L47: CBDCs and Future Trends

Module G: Regulation & Future

Blockchain & Cryptocurrency Course

December 2025

CBDCs in a Nutshell

- "We created Bitcoin to escape central bank control." – Satoshi's vision
- "We'll create our own cryptocurrency." – Central banks worldwide

[COMIC: "Government cryptocurrency" irony – A central banker proudly presents "Our Decentralized Digital Currency" on a screen. The code shows: "if (government.says.freeze) { freeze(wallet); }". Satoshi's ghost facepalms in the corner.]

[PLACEHOLDER] — CBDCs represent governments entering the digital currency space they once dismissed

Learning Objectives

- Understand Central Bank Digital Currencies (CBDCs)
- Compare retail vs wholesale CBDC designs
- Analyze privacy vs surveillance tradeoffs
- Evaluate China e-CNY and Digital Euro progress
- Identify key future trends in blockchain technology
- Assess career opportunities in the blockchain space

Building on L46: Swiss FINMA and EU MiCA

The Problem: How should governments regulate crypto?

Part 3/4: CBDCs & Future

The Challenge

As cryptocurrencies threaten monetary sovereignty and stablecoins gain adoption, central banks face a critical question: Should governments create their own digital currencies, and how can they balance innovation with control?

Why It Matters

- Without CBDCs, private stablecoins could displace national currencies
- China's e-CNY already has 260M+ wallets, potentially challenging USD dominance

What We Need

- Risk management and mitigation
- Understanding CBDC design choices and fundamental trade-offs (privacy vs. control)

The Cryptoeconomics Question

Managing systemic and idiosyncratic risks

Today's lesson: How CBDCs address monetary sovereignty while introducing new privacy and surveillance challenges

Continued

What Are Central Bank Digital Currencies?

Definition: CBDC (Central Bank Digital Currency)—digital money issued directly by a nation's central bank

Key Characteristics:

- Legal tender status
- Central bank liability
- Electronic/digital form
- May use DLT (not required)

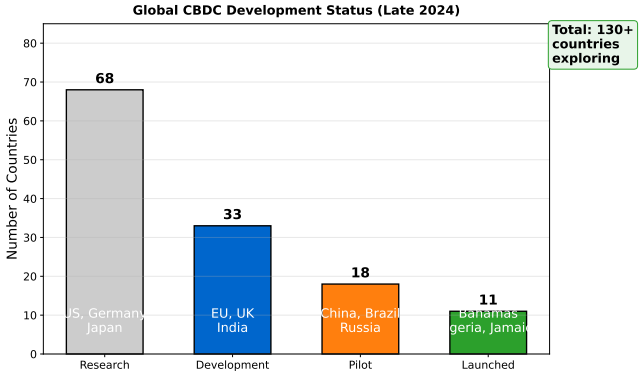
Not Cryptocurrency:
Centrally issued and controlled

Motivation:
Cash decline, stablecoins, inclusion

Status:
130+ countries (90% global GDP)

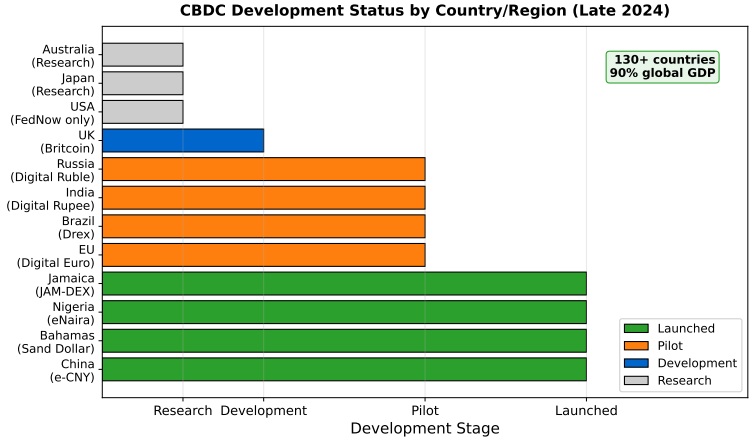
→ *Problem: How should governments regulate crypto? — What is a CBDC? CBDCs represent governments entering the digital currency space—regulate by competing rather than just restricting*

Which Countries Are Developing CBDCs?



130+ countries exploring CBDCs, representing 90% of global GDP

CBDC Development by Country



China leads with launched e-CNY; EU and India in pilot phase. US: Trump's Jan 23, 2025 Executive Order banned Federal Reserve CBDCs entirely, leaving FedNow (instant-payments rail, not a CBDC) as the only public US digital-money infrastructure

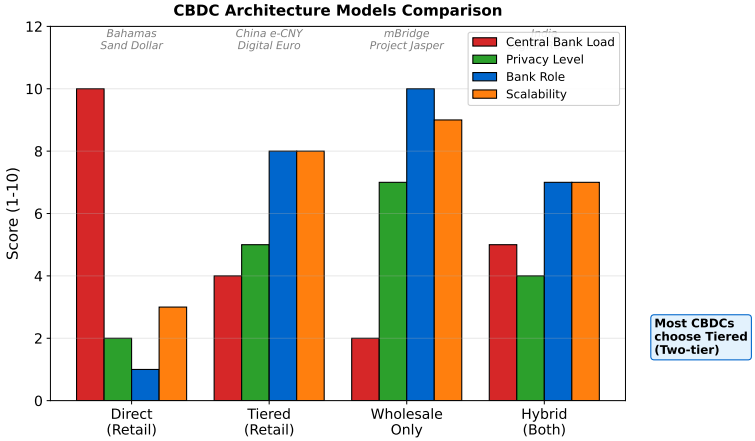
What's the Difference Between Retail and Wholesale CBDCs?

Aspect	Retail CBDC	Wholesale CBDC
Users	General public	Financial institutions
Use Case	Payments, store of value	Interbank settlement
Access	Widely accessible	Restricted to banks
Technology	Various (may use DLT)	Likely DLT (efficiency)
Privacy	Balance privacy vs AML	Less concern
Examples	e-CNY, Digital Euro	mBridge, Project Jasper

Focus: Retail CBDCs have greater societal impact and complexity

Compare the approaches shown above

How Are CBDCs Architecturally Structured?



Most CBDCs use two-tier (tiered) architecture: central bank wholesale, commercial banks retail

How Do CBDCs Balance Privacy and Surveillance?

Privacy Concerns

- Central bank sees all transactions
- Government surveillance potential
- Social credit system risks
- No cash-like anonymity

Privacy Technologies

- Zero-knowledge proofs (cryptographic methods that prove a statement is true without revealing the underlying data)
- Tiered privacy (small anonymous, large KYC)

AML/CFT Requirements

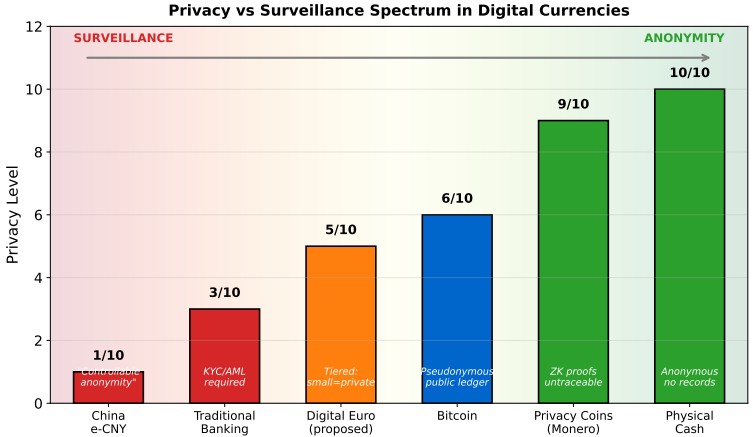
- Full anonymity enables illicit finance
- Regulatory pressure (FATF)
- Tax enforcement needs

Design Spectrum

- **Full Surveillance**: China e-CNY
- **Balanced**: Digital Euro
- **Privacy-First**: Unlikely in practice

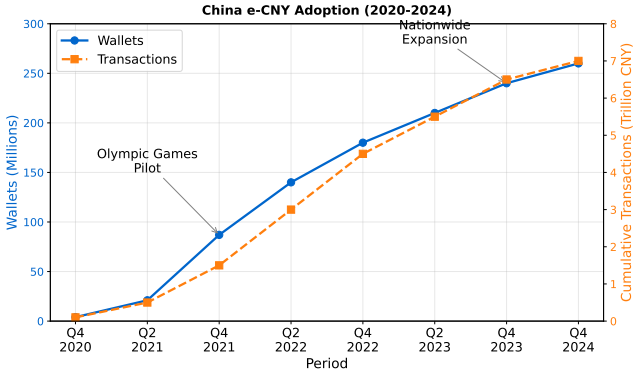
Compare the approaches shown above

Privacy Spectrum: CBDCs vs Alternatives



CBDCs offer less privacy than cash or crypto; Digital Euro aims for tiered model with privacy for small transactions

China e-CNY Adoption



Largest CBDC pilot globally, 260M+ wallets by late 2024 | → Problem: How should governments regulate crypto? — China e-CNY Adoption China's "controllable anonymity" shows one answer: full government visibility with programmable policy tools

How Does China's e-CNY Work?

Architecture:

- Two-tier: PBOC (People's Bank of China, the central bank) + commercial banks
- Centralized database
- Largest pilot (2020-present)

Features:

- Dual offline payment
- Programmable (smart contracts)
- "Controllable anonymity"

Stats (2024-2025):

- 260M+ wallets late 2024; expansion ongoing
- 7T+ yuan transactions cumulative
- 2025: nationwide retail rollout in major cities

Implications:

- Challenge USD dominance
- Surveillance concerns
- Competes with Alipay/WeChat

Compare the approaches shown above

What is the Digital Euro's Design?

Status: Prep phase 2023-2025; investigation phase concluded Oct 2025; ECB Governing Council preparing decision on next phase (verified ECB digital-euro roadmap, 2025)

Design Principles:

- Privacy-focused (¿ e-CNY)
- Offline capability
- Free for basic use
- Banks distribute

Privacy Model:

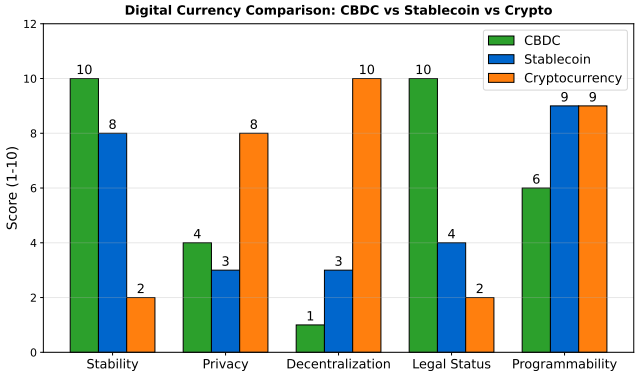
- Small tx: cash-like privacy
- Large tx: full AML compliance

Timeline:
Decision late 2025, rollout 2027-2028

Motivation:
Monetary sovereignty, counter stablecoins

Compare the approaches shown above

Digital Currency Comparison



CBDCs may crowd out stablecoins but not cryptocurrencies (different use cases)

How Does mBridge Enable Cross-Border Payments?

mBridge: Multi-CBDC platform (a cross-border payment system allowing direct central bank digital currency exchanges between participating countries)
Participants:
China, HK, Thailand, UAE, Saudi
Benefits vs SWIFT:

- Instant (vs 2-5 days)
- Lower costs
- 24/7 operation

Technology:
Permissioned blockchain
Status:
MVP June 2024, live transactions
Geopolitics:

- Bypass USD/SWIFT
- BRICS alternative system

→ *Problem: How should governments regulate crypto? — Cross-Border CBDC: mBridge mBridge enables cross-border settlement outside SWIFT—a geopolitical dimension to the regulatory question*

Problem Check-In: CBDCs & Future

Recall Our Problem

How should governments regulate crypto?

What We've Learned So Far

- CBDCs are central bank-issued digital money—not crypto, but competing with private stablecoins for digital payment dominance
- Privacy vs. surveillance tradeoff: China (full visibility) vs. Digital Euro (tiered privacy for small transactions)
- CBDCs offer an alternative approach: governments create compliant digital money rather than regulating private alternatives

Still to Address

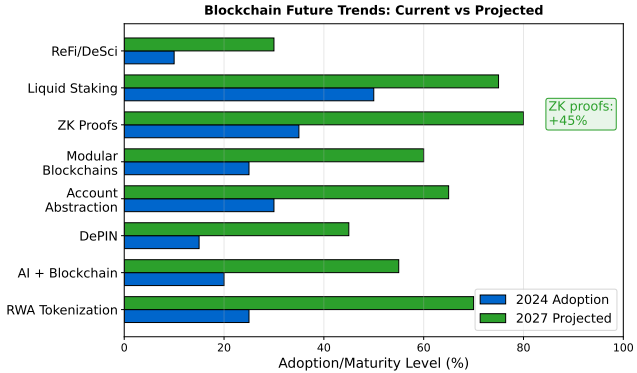
- Future trends: RWA tokenization ($16T by 2030), ZK proofs enabling privacy + compliance, AI + blockchain convergence
- Will CBDCs coexist with crypto, or will governments use them to crowd out private digital currencies?

Think About

- Based on what you've seen, how would *you* solve this problem?
- What trade-offs do you expect?

Pause and reflect: How does what we've learned so far address "How should governments regulate crypto?"?

Future Trends: Current vs Projected



ZK proofs, liquid staking, and RWA tokenization showing strongest growth

Why Are Institutions Entering Crypto Now?

2024 Drivers:

- Bitcoin ETFs (Jan 2024)
- Ethereum ETFs (Jul 2024)
- MiCA, Swiss frameworks
- Custody: Coinbase, Fidelity

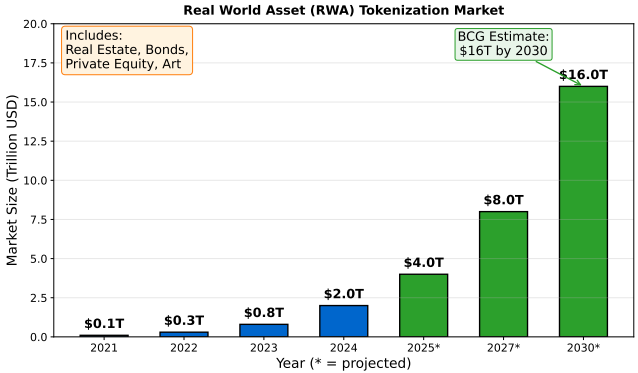
Products:

- Tokenized securities
- Crypto lending/prime brokerage
- CME futures, options

Impact:
$1T+ institutional capital by 2030

Compare the approaches shown above

RWA Tokenization Market Growth



Real world asset tokenization projected to reach $16T by 2030 (BCG estimate)

What is Real-World Asset Tokenization?

Definition:
RWA tokenization means representing real-world assets (real estate, bonds, commodities) as blockchain tokens

Asset Classes:

- Real estate (fractional)
- Private equity, VC
- Bonds (govt, corporate)
- Commodities, carbon credits

Advantages:

- Fractional ownership
- 24/7 trading
- Programmable compliance

Leaders:
Centrifuge, Ondo, Securitize, tZERO

BCG projects $16T RWA tokenization by 2030 | → Problem: How should governments regulate crypto? — Trend 2: RWA Tokenization RWA tokenization creates regulated securities on blockchain—bridging TradFi and DeFi under existing frameworks

How Are AI and Blockchain Converging?

AI for Blockchain:

- Smart contract auditing
- MEV optimization
- DeFi risk modeling
- On-chain analytics

Blockchain for AI:

- Decentralized AI training
- Verifiable AI models
- AI agent payments
- Data marketplaces

Projects:
Fetch.ai, SingularityNET, Render, Bittensor

Two-way synergy: AI improves blockchain, blockchain decentralizes AI

Why Are Zero-Knowledge Proofs Important?

ZK Maturation:
From research to production
Applications:

- ZK-Rollups (Layer 2 scaling solutions using zero-knowledge proofs to batch transactions): StarkNet, zkSync
- Privacy: Aztec, Railgun
- Identity: prove age w/o birthdate
- Compliance: private proofs

Technology:

- ZK ASICs (faster proofs)
- Polygon zkEVM, Scroll
- SNARKs vs STARKs tradeoffs

Impact:
Privacy + scalability without compromise

ZK technology enables proving statements without revealing underlying data

What Are the Emerging Risks for Crypto?

Quantum Computing:

- ECDSA (Elliptic Curve Digital Signature Algorithm, the cryptographic method securing most blockchain wallets) vulnerable (10-20 yr)
- Post-quantum migration needed

Regulatory Fragmentation:

- Conflicting national rules
- Compliance complexity

Centralization Creep:

- Lido: 30%+ staked ETH
- MEV/Flashbots dominance

Systemic DeFi Risk:

- Composability = cascading failures
- Protocol interdependencies

All risks require proactive mitigation strategies from the ecosystem

Continued

What Career Opportunities Exist in Blockchain?

Technical Roles

- Smart contract developer
- Blockchain protocol engineer
- Security auditor
- ZK cryptographer

Finance/Economics

- DeFi analyst
- Tokenomics designer
- Crypto trader/quant

Legal/Compliance

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

Business/Product

- Web3 product manager
- DAO operations
- Community manager

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

Compare the approaches shown above

Problem Solved? CBDCs & Future

The Original Problem

How should governments regulate crypto?

How CBDCs Address It

- Provide digital cash alternative (e-CNY, Digital Euro) competing with private stablecoins
- Enable efficient cross-border settlement (mBridge) with programmable policy tools
- Tiered privacy models balance AML compliance with cash-like anonymity for small transactions

Remaining Limitations

- "Controllable anonymity" enables government tracking of all transactions (China model)
- CBDCs could reduce role of commercial banks in monetary system

Open Questions

- Will CBDCs coexist with or displace cryptocurrencies and stablecoins?
- Risk: Quantum computing threatens ECDSA signatures (10-20 year horizon)

CBDCs provide government control over digital money but sacrifice privacy and may disrupt banking systems

The Economics of CBDCs & Future

Incentive Structure

- Managing systemic and idiosyncratic risks
- Risk-adjusted returns, insurance mechanisms
- Users bear risk for higher returns

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Users bear risk for higher returns

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Design Space: CBDCs & Future

Alternatives Considered

1. Risk parameters, circuit breakers
2. Traditional risk management approaches

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes

Failure Modes: CBDCs & Future

Critical Failure Mode

- **What breaks:** Black swan events, cascading failures
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

- ! Unusual economic behavior
- ! Incentive misalignment
- ! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

CBDCs: The Tradeoff

- CBDCs offer convenience: instant payments, programmable money, financial inclusion
- The cost: Every transaction visible to the government

[COMIC: "Privacy vs surveillance tension" – Split panel. Left: "Cash" – Person buys coffee, no one watching. Right: "CBDC" – Same purchase, but a government eye watches from the receipt: "Coffee, 9:03 AM, Location: Main St, Social Credit: -0.1 (excessive caffeine)"]

[PLACEHOLDER] — The fundamental CBDC tradeoff: convenience and policy tools vs. financial privacy

Summary

CBDCs:

- 130+ countries (90% GDP)
- Privacy vs surveillance tradeoff
- e-CNY: 260M+ wallets
- Digital Euro: decision late 2025
- mBridge: cross-border MVP 2024

Next Lesson: L48 – Course Synthesis

Future Trends:

- RWA tokenization: $16T by 2030
- ZK proofs: privacy + scalability
- AI + Blockchain synergies
- 50,000+ blockchain jobs

CBDCs and emerging trends will reshape global finance

Questions for Reflection

1. What are the key differences between retail and wholesale CBDCs?
2. How should CBDCs balance privacy and AML compliance?
3. Why might e-CNY adoption remain limited despite government push?
4. Which future trend (RWA, ZK, AI+Blockchain) has most potential?
5. How might mBridge affect the global financial system?

Key point: Questions for Reflection

Quiz

Quiz Questions (1–5)

Q1. What percentage of global GDP is represented by countries exploring CBDCs as of 2024?
A) 50% B) 70% C) 90% D) 100%
Answer: C – Over 130 countries representing 90% of global GDP are exploring CBDCs.

Q2. Which of the following is NOT a key characteristic of CBDCs?
A) Legal tender status B) Liability of central bank C) Must use DLT technology D) Electronic/digital form
Answer: C – CBDCs may use DLT but it is not required; technology choice varies by implementation.

Q3. Who are the primary users of wholesale CBDCs?
A) General public B) Financial institutions C) Retail merchants D) Individual consumers
Answer: B – Wholesale CBDCs are restricted to financial institutions for interbank settlement.

Q4. What is China's CBDC called?
A) Digital Yuan B) e-CNY C) China Coin D) PBOC Token
Answer: B – China's CBDC is officially called e-CNY (electronic Chinese Yuan).

Q5. How many wallets did China's e-CNY have by late 2024?
A) 50M+ B) 100M+ C) 260M+ D) 500M+
Answer: C – e-CNY had over 260 million wallets by late 2024, the largest CBDC pilot globally.

Quiz Questions (6–10)

Q6. What architecture does China's e-CNY use?
A) Fully decentralized B) Single-tier centralized C) Two-tier (PBOC wholesale, banks retail) D) Three-tier permissioned
Answer: C – e-CNY uses a two-tier system where PBOC handles wholesale and commercial banks handle retail distribution.

Q7. What privacy model does e-CNY implement?
A) Full anonymity B) Controllable anonymity C) Zero knowledge proofs D) Complete transparency
Answer: B – e-CNY uses "controllable anonymity" where the PBOC can see all transactions.

Q8. When is the Digital Euro decision expected?
A) 2024 B) Late 2025 C) 2027 D) 2030
Answer: B – The Digital Euro decision is expected late 2025, with rollout planned for 2027-2028.

Q9. How does the Digital Euro handle privacy for small transactions?
A) Full KYC required B) Cash-like privacy C) No privacy D) Blockchain transparency
Answer: B – Small transactions get cash-like privacy; large transactions require full AML compliance.

Q10. What is Project mBridge designed for?
A) Retail payments B) Cross-border CBDC settlements C) Stablecoin regulation D) NFT trading
Answer: B – mBridge is a multi-CBDC platform for cross-border payments and settlements.

Quiz Questions (11–15)

Q11. Which countries are NOT participants in Project mBridge?
A) China, Thailand B) UAE, Saudi Arabia C) USA, EU D) Hong Kong, Thailand
Answer: C – mBridge participants include China, Hong Kong, Thailand, UAE, and Saudi Arabia; not USA or EU.

Q12. When was the mBridge MVP launched?
A) January 2024 B) June 2024 C) December 2024 D) Not yet launched
Answer: B – The mBridge MVP was launched in June 2024 with live transactions completed.

Q13. What is projected market size for RWA tokenization by 2030 according to BCG?
A) $1T B) $5T C) $16T D) $50T
Answer: C – BCG estimates real world asset tokenization will reach $16 trillion by 2030.

Q14. Which is NOT an advantage of RWA tokenization?
A) Fractional ownership B) 24/7 trading C) Guaranteed profits D) Programmable compliance
Answer: C – Tokenization offers fractional ownership, 24/7 trading, and programmable compliance, but not guaranteed profits.

Q15. What percentage of staked ETH does Lido control, raising centralization concerns?
A) 10%+ B) 20%+ C) 30%+ D) 50%+
Answer: C – Lido controls over 30% of staked ETH, creating validator concentration concerns.

Quiz Questions (16–20)

Q16. What cryptographic technology enables both privacy and scalability without tradeoffs?
A) SHA-256 B) Zero-knowledge proofs C) RSA encryption D) Multi-signatures
Answer: B – Zero-knowledge proofs enable privacy and scalability simultaneously through ZK-rollups and private transactions.

Q17. What is the estimated timeline for quantum computing to threaten ECDSA signatures?
A) 2-5 years B) 5-10 years C) 10-20 years D) 50+ years
Answer: C – ECDSA signatures face quantum computing threats in a 10-20 year timeline.

Q18. How many open blockchain jobs exist globally with what annual growth rate?
A) 10,000+, 10% B) 50,000+, 30% C) 100,000+, 50% D) 500,000+, 100%
Answer: B – There are 50,000+ open blockchain jobs with 30%+ annual growth.

Q19. Which is NOT mentioned as an AI + Blockchain convergence use case?
A) Smart contract auditing B) Decentralized AI training C) Physical robot control D) AI agent payments
Answer: C – The lesson covers smart contract auditing, decentralized AI training, and AI agent payments, but not physical robot control.

Q20. What feature does e-CNY support that does NOT require internet connection?
A) International transfers B) Dual offline payment C) Smart contract execution D) Real-time auditing
Answer: B – e-CNY supports dual offline payment capability, allowing transactions without internet connection.