New Business Models Enabled by Trustless Systems

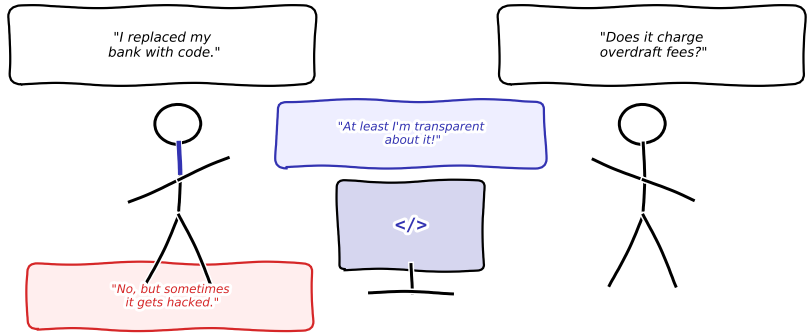
Module 3: The Trust Problem — Companion Lecture

Prof. Dr. Joerg Osterrieder

Digital Finance — BSc Course

Companion lecture — explores the business models that emerge when trust is replaced by verifiable code.

Business Models Without Trust



When "trust me" becomes "read the code" — a new era of business.

When “trust me” becomes “read the code” — an entirely new category of business emerges.

Learning Objectives

After completing this lecture, you will be able to:

1. **Explain** why removing trust intermediaries creates genuinely new business models, not just cheaper versions of old ones [Understand]
2. **Describe** six trustless business models (Decentralised Finance (DeFi) lending, tokenized assets, DAOs, supply-chain provenance, SSI, programmable money) and their mechanisms [Understand]
3. **Apply** platform economics and Coase's transaction-cost theory to explain why disintermediation works [Apply]
4. **Compare** traditional and trustless platforms on fees, access, composability, and risk [Analyze]
5. **Evaluate** the maturity, adoption trajectory, and limitations of each model [Evaluate]

Bloom's levels covered: Understand, Apply, Analyze, Evaluate

Objectives follow Bloom's taxonomy: Understand → Apply → Analyze → Evaluate.

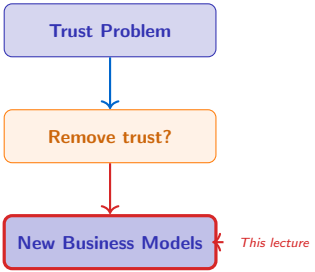
Bridge: From the Trust Problem to Business Models

The Trust Problem lecture showed us:

- Trust is invisible infrastructure — expensive and fragile
- Intermediaries extract 1–3% on every transaction
- Concentrated trust creates concentrated risk (Wirecard, FTX)

This lecture asks:

If we can remove the need for trust, what new businesses become possible?



The Trust Problem lecture identified the cost; this lecture explores the opportunity that emerges when that cost is removed.

Key Terms You Need for This Lecture

If any of these are unfamiliar, review Lesson 3.1 (Cryptographic Foundations) first.

Term	Plain-Language Definition
Blockchain	A shared digital ledger that records transactions across many computers so no single party controls the data.
Smart contract	A program stored on a blockchain that executes automatically when predefined conditions are met — like a vending machine for financial agreements.
Token	A digital unit on a blockchain that can represent ownership, voting power, currency, or access rights.
Stablecoin	A cryptocurrency designed to stay at $1 (or another fixed value), typically backed by dollar reserves or overcollateralised crypto. Examples: USDC, DAI.
Wallet	Software that stores your private keys and lets you send/receive tokens. Think of it as a digital keychain, not a money container.
ETH (Ether)	The native token of the Ethereum blockchain, used to pay transaction fees ("gas") and as collateral in DeFi.
Collateral	Assets you lock up as a guarantee when borrowing. If you cannot repay, the lender keeps the collateral.

These seven terms appear throughout this lecture and the six companion mini-lectures. Bookmark this slide for quick reference.

The Central Question

"What new business models become possible when you remove the need for trust?"

Three guiding sub-questions:

1. Which intermediaries can be **replaced by code** — and which cannot?
2. Are these models **genuinely new**, or just cheaper versions of existing services?
3. What new **risks** emerge when trust shifts from institutions to protocols?

These three questions structure the entire lecture — we return to each in the summary.

The Trust Tax

Buying a House

"How much goes to middlemen?"

Agent fees: 3–6%
Title insurance: 0.5–1%
Legal/escrow: 1–2%
Bank origination: 0.5–1%

Total: 5–10%

Source: NAR, Bankrate 2024

Sending €1,000 Abroad

"Why does it cost so much?"

Transfer fee: €5–25
FX spread: 1.5–4%
Correspondent bank: €15–30
Time: 2–5 days

Total: 3–7%

Source: World Bank Remittance Prices Q3 2024

Getting a $10K Loan

"Who takes what?"

Origination: 1–5%
Credit check: $25–50
Servicing: 0.25%/yr
Insurance: 0.5–1%

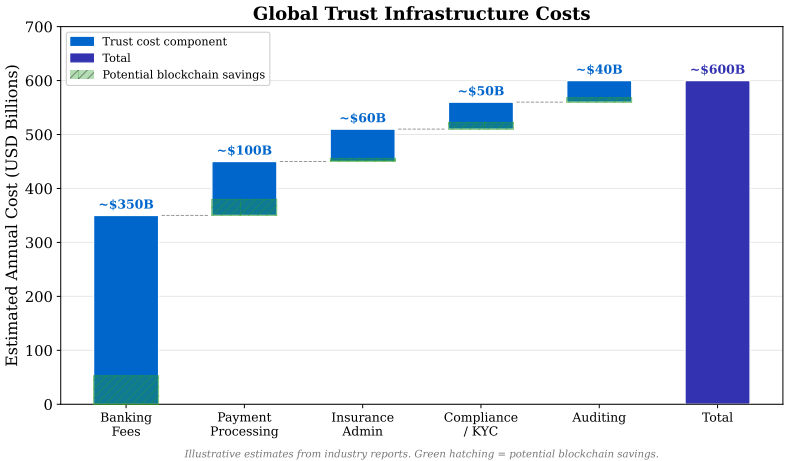
Total: 2–7%

Source: CFPB, LendingTree 2024

Pattern: Every transaction carries a hidden "trust tax" — fees paid to intermediaries who verify, enforce, and record.

Trust tax = the cumulative fees extracted by intermediaries whose primary function is establishing trust between strangers.

The Global Cost of Trust



Illustrative estimates from industry reports. Green hatching = potential blockchain savings.

What you see: The aggregate cost of trust infrastructure across sectors — banking compliance, payment processing, insurance administration, legal enforcement, and auditing. Total exceeds $2 trillion annually worldwide.

Global trust infrastructure costs exceed $2 trillion per year — Source: McKinsey Global Payments Report 2023, IIF Compliance Cost Survey 2022.

Who Cannot Afford Trust?

Each layer is a **trust gate**: you need the previous credential to get the next. No ID → no bank → no credit → no investment.

Trust infrastructure is a funnel that excludes billions — each layer requires documentation the previous layer provides.

Intermediaries as Gatekeepers

Three people, one pattern:

1. **Filipino nurse in Dubai** — sends 20% of salary home. Western Union takes 5–7% each time. Annual loss: $600–800 on a $12,000 remittance.
2. **Nigerian small-business owner** — profitable, but cannot get a loan. No credit bureau covers her region. Banks demand collateral she does not have.
3. **Syrian refugee in Germany** — has skills and savings, but no recognized ID. Cannot open a bank account for 6+ months.

The Common Pattern

In each case, a **trust intermediary** (bank, credit bureau, ID authority) is the bottleneck — not ability, not willingness, but **documentation the system demands**.

Question: What if the system verified *behavior* instead of *credentials*?

Intermediaries designed to create trust often become barriers — excluding the people who need financial services most.

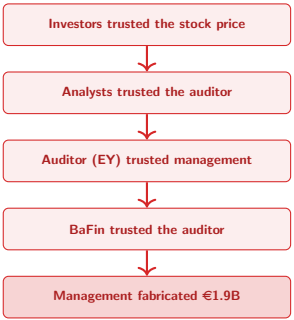
Wirecard: When Trust Fails

Timeline of a Trust Failure:

- **2002–2018:** Wirecard grows to DAX-30 member; market cap €24B at peak
- **2019 Jan:** FT publishes fraud allegations; BaFin investigates. . . the journalists
- **2019 Oct:** KPMG special audit commissioned
- **2020 Jun 18:** EY refuses to sign accounts — €1.9B "does not exist"
- **2020 Jun 25:** Wirecard files for insolvency; CEO arrested

Sources: Financial Times 2019–2020, BaFin press releases, EY audit letter June 2020

The Trust Chain That Failed:



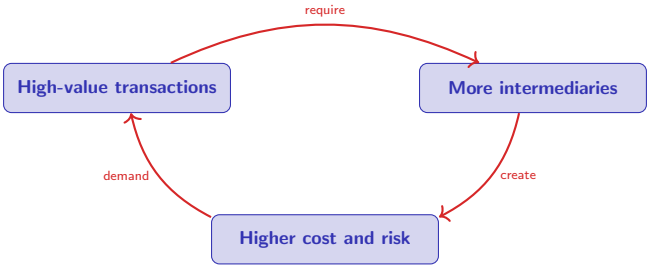
Lesson: Every link in the chain trusted the one below it. None verified independently.

Wirecard exposed the fragility of trust chains — each layer assumed the layer below had verified. On-chain records cannot be fabricated after the fact.

The Trust Paradox

"The more you concentrate trust,

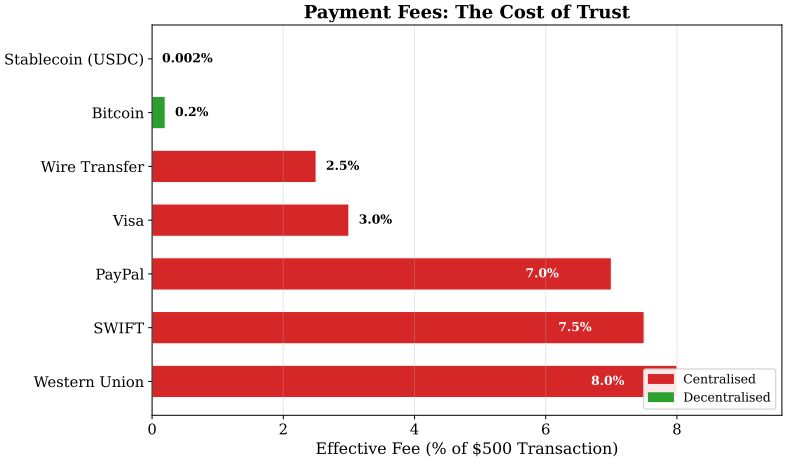
the bigger the damage when it breaks."



A **vicious cycle**: the transactions that need the most trust generate the highest fees and the greatest systemic fragility.

The trust paradox explains why the highest-value sectors (real estate, cross-border trade, capital markets) are the most ripe for trustless disruption.

The Cost of Intermediaries



What you see: Fee breakdown across payment types — card processing (1–3%), cross-border remittances (5–7%), trade finance (1.5–4%), and lending origination (1–5%). Each fee pays for a layer of trust.

Every percentage point is a trust tax — Source: World Bank Remittance Prices 2024, McKinsey Global Payments 2023.

Quick Poll: Where Do You Pay the Most Trust Tax?

Which of these costs you the most in "trust fees"?

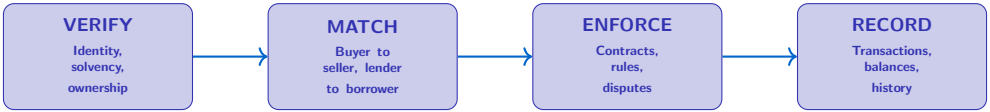
A. **Sending money internationally** (remittance fees, FX spreads)
B. **Paying with a card** (merchant processing fees passed to you)
C. **Getting a loan** (origination, insurance, credit check)
D. **Renting an apartment** (deposits, guarantees, agent fees)

30 seconds — raise your hand or use the poll tool.

Follow-up: How much would you estimate you pay per year in these hidden fees?

Most people dramatically underestimate how much they pay in trust-related fees — awareness is the first step.

What Intermediaries Actually Do



Each function adds cost, delay, and a point of failure.

Key question: Can code handle all four functions? Blockchains handle **RECORD** well. Smart contracts handle **ENFORCE**. **VERIFY** and **MATCH** are harder — they often need off-chain data.

Intermediaries perform four functions — trustless systems can automate some but not all of them.

Who Watches the Watcher?

The Socratic chain:

- Every trust mechanism requires a **higher-level** trust mechanism
- The chain must end somewhere — either in **authority** or in **mathematics**
- Centralized systems end in authority (regulators, courts)
- Decentralized systems end in cryptographic proof and economic incentives

Trust chains must terminate somewhere — the choice is between human authority and mathematical proof.

The Evolution of Trust in Commerce

- **Barter:** Trust the person in front of you (personal, limited)
- **Bookkeeping (Pacioli, 1494):** Trust the ledger — first scalable trust mechanism
- **Central banking (Bank of England, 1694):** Trust the institution
- **Digital payments (1960s):** Trust the network (Visa, SWIFT)
- **Smart contracts (Ethereum, 2015):** Trust the code — verifiable by anyone

Each era solved a trust problem — and created new ones. Smart contracts are the latest step, not the last.

Why Banks Cannot Offer 24/7 Services at 2% Fees

Bank cost structure — where does the money go?

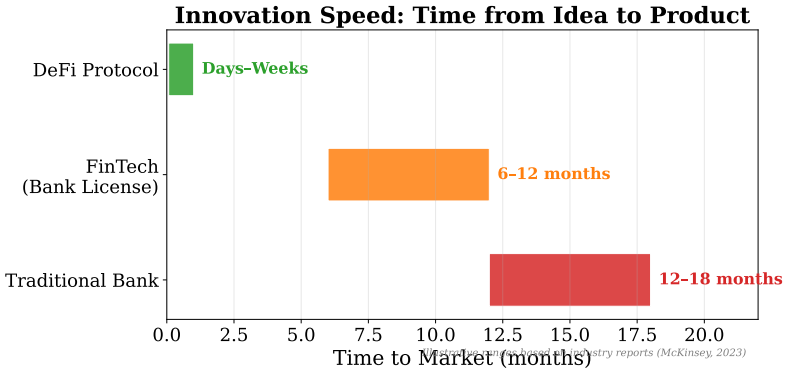
Cost Component	Source	Share of Revenue
Staff and branches	McKinsey Banking 2023	40–55%
Compliance and Know Your Customer (KYC)/AML	IIF Compliance Survey 2022	5–10%
Capital reserves (Basel III)	Basel Committee 2023	8–12%
IT legacy systems	Celent Banking IT 2023	10–15%
Settlement and clearing	EBA Clearing Report 2023	3–5%
Deposit insurance and taxes	FDIC, national schemes	2–4%
Total structural cost		**68–101%**

Result: Banks *cannot* offer low-margin, 24/7, borderless services profitably. Their cost floor is structurally above what DeFi protocols charge.

Key insight: This is not inefficiency — it is the **cost of being trusted**. Compliance, reserves, and oversight are features, not bugs.

Banks' cost floor is structural, not a sign of inefficiency — these costs are the price of institutional trust. Sources in table.

The Innovation Ceiling



What you see: How regulatory compliance, legacy infrastructure, and trust requirements create an "innovation ceiling" — a cap on how fast, cheap, or accessible traditional financial services can become.

The innovation ceiling is not a failure of banks — it is a structural consequence of centralized trust architecture.

Locked-In vs. Composable

Traditional Finance: Locked-In

- Proprietary APIs, closed protocols
- Switching costs: weeks to months
- Data siloed per institution
- Innovation requires permission
- Products bundled (account + card + loan)

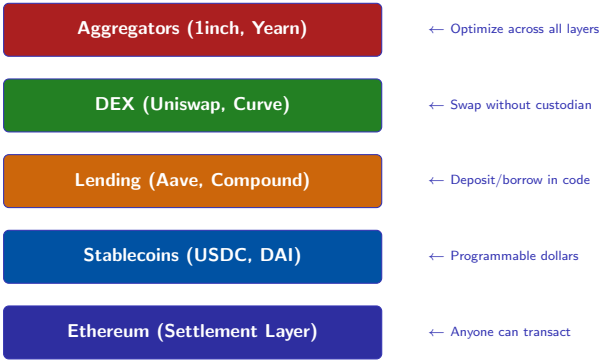
Trustless Finance: Composable

- Open-source, permissionless protocols
- Switching costs: one transaction
- Data on public ledger
- Anyone can build on top
- Products are modular "money legos"

Why composability matters: In DeFi, a lending protocol, a Decentralised Exchange (DEX), and a stablecoin can be combined in a single transaction. In traditional finance, this requires three institutions, three contracts, and three compliance checks.

Composability is the structural advantage of trustless systems — protocols can be combined like building blocks without permission.

Composability: The Money Legos



Each layer is **permissionless**: anyone can build on top without asking permission. A new protocol launched today can interact with \$100B+ of existing liquidity immediately.

"Money legos" = permissionless composability. Each protocol is a building block that others can combine without coordination.

Money Legos: Key Terms — Infrastructure

Term	Definition	Example
Ethereum (Settlement Layer)	The base blockchain that processes and finalises all transactions. Provides the security guarantee that transactions cannot be reversed.	Every Uniswap swap, Aave loan, and DAI mint settles as an Ethereum transaction.
Stablecoins (USDC, DAI)	Cryptocurrencies pegged to $1. USDC is fiat-backed (Circle holds dollars). DAI (now USDS) is crypto-backed (overcollateralised). They provide the unit of account DeFi needs.	DeFi loans are denominated in USDC because ETH is too volatile to use as a pricing unit.
Lending (Aave, Compound)	Smart contracts creating two-sided markets: depositors earn interest, borrowers post collateral. No credit check — the code enforces the rules.	Deposit 10,000 USDC into Aave at 3% APY. Borrow 5,000 USDC against ETH collateral at 5% APY.
DEX (Uniswap, Curve)	Decentralised exchanges enabling token swaps via automated market makers (AMMs). No order book, no intermediary. Liquidity providers earn trading fees.	Swap 1,000 USDC for ETH on Uniswap — no account, no KYC, settles in 12 seconds.
Aggregators (1inch, Yearn)	Protocols on TOP of the stack that optimise across all lower layers. 1inch finds the best swap price across multiple DEXs. Yearn moves deposits to maximise yield.	1inch splits a 10,000 USDC swap across Uniswap (60%) and Curve (40%) to save 0.3%.

Each layer is permissionless: anyone can build on top. A new protocol can interact with $100B+ of existing liquidity from day one.

Money Legos: Key Terms — Concepts

Composability

The ability to combine multiple protocols in a single transaction without permission. Because all DeFi protocols share the same settlement layer (Ethereum) and token standards (ERC-20), they "stack" like building blocks.

Permissionless

Anyone can use, build on, or compose with a protocol without approval. No API keys, no partnership agreements. The protocol's smart contract is the only gatekeeper. A developer in Lagos can build on Aave today without contacting Aave.

Atomic Transaction

A transaction that either executes completely or not at all. A composable DeFi transaction involving 5 protocols either succeeds at every step or reverts entirely — no partial execution, no settlement risk.

Why this matters: In traditional finance, combining a loan + swap + investment requires 3 institutions, 3 contracts, and 3 settlement cycles. In DeFi, all three happen in one atomic transaction in $\approx$12 seconds.

Composability + permissionless + atomicity = the structural advantage that makes "money legos" possible.

New vs. Cheaper: A Critical Distinction

Category	"Cheaper Old" Same service, lower cost	"Genuinely New" Impossible before
Payments	Send €100 for 0.1% vs. 5%	Flash loans: borrow $100M for 13 seconds, no collateral
Lending	Earn 4% on savings vs. 0.5%	Permissionless lending: anyone, anywhere, 24/7, no credit check
Ownership	Trade shares with lower fees	Fractional ownership: buy $50 of a $500K property

Why this matters:

- "Cheaper old" competes on price — incumbents can match it by cutting margins
- "Genuinely new" creates markets that **did not exist before** — incumbents cannot replicate them within their trust architecture

The strongest trustless models are not cheaper banks — they are things banks cannot build.

The most disruptive trustless models create new categories, not just lower prices — flash loans and fractional tokenization have no traditional equivalent.

Platform Economics 101

Definition: Platform

A **platform** is a business model that creates value by facilitating exchanges between two or more interdependent groups (e.g., buyers and sellers, lenders and borrowers).

Traditional platforms (Visa, Airbnb, NYSE):

- Owned by a company that sets rules, prices, and access
- Extract 1–30% of transaction value as platform fee
- Can de-platform users, change terms unilaterally

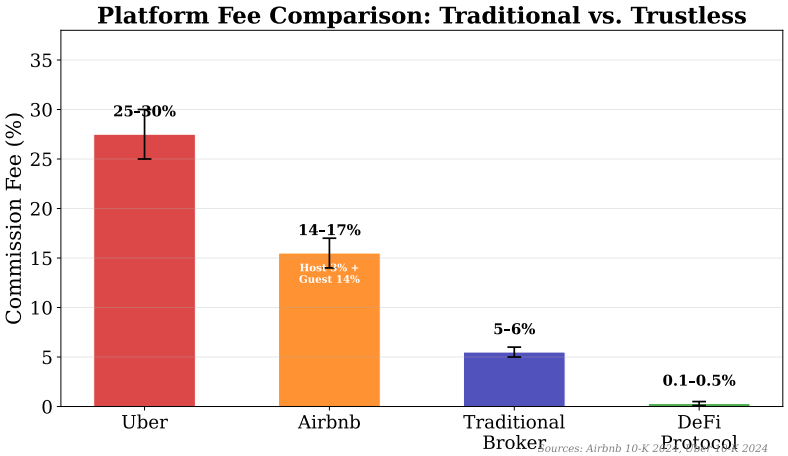
Trustless platforms (Uniswap, Aave, MakerDAO):

- Owned by token holders or nobody; rules enforced by code
- Fees set by protocol (typically 0.01–0.3%), go to liquidity providers
- Cannot de-platform users — anyone with a wallet can participate

Key difference: Traditional platforms *own* the trust layer. Trustless platforms *replace* it with cryptographic verification.

Platform economics explains why "winner takes all" in TradFi — but trustless platforms break this dynamic by eliminating the trust moat.

Two-Sided Markets: Who Pays What?

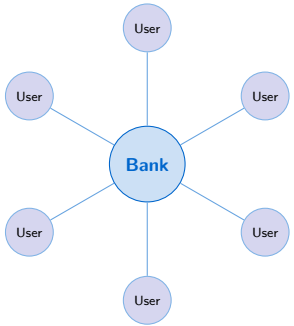


What you see: Fee comparison across traditional and trustless platforms — Visa (1.5–3%), Airbnb (14–17%), NYSE (varies), vs. Uniswap (0.3%), Aave (0.09% flash loan fee), MakerDAO (stability fee varies).

Trustless platforms charge 5–100x less than traditional ones — the difference is the cost of trust. Sources: Visa Annual Report 2023, Uniswap docs, Aave docs.

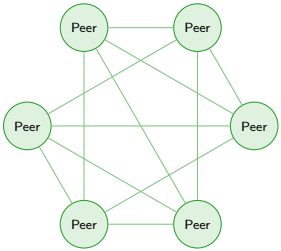
Network Effects: Two Models

Traditional: Hub-and-Spoke



Hub controls access, data, and fees. Users cannot interact directly.

Trustless: Mesh Network

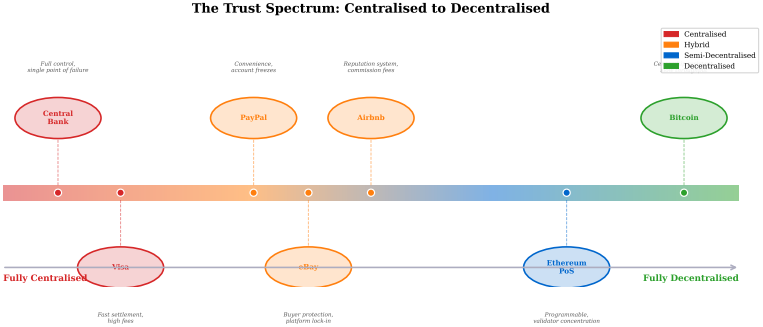


No central controller. Every peer can interact with every other peer. Protocol enforces rules.

Implication: Hub-and-spoke networks create **lock-in** (switching is costly). Mesh networks create **composability** (switching is free — just call a different smart contract).

Network topology determines power distribution — hub-and-spoke concentrates control; mesh distributes it.

Trust Spectrum: Where Do the Six Models Sit?



What you see: A spectrum from fully centralized trust (banks, courts) to fully decentralized trust (Bitcoin, pure smart contracts). The six business models from this lecture sit at different points: DeFi lending and DAOs are furthest right; supply-chain provenance and SSI are hybrid; programmable money spans the range.

No business model is purely trustless — each makes trade-offs between decentralization, usability, and regulatory compliance.

Why Do Intermediaries Exist? A Simple Analogy

Question: Why does your university have a cafeteria instead of letting students negotiate with individual food vendors every day?

Without a cafeteria (open market):

- **Search costs:** Find a vendor, check hygiene, compare prices — every single day
- **Bargaining costs:** Negotiate price and quality for each meal
- **Enforcement costs:** What if the food is bad? Who do you complain to?

With a cafeteria (intermediary):

- The university handles vendor selection, contracts, and quality control
- You just show up and eat
- **Cost:** The cafeteria takes a margin — but it is cheaper than doing everything yourself

This is Ronald Coase's insight (1937): Intermediaries exist because the cost of doing everything yourself (search + bargaining + enforcement) exceeds the intermediary's fee. The next slide formalises this.

Coase asked: why do firms exist at all? Answer: because market transaction costs are too high. Banks, exchanges, and insurers exist for the same reason.

Coase's Theorem (1937)

Firms exist because market **transaction costs** (search, bargaining, enforcement) are high. When transaction costs fall, firms shrink and markets expand.

Blockchain reduces all three Coase costs:

Cost Type	Traditional	Blockchain
Search	Brokers, agents, platforms	Permissionless global market
Bargaining	Lawyers, contracts, negotiation	Smart contracts with fixed terms
Enforcement	Courts, regulators, arbitration	Automatic on-chain execution

Prediction: As blockchain reduces transaction costs, large financial intermediaries (the "firms" in Coase's framework) should **shrink or disaggregate** into protocol-based services.

Coase's 1937 insight predicts that falling transaction costs lead to disintermediation — blockchain is a transaction-cost-reduction technology.

Worked Example: What Does a $10,000 Loan Actually Cost?

Traditional Bank Loan

Step 1: Credit check fee = **$**30
Step 2: Origination fee = 1–5% = **$**100–500
Step 3: Processing time = 3–14 days
Step 4: Legal/admin overhead = **$**50–100
Step 5: Insurance = 0.5% = **$**50
Step 6: Servicing = 0.25%/yr = **$**25/yr

Upfront cost: $230–680
Ongoing: $25+/year

Access: credit score $>$ 650

Sources: CFPB 2024, Bankrate, LendingTree

DeFi Protocol (e.g., Aave)

Step 1: Deposit **$**15,000 collateral (150% ratio)
Step 2: Gas fee = **$**2–10 (Ethereum L2)
Step 3: Processing time = 12 seconds
Step 4: No admin overhead
Step 5: No insurance (collateral covers risk)
Step 6: Variable interest only

Upfront cost: $2–10
Ongoing: interest only

Access: anyone with a wallet

Sources: Aave docs, Etherscan gas tracker 2024

Catch: DeFi requires $15,000 in collateral to borrow $10,000. The bank does not. **Both models have costs — they are just different.**

DeFi is 50–100x cheaper on fees but requires overcollateralization — each model optimizes for a different trust assumption.

Think-Pair-Share: Apply the Theory

Pick one of the six business models:

DeFi Lending — Tokenized Assets — DAOs — Supply Chain — SSI — Programmable Money

Apply Coase's transaction cost framework:

1. **Think (2 min):** What specific **search**, **bargaining**, and **enforcement** costs does this model reduce?
2. **Pair (3 min):** Compare with your neighbor — did you identify the same costs? What **new costs** does the trustless model introduce?
3. **Share (2 min):** One pair per model — present your cost analysis to the class.

Timer: 2 minutes thinking → 3 minutes pairing → 2 minutes sharing.

Applying Coase's framework to trustless models reveals that new costs (gas, collateral, smart contract risk) replace old costs (fees, delays, credit checks).

Theory-to-Practice: How Each Model Reduces Transaction Costs

Business Model	Search Cost Reduced	Bargaining Cost Reduced	Enforcement Cost Reduced
DeFi Lending	Global pool, no application	Fixed protocol rates	Auto-liquidation
Tokenized Assets	Permissionless listing	Atomic settlement	On-chain ownership proof
DAOs	Open governance forums	Token-weighted voting	Smart contract execution
Supply Chain	Shared immutable ledger	Standard data formats	Automated compliance checks
SSI	Self-serve verification	No repeated onboarding	Cryptographic credential proof
Programmable Money	Instant global transfer	Escrow in code	Conditional release logic

Pattern: Every trustless model attacks a different combination of Coase's three cost types. None eliminates all costs — they *restructure* them.

Coase's three cost categories map cleanly onto the six models — each model is a specialized transaction-cost-reduction machine.

Six Trustless Business Models at a Glance

#	Model	Replaces	How (Mechanism)
1	DeFi Lending	Banks, credit agencies	Overcollateralized smart contracts
2	Tokenized Assets	Brokers, transfer agents	Fractional on-chain ownership
3	DAOs	Boards, corporate governance	Token-weighted on-chain voting
4	Supply Chain Provenance	Auditors, certifiers	Immutable shared ledger
5	Self-Sovereign Identity	ID authorities, KYC desks	Cryptographic credentials
6	Programmable Money	Escrow, payment processors	Conditional smart contract logic

Note: Technical details (cryptography, consensus mechanisms, smart contract code) are covered in Lessons 3.1–3.4. This lecture focuses on the **business logic** and **economic impact** of each model.

Each model targets a different intermediary — together they cover lending, ownership, governance, verification, identity, and payments.

Deep dives available: Each model has a companion 10-slide mini-lecture (BM1–BM6) with worked examples, case studies, and discussion questions.

Six models, six intermediaries replaced — each leverages a different combination of blockchain, smart contracts, and cryptography.

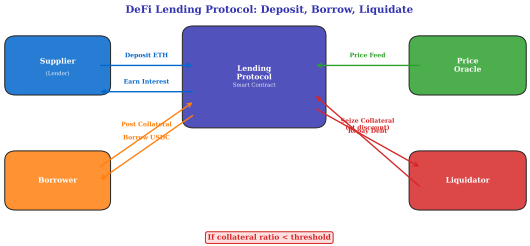
Model 1: DeFi Lending — Banking Without Banks

How It Works:

1. Depositors supply tokens to a **lending pool** (smart contract)
2. Borrowers deposit **collateral** (typically 150% of loan)
3. Interest rates adjust algorithmically based on pool utilization
4. If collateral drops below threshold → **automatic liquidation**

Key numbers:
Aave Total Value Locked (TVL): $12.5B (DeFiLlama, Dec 2024)
Compound TVL: $3.2B
Total DeFi lending: $35B+
Average collateralization: 180%

▷ Deep dive: see companion mini-lecture BM1



What you see: The flow from depositor through smart contract pool to borrower, with collateral and liquidation mechanisms.

DeFi lending replaces credit officers with collateral ratios and interest-rate algorithms — Sources: DeFiLlama Dec 2024, Aave docs.

Model 2: Tokenized Real Estate — Own $50 of a Building

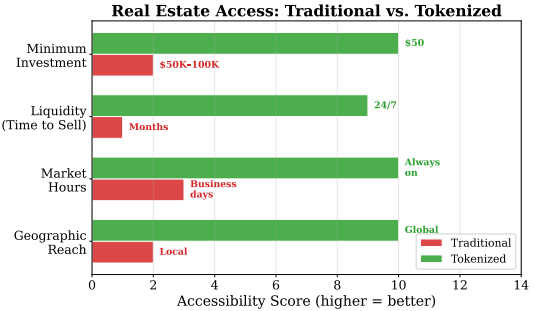
How It Works:

1. A property is placed in a legal entity (Special Purpose Vehicle (SPV))
2. Ownership is divided into **digital tokens** on a blockchain
3. Each token represents a proportional claim on rental income and sale proceeds
4. Tokens trade 24/7 on secondary markets

Key numbers:
RealT: min. investment $50 (vs. $50,000+ traditional)
Tokenized RWA market: $12B+ (RWA.xyz, 2024)
BCG projection: $16T by 2030

Settlement: minutes vs. 30–90 days

Sources: RealT platform, RWA.xyz, BCG 2022



What you see: The tokenization process — from physical property through legal wrapper to fractional digital tokens tradeable on secondary markets.

▷ Deep dive: see companion mini-lecture BM2

Tokenization lowers the minimum investment from $50K+ to $50 — opening real estate to billions of excluded investors. Sources in left column.

DeFi Lending and Tokenization: Pros and Cons

Advantages

1. **24/7 availability** — no banking hours, holidays, or cutoffs
2. **Permissionless access** — no credit score or KYC needed
3. **Transparency** — all transactions on public ledger
4. **Fractional ownership** — minimum investments drop 1000x
5. **Global liquidity** — anyone with internet can participate

Risks and Limitations

1. **Smart contract bugs** — $3.8B lost in DeFi exploits (Rekt, 2024)
2. **Overcollateralization** — locks up capital inefficiently
3. **Liquidation cascades** — price drops trigger mass selling
4. **Regulatory uncertainty** — securities law unclear for tokens
5. **Legal enforcement** — token $\neq$ legal ownership in most jurisdictions

Bottom line: DeFi and tokenization are live and growing, but smart contract risk and legal ambiguity remain significant barriers.

Every advantage creates a corresponding risk — permissionless access means no consumer protection; transparency means privacy challenges.

Model 3: DAOs — Organizations Without Managers

How It Works: A **Decentralized Autonomous Organization (DAO)** replaces corporate governance with on-chain voting.

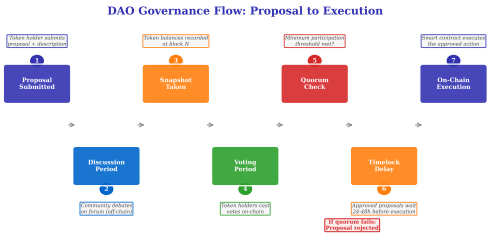
1. Members hold governance tokens
2. Proposals are submitted on-chain
3. Token holders vote (1 token = 1 vote)
4. Approved proposals execute automatically via smart contract

Key numbers:
MakerDAO: manages $8B+ in assets
Total DAO treasuries: $25B+ (DeepDAO, 2024)
Active DAOs: 13,000+ globally

Average voter participation: 3–5%

Sources: DeepDAO.io 2024, MakerDAO governance portal

▷ Deep dive: see companion mini-lecture BM3



What you see: The DAO governance cycle — from proposal submission through token-weighted voting to automatic smart contract execution.

DAOs replace boards of directors with transparent on-chain voting — but 3–5% voter turnout reveals a governance engagement problem.

Model 4: Supply Chain Provenance — Trust What You Buy

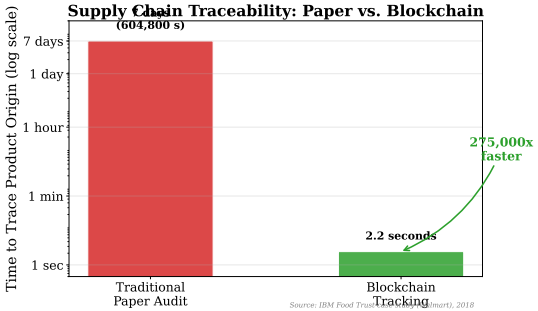
How It Works:

1. Each product gets a unique digital identity on a blockchain
2. Every handler (farm, factory, shipper, retailer) records a timestamped entry
3. The full chain of custody is immutable and publicly verifiable
4. Consumers scan a QR code to see the full history

Key numbers:
Walmart food tracing: 7 days → 2.2 seconds
Global food fraud: $40B/year (FDA est.)
Maersk TradeLens: 700+ participants (discontinued 2022)

De Beers Tracr: 200K+ diamonds tracked

Sources: Walmart/IBM press release 2019, FDA, Maersk, De Beers



What you see: A product's journey from origin through multiple handlers to consumer, with each step recorded on an immutable ledger.

▷ Deep dive: see companion mini-lecture BM4

Walmart cut food provenance tracking from 7 days to 2.2 seconds using blockchain — but TradeLens shutdown shows adoption challenges remain.

DAOs and Supply Chain: Pros and Cons

Advantages

1. **Transparent governance** — every vote and treasury move is public
2. **Global participation** — no geographic or credential barrier
3. **Immutable provenance** — records cannot be altered retroactively
4. **Reduced fraud** — fake products caught at the ledger level
5. **Speed** — verification in seconds, not days or weeks

Risks and Limitations

1. **Voter apathy** — 3–5% turnout makes DAOs oligarchies in practice
2. **Governance attacks** — hostile token accumulation for control
3. **Garbage in, garbage out** — blockchain verifies *records*, not physical reality
4. **Adoption costs** — retrofitting supply chains is expensive
5. **Consortium politics** — who controls the shared ledger?

Bottom line: Both models show real-world traction, but face human coordination problems that code alone cannot solve.

Technology solves the record-keeping problem — but governance engagement and physical-to-digital data integrity remain human challenges.

Model 5: Self-Sovereign Identity — You Own Your Data

How It Works: Self-Sovereign Identity (SSI) lets individuals control their own digital credentials without depending on a central authority.

1. Issuer (university, government) signs a **verifiable credential**
2. User stores credential in a **digital wallet**
3. Verifier checks the cryptographic proof — no need to contact the issuer
4. User decides *what* to share and with *whom*

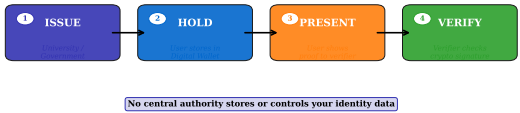
Key numbers:
850 million people lack legal ID (World Bank 2023)
EU eIDAS 2.0: digital wallet by 2026
W3C DID standard: published 2022

Repeat KYC cost: $60–500 per check

Sources: World Bank ID4D, European Commission eIDAS 2.0, W3C

▷ Deep dive: see companion mini-lecture BM5

Self-Sovereign Identity: Issue → Hold → Present → Verify



What you see: The SSI triangle — issuer, holder, and verifier. The holder controls which credentials to present, without the verifier needing to contact the issuer.

SSI flips the identity model: you carry your credentials instead of asking institutions to vouch for you each time. EU eIDAS 2.0 targets 2026 rollout.

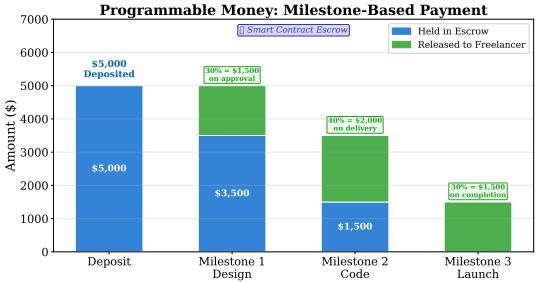
Model 6: Programmable Money — Money That Thinks

How It Works: **Programmable money** = digital currency with built-in rules that execute automatically (via smart contracts).

1. Payment conditions are coded: *"Release $5K when deliverable is approved"*
2. No escrow agent or payment processor needed
3. Conditions can include time locks, multi-signature approval, or oracle data
4. Funds move instantly when conditions are met

Example: Freelancer payment
Traditional: Invoice → 30-day wait → bank transfer
Programmable: Milestone approved → instant release
Savings: 30 days cash-flow + **$**15–50 wire fee

▷ Deep dive: see companion mini-lecture BM6



What you see: Programmable money flow — conditions are set in a smart contract, funds are locked, and release happens automatically when conditions are verified.

Programmable money replaces escrow agents and payment processors with self-executing code — the money itself enforces the contract.

Disruption Matrix: Comparing the Six Models

Model	Maturity	Disruption Level	Key Risk	Timeline
DeFi Lending	Live	High	Smart contract exploits	Now
Tokenized Assets	Growing	Very High	Legal recognition	2–5 years
DAOs	Growing	Medium	Voter apathy, attacks	3–7 years
Supply Chain	Pilots	Medium	Adoption, data quality	3–5 years
SSI	Early	Very High	Standards, regulation	5–10 years
Programmable Money	Growing	High	Regulatory clarity	2–5 years

Reading the matrix:

- **Live** = working at scale with real money today
- **Growing/Pilots** = functioning but not yet mainstream
- **Early** = technically possible but pre-adoption

DeFi lending is the most mature trustless model; SSI has the longest path to mainstream adoption but potentially the highest societal impact.

Winners and Losers in the Trustless Economy

Winners

1. **The unbanked** — 1.4B people gain access to lending, savings, and payments without needing a bank account
2. **Protocol developers** — builders of the new infrastructure earn fees and governance tokens
3. **Liquidity providers** — earn yield by supplying capital to DeFi pools (replacing bank interest)
4. **Small businesses in emerging markets** — access global capital without local banking infrastructure

Losers

1. **Payment processors** — Visa/Mastercard margins compressed by stablecoin rails
2. **Retail banks** — commodity services (payments, savings) face protocol competition
3. **Transfer agents and brokers** — tokenization eliminates their role in asset transfer
4. **KYC/AML service providers** — SSI could reduce repeat verification demand

Nuance: Winners and losers depend on **regulation and adoption speed**. If regulators ban DeFi, incumbents win. If they embrace it, disruption accelerates.

Disruption is not automatic — regulatory choices will determine which trustless models reach mainstream adoption and which remain niche.

Regulatory Response: Three Approaches

BAN

China (2021)

- All crypto transactions illegal
- Mining operations shut down
- State-controlled CBDC (e-CNY) promoted instead
- Result: activity moved offshore, not eliminated

Source: PBoC Notice 2021-237

WAIT AND SEE

USA (2020–2024)

- SEC enforcement-based approach
- No comprehensive framework
- "Regulation by enforcement"
- Result: uncertainty drove innovation abroad

Source: SEC enforcement actions 2023–2024

EMBRACE

EU (MiCA) / Singapore (MAS)

- MiCA: comprehensive crypto regulation (effective Jun 2024)
- Clear licensing for stablecoin issuers
- Singapore: sandbox for DeFi innovation
- Result: regulatory clarity attracts investment

Source: EU MiCA Regulation 2023/1114, MAS guidelines

Lesson: Banning pushes activity underground. Ignoring creates chaos. Clear frameworks channel innovation productively.

Regulatory approach determines adoption trajectory — the EU MiCA framework is becoming the global template for crypto regulation.

Case Study: Cross-Border Payments — SWIFT vs. Stablecoins

Feature	SWIFT Transfer	Stablecoin (USDC)
Speed	1–5 business days	1–60 seconds
Cost ($10,000 transfer)	$25–50 + FX spread (1–3%)	$0.01–2.00 (gas fee)
Intermediaries	2–5 correspondent banks	0 (peer-to-peer)
Availability	Business hours, Mon–Fri	24/7/365
Minimum amount	Often $50+ minimum	No minimum
KYC required	Both banks + sender/receiver	On-ramp only
Settlement finality	T+1 to T+5	12 seconds (Ethereum)
Transparency	Opaque (fees hidden)	Fully on-chain

Real-world impact: Average remittance cost worldwide is 6.2% (World Bank, Q3 2024). On $656B in global remittances (World Bank 2023), that is **$40B/year in fees** — overwhelmingly paid by migrant workers sending money to families in developing countries.

Stablecoins can reduce cross-border payment costs by 95%+ — Sources: World Bank Remittance Prices Q3 2024, SWIFT gpi data, Circle USDC docs.

Discussion: Rank the Six Models

Which model will reach mainstream adoption first?

Which will have the greatest societal impact?

Instructions:

1. **Form groups of 3–4** (5 minutes):
   - Rank the 6 models by **adoption likelihood** (most to least)
   - For your top pick: *What is the single biggest barrier to adoption?*
   - For your bottom pick: *Could anything change your ranking?*
2. **Share** (3 minutes): Each group presents their top and bottom picks with reasoning

Timer: 5 minutes discussion → 3 minutes sharing.

There is no single right ranking — the goal is to practice defending your analysis with evidence from the lecture.

What Trustless Systems Do **Not** Solve

Five honest limitations:

1. **The Oracle Problem** — Smart contracts cannot verify real-world data on their own. They need "oracles" (data feeds), which reintroduce trust.
2. **User Error** — Send tokens to the wrong address? There is no customer service, no chargebacks, no undo. Irreversibility is a feature *and* a risk.
3. **Smart Contract Bugs** — Code is law, but code can have bugs. $3.8B lost to DeFi exploits in 2020–2024 (Rekt leaderboard).
4. **Governance Capture** — DAOs with low voter turnout (3–5%) can be controlled by whales who accumulate governance tokens.
5. **Regulatory Uncertainty** — Most jurisdictions have not decided whether DeFi tokens are securities, commodities, or something new entirely.

Trustless $\neq$ riskless. The risks shift from institutional failure to code failure and user error.

Intellectual honesty requires acknowledging that trustless systems trade one set of risks for another — they do not eliminate risk.

The Oracle Problem: Achilles' Heel of Trustless Systems

What Is an Oracle?

An **oracle** is a service that feeds real-world data (prices, weather, delivery status) into a smart contract. Without oracles, contracts can only reason about on-chain data.

Why oracles matter:

- DeFi lending needs **price feeds** to trigger liquidations
- Insurance contracts need **event data** (flood, flight delay)
- Supply-chain contracts need **sensor readings**

The paradox: A "trustless" system that relies on a trusted oracle is only as trustless as the oracle itself.

Real-World Failures:

Chainlink: Largest oracle network. Secures $75B+ in DeFi value. Decentralized but not infallible.

Mango Markets exploit (Oct 2022):

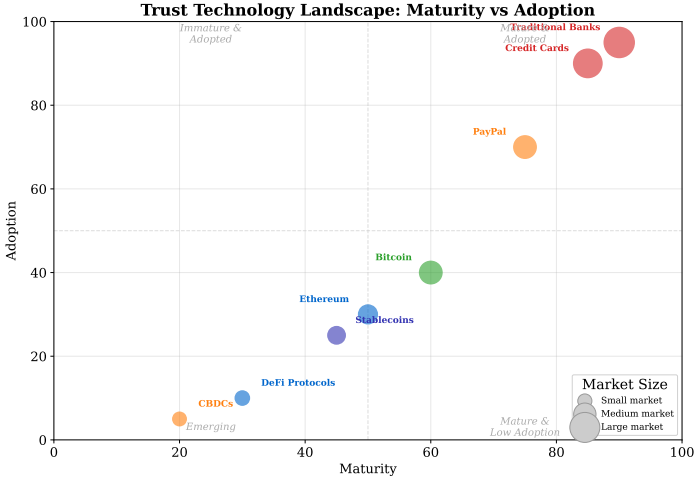
- Attacker manipulated oracle price of MNGO token
- Artificially inflated collateral value
- Borrowed $114M against fake collateral
- Protocol drained in minutes

Sources: Chainlink docs, Mango Markets post-mortem, CoinDesk Oct 2022

Lesson: Oracle attacks are the most common vector for DeFi exploits — the bridge between on-chain and off-chain is the weakest link.

The oracle problem is fundamental — trustless on-chain logic depends on trusted off-chain data. Chainlink mitigates but does not eliminate this.

Maturity Landscape: Where Are We Now?



What you see: Maturity map: DeFi and stablecoins (right, mature); SSI and CBDCs (left, early). DAOs and supply chain in between.

Maturity varies widely — DeFi is live with real money; SSI is mostly pilots and standards development. Investment timing depends on where each model sits.

Key Takeaways

1. **Trust is invisible infrastructure** — removing it creates new possibilities, not just cost savings. The trust tax exceeds $2 trillion/year globally.

2. **Six models replace intermediaries with protocols** — DeFi lending, tokenized assets, DAOs, supply-chain provenance, SSI, and programmable money. These are not just cheaper — they are genuinely new.

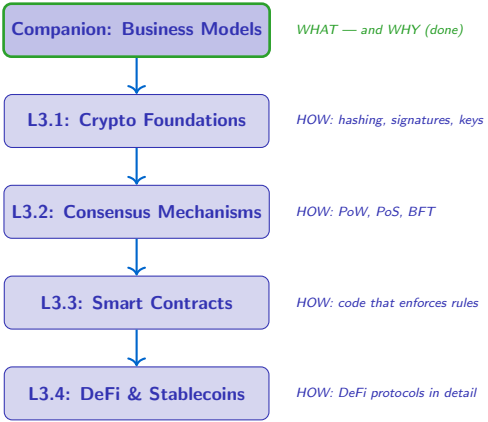
3. **Platform economics and Coase explain WHY disintermediation works** — blockchains reduce search, bargaining, and enforcement costs, shrinking the role of firms.

4. **Adoption varies widely** — DeFi lending is live with $35B+ TVL; SSI is 5–10 years from mainstream; regulation is the key variable.

5. **Trustless $\neq$ riskless** — the oracle problem, smart contract bugs, governance capture, and regulatory uncertainty are real and unsolved.

These five takeaways map directly to the five learning objectives on Slide 3 — revisit those objectives to check your understanding.

What Comes Next: The Module 3 Roadmap

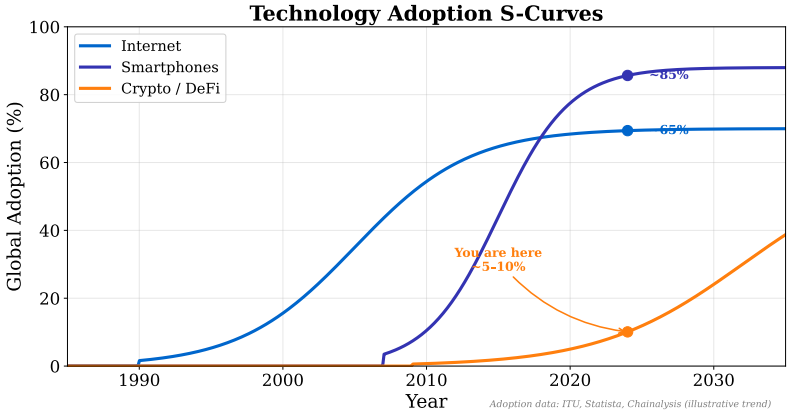


You now understand WHAT trustless business models are and WHY they work economically.

Next: Lessons 3.1–3.4 will teach you **HOW** — the cryptographic, consensus, and smart contract mechanisms that make them possible.

This companion lecture provides the business context; the four core lessons provide the technical depth. Together they cover the full trust story.

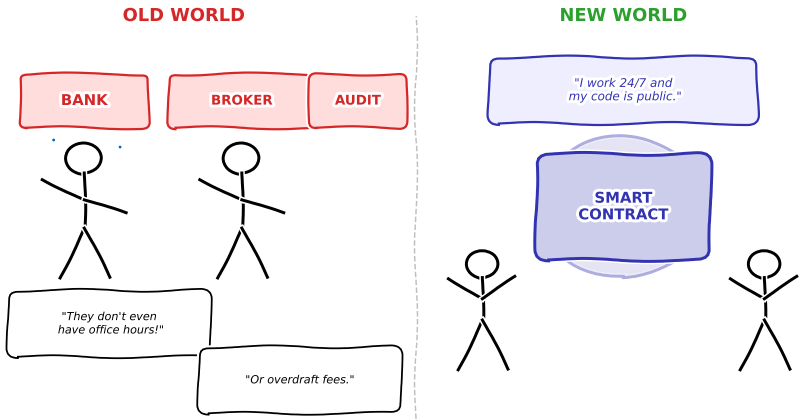
Adoption S-Curve: Where Is Crypto?



What you see: Technology adoption S-curves for the internet (1990s), smartphones (2007+), and crypto/blockchain (2009+). Crypto adoption in 2024 mirrors internet adoption circa 1997 — roughly 5–8% of the global population, before the steep acceleration phase.

If crypto follows the internet/smartphone adoption pattern, mainstream adoption (50%+) is approximately 8–12 years away. Source: Statista, a16z State of Crypto 2024.

The Future of Trust



The intermediaries are not disappearing — they are being replaced by math.

The intermediaries are not disappearing — they are being replaced by verifiable code.

Appendix A: "Trustless" in Name Only

Every slide in this lecture uses the word "trustless." A working professional must be able to enumerate exactly what remains trusted after the central intermediary is removed.

The 8 parties you still trust

1. **Protocol developers** — authorship of Solidity/Rust source
2. **Upgrade-key holders** — most "immutable" DeFi has 3-of-5 or 5-of-9 multisigs (*DeFiLlama governance dashboard 2024*, 2024)
3. **Stablecoin issuers** — Circle, Tether, Paxos reserve attestations
4. **Oracles** — Chainlink, Pyth, RedStone price feeds
5. **Audit firms** — OpenZeppelin, Trail of Bits, CertiK (and they miss things)
6. **Front-end hosts** — Vercel, IPFS pinning, ENS/DNS resolution
7. **Bridge operators** — validators on Wormhole, LayerZero, Axelar
8. **MEV / block builders** — Flashbots, Titan, Rsync extract value

What this actually means

- "Minimized-trust" is accurate
- "Permissionless" is accurate (anyone can interact)
- "Code-enforced subject to the 8 assumptions at left" is accurate
- **"Trustless" is marketing.**

Preferred language in this course:

- "minimized-trust"
- "permissionless"
- "code-enforced" (with the assumption stack specified)

When a slide or whitepaper says "trustless," ask: which of the 8 parties above is this actually removing? Often the answer is: only the bank-as-intermediary. The other 7 remain — and have failed in public.

Appendix B: Failed Trust Assumptions — Bridge Exploit Graveyard

Cross-chain bridges are the largest recorded failure of the "trustless" design claim. Every exploit below compromised an assumption explicitly listed on the prior slide.

Protocol	Date	Amount	Root cause	Assumption violated
Ronin Bridge	Mar 2022	$625M (*Chainalysis, Ronin post-mortem 2022*, 2022)	Validator keys (5 of 9)	Bridge validator honesty
Wormhole	Feb 2022	$325M (*Jump Crypto / Wormhole 2022*, 2022)	Signature-verif. bug	Protocol-code correctness
Nomad	Aug 2022	$190M (*Nomad Bridge incident report 2022*, 2022)	Replay / init bug	Upgrade-deploy auditing
Poly Network	Aug 2021	$610M (*Poly Network / SlowMist 2021*, 2021)	Cross-chain auth flaw	Code-auditor coverage
Harmony Horizon	Jun 2022	$100M (*Harmony / Elliptic 2022*, 2022)	Multisig keys (2 of 5)	Key-custody op. security

Aggregate: **$2.5B+ lost (Chainalysis Crypto Crime Report 2023, 2023)** to bridge exploits 2021–2023 — the single largest category of crypto theft over that window. Every case is a violation of an "8 parties" assumption, not a failure of the underlying chains themselves. **Pedagogical point:** The failures are not "the base-layer blockchain was hacked."

They are "the off-chain humans we trusted to guard the bridge failed." This is the normal mode of failure for minimized-trust systems — and it looks exactly like the normal mode of failure for banks (insider fraud, key compromise, software bugs, operational failures).

Every bridge-exploit announcement includes "the smart-contract code worked as designed." That is almost always true. The humans around the contract are what failed. See Chainalysis Crypto Crime Report 2023, Chapter 4.

Appendix C: Why Intermediaries Persist

Every "disintermediated" business model in this lecture competes with a service performed by a regulated intermediary. Here is why the intermediary often wins anyway.

Economic functions intermediaries provide

- **Maturity transformation** — deposits (short) funding loans (long), with liquidity support
- **Credit screening** — soft-information loan officers beat pure on-chain credit scores on SME lending
- **Loss absorption** — bank equity absorbs loss; DeFi sockets loss onto depositors
- **Dispute resolution** — chargebacks, fraud reversal, estate recovery
- **Regulatory compliance** — KYC, AML, sanctions, tax reporting outsourced to the bank

What "pure disintermediation" misses

- Users value **reversibility** — pure code-enforced settlement does not reverse
- Users value **someone to sue** — litigation is a feature, not a bug
- The unbanked often have **no smartphone, no ID, no capital** — DeFi does not solve any of these
- Regulatory moats mean intermediaries can serve $\sim$80% of EU/US retail flows (*BIS CPMI Red Book 2024*, 2024) at costs the regulated DeFi protocols cannot yet match

The honest reading: Decentralized finance wins in specific niches (cross-border transfers in hyperinflationary economies, programmable-collateral lending, global dollar access, censorship-resistant donations). It does not yet win as a general replacement for retail banking in functioning legal systems — and claiming otherwise is the 2017 pitch, not the 2026 reality.

For the steelman of this framing: Diamond & Dybvig (1983) on banks as liquidity insurers; Philippon (2015) on intermediation costs; DeFiLlama TVL vs. global bank-deposit scale. The gap is still $\sim$3 orders of magnitude.