Topic 6.4: What's Next?

The Future of Digital Finance

Joerg Osterrieder

Digital Finance

2026

What You Will Learn in This Topic

By the end of this session, you will be able to:

1. **Identify** the genuinely open questions shaping digital finance's next decade
2. **Analyze** the interoperability debate and future chain architectures
3. **Evaluate** the CBDC vs. private digital money landscape
4. **Understand** emerging threats from quantum computing and AI
5. **Develop** informed hypotheses about the future of money
6. **Synthesize** key learnings from the entire course

Course Finale

This is the concluding topic of Digital Finance. We look forward while consolidating everything learned.

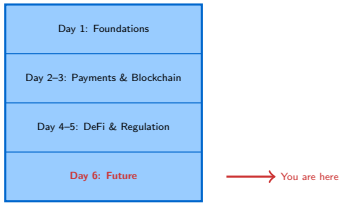
Prerequisites: Building on Everything

What you should know:

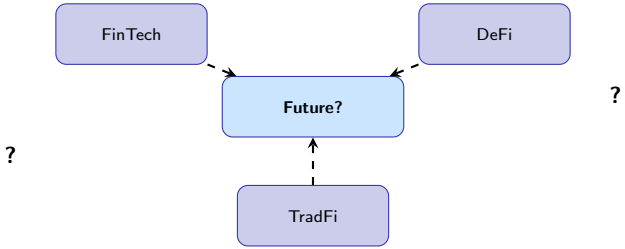
- Digital payments and FinTech (Day 2)
- Blockchain fundamentals (Day 3)
- Smart contracts and DeFi (Day 4)
- Stablecoins and tokenization (Day 4)
- Regulatory frameworks (Day 5)
- Convergence thesis (Day 6)

Key concepts to recall:

- Consensus mechanisms
- Layer 1 vs. Layer 2 scaling
- CBDC architectures
- AI in finance applications



The Big Picture: Why "What's Next" Matters



The honest answer: We don't know exactly what the future holds.

But we can identify:

- The genuinely open questions that will shape outcomes
- The forces and trends likely to matter
- The frameworks for thinking about any future development

The Genuinely Open Questions

These questions will shape the next decade of digital finance:

1. **Interoperability**: Will we see one dominant chain, many chains, or seamless cross-chain?
2. **CBDC vs. Private Money**: Will central bank digital currencies dominate, or coexist with stablecoins?
3. **Decentralized Identity**: Will blockchain-based identity systems achieve adoption?
4. **Quantum Threats**: How will cryptography adapt to quantum computing?
5. **AI Autonomy**: Will AI agents hold assets and transact independently?
6. **Regulatory Equilibrium**: Where will global regulation settle?
7. **The Future of Money**: What *is* money in 2035?

Open Question: Interoperability

Current State:

- Multiple Layer 1 chains (Ethereum, Solana, etc.)
- Multiple Layer 2s (Layer 1 is the main blockchain; Layer 2 is a faster layer built on top: Arbitrum, Optimism, Base)
- Fragmented liquidity
- Bridge vulnerabilities ($2B+ hacked cumulative, 2020–2023)
- Poor user experience

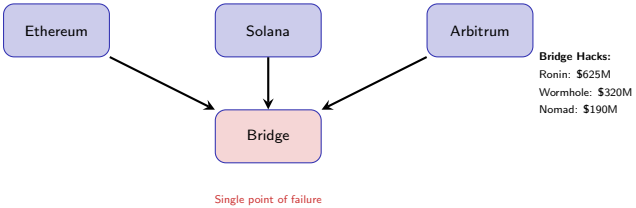
Possible Futures:

- **One chain wins**: Network effects concentrate
- **Chain abstraction**: Users don't know/care which chain
- **Specialized chains**: Different chains for different uses
- **Traditional wins**: Banks don't need public chains

Discussion Question

Is the future of blockchain "one chain to rule them all" or an interoperable multi-chain world? What are the arguments for each?

Interoperability: Technical Deep Dive



The Bridge Trilemma:

- **Security**: Minimizing trust assumptions
- **Speed**: Fast finality across chains
- **Generalizability**: Works for any chain pair

Current Reality

Most bridges sacrifice security for speed and generalizability, creating systemic risk.

Open Question: CBDCs vs. Private Digital Money

Arguments for CBDCs:

- Central bank backing = safe
- Monetary policy transmission
- Financial inclusion
- Reduced settlement risk
- Programmable policy tools

Status: 130+ countries exploring (source: Atlantic Council CBDC Tracker, 2024); China, Nigeria, Bahamas live

Arguments for Private Money:

- Innovation at the edge
- Competition improves quality
- Privacy from government
- Borderless by design
- Decentralization values

Stablecoin market cap: $230B+ (as of late 2024)

The Coexistence Hypothesis

Most likely: CBDCs for domestic retail, regulated stablecoins for crypto/DeFi, and continued competition between payment systems.

CBDC Implementation Models

Governments are exploring three broad architectures for issuing digital currency. Each makes different trade-offs between central bank control, citizen access, and the role of existing banks.

Privacy Spectrum:

- Full anonymity (cash-like)
- Tiered limits (small = anonymous)
- Full transparency (all tracked)

Design Choices:

- Token vs. account-based
- Interest-bearing or not
- Programmable features

Open Question: Decentralized Identity

The Problem

Online identity today is fragmented, insecure, and controlled by platforms. Can blockchain fix this?

DID/SSI Vision (Self-Sovereign Identity / Decentralized Identifiers — letting individuals control their own digital identity):

- Self-sovereign identity
- User controls their data
- Selective disclosure
- Portable across platforms
- Verifiable credentials

Challenges:

- Key management for everyday users
- Recovery when keys lost
- Adoption chicken-and-egg
- Regulatory acceptance
- Competition from Big Tech

Key projects to watch:

- **EU eIDAS 2.0**: The EU's regulation for digital identity wallets—aims to give every EU citizen a government-backed digital ID
- **Worldcoin**: Iris-scanning project to create a global identity layer
- **ENS** (Ethereum Name Service): Human-readable blockchain addresses (e.g., "alice.eth" instead of a 42-character address)

Open Question: Quantum Computing Threats

What's at Risk:

- ECDSA (Elliptic Curve Digital Signature Algorithm — the math that secures blockchain signatures, used by Bitcoin, Ethereum)
- RSA (a widely used encryption algorithm)
- Current digital signatures
- Potentially: all historical transactions

"Harvest Now, Decrypt Later": Adversaries may be storing encrypted data to break when quantum arrives.

Mitigation Paths:

- Post-quantum cryptography (NIST standards)
- Hash-based signatures (already quantum-resistant)
- Migration plans for blockchains
- Timeline uncertainty (10–30 years? Experts disagree widely on timing, but NIST has already begun standardizing post-quantum cryptography.)

Good news: Most blockchain systems can upgrade signature schemes.

Quantum: Timeline and Preparation

Post-Quantum Cryptography: In 2024, NIST (the US National Institute of Standards and Technology) approved new encryption standards designed to be safe from quantum computers:

- **ML-KEM** (formerly CRYSTALS-Kyber): For secure key exchange
- **ML-DSA** (formerly CRYSTALS-Dilithium): For digital signatures
- **SLH-DSA** (formerly SPHINCS+): A conservative backup option

Blockchain Implications

Bitcoin and Ethereum communities actively discussing quantum-resistant upgrades. Key challenge: coordinating migration without disruption.

Open Question: AI Agents in Finance

The Emerging Possibility

AI agents that autonomously hold assets, execute transactions, and make financial decisions.

Current Reality:

- Bots executing programmed strategies
- Human-supervised automation
- Narrow, well-defined tasks

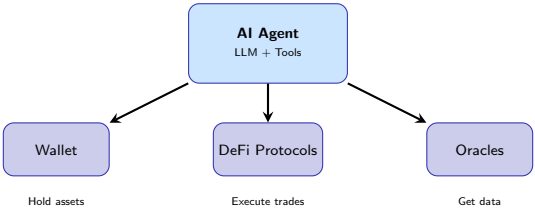
Speculative Future:

- AI agents with their own wallets
- Agent-to-agent transactions
- AI-managed DAOs
- Autonomous economic actors

Legal and Ethical Questions

Can an AI agent be a legal entity? Who is liable when an AI makes a bad financial decision? How do we prevent AI agents from being used for money laundering?

AI Agents: Technical Architecture



Current Examples:

- **Fetch.ai**: Autonomous economic agents
- **Autonolas**: Agent services framework
- **AI DAOs**: Experimental governance by AI

Key Insight

Blockchain provides the trust layer that enables AI agents to transact autonomously without human intermediation.

Open Question: The Future of Money

What will "money" mean in 2035?

Continuity View:

- Central banks remain dominant
- Digital but still state-controlled
- Private innovation at the margins
- Regulation tightens
- Status quo with better UX

Disruption View:

- Multiple competing currencies
- Programmable money standard
- Algorithmic monetary policy
- Borderless by default
- Fundamental restructuring

The only certainty: more change is coming.

Emerging Technology: Zero-Knowledge Proofs

What Are ZK Proofs?

Cryptographic methods to prove a statement is true without revealing the underlying data.

ZK for Scaling:

- **ZK-Rollups**: Bundle transactions, prove validity
- **zkSync, StarkNet**: Production systems
- 100x+ throughput improvements
- Inherit L1 security

ZK for Privacy:

- Prove you're over 18 without revealing age
- Prove you have funds without showing balance
- Regulatory-compliant privacy
- Selective disclosure

Why ZK Matters

Zero-knowledge proofs may solve the privacy vs. compliance dilemma that has plagued digital finance.

Emerging Technology: Account Abstraction

ERC-4337: Account Abstraction

ERC-4337 is a standard that makes cryptocurrency wallets work more like regular app accounts, with features like password recovery. It makes blockchain accounts programmable, dramatically improving user experience.

Current Problems:

- Seed phrase = single point of failure
- Gas fees in native token only
- One transaction at a time
- No recovery options

Account Abstraction Enables:

- Social recovery (friends as backups)
- Pay gas in any token
- Batch multiple transactions
- Spending limits and rules
- Session keys for apps

Key Insight

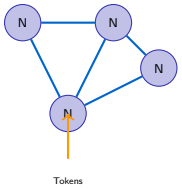
Account abstraction could make crypto as user-friendly as traditional finance while preserving self-custody.

Decentralized Physical Infrastructure Networks

Using token incentives to coordinate real-world infrastructure deployment. **Note:** DePIN is still experimental with limited real-world adoption beyond niche applications.

Examples:

- **Helium**: Decentralized wireless networks
- **Filecoin**: Decentralized storage
- **Render**: Distributed GPU computing
- **Hivemapper**: Crowdsourced mapping



The Model:

1. Deploy physical infrastructure
2. Earn tokens for providing service
3. Network grows through incentives

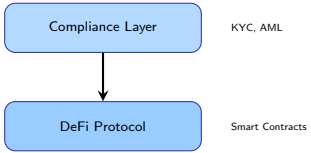
Institutional DeFi: The Convergence Frontier

What Makes It "Institutional":

- Whitelisted addresses only
- KYC/AML verification required
- Permissioned access layers
- Same smart contracts underneath

Examples:

- Aave Arc (limited adoption)
- Compound Treasury
- JPM Onyx
- Securitize



Key Difference

Same efficiency gains, but with regulatory compliance baked in.

Tokenized Deposits vs. Stablecoins

Feature	Tokenized Deposits	Stablecoins
Issuer	Commercial banks	Non-bank entities
Liability	Bank liability	Issuer liability
Insurance	FDIC insured*	No deposit insurance
Regulation	Bank charter	Varies by jurisdiction
Example	JPM Coin	USDC, USDT
Settlement	Private blockchain	Public/private
Access	Bank customers only	Permissionless

*FDIC = Federal Deposit Insurance Corporation (US). Similar: FSCS (UK), Einlagensicherung (EU).

Tokenized Deposits:

- Trusted, regulated
- Limited access
- Existing relationships

Stablecoins:

- Global, permissionless
- Reserve transparency varies
- DeFi composability

Career Paths in Digital Finance

Technical Roles:

- Smart contract developer
- Protocol engineer
- Security auditor
- Blockchain infrastructure
- Data scientist (on-chain analytics)

Finance Roles:

- DeFi strategist
- Digital asset trader
- Tokenization specialist
- Risk manager (crypto)

Hybrid Roles:

- Compliance/regulatory analyst
- Product manager (crypto)
- Research analyst
- Business development

Emerging Roles:

- AI x Crypto specialist
- CBDC consultant
- DAO governance expert
- Digital identity architect

Key Insight

Cross-disciplinary skills are most valuable: technical + financial + regulatory understanding.

Skills for the Future of Digital Finance

Technical Skills:

- Solidity/smart contracts
- Python for data analysis
- Cryptography basics
- API integration
- Security fundamentals

Financial Skills:

- Risk management
- Incentive analysis
- Market microstructure
- Valuation methods

Soft Skills:

- Cross-functional communication
- Rapid learning ability
- Regulatory awareness
- Critical evaluation

Meta-Skills:

- Separating hype from substance
- Identifying trade-offs
- Building mental models
- Asking the right questions

Regulatory Evolution: Three Scenarios

Key Regulatory Questions:

- Is this a security, commodity, or new asset class?
- Who is liable when things go wrong?
- How do we balance innovation with consumer protection?
- Can regulation keep pace with technology?

The Innovation Scorecard: Your Framework

Six Questions for Any Digital Finance Innovation

1. **PROBLEM**: What real problem does this solve, and for whom?
   Red flag: Vague problem statement or only solves crypto-native problems
2. **MECHANISM**: How does it actually work (technically and economically)?
   Red flag: "It's decentralized" without specifics
3. **TRADEOFFS**: What are the key tradeoffs and design choices?
   Red flag: Claims of "no tradeoffs" or "best of all worlds"
4. **RISKS**: What could go wrong (technical, economic, regulatory)?
   Red flag: Claims of "no risk" or "guaranteed returns"
5. **REGULATORY STATUS**: Where does it fit in the regulatory landscape?
   Red flag: Regulatory arbitrage as the main strategy
6. **WHO BENEFITS**: Who captures value, and who bears costs?
   Red flag: Unclear value capture or misaligned incentives

Course Summary: The Six-Day Journey

Day	Theme	Key Takeaways
1	Foundations	Money, financial system, FinTech vs. DeFi, landscape overview
2	Digital Finance	Payments, API economy, data-driven finance, platform economics
3	Blockchain	Cryptography, mechanics, wallets, Bitcoin vs. Ethereum
4	Smart Contracts	Smart contracts, DeFi primitives, stablecoins, tokenization & CBDCs
5	Risk & Regulation	Failures, regulation, DAO governance, privacy & inclusion
6	Future	Convergence, AI & digital finance, synthesis framework, what's next

Key Competencies You've Developed

Technical Understanding:

- How blockchains achieve consensus
- Smart contract mechanics
- DeFi protocol design
- Security considerations

Economic Reasoning:

- Incentive analysis
- Market structure effects
- Risk-return tradeoffs
- Value capture dynamics

Regulatory Awareness:

- Classification frameworks
- Jurisdictional differences
- Compliance requirements
- Regulatory trajectory

Critical Evaluation:

- Separating hype from substance
- Identifying risks and tradeoffs
- Asking the right questions
- Framework for any innovation

The Durable Lessons

1. **No free lunch**: Every design choice involves tradeoffs. Be skeptical of claims that offer everything.
2. **Incentives matter**: Understand who profits and how. Follow the money.
3. **Technology is not enough**: Great tech fails without regulatory clarity, user adoption, and sustainable economics.
4. **Regulation follows innovation**: The rules will change. Build with regulatory evolution in mind.
5. **Decentralization is a spectrum**: Most systems are more centralized than marketed. That's not always bad.
6. **Convergence is coming**: The FinTech-DeFi divide is dissolving. Prepare for hybrid futures.
7. **Stay curious, stay skeptical**: This field moves fast. Your framework for evaluation matters more than any specific fact.

Resources for Continued Learning

News and Analysis:

- The Block, CoinDesk (crypto)
- Risk.net, American Banker (TradFi)
- a16z crypto blog (`a16zcrypto.com`)
- BIS working papers

Technical Deep Dives:

- Ethereum docs
- DeFi protocol documentation
- Academic papers (SSRN, NBER)

Regulatory Updates:

- SEC, CFTC releases
- EU MiCA documentation
- FSB reports

Communities:

- Protocol governance forums
- Twitter/X crypto finance
- Academic conferences (AFA, WFA)

The course ends here. Your journey continues.

Group Discussion: Your Hypotheses

Instructions (15 minutes)

Form small groups (3–4 students). Each group picks one open question and develops a hypothesis about how it will unfold over the next decade. Be prepared to defend your view.

Structure your hypothesis:

1. **Claim**: What do you think will happen?
2. **Evidence**: What current trends support this?
3. **Assumptions**: What must be true for your prediction to hold?
4. **Risks to thesis**: What could prove you wrong?
5. **Implications**: If you're right, what follows?

Application: Scenario Planning Exercise

Exercise: The Year is 2030

Consider these scenarios and their implications:

Scenario A: CBDC Dominance

- Major economies launch retail CBDCs
- Stablecoins heavily regulated
- DeFi moves fully on-chain KYC
- Privacy a major political issue

Scenario B: Crypto Mainstream

- Bitcoin ETFs widely held
- DeFi 2.0 with real-world integration
- Traditional banks offer crypto services
- Regulatory clarity achieved

Discussion Questions:

- Which scenario seems more likely? Why?
- What would you do differently in each scenario?
- What signals would indicate which scenario is emerging?

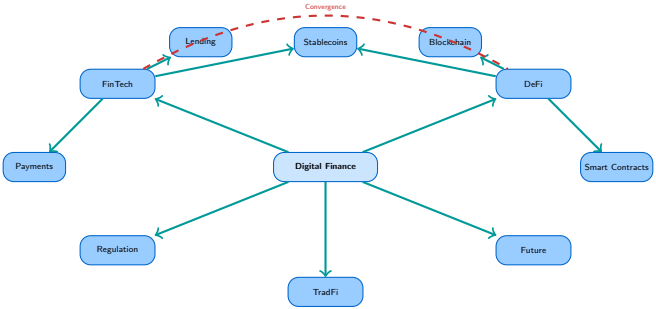
Key Takeaways from Topic 6.4

1. **Seven open questions** will shape digital finance's next decade
   Interoperability, CBDCs, identity, quantum, AI, regulation, money itself
2. **No single "winner"** is predetermined
   Multiple futures possible; coexistence likely
3. **Technology continues accelerating**
   ZK proofs, account abstraction, DePIN changing what's possible
4. **Careers require cross-disciplinary skills**
   Technical + financial + regulatory understanding most valuable
5. **Your evaluation framework matters most**
   The Innovation Scorecard works for any future development

The Big Idea

Uncertainty about the future is not a weakness—it's an opportunity for those who build good mental models.

Concept Map: The Digital Finance Landscape



Key Insight: All components are interconnected. Understanding one requires understanding all.

Key Terms & Definitions (I)

Interoperability The ability of different blockchain systems to communicate and transact with each other seamlessly.

CBDC Central Bank Digital Currency—a digital form of fiat currency issued directly by the central bank.

Post-Quantum Cryptography Cryptographic algorithms designed to resist attacks from quantum computers.

Zero-Knowledge Proof A cryptographic method to prove a statement is true without revealing the underlying data.

Account Abstraction Making blockchain accounts programmable with features like social recovery and batched transactions.

Key Terms & Definitions (II)

DePIN Decentralized Physical Infrastructure Networks—using token incentives to coordinate real-world infrastructure.

Chain Abstraction A future state where users don't need to know or care which blockchain they're using.

Institutional DeFi DeFi protocols with added compliance layers (KYC/AML) for institutional participants.

Tokenized Deposits Bank deposits represented on blockchain, maintaining FDIC (Federal Deposit Insurance Corporation — the US bank deposit insurance agency; similar schemes: FSCS in the UK, Einlagensicherung in the EU) insurance and bank liability status.

AI Agent An autonomous AI system capable of holding assets and executing transactions independently.

Coexistence Hypothesis The view that multiple forms of digital money (CBDCs, stablecoins, crypto) will coexist rather than one winning.

Common Misconceptions

Misconception	Reality
"One blockchain will win everything"	Multiple chains will likely coexist with different specializations
"CBDCs will eliminate crypto"	Coexistence more likely; different use cases, different systems
"Quantum will break all crypto soon"	Timeline is 10-30 years; migration paths exist
"The future is predictable"	Genuine uncertainty exists; frameworks matter more than predictions

Critical Thinking

Be wary of anyone claiming certainty about the future. The best we can do is build good mental models and stay adaptable.

Self-Assessment: Question 1

Question

How many countries are currently exploring Central Bank Digital Currencies (CBDCs)?

A. 50+ countries
B. 80+ countries
C. 130+ countries
D. 200+ countries

Self-Assessment: Question 1

Question

How many countries are currently exploring Central Bank Digital Currencies (CBDCs)?

A. 50+ countries
B. 80+ countries
C. 130+ countries
D. 200+ countries

Answer: C

Explanation: Over 130 countries are exploring CBDCs, with China, Nigeria, and the Bahamas having already launched live implementations. This represents a significant shift in how central banks view digital currency.

Self-Assessment: Questions 2-3

Question 2

What is the estimated timeline for quantum computers posing a practical threat to current blockchain cryptography?

Answer: 10-30 years, with significant uncertainty. This timeline gives the industry time to migrate to post-quantum cryptographic standards.

Question 3

What does the course identify as the most likely future for blockchain interoperability?

Answer: The future is genuinely uncertain, with multiple possibilities: one dominant chain, chain abstraction hiding complexity, specialized chains for different uses, or traditional institutions not needing public chains at all. No single outcome is predetermined.

Next Steps: Your Continued Learning

Immediate Actions:

1. Review course materials
2. Build a project (DeFi app, analysis)
3. Follow key news sources
4. Join relevant communities

Medium-term Goals:

- Deep dive into one area
- Contribute to open-source
- Attend conferences/meetups
- Consider certifications

Certifications to Consider:

- CFA (traditional finance)
- CAIA (alternative investments)
- Blockchain developer certs
- Compliance certifications

Advanced Study:

- Master's in FinTech
- Specialized courses (DeFi, ML)
- Research opportunities
- Industry internships

Remember

The field changes faster than any curriculum. Your ability to learn and adapt matters more than any credential.

Resources & References

Key Publications:

- BIS: "The Future of the Monetary System" (Annual Economic Report)
- Atlantic Council: CBDC Tracker (`atlanticcouncil.org/cbdctracker`)
- NIST: Post-Quantum Cryptography Standards

Research Sources:

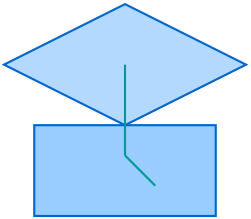
- SSRN FinTech and DeFi research papers
- Ethereum Foundation research blog
- a16z State of Crypto reports

Industry Resources:

- Messari, Delphi Digital (research reports)
- Chainalysis (on-chain analytics)
- Protocol governance forums (Compound, Aave, etc.)

Course Materials: All slides and notebooks available on the course website.

Course Complete



“The best way to predict the future is to invent it.”

— Alan Kay

You now have the tools to not just observe digital finance, but to **critically evaluate**, **thoughtfully participate**, and perhaps **help shape** its future.