Topic 5.4: Privacy, Surveillance, and Financial Inclusion

Who Benefits and Who Is Harmed?

Joerg Osterrieder

Digital Finance

2025

Learning Objectives

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

1. **Articulate** the privacy-transparency tradeoff in digital finance
2. **Evaluate** financial inclusion claims critically
3. **Form** a reasoned position on surveillance in finance
4. **Understand** who benefits from different design choices
5. **Analyze** CBDC (Central Bank Digital Currency) privacy implications and programmable money
6. **Compare** privacy technologies and their regulatory status

Key Competency: Critically evaluate the distributional consequences of privacy and transparency choices in financial system design.

This topic synthesizes Day 5 themes: risks, regulation, governance, and inclusion

Why This Topic Now?

Connection to T5.3

In T5.3 we explored how DAOs try to govern themselves. Now we face a deeper question: in a world of digital money, **who can see what you do with your money**—and should they?

From Governance to Privacy:

- T5.3 asked: Who decides the rules?
- T5.4 asks: Who watches you follow them?
- Governance and surveillance are two sides of the same coin

What We Will Cover:

- Privacy vs. transparency tradeoffs
- Privacy technologies and how they work
- Blockchain surveillance and its tools
- CBDCs and programmable money
- Financial inclusion: promise vs. reality
- Who benefits and who is harmed

Prerequisites: Understanding Financial Privacy

What is Financial Privacy?

- Control over who sees your transactions
- Ability to transact without surveillance
- Protection of financial data from third parties
- The economic dimension of personal privacy

Why Privacy Matters:

- Financial data reveals beliefs, health, relationships
- Transactions indicate political views, religion
- Purchase patterns expose sensitive behaviors
- Location data from payment records

Historical Context

- Cash provided natural privacy
- Bank secrecy was traditional norm
- Digital transactions create permanent records
- Post-9/11: After the September 11, 2001 terrorist attacks, governments worldwide dramatically expanded financial surveillance laws, requiring banks to monitor and report suspicious transactions more aggressively than ever before

The Central Tension

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

Prerequisites: Understanding Financial Transparency

What is Financial Transparency?

- Visibility of transactions to authorized parties
- Traceability of fund flows
- Auditability of financial activity
- Accountability for financial behavior

Key Regulatory Frameworks:

- KYC: Know Your Customer
- AML: Anti-Money Laundering
- CFT: Countering Financing of Terrorism
- FATF: The Financial Action Task Force—an international body that sets anti-money-laundering standards. Its **Travel Rule** requires financial institutions to share sender and receiver information for transfers above a certain amount—like putting a return address on a package

Why Transparency Matters

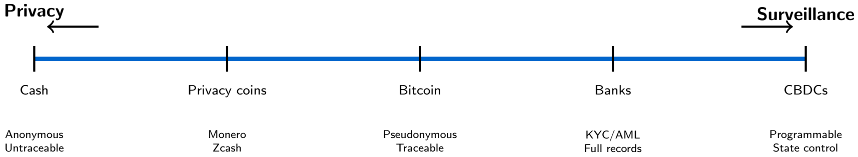
- Enables crime prevention
- Supports tax compliance
- Allows fraud recovery
- Creates institutional accountability

The Statistics:

- \$800B–\$2T laundered annually
- Financial crime enables all other crime
- Sanctions depend on traceability
- Consumer protection requires records

The Privacy-Transparency Spectrum

Recall from Day 3: Bitcoin transactions are **pseudonymous**—they are linked to addresses (like account numbers) rather than real names. But these addresses can potentially be traced back to real identities.



Privacy ←

→ **Surveillance**

Cash

Anonymous
Untraceable

Privacy coins

Monero
Zcash

Bitcoin

Pseudonymous
Traceable

Banks

KYC/AML
Full records

CBDCs

Programmable
State control

Key Question

Where on this spectrum should financial systems be? Different societies, different answers.

Note: Most people assume they're somewhere in the middle—reality may differ.

Arguments for Financial Privacy

Individual Rights:

- Financial data reveals beliefs, health, relationships
- Surveillance chills free expression
- Protection from domestic abuse
- Competitive business information
- Freedom to make unpopular purchases

Historical Precedent:

- Nazi Germany: bank records used for persecution
- Apartheid South Africa: financial records identified anti-apartheid activists
- Authoritarian states freeze activist accounts
- Corporate surveillance for profit

Fungibility Principle:

- Money should be interchangeable
- "Tainted" coins create second-class money
- Privacy preserves fungibility
- Without fungibility, money becomes trackable assets

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 prevention
- Tax evasion detection
- Sanctions enforcement
- Fraud detection and recovery

Consumer Protection:

- Dispute resolution requires records
- Fraud recovery needs traceability
- Accountability for institutions
- Insurance of deposits

Market Integrity:

- Insider trading detection
- Market manipulation prevention
- Fair price discovery
- Systemic risk monitoring

The AML Argument

$800B–$2T laundered annually worldwide.
Transparency enables enforcement.

The controversial claim: "Nothing to hide, nothing to fear."

Privacy Techniques: Hiding the Sender

Note: If you covered the optional Topic 4.5 on zero-knowledge proofs, parts of this section will be a review. If not, don't worry—we explain everything you need here.

Ring Signatures (used by Monero):

- Imagine 10 people each have a key. One of them signs a document, but nobody can tell *which* one signed it
- The signature is valid, but the signer is hidden among the group
- **Analogy:** Like signing a petition where any of 10 members could have written it—the signature is real, but the author is unknown

CoinJoin / Mixing:

- **CoinJoin**: Multiple people combine their transactions into one, making it hard to trace who paid whom. **Analogy:** Like several people putting cash into a hat and each taking out the same amount—observers cannot tell who paid whom
- Used by: Dash ("PrivateSend"), Wasabi Wallet, JoinMarket
- **Tumbling (mixing) services**: Third parties that mix many people's crypto together to break the trail. Controversial because they are also used for money laundering

Privacy Techniques: Hiding the Receiver

Stealth Addresses (used by Monero):

- Like having a PO box that automatically creates a new, unique address for every letter you receive
- The sender can send to you, but observers cannot link your different addresses together
- Each transaction creates a one-time address—even if someone knows your public address, they cannot tell which transactions are yours

Result:
The *receiver* of every transaction is hidden from outside observers.

Mixing Protocols on Ethereum:

- **Tornado Cash**: Users deposit ETH into a smart contract (recall: a program that runs automatically on a blockchain), then withdraw to a different address
- Zero-knowledge proofs verify the deposit was valid without revealing which deposit matches which withdrawal
- Breaks the on-chain link between sender and receiver

Key Distinction

Ring signatures hide the sender within a group. Stealth addresses hide the receiver by generating unique one-time addresses.

Privacy Techniques: Hiding the Amount

RingCT (Ring Confidential Transactions):

- Used by Monero—combines ring signatures with hidden amounts
- Not only is the sender hidden, but the amount transferred is also encrypted
- The blockchain can still verify that no money was created or destroyed (inputs = outputs), without anyone seeing the actual numbers

Bulletproofs:

- A type of **range proof**: a way to prove a number is within a valid range (e.g., "my balance is between 0 and 1,000") without revealing the exact number
- **Analogy:** Like proving you are old enough to drink without showing your exact birthday
- Used by Monero to make RingCT more efficient

Zero-Knowledge Proofs for Amounts:

- **Analogy:** Imagine proving you know a secret password without ever saying the password out loud. That is a zero-knowledge proof—you prove you *know* something without *revealing* what you know
- **zk-SNARKs** (used by Zcash): Very fast to verify, but require a **trusted setup**—a one-time ceremony to create the system's initial parameters. If anyone involved cheats during setup, they could create fake proofs forever
- **zk-STARKs**: No trusted setup needed, but proofs are larger

Emerging Possibility

Privacy-preserving compliance: Prove you are compliant WITHOUT full surveillance. Technically possible, politically challenging.

Zero-Knowledge Proofs: Technical Foundation

Start with the Analogy:
Imagine proving you know a secret password without ever saying the password out loud. You demonstrate knowledge without revealing the knowledge itself. That is a zero-knowledge proof.

More Formally:

- Cryptographic method where a prover convinces a verifier of a statement's truth
- Without revealing ANY information beyond the truth itself
- Neither party learns anything extra

Classic Analogy: Color-Blind Friend

1. Friend cannot distinguish red/green balls
2. You prove they are different colors
3. Without telling which is which
4. Repeated trials create confidence

Financial Applications:

- Prove age $\geq$ 18 without DOB
- Prove balance $\geq$ X without showing balance
- Prove not on sanctions list without revealing identity
- Prove income meets threshold without disclosing amount

Key Implementations

- **zk-SNARKs**: Used by Zcash. Fast verification, but requires a **trusted setup**—like building a vault where the builders must be trusted, even though later users don't need to trust each other
- **zk-STARKs**: No trusted setup needed, but larger proofs
- **Bulletproofs**: Monero's **range proofs**—prove a value is in a valid range without showing the value

Privacy Coin Deep Dive: Monero's Privacy Stack

Monero (XMR)—Privacy by Default:

- **Ring Signatures:** Mix your transaction with decoys—sender hidden among group. **Analogy:** Imagine 10 people each have a key; one signs, but nobody can tell which one
- **Stealth Addresses:** One-time addresses for each transaction—receiver unlinkable. **Analogy:** A PO box that auto-generates a new address for every letter received
- **RingCT:** Confidential transactions hide amounts while proving no money was created or destroyed
- **Dandelion++:** A privacy technique for broadcasting transactions. Instead of announcing a transaction to everyone simultaneously, it first passes through a random chain of nodes—like whispering a message through several people before announcing it publicly

Result:

- Sender, receiver, amount all hidden
- Blockchain analysis extremely difficult
- Default privacy (not optional like Zcash)

Regulatory Response

- Delisted from many exchanges
- Japan, South Korea banned
- Australia exchanges removed
- IRS bounty for tracing ($625K)

The Regulation of Privacy Coins

How Governments Mandate Transparency:

- Exchange delistings: Regulators pressure exchanges to remove privacy coins
- Travel Rule enforcement: Require sender/receiver data for transfers
- Outright bans: Some countries prohibit privacy coins entirely
- Bounties: Governments offer rewards for breaking privacy (e.g., IRS $625K Monero bounty)

The Policy Tension:

- Privacy coins have legitimate uses: dissidents, activists, abuse survivors
- But also used for ransomware and tax evasion
- Regulators rarely distinguish between the two

Use Cases—Both Sides:

- Legitimate: Dissidents and activists under authoritarian regimes
- Legitimate: Businesses protecting competitive information
- Illicit: Ransomware payments
- Illicit: Tax evasion and sanctions circumvention

Key Question

Should a technology be banned because it *can* be misused? Cash can also be used for crime, but nobody proposes banning cash entirely.

Case Study: Tornado Cash Sanctions

What is Tornado Cash?

- Ethereum mixing protocol (a smart contract—recall: a program that runs automatically on a blockchain)
- Users deposit ETH, withdraw to different address
- Zero-knowledge proofs verify valid deposit
- Breaks on-chain link between sender/receiver

August 2022: OFAC Sanctions

- US Treasury sanctions Tornado Cash
- First time: sanctions on code/protocol, not entity
- Developer arrested in Netherlands
- GitHub repositories removed

The Debate:

- **Government**: $7B laundered, including North Korea hacks
- **Critics**: Can you sanction open-source code? Neutral tool.

Legal Questions

- Is code speech? (The First Amendment to the US Constitution protects free speech—relevant because some argue writing code is a form of speech)
- Can immutable smart contracts be sanctioned?
- What about users who need privacy legitimately?

2024 Update: Court challenges ongoing.

Blockchain Surveillance: The Other Side

Blockchain Analysis Companies:
Think of blockchain analysts as forensic accountants examining a public ledger—every transaction is visible, they just need to figure out which entries belong to whom.

- **Chainalysis**: Market leader, works with governments
- **Elliptic**: UK-based, financial institutions
- **TRM Labs**: Growing player
- **CipherTrace**: Acquired by Mastercard

Pattern-Matching Techniques:

- **Clustering**: Link addresses to same entity
- Analysts look for clues like “these addresses always transact together” (**common ownership**) or “this leftover amount went back to the sender” (**change detection**)
- **Exchange KYC**: Link to real identities
- **IP tracking**: Network-level analysis

What They Can Do

- Trace fund flows across chains
- Identify exchange deposit addresses
- Flag “tainted” coins
- Link wallets to real identities
- Build transaction graphs

Key Insight:
Bitcoin is **pseudonymous**, not anonymous. With enough data, most users can be identified.

Pseudonymity vs. Anonymity: Critical Distinction

Pseudonymity (Bitcoin, Ethereum):

- Addresses are pseudonyms
- All transactions publicly visible
- Same address can be linked
- Exchange KYC links to identity
- Chain analysis can de-anonymize

Why Pseudonymity Is Weaker:
Pseudonyms can be **unmasked retroactively**. If anyone ever links your real identity to your Bitcoin address, they can trace ALL your past transactions. **Analogy:** Like writing under a pen name—once someone discovers your real name, every book you ever wrote is exposed.

Anonymity (Monero, Zcash shielded):

- Sender hidden by ring signatures
- Receiver hidden by stealth addresses
- Amounts hidden by encryption
- Linkage between transactions broken
- Much harder (not impossible) to trace

Practical Reality

Even “anonymous” systems have weaknesses:

- Exchange on/off ramps require KYC
- IP addresses can be tracked
- Human errors in operational security (OpSec)—the practice of protecting sensitive information from being discovered

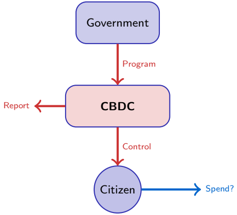
CBDCs: The Ultimate Surveillance Tool?

CBDC (Central Bank Digital Currency) Capabilities:

- Complete transaction visibility
- Programmable spending restrictions
- Automatic tax collection
- **Expiring money (demurrage)**: money that loses value over time if you don't spend it—like a gift card with an expiration date. This encourages spending rather than hoarding
- Geographic restrictions
- **Social credit integration**: Social credit systems assign citizens a score based on their behavior—paying bills on time, obeying traffic laws, or even what they post online. In China's system, a low score can restrict travel, loan access, and even children's school options
- Remote freezing/confiscation

China's e-CNY (Digital Yuan):

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



CBDC Privacy: Design Choices Matter

Full Surveillance Model:

- Central bank sees all transactions
- Real-time monitoring possible
- Maximum control and AML capability
- Minimal user privacy
- Example: China's e-CNY approach

Tiered Privacy Model:

- Small transactions anonymous
- Larger transactions tracked
- Balance limits without KYC
- European approach (proposed)

Privacy-Preserving Model:

- Zero-knowledge proofs for compliance
- Central bank cannot see individual transactions
- Only aggregate data visible
- Technically challenging

European Digital Euro Proposal

- Offline capability for small payments
- Privacy similar to cash for low-value
- Higher thresholds require ID
- Still under development (2024)

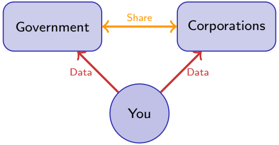
The Surveillance Capitalism Connection

Financial Data as Product:

- Transaction data sold to advertisers
- Credit scoring as control mechanism
- Behavioral prediction: companies use your transaction data to predict what you will buy, how risky you are, and what ads to show you
- Insurance discrimination
- Targeted pricing based on purchase history

Corporate vs. State Surveillance:

- PayPal, Visa see all transactions
- Data shared with governments
- No warrant needed for corporate data
- “Third-party doctrine” (US)



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

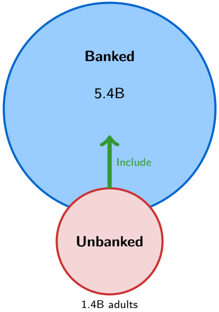
The Financial Inclusion Promise

The Narrative:

- According to the World Bank (2021), 1.4 billion adults remain unbanked globally
- Mobile phones reach areas banks don't
- Crypto bypasses traditional gatekeepers
- "Bank the unbanked" rallying cry
- Permissionless access for all

Success Stories:

- M-Pesa in Kenya: 50M+ users
- Remittances via stablecoins
- Microloans via DeFi protocols
- Cross-border payments simplified



Key Question:
Does digital finance actually serve the unbanked, or mainly the already-served?

Financial Inclusion: Barriers That Remain

Traditional Barriers:

- Geographic distance to banks
- Documentation requirements (ID, proof of address)
- Minimum balance requirements
- High fees for small transactions
- Lack of credit history
- Language and literacy barriers

Digital Finance "Solutions" Create New Barriers:

- Internet access required
- Smartphone/device costs
- Technical literacy needed
- Complex UX excludes many
- Gas fees price out small transactions
- Volatility hurts the poor most
- Regulatory uncertainty creates risk

Critical Question

Is crypto solving inclusion, or repackaging exclusion in new forms? The unbanked often become the "un-crypto'd" too.

The Financial Inclusion Critique

Who Actually Benefits:

- Tech-savvy early adopters
- Those with capital to invest
- Speculators and traders
- People already financially included
- Venture capital investors
- Exchange operators

New Exclusions Created:

- Scams disproportionately hurt naive users
- Rug pulls target newcomers
- Complex DeFi requires expertise
- No consumer protections

The “Last Mile” Problem:

- On-ramps require KYC (excludes undocumented)
- Off-ramps require bank accounts
- Local currency conversion expensive
- Merchant acceptance limited
- User education lacking

Reality Check

Chainalysis (2023) reports that emerging markets account for the highest crypto adoption rates—but proponents argue this reflects genuine financial need, while critics counter that adoption correlates more with speculation interest than financial exclusion.

Case Study: El Salvador Bitcoin Experiment

What Happened (September 2021):

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

Stated Goals:

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

Results (2024):

- Daily use: limited adoption
- Remittances: mostly traditional still
- Volatility: government paper losses
- IMF: ongoing concerns
- Tourism: some “crypto tourists”

Verdict

Mixed at best. Inclusion gains modest; volatility risks real; adoption limited to merchants near tourists. Not the revolution promised.

Success Story: M-Pesa (Not Crypto)

What is M-Pesa?

- Mobile money platform (Kenya, 2007)
- Works on basic feature phones via SMS
- No smartphone or internet required
- Agent network for cash-in/cash-out
- Now: 50M+ users across Africa

Why It Worked:

- Built on existing infrastructure (SMS)
- Local agent network (human touch)
- Simple, intuitive interface
- Regulatory support from Kenya
- Addressed real needs (P2P transfers)

Inclusion Impact:

- 2% of Kenyans lifted from poverty
- Women especially benefited
- Rural access dramatically improved
- Enabled small business growth

The Lesson

Financial inclusion success came from:

- Appropriate technology (not cutting-edge)
- Human infrastructure (agents)
- Regulatory cooperation
- NOT from cryptocurrency

Comparing Inclusion Approaches: What Works?

Factor	**M-Pesa (Kenya)**	**Bitcoin (El Salvador)**
Technology	Basic SMS phones	Smartphone app
Complexity	Very simple	Complex (wallets, keys)
Volatility	None (pegged to shilling)	High (Bitcoin price swings)
Human support	250K+ local agents	Limited
Adoption	50M+ active users	Low daily usage
Inclusion result	2% poverty reduction	Modest at best
Regulatory fit	Government-supported	IMF concerns

Key Insight

What worked: appropriate technology, human infrastructure, regulatory support.
What struggled: cutting-edge technology, top-down mandates, volatile assets.

Who Benefits? Who Is Harmed?

Design Choice	Benefits	Harms
Full transparency	Regulators, auditors	Privacy-seekers, dissidents
Full privacy	Individuals, activists	Law enforcement, crime victims
Pseudonymity (Bitcoin)	Moderate privacy seekers	Those needing true anonymity
CBDCs	Governments, AML	Individual autonomy
KYC requirements	Compliance, banks	Undocumented, unbanked
Permissionless access	Underserved, censored	May enable criminal use

No Neutral Design

Every architectural choice has distributional consequences. Technology is not neutral—it embeds values and determines who wins and who loses.

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 systems
- Verifiable credentials

Example: Proving Non-Sanction

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

The Vision

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

Self-Sovereign Identity: A Middle Path?

What is Self-Sovereign Identity (SSI)?
Analogy: Think of SSI as a digital wallet containing verified credentials—like carrying your passport, diploma, and bank statement in your phone, but you choose which to show and to whom.

- Users control their own identity data
- No reliance on centralized authority
- Selective disclosure of attributes
- Cryptographic verification

How It Works:

- Issuer provides verifiable credential
- User stores in digital wallet
- User presents proof to verifier
- Verifier checks cryptographic validity

Financial Applications:

- KYC once, use everywhere
- Prove **creditworthiness** (whether a borrower is likely to repay a loan, based on their financial history) without revealing exact credit score
- Age verification for services
- **Accredited investor** status (a legal designation meaning you meet income or wealth thresholds required to invest in certain high-risk products)

The Promise

- User privacy enhanced
- Compliance still achievable
- Reduced data breach risk
- Portable across services

Projects: Microsoft ION, Civic, Worldcoin (controversial—it collects iris scans, raising concerns about biometric data privacy and consent, especially in developing countries)

Day 5 Synthesis: The Risk Framework

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?"

Day 5 Arc: From Failures to Values

What We Covered:

1. **Failures (5.1):** Technical, economic, human failures in DeFi
2. **Regulation (5.2):** US fragmentation, EU MiCA, Asia divergence
3. **Governance (5.3):** DAO mechanisms and attack surfaces
4. **Privacy (5.4):** 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)

Additional Content: The Political Nature of Money

Money as Power:

- Control over money = political power
- Monetary policy shapes society
- Financial access determines opportunity
- Payment rails enable or restrict activity

Historical Examples:

- Bank derisking of legal industries
- **WikiLeaks** (2010): A website that published secret government documents; banks and payment processors (Visa, Mastercard, PayPal) cut off its funding under government pressure
- **Canadian trucker convoy** (2022): Protesters' bank accounts were frozen by government order under emergency powers
- **#EndSARS** (Nigeria, 2020): Protesters against police brutality used crypto to receive donations after banks froze activist accounts

Crypto as Political Statement:

- Bitcoin: separation of money and state
- Privacy coins: individual sovereignty
- DeFi: financial system without gatekeepers
- DAOs: new governance experiments

The Core Question

Who should control money?

- Governments (fiat, CBDCs)
- Corporations (stablecoins, big tech)
- Protocols (Bitcoin, Ethereum)
- No one (cash, privacy coins)

Additional Content: Global Privacy Perspectives

European Approach:

- GDPR: Strong data protection
- Digital Euro: Privacy by design (proposed)
- Right to be forgotten
- Data minimization principles

US Approach:

- Sectoral privacy laws
- Third-party doctrine: less protection
- Bank Secrecy Act: financial surveillance
- No comprehensive federal privacy law

China Approach:

- Digital Yuan: state visibility
- Social credit integration (see earlier definition)
- Tight capital controls
- Crypto banned domestically

India and Africa:

- **India**: 30% crypto tax imposed (2022); attempted outright ban failed; world's largest biometric ID system (Aadhaar) creates unique privacy tensions
- **Africa**: Mobile money revolution (M-Pesa); Nigeria and Kenya lead crypto adoption in Africa, driven by remittances and currency instability

The Divergence

Different societies, different conclusions:

- EU: Privacy as human right
- US: Security/AML as priority
- China: State control as goal

Discussion: Where Do You Stand?

Team Privacy Argues:

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

Team Transparency Argues:

- Privacy enables crime
- Society needs accountability
- Victims deserve recourse
- "Sunlight is the best disinfectant" (meaning: making information public is the best way to prevent corruption and wrongdoing)
- Democratic oversight requires visibility

Discussion Questions

- Should there be a right to financial privacy? How absolute?
- Who gets to decide the privacy-transparency tradeoff?
- Is financial inclusion marketing or genuine social benefit?
- Would you use a CBDC? Under what conditions?

Application: Your Personal Privacy Choices

Questions to Consider:

- What financial data do you generate daily?
- Who has access to your transaction history?
- What does your spending reveal about you?
- How would you feel if it was public?

Practical Steps:

- Review privacy policies of financial apps
- Consider data shared with third parties
- Evaluate trade-offs of convenience vs. privacy
- Understand your rights under local law

Framework for Evaluation:

1. What data is collected?
2. Who has access?
3. How long is it retained?
4. Can it be deleted?
5. Is it sold to third parties?
6. What's the worst-case misuse?

Action Item

Pick one financial service you use. Read its privacy policy. Understand what you're consenting to.

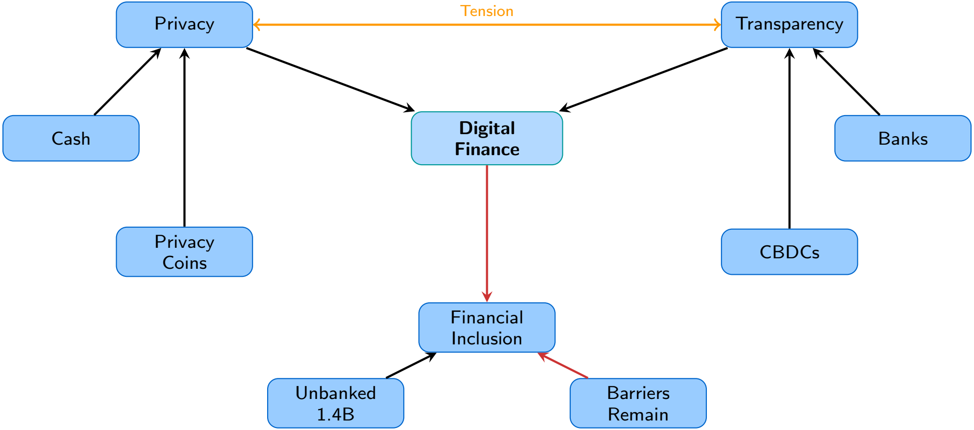
Executive Summary: Key Takeaways

The Five Things to Remember

1. **Privacy-transparency is a spectrum**: Cash to CBDCs, with different tradeoffs at each point. No position is neutral.
2. **Technology embeds values**: Every design choice (privacy coins, CBDCs, KYC) has distributional consequences. Technology is political.
3. **Financial inclusion is complex**: 1.4B unbanked, but crypto adoption correlates more with speculation than solving exclusion. M-Pesa succeeded; El Salvador is mixed.
4. **Surveillance is multi-directional**: Governments AND corporations monitor transactions. You are the product.
5. **Privacy-preserving compliance is possible**: Zero-knowledge proofs offer a path to both privacy and regulatory compliance, but adoption is nascent.

Bottom Line: The future of financial privacy is being decided now. Your values should inform your position.

Concept Map: Privacy, Surveillance, and Inclusion



Red: Challenges/gaps   Orange: Core tension

Key Terms & Definitions (1/3)

Financial Privacy Control over who can see your financial transactions and data.

Pseudonymity Using identifiers (like Bitcoin addresses) not directly linked to real identity, but potentially traceable. Weaker than anonymity because unmasking one link exposes all history.

Anonymity True unlinkability between transactions and identity; much stronger than pseudonymity.

Zero-Knowledge Proof Cryptographic method to prove a statement is true without revealing any additional information. Like proving you know a password without saying it.

CBDC Central Bank Digital Currency—digital money issued directly by a central bank, with various privacy models possible.

Key Terms & Definitions (2/3)

Privacy Coin Cryptocurrency designed to hide transaction details (sender, receiver, amount). Examples: Monero, Zcash.

Financial Inclusion Providing access to useful, affordable financial services to underserved populations.

KYC/AML Know Your Customer / Anti-Money Laundering—regulatory requirements for identity verification.

Self-Sovereign Identity (SSI) Identity model where individuals control their own data without centralized authority—like a digital wallet with verified credentials you choose to share.

Surveillance Capitalism Economic system where personal data is collected and monetized, often without meaningful consent.

Key Terms & Definitions (3/3)

Ring Signature A cryptographic signature that proves one member of a group signed, without revealing which member. Used by Monero to hide the sender.

Stealth Address A one-time address generated for each transaction, preventing observers from linking transactions to the same receiver.

FATF Travel Rule Requirement by the Financial Action Task Force that financial institutions share sender/receiver information for transfers above a threshold.

Demurrage Money that loses value over time if not spent—like a gift card with an expiration date. Encourages spending over hoarding.

Trusted Setup A one-time ceremony to generate cryptographic parameters. If compromised, fake proofs could be created. Required by zk-SNARKs but not zk-STARKs.

Social Credit System A system that assigns scores to citizens based on behavior, potentially restricting access to services for low scores.

OpSec Operational security—the practice of protecting sensitive information from being discovered or exploited.

Common Misconceptions: Myth vs. Reality

Myth 1

“Bitcoin is anonymous.”

Reality: Bitcoin is pseudonymous. All transactions are public. Chain analysis companies can often identify users.

Myth 2

“Crypto will bank the unbanked.”

Reality: Crypto adoption correlates more with speculation interest than financial exclusion. M-Pesa (not crypto) succeeded at inclusion.

Myth 3

“Privacy = criminal intent.”

Reality: Privacy is a human right. Dissidents, abuse survivors, businesses, and ordinary people have legitimate privacy needs.

Myth 4

“CBDCs are just digital cash.”

Reality: CBDCs can have surveillance capabilities far beyond physical cash—programmable, trackable, freezable.

Self-Assessment: Test Your Understanding (1/2)

Question 1: Financial Barriers (Quiz Q3)

What are common barriers to financial access for unbanked populations?

A) Lack of interest in financial services

B) Geographic distance to banks, high fees, documentation requirements, and lack of credit history

C) Government restrictions on all forms of money

D) Absence of currency in developing regions

Self-Assessment: Test Your Understanding (1/2)

Question 1: Financial Barriers (Quiz Q3)

What are common barriers to financial access for unbanked populations?

A) Lack of interest in financial services

B) Geographic distance to banks, high fees, documentation requirements, and lack of credit history

C) Government restrictions on all forms of money

D) Absence of currency in developing regions

Answer: B—Barriers include physical distance, fees, ID requirements, and no credit history. These factors disproportionately affect low-income, rural, and marginalized populations.

Question 2: Blockchain Surveillance (Quiz Q11)

What tools enable blockchain surveillance and transaction tracking?

A) Only government intelligence agencies

B) Blockchain analysis tools like Chainalysis, Elliptic, and TRM Labs

Self-Assessment: Test Your Understanding (1/2)

Question 1: Financial Barriers (Quiz Q3)

What are common barriers to financial access for unbanked populations?

A) Lack of interest in financial services

B) Geographic distance to banks, high fees, documentation requirements, and lack of credit history

C) Government restrictions on all forms of money

D) Absence of currency in developing regions

Answer: B—Barriers include physical distance, fees, ID requirements, and no credit history. These factors disproportionately affect low-income, rural, and marginalized populations.

Question 2: Blockchain Surveillance (Quiz Q11)

What tools enable blockchain surveillance and transaction tracking?

A) Only government intelligence agencies

B) Blockchain analysis tools like Chainalysis, Elliptic, and TRM Labs

Answer: B—Commercial firms provide blockchain analysis to governments, exchanges, and financial institutions.

Self-Assessment: Test Your Understanding (2/2)

Question 3: Cryptocurrency and Remittances (Quiz Q19)

How can cryptocurrency potentially reduce remittance costs?

A) By eliminating all fees completely

B) Through peer-to-peer transfers using stablecoins, avoiding traditional correspondent banking networks and their fees

C) By increasing fees to improve service quality

D) Cryptocurrency cannot be used for remittances

Self-Assessment: Test Your Understanding (2/2)

Question 3: Cryptocurrency and Remittances (Quiz Q19)

How can cryptocurrency potentially reduce remittance costs?

A) By eliminating all fees completely

B) Through peer-to-peer transfers using stablecoins, avoiding traditional correspondent banking networks and their fees

C) By increasing fees to improve service quality

D) Cryptocurrency cannot be used for remittances

Answer: B—Traditional remittances cost 5–10% through correspondent banking. Stablecoins enable direct P2P transfers with potentially lower fees, valuable for corridors where remittances are significant GDP share (e.g., 20% for El Salvador).

Reflection Questions:

- Where on the privacy-transparency spectrum do you think finance should be?
- What legitimate privacy needs exist beyond criminal use?
- How should we balance inclusion promises against inclusion reality?

What's Next: Day 6 – Convergence and the Future

Preview: Where Is Digital Finance Going?

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

Key Questions for Day 6:

- What will survive regulatory scrutiny?
- How will institutions and DeFi coexist?
- What does 2030 finance look like?

Connection to This Topic

- Privacy choices shape future adoption
- Inclusion claims will be tested
- CBDC designs will crystallize
- Regulatory frameworks will mature

Preparation:

- Reflect: What would YOU build?
- Think: What regulations would YOU write?
- Consider: Whose values should prevail?

Resources for Further Learning

Academic and Policy:

- Chainalysis Crypto Crime Report (annual)
- BIS papers on CBDCs and privacy
- EU Digital Euro documentation
- FATF Virtual Asset Guidance

Books:

- *The Age of Surveillance Capitalism* (Zuboff)
- *Digital Cash* (Brunton)
- *The Bitcoin Standard* (Ammous)
- *Attack of the 50 Foot Blockchain* (Gerard)

Technical Deep Dives:

- Monero whitepaper and documentation
- Zcash protocol specification
- Zero-knowledge proof tutorials (zkSNARKs)
- Tornado Cash code (educational)

News and Analysis:

- CoinDesk, The Block (industry)
- Molly White's Web3isgoinggreat.com (critical)
- EFF on financial privacy
- Privacy International

Case Studies:

- El Salvador Bitcoin adoption
- M-Pesa in Kenya
- China's Digital Yuan pilot

Questions?

Topic 5.4: Privacy, Surveillance, and Financial Inclusion
Who Benefits and Who Is Harmed?

Joerg Osterrieder
Digital Finance
joerg.osterrieder@ifi.uzh.ch

Next Up: Day 6 – Convergence and the Future