Chapter 6

THE FUTURE OF BLOCKCHAIN TECHNOLOGY

TP. HCM 2022

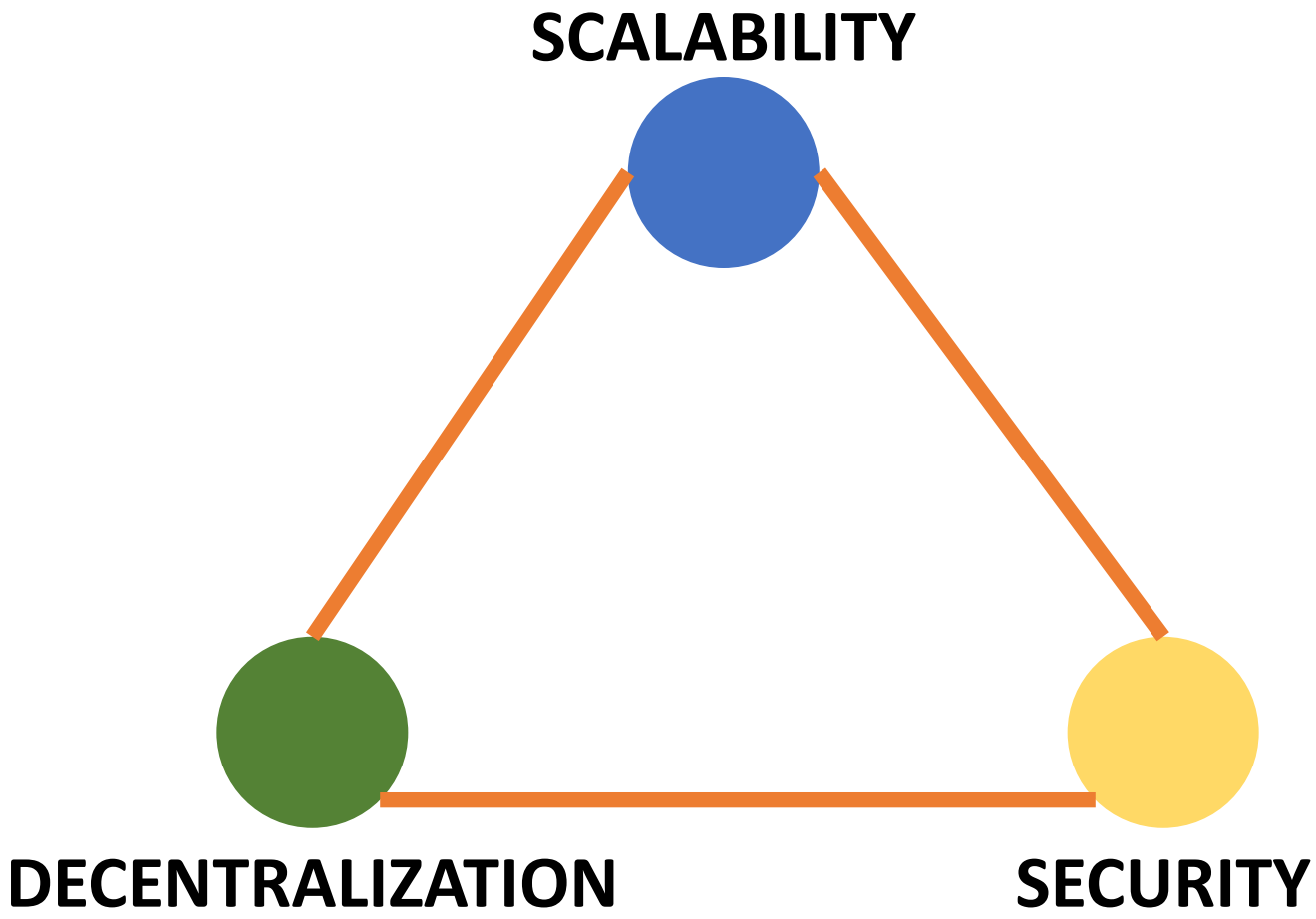
OVERVIEW

- Permissionless vs permissioned blockchain: A review
- Blockchain use-cases
- Blockchain – Metaverse and Payment systems

CHALLENGES WITH BLOCKCHAIN TECHNOLOGY

- Performance, Scalability, & Efficiency
- Privacy & Security
- Interoperability
- Governance & Collective Action
- Commercial Use Cases
- Public Policy & Legal Frameworks

VITALIK BUTERIN TRILEMMA



BLOCKCHAIN – TECHNICAL FEATURES

BITCOIN - PERMISSIONLESS	PERMISSIONED
Cryptography & Timestamped Logs	**YES**
▪ Cryptographic Hash Functions	▪ ✓
▪ Timestamped Append-only Logs (Blocks)	▪ ✓
▪ Block Headers & Merkle Trees	▪ ✓
▪ Asymmetric Cryptography & Digital Signatures	▪ ✓
▪ Addresses	▪ ✓
Decentralized Network Consensus	**NO**
▪ Consensus through Proof of Work	▪ PBFT, Notary Nodes, etc.
▪ Network of Nodes	▪ ✓
▪ Native Currency	▪ ✓
Transaction Script & UTXO	**YES**
▪ Transaction Inputs & Outputs	▪ ✓
▪ Unspent Transaction Output (UTXO)	▪ ✓
▪ Scripting language	▪ ✓

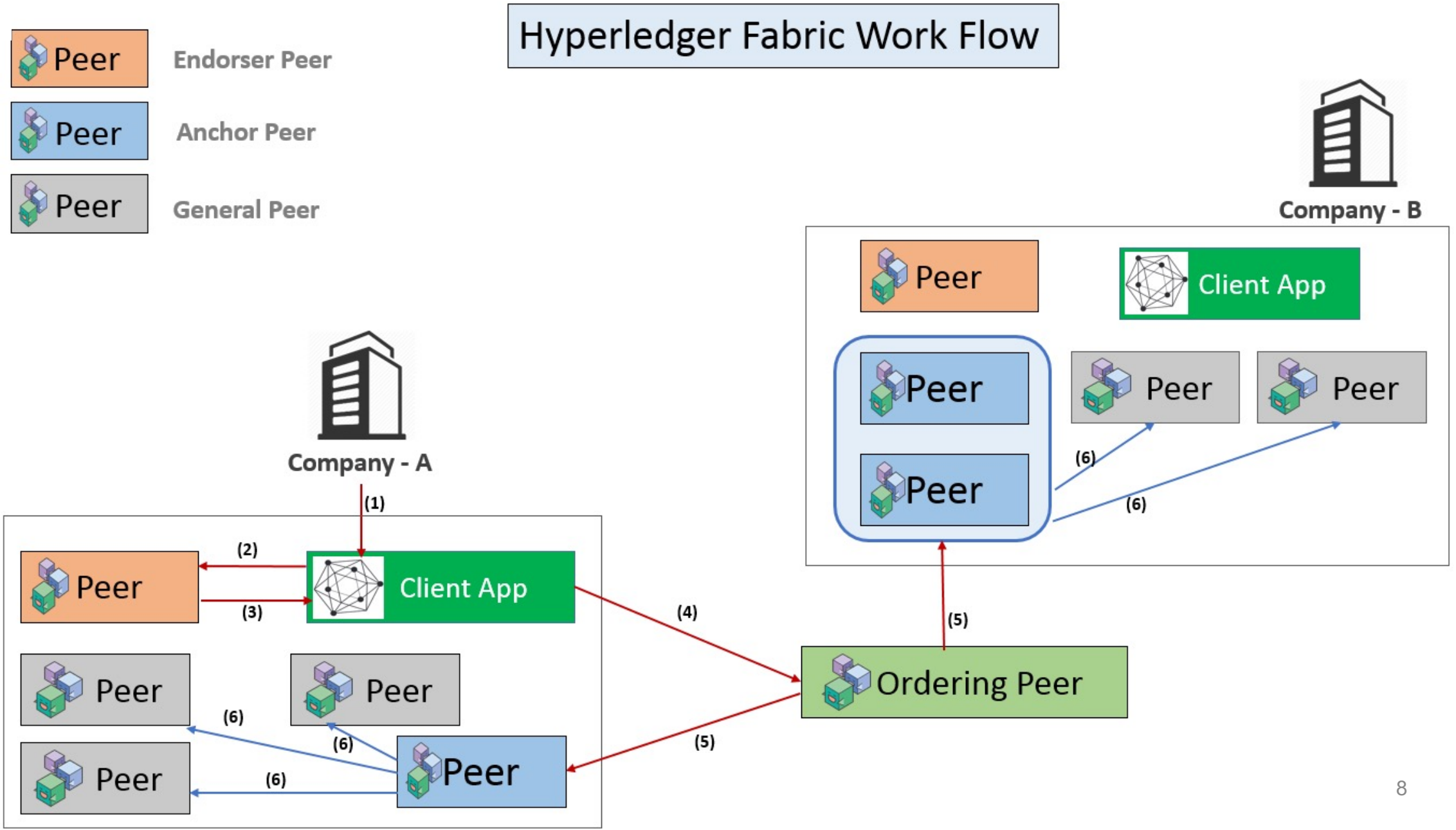
PERMISSIONED PRIVATE BLOCKCHAINS

Key Design Features

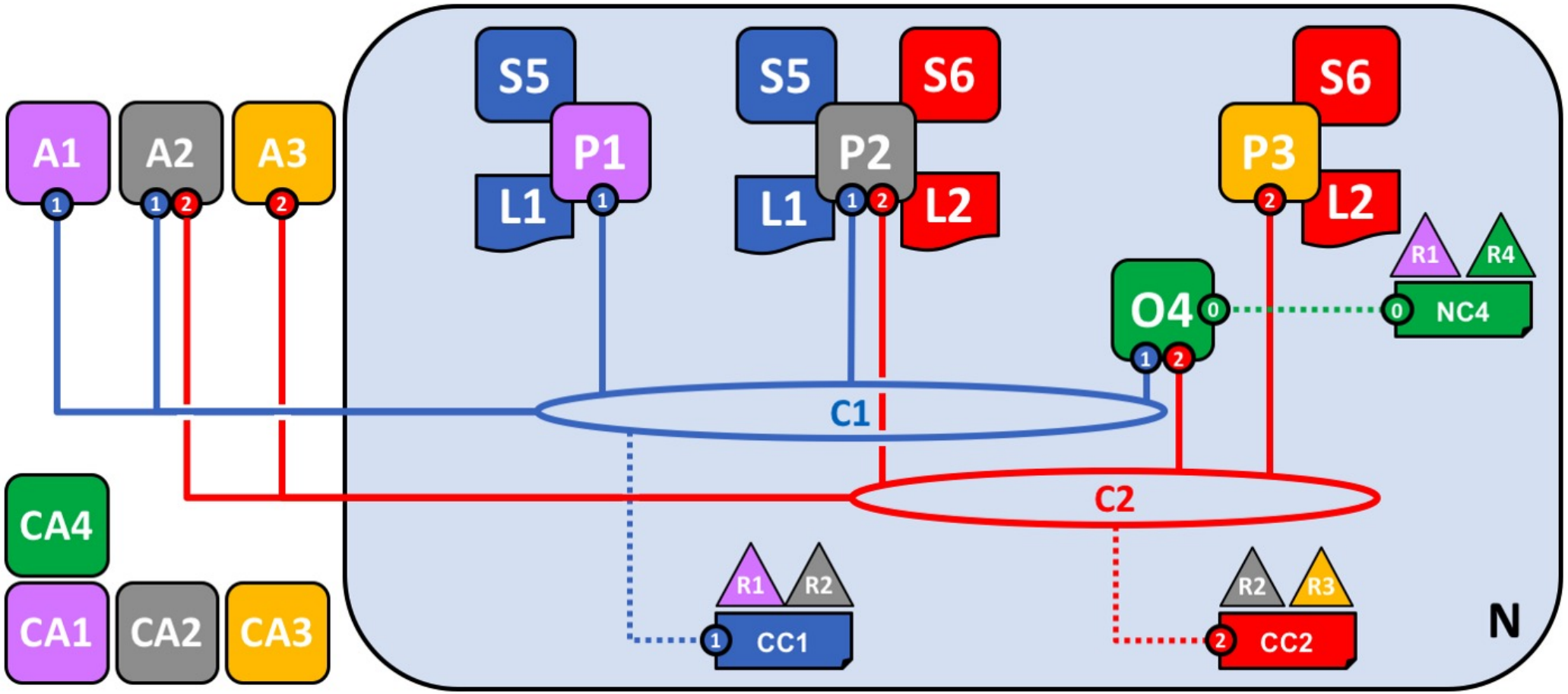
- Membership Limited to **Authorized Nodes**
- Transactions can also be Limited to **Authorized Known Participants**
- Data & Ledgers can be **Partitioned to Keep amongst Subgroups of Nodes**
- Consensus built on Permissioned, Private Protocols – Globally or Modular between **Transacting Parties**.
  - Practical Byzantine Fault Tolerance
  - Delegated Notary Nodes
  - Diverse Protocols – from Protocols for Multi Party Consensus to Crash Fault Tolerant for 1 Party
- Uses Cryptography and Registration Authorities to Mask User Data
- Facilitates Smart Contracts using Chaincode or other Programming Language
- **No Native Currency** – Possible, though, with Smart Contracts
- Code Generally **Open Source**

HYPERLEDGER FABRIC

HYPERLEDGER FABRIC



HYPERLEDGER FABRIC



A1 - application.
P1 - peer node.
S5 - smart contract.

L1 - ledger.
C1 - channel.
CA - certificate authority.

NC4 - network configuration.
R1 - organization.
CC1 - channel configuration.

O4 - ordering service.
N - Hyperledger network.

HYPERLEDGER FABRIC vs ETHEREUM

FEATURE	ETHEREUM	HYPERLEDGER
Confidentiality	Public blockchain	Private blockchain
Purpose	Client-side B2C applications	Enterprise-level B2B applications
Governance	Ethereum Developers	Linux Foundation
Participation	Anyone	Organizations having Certificate of Authorization
Programming Language	Solidity	Golang, JavaScript, or Java
Consensus Mechanism	POW- Proof of Work Mechanism	Pluggable consensus mechanism
Speed of Transactions	Less	More
Cryptocurrency	Ether or Ethereum	None

BLOCKCHAINS vs TRADITIONAL DATABASES

Access Control Protocol

Open Permissionless | Multiple Permissionless | Client – Server

PUBLIC BLOCKCHAIN

- Public Write Capability
- P2P transactions
- No Central Intermediaries
- Token economics

PRIVATE BLOCKCHAIN

- Private Write Capability
- Finality of Data in Append Only Log
- Public Verifiability

TRAND. DBS

- Trusted Party host data
- Trusted Party can "CRUD"
- Client – Server architecture

BLOCKCHAIN APPLICATIONS

- Money transfer
- Smart contracts
- Internet of Things (IoT)
- Personal identity security
- Healthcare
- Logistics
- Non-fungible tokens (NFTs)
- Government
- Media

FINANCIAL SECTOR POTENTIAL USE CASES

- Venture Capital - Crowdfunding through Initial Coin Offerings
- Payment Systems - Cross border, Large interbank, & Retail
- Loan Issuance & Trade Finance - Digitizing paper-based processes
- Clearing, Settlement and Processing – Securities & Derivatives
- Digital IDs and Data Reporting
- Central Bank Digital Currency & Private Stable Value Tokens

USE CASES: ASSESSING COSTS & BENEFITS

Strategic questions?

- What is the value creation proposition?
- What problem or ‘pain point’ is being solved?
- What are competitors doing to address similar ‘pain points’?
- Why is blockchain technology and native token the best solution?

Specifics of the blockchain technology and native token use case?

- Which costs of verification or networking can be reduced?
- Which transactions need recording?
- Which stakeholders need write and read access to ledgers?
- What is the customer interface and how is it better than current interface?

USE CASES: ASSESSING COSTS & BENEFITS

Costs of technical challenges and transition?

- What tradeoffs are necessary?
  - scalability, performance, privacy, security, interoperability & coordination
- Can Permissioned blockchain or Traditional Data Base adequately address use case?
- How can broad adoption be realized?

Are net benefits sufficient?

METAVERSE

The **metaverse** is a concept of a persistent, online, 3D universe that combines multiple different virtual and physical spaces. Metaverse is the future iteration of the internet. The metaverse will allow users to work, meet, game, and socialize together in these 3D spaces.

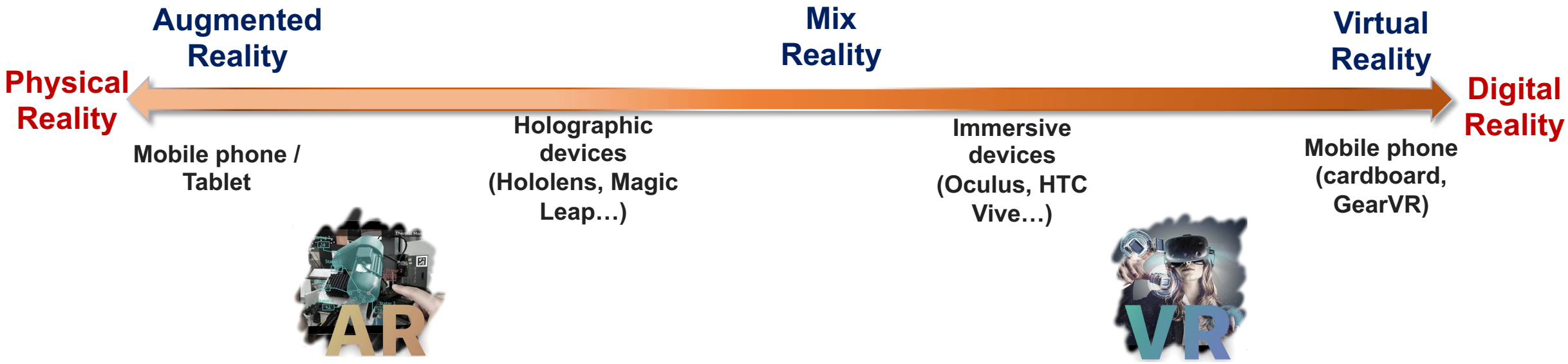
METAVERSE 7 LỚP

Understanding the Seven Layers of the Metaverse

METAVERSE

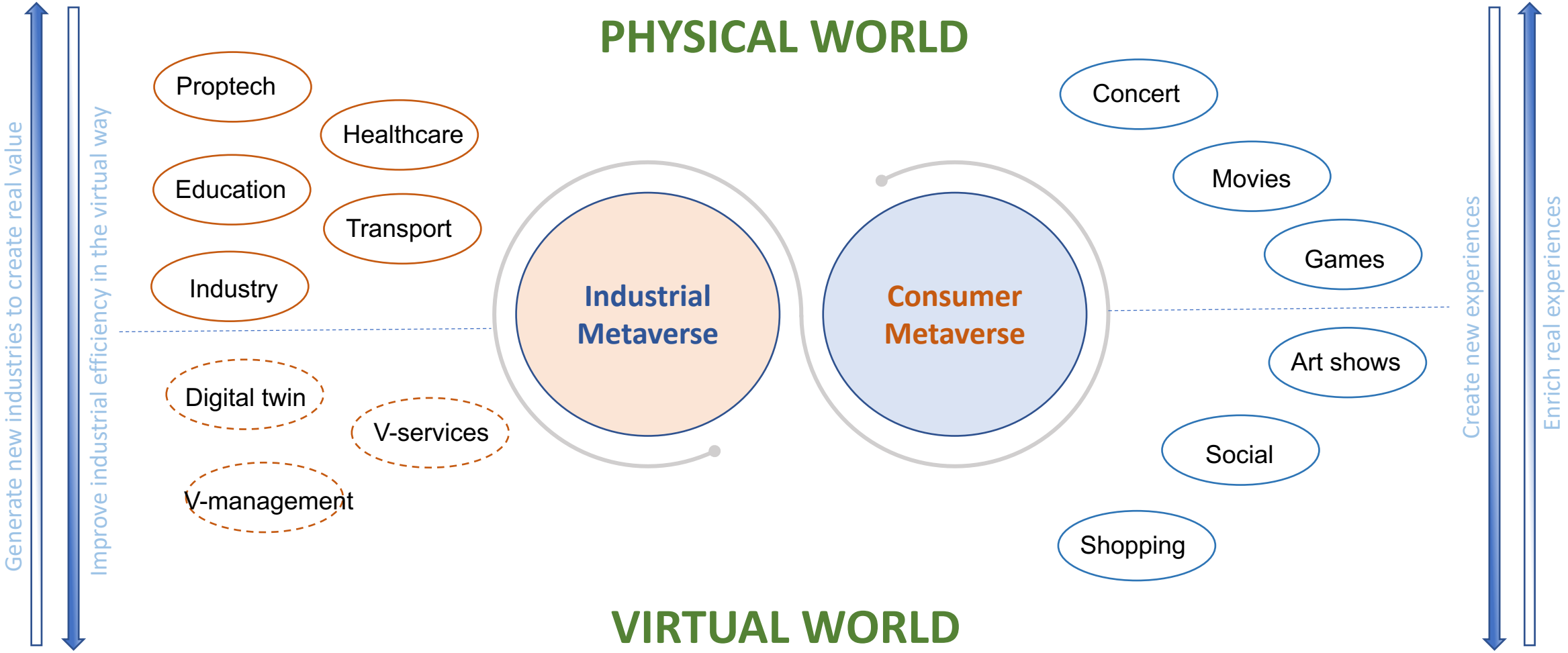

ECONOMIC SYSTEM
UNLIMITED
PERSONALIZED
INTEROPERABILITY
PERSISTENT
IMMERSIVE
OPENESS
FREE
METAVERSE

METAVERSE



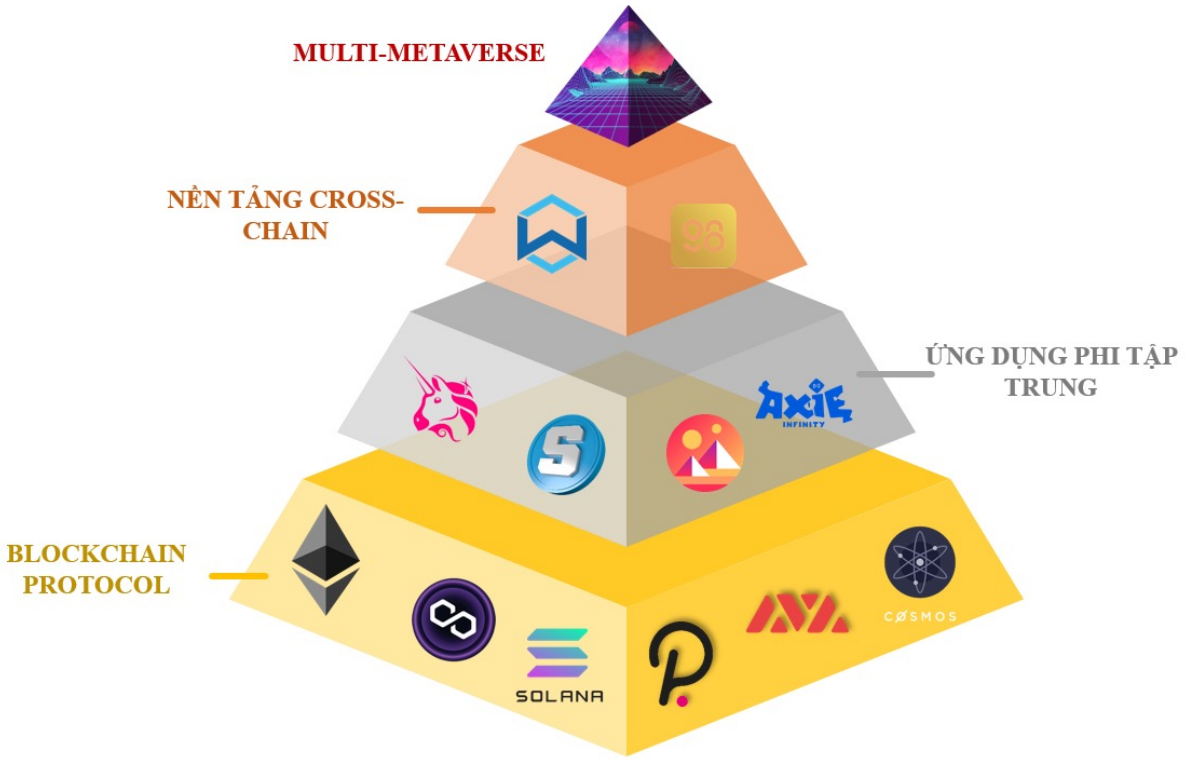
- AR/VR is one of various tools to communicate with Metaverse
- AR/VR applications are **NOT** Metaverse
- AR/VR provides a more realistic experience than the traditional way

METAVERSE USE-CASES



BLOCKCHAIN & METAVERSE

- Blockchain promotes the development of a “flat” economic system on Metaverse
- Blockchain supports digital asset management (NFT, tokens)
- Blockchain supports automatic transactions through smart contracts
- The blockchain economic platform is “open” to all parties in Metaverse



QUESTIONS

1. What are the tradeoffs of centralized institutions and markets in the financial sector?
2. Which challenges of the financial sector – periodic crises, concentrated risks, economic rents, legacy systems, processing risks, financial inclusion – might present opportunities for blockchain applications?
3. How does blockchain technology fit within other trends – particularly with regard to technology - facing the financial sector?

READINGS

1. *Sheila Bair on What Hasn't Changed since the Great Recession*
2. *The Rise of Market Concentration and Rent Seeking in Financial Sector*
3. *Ten Years after the Crash, We are Living in a World it Brutally Remade*

DISCUSSION