Day 5: Risk, Regulation, and the Dark Side

What Goes Wrong and Who Decides What's Allowed

Joerg Osterrieder

Digital Finance

2025

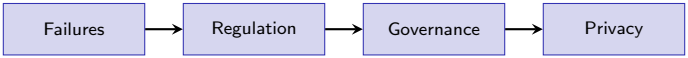
Today's Journey

Where We're Going:

- What fails in digital finance?
- How do governments respond?
- Who governs decentralized systems?
- Who benefits and who is harmed?

By Day's End, You Will:

- Categorize failure modes and exploits
- Compare regulatory frameworks globally
- Evaluate DAO governance tradeoffs
- Form positions on privacy vs. surveillance



5.1 What Goes Wrong

Failures, Hacks, and Systemic Risk in Digital Finance

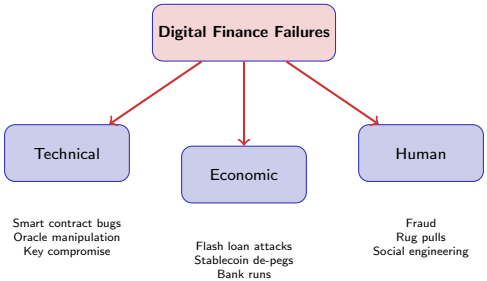
Learning Objectives:

- Categorize types of digital finance failures
- Explain mechanics of major exploit types
- Assess systemic risk implications
- Develop genuine risk awareness

Hands-On Component

Colab notebook (NB11) simulating historical DeFi exploits—run reentrancy, flash loan, and oracle manipulation scenarios to understand how attacks work.

A Taxonomy of Failures



Category 1: Technical Failures

Smart Contract Bugs:

- Reentrancy attacks
- Integer overflow/underflow
- Logic errors
- Access control flaws

Infrastructure Failures:

- Oracle manipulation
- Bridge vulnerabilities
- Consensus bugs
- Key management failures

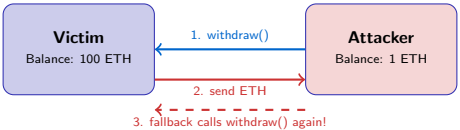
The DAO Hack (2016)

Loss: $60M (3.6M ETH)
Cause: Reentrancy bug
Result: Ethereum hard fork
Lesson: Code is NOT always law

Wormhole Bridge (2022)

Loss: $320M
Cause: Signature verification bug
Attacker minted unbacked tokens

Deep Dive: Reentrancy Attack



The Problem:

1. Victim sends ETH *before* updating balance
2. Attacker's fallback function calls withdraw() again
3. Balance not yet updated, so check passes again
4. Repeat until contract drained

Prevention

Check-Effects-Interactions pattern: Update state BEFORE external calls.

Reentrancy: Vulnerable vs. Safe (Pseudocode)

Vulnerable Process:

1. Check: Does user have a balance? ✓
2. **Send money to user**
   → Attacker calls back HERE
   → Repeat step 2 (loop!)
3. Update records: set balance to 0
   → Too late—money already sent multiple times!

Safe Process:

1. Check: Does user have a balance? ✓
2. **Update records FIRST:** set balance to 0
3. **Then send money**
   → If attacker calls back, balance is already 0
   → Attack fails!

Check-Effects-Interactions Pattern

1. **Check:** Validate conditions (is the request valid?)
2. **Effects:** Update your records (mark as done)
3. **Interactions:** Send money last (external calls at the end)

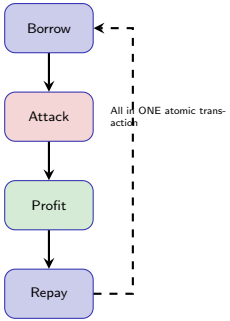
Category 2: Economic Attacks

Flash Loan Attacks:

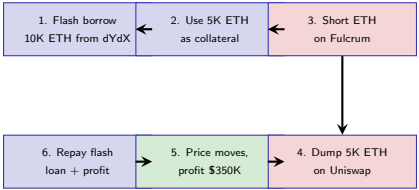
- Borrow millions, attack, repay—all in one transaction
- No collateral needed
- Exploit price discrepancies
- Manipulate governance votes

How Flash Loans Work:

1. Borrow $100M (uncollateralized)
2. Execute attack strategy
3. Repay $100M + fee
4. If any step fails, entire tx reverts



Flash Loan Attack Example: bZx (2020)



Key insight: Capital requirement to manipulate markets dropped from millions to **zero**.

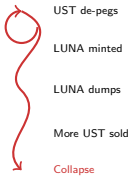
Category 3: Stablecoin Failures

UST/LUNA Collapse (May 2022):

- Algorithmic stablecoin
- Market cap: $18B at peak
- De-pegged from $1 to $0.10
- LUNA: $80 to $0.0001
- Total value destroyed: $40B+

The Death Spiral:

1. Large UST sell-off
2. Peg breaks, panic ensues
3. LUNA minted to defend peg
4. LUNA hyperinflates
5. Both collapse to zero



Lesson

Algorithmic stability requires robust mechanisms—"code" alone is insufficient.

Category 4: Centralized Exchange Collapses

FTX Collapse (Nov 2022):

- 2nd largest crypto exchange
- $32B valuation
- Customer funds misappropriated
- $8B+ missing
- CEO convicted of fraud

Mt. Gox (2014):

- 70% of Bitcoin trading
- 850,000 BTC "lost"
- Combination of hack + fraud
- 10+ years to partial recovery

Common Patterns:

1. Opaque operations
2. Commingled funds
3. Lack of proof of reserves
4. Regulatory arbitrage
5. Charismatic founders

Not Your Keys, Not Your Coins

Centralized custodians reintroduce the trust problems DeFi was designed to solve.

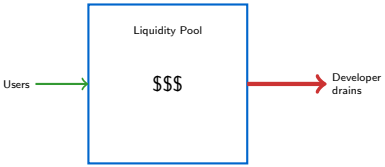
Category 5: Rug Pulls and Fraud

Types of Rug Pulls:

- **Liquidity pull:** Developers drain LP tokens
- **Limiting sell orders:** Hidden code prevents selling
- **Dumping:** Team sells massive holdings
- **Exit scam:** Project disappears with funds

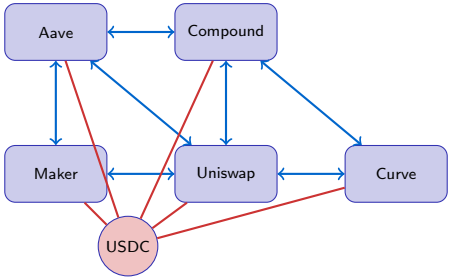
Red Flags:

- Anonymous team
- Unlocked liquidity
- No audit
- Unrealistic promises
- FOMO marketing
- Celebrity endorsements



2021 Stats:
$2.8B lost to rug pulls (Chainalysis)

Systemic Risk in Digital Finance



DeFi Composability = Systemic Risk:

- Protocols depend on each other ("money legos")
- Stablecoins are systemic (USDC freeze = cascade)
- Oracle failure affects ALL dependent protocols
- Smart contract bug can propagate through ecosystem

Largest DeFi Exploits (2020-2024)

Protocol	Loss	Type	Year
Ronin Bridge	$625M	Bridge exploit	2022
Poly Network	$611M	Bridge exploit	2021
FTX	$477M	Hack post-bankruptcy	2022
Wormhole	$320M	Bridge exploit	2022
Nomad Bridge	$190M	Bridge exploit	2022
Beanstalk	$182M	Flash loan governance	2022
Wintermute	$160M	Key compromise	2022

Pattern Recognition

Bridges are the weakest link. Cross-chain bridges hold massive TVL but have complex attack surfaces.

Simulate Real Exploit Scenarios

In the Colab notebook, we will:

1. Run simulations of exploit scenarios (reentrancy, flash loans, oracle manipulation)
2. Model how each attack type drains funds step-by-step
3. Identify the attack patterns and vulnerabilities
4. Calculate attacker profit in simulated scenarios
5. Discuss what could have prevented each exploit

Access the Notebook

`day_05/notebooks/NB11_DeFi_Exploits.ipynb`

We'll simulate real exploit types to understand how they work.

Time: 20-25 minutes for guided exploration

Discussion: Risk Awareness

Questions to Consider:

1. Should smart contracts be audited before deployment?
2. Who is liable when code fails?
3. Is "code is law" a feature or a bug?
4. How do we balance innovation with safety?

Key Takeaways:

- Failures are inevitable—design for them
- Technical, economic, and human risks compound
- Transparency enables post-mortem but not prevention
- Systemic risk grows with interconnection

Risk Framework

For any protocol: What can go wrong technically? Economically? Who has the keys? What happens when it fails?

5.2 Regulatory Landscapes

How Governments Respond to Digital Finance

Learning Objectives:

- Compare major regulatory frameworks (US, EU, Asia)
- Explain policy rationale behind key regulations
- Predict how regulation shapes innovation trajectories
- Understand why the same technology gets treated differently

Why Regulation Matters

Regulation determines which innovations survive. Understanding regulatory logic helps you build compliant products and predict market evolution.

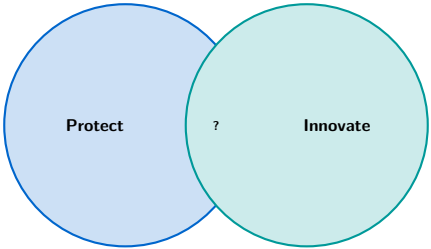
The Regulatory Challenge

What regulators want:

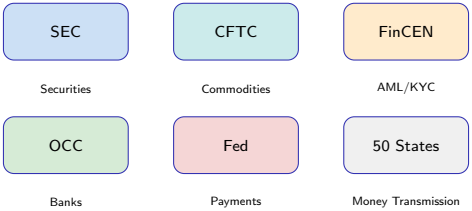
- Consumer protection
- Market integrity
- Financial stability
- Anti-money laundering
- Tax compliance
- National security

What innovators want:

- Permissionless access
- Privacy
- Speed to market
- Global reach
- Minimal compliance costs
- Regulatory clarity



United States: Fragmented Landscape



Key issue: No single regulator. Turf wars between SEC and CFTC.

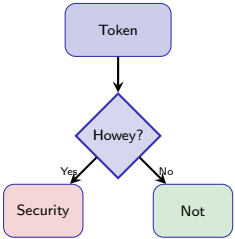
US: The Howey Test

Is it a security?
A token is a security if it involves:

1. **Investment of money**
2. **In a common enterprise**
3. **With expectation of profits**
4. **Derived from others' efforts**

SEC Position:

- Most ICOs were securities
- Many tokens are securities
- ETH and BTC are NOT securities
- "Come in and register"



Consequences:
Securities require registration, prospectus, qualified investors only.

US Enforcement Actions (2023-2024)

Target	Allegation	Status
Coinbase	Operating unregistered exchange	Ongoing litigation
Binance	Multiple securities violations	$4.3B settlement
Kraken	Unregistered staking service	$30M settlement
Ripple (XRP)	Unregistered securities	Partial win for Ripple
Terraform	Securities fraud (UST)	Founders charged

Regulation by Enforcement

US lacks comprehensive crypto legislation. SEC and CFTC establish rules through lawsuits rather than clear guidelines.

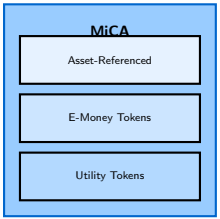
European Union: MiCA Framework

Markets in Crypto-Assets (MiCA):

- First comprehensive crypto regulation
- Effective 2024-2025
- Harmonized across 27 countries
- Clear licensing requirements

Key Provisions:

1. Crypto-Asset Service Providers (CASPs) licensed
2. Stablecoin issuers must hold reserves
3. Whitepaper requirements for token issuance
4. Consumer protection rules
5. Market manipulation prohibited



Not covered:
DeFi, NFTs (mostly), CBDCs

MiCA: Stablecoin Rules

Asset-Referenced Tokens (ARTs):

- Backed by multiple assets
- Issuer must be authorized
- Reserve requirements
- No interest payments
- If "significant": stricter rules

E-Money Tokens (EMTs):

- Single fiat currency reference
- Must be e-money institution
- 1:1 redemption rights
- Segregated reserves

Significance Thresholds

"Significant" ART/EMT if:

- 10M+ holders
- €5B+ market cap
- 2.5M+ daily transactions
- €500M+ daily value

Higher capital, stricter oversight.

Impact on USDT/USDC:
Must comply or delist from EU exchanges.

Asia: Diverse Approaches

Japan

Licensed exchanges
Crypto legal tender nearby

Singapore

Innovation hub
MAS licensing

China

Total ban
CBDC push (e-CNY)

South Korea

Strict compliance
Travel rule enforced

China: Complete Ban + CBDC

What's Banned:

- Cryptocurrency trading
- Crypto mining (since 2021)
- ICOs
- Crypto exchanges
- Providing crypto services

Penalties:

- Criminal prosecution possible
- Businesses shut down
- Mining operations seized

Digital Yuan (e-CNY):

- Central Bank Digital Currency
- Controlled by PBoC
- Two-tier distribution
- Programmable money
- Pilot programs in major cities

The Strategy

Ban decentralized crypto, promote centralized CBDC. Maximum control, full surveillance.

Regulatory Comparison Matrix

Aspect	US	EU (MiCA)	Singapore	China
Crypto trading	Varies	Licensed	Licensed	Banned
Token issuance	Case-by-case	Whitepaper	Licensed	Banned
Stablecoins	Unclear	Regulated	Licensed	Banned
DeFi	Unclear	Unclear	Evolving	Banned
NFTs	Unclear	Mostly exempt	Evolving	Gray area
CBDC	Researching	Exploring	Exploring	Live
Clarity	Low	High	Medium	High (ban)

Key Insight

Regulatory arbitrage is real. Projects choose jurisdictions strategically. Clear rules (even strict ones) often preferred over uncertainty.

The Travel Rule

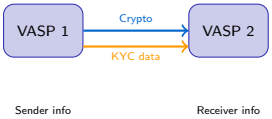
What is it?
FATF requirement: Virtual Asset Service Providers (VASPs) must share sender/receiver information for transfers above thresholds.

Information Required:

- Sender name
- Sender account number
- Sender address or ID
- Beneficiary name
- Beneficiary account number

Thresholds:

- US: $3,000+
- EU: €0 (all transfers!)
- FATF guidance: $1,000



DeFi Challenge

How do you apply Travel Rule to non-custodial wallets and DEXs?

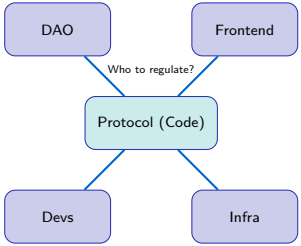
DeFi Regulatory Challenges

The Fundamental Problem:

- Who is the "operator"?
- Where is it located?
- Who do you regulate?
- How do you enforce?

Potential Targets:

- Frontend interfaces
- Token holders with governance power
- Core developers
- Infrastructure providers



Emerging Approach

Target the chokepoints: fiat on/off ramps, centralized frontends, infrastructure providers.

Case Study: Tornado Cash Sanctions

What Happened (Aug 2022):

- US Treasury sanctioned Tornado Cash
- Smart contract addresses added to OFAC list
- Developer arrested in Netherlands
- First time: CODE itself sanctioned

Consequences:

- GitHub removed repo
- Circle froze USDC in addresses
- Exchanges blocked deposits
- Alchemy/Infura blocked RPC access

Legal Questions

- Can you sanction open-source code?
- Is running a mixer illegal?
- What about privacy rights?
- First Amendment implications?

Outcome:
Court ruled some sanctions overreach (2024).
Case ongoing.

Discussion: Regulatory Philosophy

Argument for Strict Regulation:

- Protect consumers from fraud
- Prevent money laundering
- Ensure financial stability
- Level playing field with TradFi
- Accountability for failures

Argument for Light Touch:

- Enable innovation
- Avoid regulatory arbitrage
- Code is speech (1st Amendment)
- Self-sovereignty rights
- Regulation kills jobs

Discussion Questions

- Should DeFi protocols be regulated like banks?
- Is "code is law" compatible with rule of law?
- What's the right balance for stablecoins?
- Where would you launch a crypto startup?

5.3 DAO Governance

DAOs and the Limits of Code

Learning Objectives:

- Explain DAO governance mechanisms
- Identify governance attack vectors
- Evaluate tradeoffs between on-chain and off-chain governance
- Understand why "code is law" is insufficient

Hands-On Component

Colab notebook (NB12) simulating a DAO vote—model different token distributions and observe how governance outcomes change with concentration of voting power.

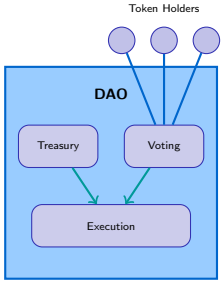
What is a DAO?

Decentralized Autonomous Organization:

- Rules encoded in smart contracts
- Decisions via token holder voting
- Treasury managed on-chain
- No traditional legal structure
- "Code is law" philosophy

Common Functions:

- Protocol upgrades
- Parameter changes
- Treasury allocation
- Grant distribution
- Strategic direction



DAO Governance Mechanisms

Token-Based Voting:

- 1 token = 1 vote
- Simple and transparent
- But: plutocracy problem

Quadratic Voting:

- Cost increases quadratically
- Reduces whale dominance
- But: Sybil vulnerable

Conviction Voting:

- Votes accumulate over time
- Rewards long-term alignment
- But: slow decision-making

Delegation:

- Delegate votes to experts
- Addresses voter apathy
- But: concentrates power

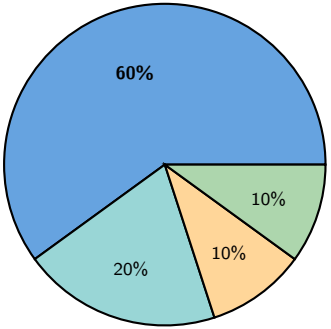
Multi-sig:

- N-of-M signers required
- Fast execution
- But: centralized trust

Optimistic Governance:

- Proposals pass unless vetoed
- Efficient for routine decisions
- But: requires active monitoring

The Plutocracy Problem



Top 10 wallets: 60%

Next 100: 20%

Next 1000: 10%

Everyone else: 10%

Reality: Most DAOs have highly concentrated token distributions.
Result: A few whales control most decisions. “Decentralized” in name only.

Governance Attack Vectors

Flash Loan Governance Attack:

1. Borrow millions in governance tokens
2. Vote on malicious proposal
3. Execute immediately
4. Repay loan, keep profits

Beanstalk Attack (2022):

- Flash borrowed $1B in tokens
- Passed proposal in one block
- Drained $182M from treasury
- All in a single transaction

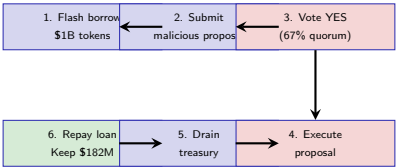
Other Attack Vectors:

- **Vote buying:** Purchase votes off-chain
- **Dark DAOs:** Coordinate attacks privately
- **51% attack:** Accumulate majority
- **Delegation hijacking:** Compromise delegates
- **Social engineering:** Manipulate key members

Key Insight

Governance is the attack surface. Secure code means nothing if governance can change it.

Case Study: Beanstalk Governance Attack



Critical flaw: No time delay between vote and execution.
Fix: Timelocks, snapshot voting, flash loan protection.

Governance Defenses

Timelocks:

- Delay between approval and execution
- Gives time to react to attacks
- Standard: 24-48 hours minimum

Vote Escrow:

- Lock tokens to vote (veTokens)
- Longer lock = more voting power
- Prevents flash loan attacks

Snapshot Voting:

- Balance at specific block height
- Cannot borrow tokens after snapshot

Quorum Requirements:

- Minimum participation threshold
- Higher for critical decisions
- Risk: voter apathy blocks everything

Guardian/Veto Power:

- Multi-sig can block malicious proposals
- Centralization tradeoff
- "Emergency brake"

Optimistic Execution:

- Proposals pass unless vetoed
- Challenge period for objections

On-Chain vs. Off-Chain Governance

Aspect	On-Chain	Off-Chain
Binding	Automatic execution	Requires implementation
Transparency	Fully verifiable	Forum/snapshot
Cost	Gas fees	Usually free
Speed	Blockchain constrained	Faster iteration
Flexibility	Rigid (code)	Adaptable
Attacks	Flash loans, 51%	Social, coordination
Examples	Compound, Uniswap	Bitcoin, Ethereum L1

Hybrid Approaches

Most successful DAOs use both: off-chain discussion/signaling, on-chain execution with safeguards.

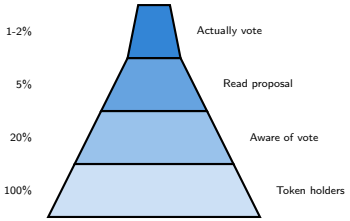
The Voter Apathy Problem

Reality of DAO Participation:

- Typical turnout: 1-5% of tokens
- Most token holders never vote
- Few wallets dominate decisions
- Governance fatigue is real

Why People Don't Vote:

- Gas costs (on-chain)
- Time to understand proposals
- Rational ignorance (1 vote doesn't matter)
- Token holders $\neq$ users



"Code is Law" vs. Rule of Law

"Code is Law" Philosophy:

- Smart contract IS the agreement
- No external intervention
- Predictable, immutable
- "If the code allows it, it's allowed"

The DAO Hack Challenge:

- Hacker used code as designed
- Was it theft or legitimate use?
- Ethereum community chose to fork
- "Code is law" violated by humans

Traditional Rule of Law:

- Intent matters (mens rea)
- Fairness considerations
- Courts interpret disputes
- Law evolves with society

The Tension

Code cannot encode intent, fairness, or context. Pure "code is law" may be unjust. But human intervention undermines decentralization.

Model How Token Distribution Affects Governance

In the Colab notebook, we will:

1. Create token distributions with varying concentration
2. Simulate voting on proposals
3. Calculate Gini coefficients for voting power
4. Test attack scenarios (whale dominance, flash loans)
5. Explore defense mechanisms (quadratic voting, delegation)

Access the Notebook

`day_05/notebooks/NB12_DAO_Governance.ipynb`

See how 1 whale with 51% can override 10,000 small holders.

Time: 20-25 minutes for guided exploration

Discussion: Governance Tradeoffs

Questions to Consider:

1. Is plutocracy inherent to token voting?
2. Should DAOs have constitutions?
3. When is centralization acceptable?
4. Can code ever fully replace human judgment?

Key Takeaways:

- Governance IS the attack surface
- Token distribution = power distribution
- "Decentralized" often isn't
- Hybrid models emerging

The Governance Trilemma

You can optimize for two of three: **Decentralization**, **Efficiency**, **Security**. Pick which one to sacrifice.

5.4 Privacy, Surveillance, and Financial Inclusion

Who Benefits and Who Is Harmed?

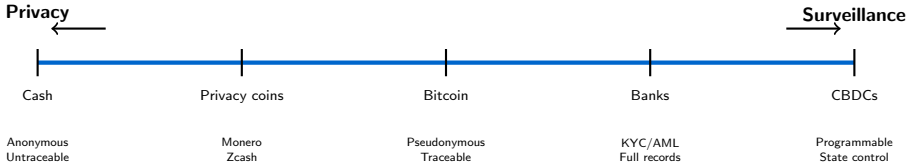
Learning Objectives:

- Articulate the privacy-transparency tradeoff
- Evaluate financial inclusion claims critically
- Form a reasoned position on surveillance in finance
- Understand who benefits from different design choices

The Central Tension

Digital finance creates unprecedented transparency (for regulation, trust) and unprecedented surveillance (of individuals, by states and corporations).

The Privacy-Transparency Spectrum



Key question: Where on this spectrum should financial systems be?

Arguments for Financial Privacy

Individual Rights:

- Financial data reveals beliefs, health, relationships
- Surveillance chills free expression
- Protection from domestic abuse
- Competitive business information

Historical Precedent:

- Nazi Germany: bank records used for persecution
- Authoritarian states freeze activist accounts
- Corporate surveillance for profit

Fungibility Principle:

- Money should be interchangeable
- Tainted coins create second-class money
- Privacy preserves fungibility

Human Rights Perspective

UN Declaration of Human Rights, Article 12:
"No one shall be subjected to arbitrary interference with his privacy."

Arguments for Financial Transparency

Anti-Crime Rationale:

- Money laundering enables crime
- Terrorist financing
- Tax evasion
- Sanctions enforcement
- Fraud detection

Consumer Protection:

- Dispute resolution
- Fraud recovery
- Accountability for institutions

Market Integrity:

- Insider trading detection
- Market manipulation prevention
- Fair price discovery

The AML Argument

$800B-$2T laundered annually. Transparency enables enforcement. "Nothing to hide, nothing to fear."

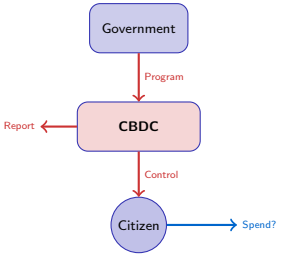
CBDCs: The Ultimate Surveillance Tool?

CBDC Capabilities:

- Complete transaction visibility
- Programmable spending restrictions
- Automatic tax collection
- Expiring money (demurrage)
- Geographic restrictions
- Social credit integration

China's e-CNY:

- Real-time government visibility
- Can be programmed for uses
- Integrated with social systems
- Pilot: 260M wallets



Dystopian Scenario

Money that watches you, judges you, and can be remotely disabled.

Privacy Technologies

Privacy Coins:

- **Monero (XMR):** Ring signatures, stealth addresses
- **Zcash (ZEC):** zk-SNARKs, shielded transactions
- **Dash:** CoinJoin mixing

Mixing Services:

- Tornado Cash (sanctioned)
- CoinJoin implementations
- Tumbling services

Zero-Knowledge Proofs:

- Prove something without revealing it
- "I'm over 18" without showing ID
- "I have funds" without showing balance

zk-Proofs for Compliance

Emerging: Prove you're not on sanctions list WITHOUT revealing identity. Privacy AND compliance.

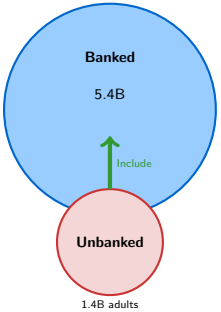
The Financial Inclusion Promise

The Narrative:

- 1.4 billion unbanked adults
- Mobile phones everywhere
- Crypto bypasses gatekeepers
- "Bank the unbanked"

Success Stories:

- M-Pesa in Kenya (FinTech)
- Remittances via stablecoins
- Bitcoin in El Salvador (controversial)
- Microloans via DeFi



The Financial Inclusion Critique

Barriers Remain:

- Internet access required
- Smartphone/device costs
- Technical literacy
- Language barriers
- Volatility hurts the poor most

Who Actually Benefits:

- Tech-savvy early adopters
- Those with capital to invest
- Speculators and traders
- Not primarily the unbanked

New Exclusions Created:

- Complex UX excludes many
- Gas fees price out small transactions
- Scams disproportionately hurt naive users
- Regulatory uncertainty creates risk

Critical Question

Is crypto solving inclusion, or repackaging exclusion in new forms?

Case Study: El Salvador Bitcoin Experiment

What Happened (Sept 2021):

- Bitcoin made legal tender
- $30 Bitcoin airdrop to citizens
- Government-backed Chivo wallet
- Volcano-powered mining

Stated Goals:

- Financial inclusion (70% unbanked)
- Cheaper remittances (20% of GDP)
- Attract investment
- Reduce dollar dependence

Results (2024):

- Adoption: limited daily use
- Remittances: mostly traditional
- Volatility: government losses
- IMF concerns
- Tourism boost (crypto tourists)

Verdict

Mixed at best. Inclusion gains modest; volatility risks real; adoption limited to merchants near tourists.

Who Benefits? Who Is Harmed?

Design Choice	Benefits	Harms
Full transparency	Regulators, auditors	Privacy-seekers, dissidents
Full privacy	Individuals, activists	Law enforcement, victims
Pseudonymity (Bitcoin)	Moderate privacy	Linkability risk
CBDCs	Governments, AML	Individual autonomy
KYC requirements	Compliance, banks	Unbanked, privacy
Permissionless access	Underserved, censored	May enable crime

No Neutral Design

Every architectural choice has distributional consequences. Technology is not neutral—it embeds values.

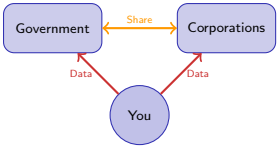
The Surveillance Capitalism Connection

Financial Data as Product:

- Transaction data sold to advertisers
- Credit scoring as control mechanism
- Behavioral prediction markets
- Insurance discrimination

Corporate vs. State Surveillance:

- PayPal, Visa see all transactions
- Data shared with governments
- No warrant needed for corporate data
- "Third-party doctrine" in US



You are the product.
Your transactions are the data.
Privacy is the cost.

Emerging Privacy Solutions

Selective Disclosure:

- Reveal only what's needed
- Age verification without DOB
- Solvency proof without balance
- Compliance without surveillance

Privacy-Preserving Compliance:

- zk-proofs for sanctions screening
- Encrypted transaction monitoring
- Decentralized identity

Example: Proving Non-Sanction

1. Hash your identity locally
2. Prove hash NOT on OFAC list
3. Zero-knowledge proof sent
4. Never reveal actual identity

The Vision

Compliance without surveillance. Privacy AND legitimacy. Technically possible, politically challenging.

Discussion: Where Do You Stand?

Team Privacy Argues:

- Privacy is a human right
- Surveillance enables authoritarianism
- Financial freedom requires anonymity
- Technology should protect individuals

Team Transparency Argues:

- Privacy enables crime
- Society needs accountability
- Victims deserve recourse
- "Sunlight is the best disinfectant"

Discussion Questions

- Should there be a right to financial privacy?
- Who gets to decide the tradeoff?
- Is financial inclusion marketing or reality?
- Would you use a CBDC?

Day 5 Synthesis

Day 5 Synthesis

What We Covered:

1. **Failures:** Technical, economic, human
2. **Regulation:** US fragmentation, EU MiCA, Asia divergence
3. **Governance:** DAO mechanisms and attacks
4. **Privacy:** Surveillance vs. autonomy tradeoffs

Key Takeaways:

- Failures are inevitable—design for them
- Regulation shapes what survives
- Governance IS the attack surface
- Privacy vs. transparency is political
- Financial inclusion: promise vs. reality

Day Arc

What fails (5.1) → Who governs from outside (5.2) → Who governs from inside (5.3) → Who benefits and who is harmed (5.4)

For Any Digital Finance System, Ask:

1. **Technical:** What can go wrong with the code/infrastructure?
2. **Economic:** What incentive attacks are possible?
3. **Human:** Who has power and might abuse it?
4. **Regulatory:** What jurisdiction risks exist?
5. **Governance:** Who decides changes, and how?
6. **Privacy:** Who sees what, and what can they do with it?
7. **Inclusion:** Who benefits, who is excluded, who is harmed?

The Critical Mindset

Move from "what can this do?" to "what can go wrong, and for whom?"

Convergence and the Future: Where Is Digital Finance Going?

We'll explore:

- TradFi + DeFi convergence
- Institutional adoption
- CBDCs and the future of money
- AI + Finance integration
- Your role in shaping this future

Preparation:

- Complete Day 5 notebooks (NB11, NB12)
- Reflect: What would YOU build?
- Think: What regulations would YOU write?

Resources

Notebooks:

- `day_05/notebooks/NB11_DeFi_Exploits.ipynb`
- `day_05/notebooks/NB12_DAO_Governance.ipynb`

Further Reading:

- EU MiCA Regulation (EUR-Lex)
- FATF Guidance on Virtual Assets
- Chainalysis Crypto Crime Report
- Vitalik Buterin on Governance

Concepts to Review:

- Reentrancy attacks, flash loans
- Howey Test, MiCA categories
- DAO governance mechanisms
- Privacy-transparency tradeoff

Questions?

Day 5: Risk, Regulation, and the Dark Side

What Goes Wrong and Who Decides What's Allowed

Next: Day 6 – Convergence and the Future