, post proofs/data to L1; L1 provides settlement and security. EIPs progressively optimize L2 costs.
- **Security/incentives**: Native fee asset **ETH**; basefee (EIP-1559) + priority tips; validator rewards/penalties/slashing align honest behavior

Figure 5-2 Etherium workflow



5.4.3 What's Hyperledger

Hyperledger (Linux Foundation) is a **family of open-source, permissioned DLT** projects tailored for enterprise consortia. Key components:

- **Hyperledger Fabric**: modular permissioned ledger with channels (private sub-ledgers), **peers** (endorsement/commit), **orderers** (Raft ordering), **MSP (PKI-based identities),** and chaincode (smart contracts) in mainstream languages (Go/Java/Node). Endorsement policies define which orgs must sign a transaction before it's ordered and committed.
- **Hyperledger Besu**: an Ethereum client (EL) that can run public or permissioned ETH networks (with IBFT/QBFT). Bridges enterprise needs with EVM compatibility.
- Other projects: Indy/Aries (DID/VC identity), Iroha, Cacti (interoperability), etc.

5.4.4 Ten differences across Ethereum, Hyperledger (Fabric/Besu), Bitcoin, and Dogecoin

Dimension	Ethereum	Hyperledger (Fabric/Besu)	Bitcoin	Dogecoin
Primary purpose	Programmable smart-contract platform (DeFi/NFT/L2)	Enterprise consortia workflows, private data sharing	Sound money & payments ("digital gold")	Meme-origin payments, tipping, casual commerce
Access model	**Public, permissionless**	**Permissioned** (known orgs; ACL/MSP); Besu can be public/permissioned	Public, permissionless	Public, permissionless
Ledger model	**Account-based** (EVM state)	Account-based; Fabric uses key-value world state + channels	**UTXO**	**UTXO**
Consensus	**PoS** (Beacon: proposer/attesters; LMD-GHOST + FFG finality)	**Raft/IBFT/QBFT** (Fabric/ Besu); BFT-style finality; no mining	**PoW (SHA-256)**	**PoW (Scrypt)**; merge-mined with Litecoin
Finality	**Economic finality** (epochs, minutes)	**Deterministic finality** after ordering/commit	**Probabilistic**(confirmations)	**Probabilistic** (fast blocks, 1 min)
Native asset & supply	**ETH**; issuance adjusts; EIP-1559 burns basefee	**No required native coin** in Fabric; Besu follows ETH if public	**BTC**; capped **21M**	**DOGE**; **inflationary** (fixed yearly issuance)
Smart contracts	**EVM** (Solidity/Vyper); rich DeFi/NFT ecosystems	**Chaincode** (Go/Java/ Node) & private data; Besu supports EVM	Script (non-Turing complete)	Script (Bitcoin-like)

Dimension	Ethereum	Hyperledger (Fabric/Besu)	Bitcoin	Dogecoin
Privacy	Public by default; app-level/ZK/privacy L2s	**Strong privacy** via channels, private data collections, org-level ACL	Public, pseudonymous	Public, pseudonymous
Throughput/ latency	Moderate on L1; scaled via **L2 rollups**	**Higher TPS**; low latency via permissioned ordering	Low TPS, \~10-min blocks	Higher TPS than BTC; \~1-min blocks
Governance /operations	Open-source client diversity; EIP process; validators	**Consortium governance**, explicit policies, PKI identities	Rough consensus/BIPs ; miners/nodes	Informal dev governance; miners/nodes
Economics/ fees	Gas market (EIP-1559 basefee + tips)	No mining fees in Fabric; policy-driven costs	Fee market; block subsidy halvings	Fee market; no hard cap (ongoing subsidy)

References

[1]. Entriken, W., Shirley, D., Evans, J., & Sachs, N. (2018). ERC-721: Non-Fungible Token Standard (EIP-721). Ethereum Improvement Proposals. https://eips.ethereum.org/EIPS/eip-721

[2]. Radomski, W., Cooke, A., Castonguay, P., Binet, R., & Etho, A. (2019). ERC-1155: Multi Token Standard (EIP-1155). Ethereum Improvement Proposals. https://eips.ethereum.org/EIPS/eip-1155

[3]. DeFiLlama. (2025). DeFi TVL & analytics. Retrieved September 13, 2025, from https://defillama.com/

[4]. Chainalysis. (2025). Geography of Cryptocurrency: Global Crypto Adoption Index. Retrieved September 13, 2025, from https://www.chainalysis.com/blog/2025-global-crypto-adoption-index/

[5]. NonFungible.com. (2022). 2021 NFT market report (year-end overview). Retrieved September 13, 2025, from https://nonfungible.com/

[6]. Merkle Science. (2022, March 29). Ronin Bridge (Axie Infinity) hack analysis. Retrieved September 13, 2025, from https://www.merklescience.com/

[7]. Electric Coin Company. (n.d.). zk-SNARKs: Privacy-preserving cryptography. Retrieved September 13, 2025, from https://z.cash/technology/zksnarks/

[8]. Protocol Labs. (n.d.). IPFS documentation. Retrieved September 13, 2025, from https://docs.ipfs.tech/

[9]. Hunton Andrews Kurth LLP. (n.d.). EU GDPR & blockchain guidance (Inside Privacy blog). Retrieved September 13, 2025, from https://www.insideprivacy.com/

[10]. arXiv. (2025). SoK: Cross-chain bridge vulnerabilities (preprint). Retrieved September 13, 2025, from https://arxiv.org/

[11]. Government of Vietnam. (2024). Decree No. 52/2024/NĐ-CP Digital Asset Management. Retrieved September 13, 2025, from https://vbpl.vn/

[12]. Cyber security tin the Blockchain. Anand Nayyar. DSA741-Blockchain.

[13]. Blockchain’s Promise for Cyber Security. Anand Nayyar . DSA741-Blockchain.

[14]. Decentralized finance (DeFi) 101. Anand Nayyar. DSA741-Blockchain.

[15]. Non-fungible tokens (NFTs). Anand Nayyar. DSA741-Blockchain.