L47: CBDCs and Future Trends

Module G: Regulation & Future

Blockchain & Cryptocurrency Course

December 2025

What is a CBDC?

- **Definition**: Digital form of central bank money (fiat currency)
- **Not Cryptocurrency**: Centrally issued and controlled by central bank
- **Key Characteristics**:
    - Legal tender status
    - Liability of central bank (not commercial bank)
    - Electronic/digital (not physical cash)
    - May use blockchain/DLT (but not required)
- **Motivation**: Respond to decline in cash usage, private stablecoins, financial inclusion
- **Status**: 130+ countries exploring CBDCs (90% of global GDP)
- **Operational**: Bahamas (Sand Dollar), Nigeria (eNaira), Jamaica (JAM-DEX)
- **Pilots**: China (e-CNY), EU (Digital Euro), India (e-Rupee)

Retail vs Wholesale CBDCs

Aspect	Retail CBDC	Wholesale CBDC
Users	General public	Financial institutions
Use Case	Payments, store of value	Interbank settlement
Access	Widely accessible	Restricted to banks
Amount	Small transactions	Large-value transfers
Technology	May use DLT	Likely DLT (efficiency)
Competition	Competes with bank deposits	Complements RTGS systems
Privacy	Balance privacy vs AML	Less privacy concern
Examples	e-CNY, Digital Euro	Project Ubin (Singapore) Project Jasper (Canada)

Focus: Retail CBDCs have greater societal impact and complexity

Retail CBDC: Design Choices

1. **Architecture**:
   - **Direct**: Central bank manages all accounts (Sweden Riksbank model)
   - **Hybrid**: Central bank ledger, commercial banks interface with users (e-CNY model)
   - **Intermediated**: Commercial banks hold CBDC, central bank wholesale only
2. **Technology**:
   - DLT/blockchain vs centralized database
   - Permissioned ledger (if DLT)
   - Offline capability (for unbanked areas)
3. **Access**:
   - Account-based vs token-based
   - Identification requirements (KYC levels)
   - Limits on holdings (prevent bank disintermediation)
4. **Interest**: Pay interest on CBDC balances or not?

Privacy vs Surveillance Tradeoff

Privacy Concerns

- Central bank sees all transactions
- Potential for government surveillance
- Social credit system risks (e.g., China)
- Chilling effect on lawful activities
- No cash-like anonymity

Privacy-Enhancing Technologies

- Zero-knowledge proofs (prove validity, hide details)
- Tiered privacy (small transactions anonymous, large KYC)
- Blind signatures (central bank can't link user to transaction)

AML/CFT Requirements

- Full anonymity enables illicit finance
- Regulatory pressure (FATF standards)
- Tax enforcement needs
- Counter-terrorism financing

Design Spectrum

- **Full Surveillance**: China e-CNY (central visibility)
- **Balanced**: Digital Euro (privacy for small, KYC for large)
- **Privacy-First**: Hypothetical (similar to cash, unlikely)

CBDC Risks and Challenges

1. **Bank Disintermediation**:
   - If CBDC pays interest, users move deposits from banks to CBDC
   - Banks lose funding → reduced lending → economic contraction
   - Mitigation: Caps on CBDC holdings, no/low interest
2. **Bank Runs**:
   - Crisis triggers instant flight from bank deposits to CBDC (digital bank run)
   - Faster and larger than traditional bank runs
   - Mitigation: Holding limits, transfer limits
3. **Cybersecurity**:
   - Central point of failure (entire monetary system)
   - DDoS, hacking, quantum computing threats
4. **Cross-Border Implications**:
   - Currency substitution (dollarization/yuan-ization via CBDC)
   - Capital controls circumvention

Case Study: China's e-CNY (Digital Yuan)

- **Status**: Largest CBDC pilot globally (2020-present)
- **Architecture**: Two-tier (PBOC wholesale, banks retail)
- **Technology**: Centralized with distributed database (not blockchain)
- **Features**:
  - Dual offline payment (no internet required)
  - Programmability (smart contracts)
  - Controllable anonymity (PBOC sees, commercial banks don't)
- **Adoption Tactics**:
  - Free e-CNY airdrops (lotteries)
  - Integration with AliPay, WeChat Pay
  - Salary payments in e-CNY (government workers)
- **Geopolitical Angle**: Challenge USD dominance, cross-border CBDC settlement
- **Concerns**: Surveillance (integration with social credit system)

Case Study: Digital Euro

- **Status**: Investigation phase (2021-2023), preparation phase (2024-2026)
- **Motivation**: Preserve monetary sovereignty, counter private stablecoins (Libra/Diem scare)
- **Design Principles**:
  - Privacy-focused (stronger than e-CNY)
  - Offline capability (like cash)
  - Free for basic use (no transaction fees for users)
  - Intermediated model (banks distribute)
- **Privacy Model**:
  - ECB sees aggregate data only
  - Commercial banks handle KYC
  - Small transactions: Cash-like privacy
  - Large transactions: Full AML compliance
- **Timeline**: Launch decision expected 2025, rollout 2027-2028
- **Challenge**: Coordination across 20 Eurozone countries

Cross-Border CBDC: mBridge Project

- **Project mBridge**: Multi-CBDC platform for cross-border payments
- **Participants**: China, Hong Kong, Thailand, UAE, Saudi Arabia (BIS Innovation Hub)
- **Goal**: Replace SWIFT for cross-border settlements
  - Instant settlement (vs 2-5 days)
  - Lower costs (no correspondent banking fees)
  - 24/7 operation
- **Technology**: Permissioned blockchain (customized DLT)
- **Mechanism**:
  - Central banks issue CBDCs on shared ledger
  - Atomic swaps between currencies (no intermediary)
  - Smart contracts for compliance (AML checks)
- **Geopolitical Implications**: Bypass USD-dominated SWIFT system
- **Status**: Pilot phase, live transactions completed

CBDCs vs Stablecoins vs Crypto

Property	**CBDC**	**Stablecoin**	**Cryptocurrency**
Issuer	Central bank	Private company	Decentralized protocol
Backing	Sovereign fiat	Reserves or algorithm	Consensus mechanism
Legal Tender	Yes	No	No
Volatility	None (= fiat)	Low (if properly backed)	High
Privacy	Variable (design choice)	Low (KYC required)	High (pseudonymous)
Programmability	Possible	Yes	Yes
Control	Centralized	Centralized	Decentralized
Use Case	Payments, settlement	DeFi, payments	Speculation, store of value

Competition: CBDCs may crowd out stablecoins, not cryptocurrencies (different use cases)

Trend 1: Institutional Adoption Acceleration

- **2024 Status**: Crypto assets mainstream in institutional portfolios
- **Drivers**:
  - Spot Bitcoin ETFs (approved US 2024, Europe, Asia following)
  - Ethereum ETFs (post-Merge institutional interest)
  - Regulatory clarity (MiCA, Swiss framework)
  - Custody solutions (Coinbase Prime, Fidelity Digital Assets, BNY Mellon)
- **Institutional Products**:
  - Tokenized securities (bonds, real estate, funds)
  - Crypto lending and prime brokerage
  - Derivatives (CME Bitcoin futures, options)
  - Yield products (staking as a service)
- **Impact**: $1T+ institutional capital in crypto by 2030 (estimates)

Trend 2: Tokenization of Real-World Assets (RWA)

- **RWA Tokenization**: Representing real assets on blockchain
- **Asset Classes**:
  - Real estate (fractional ownership, REITs)
  - Private equity and venture capital
  - Bonds (government, corporate)
  - Commodities (gold, carbon credits)
  - Art and collectibles
- **Advantages**:
  - Fractional ownership (lower barriers to entry)
  - 24/7 trading (no market hours)
  - Programmable compliance (smart contracts enforce regulations)
  - Global liquidity pools
- **Market Size**: \$10T+ tokenized assets by 2030 (BCG estimate)
- **Leaders**: Centrifuge, Ondo Finance, Securitize, tZERO

Trend 3: AI + Blockchain Convergence

- **AI for Blockchain**:
  - Smart contract auditing (automated vulnerability detection)
  - MEV optimization (machine learning for transaction ordering)
  - DeFi risk modeling (predictive analytics)
  - On-chain analytics (pattern detection, fraud identification)
- **Blockchain for AI**:
  - Decentralized AI training (Bittensor, Ocean Protocol)
  - Verifiable AI models (proof of training, model provenance)
  - AI agent payments (micropayments for AI services)
  - Data marketplaces (tokenized datasets with access control)
- **Emerging Projects**:
  - Fetch.ai: Autonomous economic agents
  - SingularityNET: Decentralized AI marketplace
  - Render Network: GPU compute for AI/rendering

Trend 4: DePIN (Decentralized Physical Infrastructure Networks)

- **DePIN**: Blockchain-incentivized physical infrastructure
- **Categories**:
  1. **Wireless Networks**:
     - Helium: Decentralized LoRaWAN and 5G (IoT connectivity)
     - XNET: Decentralized mobile network
  2. **Compute/Storage**:
     - Filecoin: Decentralized storage
     - Akash: Decentralized cloud compute
     - Render Network: GPU rendering
  3. **Energy**:
     - Powerledger: P2P energy trading
     - LO3 Energy: Local energy markets
  4. **Sensors/Mapping**:
     - FOAM: Decentralized location services
     - Hivemapper: Crowdsourced mapping
- **Value Proposition**: Token incentives bootstrap network effects

Trend 5: Account Abstraction (ERC-4337)

- **Problem**: Current wallets (EOAs) have poor UX
  - Seed phrases (lose it = lose funds)
  - Gas fees paid in native token (ETH)
  - No transaction batching or automation
- **Account Abstraction**: Smart contract wallets as first-class citizens
- **ERC-4337 Features**:
  - **Social Recovery**: Multi-sig guardians can recover account
  - **Gas Abstraction**: Pay fees in any token (USDC, DAI) or sponsor transactions
  - **Batching**: Multiple operations in one transaction
  - **Automation**: Scheduled payments, limit orders
  - **Session Keys**: Temporary permissions for dApps (no approval fatigue)
- **Impact**: UX comparable to Web2 (no seed phrases, no gas headaches)
- **Adoption**: Deployed on Ethereum (2023), gaining traction

Trend 6: Modular Blockchains

- **Monolithic Blockchains**: Single chain handles execution, consensus, data availability
  - Examples: Bitcoin, Ethereum L1
  - Limitation: Scalability bottleneck
- **Modular Architecture**: Separate layers for different functions
  1. **Execution Layer**: Process transactions (rollups)
  2. **Consensus Layer**: Order and finalize blocks (Ethereum PoS)
  3. **Data Availability Layer**: Store transaction data (Celestia, EigenDA)
- **Advantages**:
  - Specialization (each layer optimized)
  - Scalability (parallel execution)
  - Flexibility (swap layers)
- **Projects**: Celestia, Fuel, Eclipse, Sovereign SDK
- **Vision**: Thousands of app-specific rollups sharing infrastructure

Trend 7: Zero-Knowledge Proofs Everywhere

- **ZK Technology Maturation**: From research to production
- **Applications**:
  1. **ZK-Rollups**: Scalability (StarkNet, zkSync, Polygon zkEVM)
  2. **Privacy**: Private transactions (Zcash, Aztec, Railgun)
  3. **Identity**: Prove attributes without revealing data
     - Age verification (prove ¿18 without revealing birthdate)
     - Creditworthiness (prove credit score ¿X without revealing full history)
  4. **Interoperability**: Cross-chain bridges with validity proofs
  5. **Compliance**: Prove regulatory compliance without exposing data
- **Developer Tools**: Improved (Circom, Noir, o1js)
- **Hardware Acceleration**: ZK ASICs for faster proof generation
- **Impact**: Privacy + scalability without tradeoffs

Trend 8: Regenerative Finance (ReFi)

- **ReFi**: Using crypto/blockchain for environmental and social impact
- **Use Cases**:
  1. **Carbon Credits**:
     - Tokenized carbon offsets (KlimaDAO, Toucan Protocol)
     - Transparent tracking, retirement on-chain
     - Liquid carbon markets
  2. **Biodiversity Credits**:
     - Tokenize conservation outcomes
     - Fund nature restoration via DeFi mechanisms
  3. **Quadratic Funding**:
     - Gitcoin Grants: Democratic funding for public goods
     - Matching pools amplify small donations
  4. **Universal Basic Income (UBI)**:
     - GoodDollar: Blockchain-based UBI distribution
- **Philosophy**: Align financial incentives with planetary regeneration

Trend 9: Decentralized Science (DeSci)

- **DeSci**: Blockchain for scientific research and collaboration
- **Problems Addressed**:
  - Publication paywalls (taxpayer-funded research locked behind fees)
  - Peer review inefficiency (slow, unpaid reviewers)
  - Funding bias (established labs favored over novel ideas)
  - Data sharing barriers (no incentives to share)
- **Blockchain Solutions**:
  - **IP-NFTs**: Intellectual property as tradeable NFTs (Molecule Protocol)
  - **DAOs for Research Funding**: Community-governed grants (VitaDAO for longevity research)
  - **Data Marketplaces**: Researchers compensated for data sharing (Ocean Protocol)
  - **Open Access Publishing**: Immutable, timestamped publications on-chain
- **Projects**: Molecule, VitaDAO, ResearchHub, LabDAO

Trend 10: Liquid Staking Derivatives (LSD)

- **Problem**: Staked ETH (PoS) is illiquid (locked in validator)
- **Solution**: Liquid staking tokens represent staked assets
  - Lido: stETH (staked ETH)
  - Rocket Pool: rETH
  - Frax: frxETH
- **Mechanism**:
  1. User deposits ETH to protocol
  2. Protocol stakes ETH in validators
  3. User receives liquid staking token (stETH)
  4. stETH tradeable, usable in DeFi (collateral, liquidity pools)
  5. Earns staking yield while remaining liquid
- **Adoption**: $40B+ in liquid staking (2024)
- **Risk**: Centralization (Lido has 30%+ of all staked ETH)
- **Future**: Liquid staking for all PoS chains (Solana, Cosmos, Polkadot)

Emerging Risks and Challenges

1. **Quantum Computing Threat**:
   - ECDSA signatures vulnerable to Shor's algorithm
   - Timeline: 10-20 years to quantum computers breaking crypto
   - Mitigation: Post-quantum cryptography research, migration plans
2. **Regulatory Fragmentation**:
   - Conflicting national regulations (compliance complexity)
   - Stifling innovation vs jurisdictional arbitrage
3. **Centralization Creep**:
   - Validator concentration (Lido, large staking pools)
   - MEV centralization (Flashbots dominance)
   - Infrastructure providers (Infura, Alchemy)
4. **Systemic DeFi Risk**:
   - Composability creates cascading failures
   - Lack of circuit breakers in protocols

Career Paths in Blockchain (2025 and Beyond)

Technical Roles

- Smart contract developer (Solidity, Rust)
- Blockchain protocol engineer
- Security auditor
- ZK cryptographer
- DevOps (node operations, infrastructure)

Finance/Economics

- DeFi analyst
- Tokenomics designer
- Crypto trader/quant
- Institutional crypto advisor
- DAO treasury manager

Legal/Compliance

- Crypto regulatory specialist
- AML/CFT compliance officer
- Web3 lawyer
- Policy analyst

Business/Product

- Web3 product manager
- DAO operations
- Community manager
- Business development (partnerships)
- Crypto marketing/growth

Demand: 50,000+ open blockchain jobs (2024), growing 30%+ annually

Resources for Continued Learning

- **Developer Resources**:
  - Ethereum.org, Solidity docs, OpenZeppelin
  - CryptoZombies (Solidity tutorial)
  - Foundry, Hardhat (development frameworks)
- **Research and News**:
  - Vitalik Buterin's blog, Ethereum Research Forum
  - a16z Crypto Research, Messari, The Block
  - Bankless podcast, Unchained podcast
- **Online Courses**:
  - Coursera: Blockchain Specialization (University at Buffalo)
  - Udemy: Ethereum and Solidity courses
  - Alchemy University (free, developer-focused)
- **Communities**: Twitter Crypto, Discord servers, local blockchain meetups

Summary

- **CBDCs**: 130+ countries exploring, retail vs wholesale designs
- **Privacy vs surveillance**: Key CBDC design tradeoff
- **e-CNY**: Largest pilot, geopolitical implications (USD challenge)
- **Digital Euro**: Privacy-focused, launch 2027-2028
- **Cross-border CBDCs**: mBridge project (bypass SWIFT)
- **Future trends**: Institutional adoption, RWA tokenization, AI+crypto, DePIN, account abstraction
- **ZK proofs everywhere**: Privacy + scalability convergence
- **Modular blockchains**: Separation of execution, consensus, data availability
- **Emerging risks**: Quantum computing, regulatory fragmentation, centralization
- **Career opportunities**: 50,000+ jobs, diverse roles across tech, finance, legal