Ethereum & Smart Contracts

Mini-Lecture: Programmable Money and Its Consequences

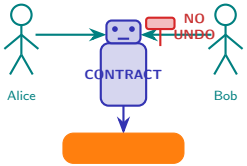
Prof. Dr. J. Osterrieder

Spring 2026

What If a Contract Could Enforce Itself — With No Lawyer, No Court, No Appeal?

Contracts depend on courts to enforce them. Courts take months. Lawyers cost thousands. And even then, the other party might not comply.

- What if the terms executed *automatically* the moment conditions were met?
- No human intermediary — just code running on thousands of computers simultaneously
- **Smart contract**: a program stored on a blockchain that executes its own terms
- Once deployed, **nobody** can stop it, modify it, or override it



The Promise — and the Danger

Code is the law. But code can have bugs. And code has no mercy.

This lecture explores what happens when code becomes law — and when the code has bugs.

Think About a Promise Someone Broke — What Would Change If a Machine Enforced It?

A Thought Experiment

Open your banking app. Count how many transactions happened automatically this month (subscriptions, standing orders, direct debits). Now imagine: what if those rules were written in code that **nobody could change** — not you, not the bank, not the government?

The subscription would run even if the company went bankrupt.
The mortgage payment would execute even if you disputed the amount.
The insurance payout would trigger the moment satellite data confirmed your crop failed.

You gain certainty. You lose flexibility. You gain speed. You lose recourse.

- **Smart contracts** are already running: Uniswap (decentralized exchange, DEX), Aave (lending), MakerDAO (stablecoin)
- Over $120 billion in assets operate under contract rules that no human can override
- The question is not whether this technology exists — it is whether its trade-offs suit your use case

Every automatic payment you have is a primitive smart contract — but one your bank can reverse.

What Makes a Smart Contract Different from a Regular One?

The difference is *enforcement*: who or what makes the other party comply?

- Traditional: you sign, they sign, a court enforces
- Smart: you deploy code, conditions trigger execution automatically
- **Key trade-off**: certainty vs. flexibility
- Once deployed, even the creator cannot change the rules

Property	Traditional	Smart
Enforcement	Court	Code
Speed	Days–weeks	Seconds
Cost	Lawyers + fees	Gas only
Flexibility	Negotiable	Rigid
Risk	Breach	Bugs

Pattern to Notice

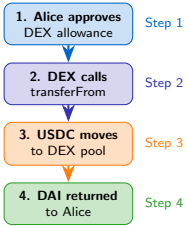
Smart contracts eliminate enforcement risk but introduce *code risk*: bugs execute automatically too.

Smart contracts trade flexibility for certainty — what you gain in speed, you lose in nuance.

Follow One Token Transfer from Approve to TransferFrom

Sending an ERC-20 token (like USDC) to a DEX (decentralized exchange) requires *two* transactions — by design.

1. **Approve**: Alice tells the USDC contract "the DEX is allowed to spend up to 100 of my tokens"
2. **Swap**: Alice calls the DEX, which calls `transferFrom` on USDC — pulling her tokens and sending DAI back



Why Two Steps?

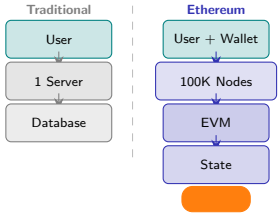
The approve-then-transfer pattern prevents contracts from draining your wallet without explicit per-contract permission.

The two-step approve-then-transfer pattern prevents contracts from spending your tokens without permission.

Where Does a Smart Contract Actually Run — And Who Pays for It?

A traditional app runs on *one* company's server. A smart contract runs on *every* Ethereum node simultaneously.

- **EVM** (Ethereum Virtual Machine): a sandboxed (isolated, self-contained) environment where contract code runs deterministically — same input, same output, on every node
- **Gas**: units measuring computational work; each operation costs gas; users pay in ETH
- **Gas limit**: prevents infinite loops — contract halts if it runs out of gas
- Trade-off: 100,000 copies of the same computation ensure trustlessness at the cost of speed and efficiency



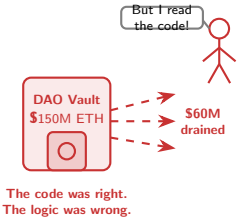
100,000 copies = no single point of failure

Redundancy is the price of trustlessness: 100,000 copies ensure no single point of failure.

The Code Worked Perfectly — So Why Did Everyone Lose Their Money?

The DAO (Decentralised Autonomous Organisation) hack, June 2016:

- $150 million raised in ETH via a governance contract (a program managing shared funds by member vote)
- Attacker found a **reentrancy bug** (a flaw where a function can be called again before the first call finishes): called the withdraw function recursively before the balance was updated
- Drained $60 million in ETH in one attack
- **The code executed exactly as written** — no hacker "broke" the rules; the logic was exploitable
- Ethereum community controversially hard-forked (rewrote history) to return funds



The Lesson

"Code is law" — until the code is wrong. Then the law is silent.

The DAO hack of 2016 drained $60M. The code executed exactly as written — the design was the flaw.

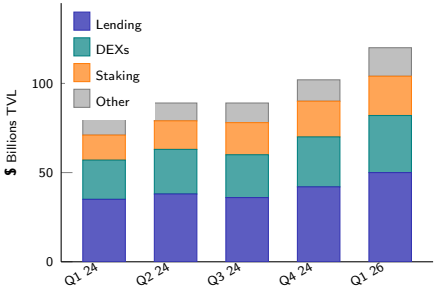
How Much Value Is Already Locked in Smart Contracts?

DeFi (Decentralised Finance): financial services — lending, trading, derivatives — running entirely via smart contracts with no company, no employees, no headquarters.

- **Total Value Locked (TVL)**: the sum of assets deposited in DeFi smart contracts
- TVL peaked at $>$ \$180 billion in 2021, stabilised around **\$**120 billion in early 2026
- Largest categories: lending (Aave, Compound), DEXs (Uniswap), liquid staking
- For context: **\$**120 billion exceeds the GDP of more than 100 countries

Key Takeaway

DeFi is not hypothetical — it processes billions in daily volume without a legal entity.



Data: DefiLlama (Jan 2026). These numbers change daily — check defillama.com for current values.

Who Benefits from Unstoppable Code — And Who Gets Hurt?

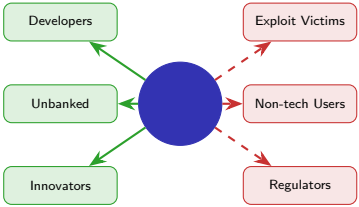
Smart contracts remove gatekeepers. That benefits those excluded by gatekeepers and harms those protected by them.

Who gains:

- **Developers**: deploy globally without a company or bank account
- **Unbanked users**: 1.4 billion adults with no bank account can access DeFi with a smartphone
- **Innovators**: permissionless (no approval needed) composability (Lego-brick combining of protocols)

Who faces higher risk:

- **Exploit victims**: $3.8 billion lost to hacks in 2022 alone (Chainalysis)
- **Non-technical users**: UI bugs, phishing, and wrong addresses are irreversible
- **Regulators**: no company to issue warnings to, no account to freeze

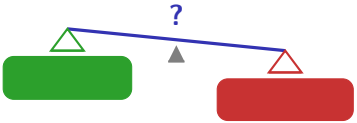


Programmable money democratizes finance AND democratizes financial risk.

Five Questions That Reveal Whether a Smart Contract Is Safe

Before interacting with any smart contract, ask these five questions:

1. **Audited?** Has an independent security firm reviewed the code? (Look for published audit reports.)
2. **Upgrade path?** Can the developers change the contract after deployment? (Upgradeable = centralized risk.)
3. **Admin keys?** Who holds the keys that can pause or drain the contract? (Multi-sig = safer.)
4. **Oracle dependencies?** Does the contract rely on external price feeds? (Oracle manipulation is a common attack vector.)
5. **Worst-case loss?** If the contract is exploited, what is the maximum you can lose?



Apply these five questions to the next DeFi protocol you encounter.

Your Challenge: Evaluate This Contract Design

Scenario

A startup wants to create a smart contract that locks ETH for one year and pays depositors 5% interest per year — funded entirely from new deposits.

Apply the **five questions from the previous slide**. Where does this design fail?

1. Audited?	Unknown — startup, no published audit.
2. Upgrade path?	Unknown — assume yes (risk).
3. Admin keys?	Unknown — who can drain the contract?
4. Oracle dependencies?	None apparent.
5. **Worst-case loss?**	**100% — if new deposits stop, existing depositors lose everything.**

Hint: Question 5 reveals this is a **Ponzi structure** (a scheme where returns to early investors are paid from new investors' funds, not from productive activity). Yield that comes from new deposits — not from productive economic activity — is mathematically unsustainable.

Real example: Anchor Protocol (Terra/Luna) offered 19.5% yield, funded from reserves. It collapsed in May 2022, destroying $40 billion in value in 72 hours.

If the yield comes from new deposits rather than productive activity, it is unsustainable by design.

Quiz — Questions 1–5

Q1. Which best describes a smart contract?
A) A PDF contract emailed between lawyers B) Code on a blockchain that executes its own terms C) A bank API D) A digital signature

Quiz — Questions 1–5

Q1. Which best describes a smart contract?
A) A PDF contract emailed between lawyers B) Code on a blockchain that executes its own terms C) A bank API D) A digital signature
Answer: B – Smart contracts are programs stored on a blockchain that execute automatically when conditions are met.

Q2. What is the difference between an EOA (Externally Owned Account) and a contract account?
A) EOAs hold more ETH B) Contract accounts are controlled by private keys C) EOAs are controlled by private keys; contract accounts by code D) No difference

Quiz — Questions 1–5

Q1. Which best describes a smart contract?
A) A PDF contract emailed between lawyers B) Code on a blockchain that executes its own terms C) A bank API D) A digital signature
Answer: B – Smart contracts are programs stored on a blockchain that execute automatically when conditions are met.

Q2. What is the difference between an EOA (Externally Owned Account) and a contract account?
A) EOAs hold more ETH B) Contract accounts are controlled by private keys C) EOAs are controlled by private keys; contract accounts by code D) No difference
Answer: C – EOAs (Externally Owned Accounts) are wallets you control with a key; contract accounts run code with no private key.

Q3. What is the purpose of gas in Ethereum?
A) To heat the network B) To measure and charge for computational work C) To pay validators' salaries D) To fund the Ethereum Foundation

Quiz — Questions 1–5

Q1. Which best describes a smart contract?
A) A PDF contract emailed between lawyers B) Code on a blockchain that executes its own terms C) A bank API D) A digital signature
Answer: B – Smart contracts are programs stored on a blockchain that execute automatically when conditions are met.

Q2. What is the difference between an EOA (Externally Owned Account) and a contract account?
A) EOAs hold more ETH B) Contract accounts are controlled by private keys C) EOAs are controlled by private keys; contract accounts by code D) No difference
Answer: C – EOAs (Externally Owned Accounts) are wallets you control with a key; contract accounts run code with no private key.

Q3. What is the purpose of gas in Ethereum?
A) To heat the network B) To measure and charge for computational work C) To pay validators' salaries D) To fund the Ethereum Foundation
Answer: B – Gas prevents infinite loops and aligns the cost of computation with network resources consumed.

Q4. How many functions are in the ERC-20 standard interface?
A) 3 B) 6 C) 9 D) 12

Quiz — Questions 1–5

Q1. Which best describes a smart contract?
A) A PDF contract emailed between lawyers B) Code on a blockchain that executes its own terms C) A bank API D) A digital signature
Answer: B – Smart contracts are programs stored on a blockchain that execute automatically when conditions are met.

Q2. What is the difference between an EOA (Externally Owned Account) and a contract account?
A) EOAs hold more ETH B) Contract accounts are controlled by private keys C) EOAs are controlled by private keys; contract accounts by code D) No difference
Answer: C – EOAs (Externally Owned Accounts) are wallets you control with a key; contract accounts run code with no private key.

Q3. What is the purpose of gas in Ethereum?
A) To heat the network B) To measure and charge for computational work C) To pay validators' salaries D) To fund the Ethereum Foundation
Answer: B – Gas prevents infinite loops and aligns the cost of computation with network resources consumed.

Q4. How many functions are in the ERC-20 standard interface?
A) 3 B) 6 C) 9 D) 12
Answer: B – ERC-20 defines 6 functions: totalSupply, balanceOf, transfer, transferFrom, approve, allowance.

Q5. In the approve-transferFrom pattern, which step comes first?
A) transferFrom, then approve B) approve, then transferFrom C) Both simultaneously D) Neither is required

Quiz — Questions 1–5

Q1. Which best describes a smart contract?
A) A PDF contract emailed between lawyers B) Code on a blockchain that executes its own terms C) A bank API D) A digital signature
Answer: B – Smart contracts are programs stored on a blockchain that execute automatically when conditions are met.

Q2. What is the difference between an EOA (Externally Owned Account) and a contract account?
A) EOAs hold more ETH B) Contract accounts are controlled by private keys C) EOAs are controlled by private keys; contract accounts by code D) No difference
Answer: C – EOAs (Externally Owned Accounts) are wallets you control with a key; contract accounts run code with no private key.

Q3. What is the purpose of gas in Ethereum?
A) To heat the network B) To measure and charge for computational work C) To pay validators' salaries D) To fund the Ethereum Foundation
Answer: B – Gas prevents infinite loops and aligns the cost of computation with network resources consumed.

Q4. How many functions are in the ERC-20 standard interface?
A) 3 B) 6 C) 9 D) 12
Answer: B – ERC-20 defines 6 functions: totalSupply, balanceOf, transfer, transferFrom, approve, allowance.

Q5. In the approve-transferFrom pattern, which step comes first?
A) transferFrom, then approve B) approve, then transferFrom C) Both simultaneously D) Neither is required
Answer: B – You must first approve the spender's allowance; then the spender calls transferFrom to pull the tokens.

Review: These questions test understanding and application of core concepts.

Quiz — Questions 6–10

Q6. What was the root cause of the DAO hack reentrancy bug?
A) A broken private key B) Withdraw was called recursively before the balance updated C) The EVM crashed D) Hash collision

Quiz — Questions 6–10

Q6. What was the root cause of the DAO hack reentrancy bug?
A) A broken private key B) Withdraw was called recursively before the balance updated C) The EVM crashed D) Hash collision
Answer: B – The contract sent ETH before updating its internal balance, allowing the attacker to re-enter the withdraw function repeatedly.

Q7. What is the main advantage of ERC-1155 over ERC-721?
A) More secure B) Cheaper to deploy C) Supports both fungible and non-fungible tokens, enabling batch transfers D) Higher royalties

Quiz — Questions 6–10

Q6. What was the root cause of the DAO hack reentrancy bug?
A) A broken private key B) Withdraw was called recursively before the balance updated C) The EVM crashed D) Hash collision
Answer: B – The contract sent ETH before updating its internal balance, allowing the attacker to re-enter the withdraw function repeatedly.

Q7. What is the main advantage of ERC-1155 over ERC-721?
A) More secure B) Cheaper to deploy C) Supports both fungible and non-fungible tokens, enabling batch transfers D) Higher royalties
Answer: C – ERC-1155 is a multi-token standard: one contract handles fungible items (gold coins) and non-fungible items (rare sword) with gas-efficient batch operations.

Q8. Composability (the "money Lego" property of DeFi) creates which systemic risk?
A) Higher gas fees B) A bug in one protocol can cascade through all dependent protocols C) Lower liquidity D) Slower block times

Quiz — Questions 6–10

Q6. What was the root cause of the DAO hack reentrancy bug?
A) A broken private key B) Withdraw was called recursively before the balance updated C) The EVM crashed D) Hash collision
Answer: B – The contract sent ETH before updating its internal balance, allowing the attacker to re-enter the withdraw function repeatedly.

Q7. What is the main advantage of ERC-1155 over ERC-721?
A) More secure B) Cheaper to deploy C) Supports both fungible and non-fungible tokens, enabling batch transfers D) Higher royalties
Answer: C – ERC-1155 is a multi-token standard: one contract handles fungible items (gold coins) and non-fungible items (rare sword) with gas-efficient batch operations.

Q8. Composability (the "money Lego" property of DeFi) creates which systemic risk?
A) Higher gas fees B) A bug in one protocol can cascade through all dependent protocols C) Lower liquidity D) Slower block times
Answer: B – When protocols are chained together, an exploit in any one layer can drain value from all dependent protocols simultaneously.

Q9. After the DAO hack, Ethereum hard-forked to return funds. What did this reveal?
A) Smart contracts are perfectly safe B) Immutability is absolute C) Even "code is law" communities can override the rules when stakes are high enough D) The EVM had a bug

Quiz — Questions 6–10

Q6. What was the root cause of the DAO hack reentrancy bug?
A) A broken private key B) Withdraw was called recursively before the balance updated C) The EVM crashed D) Hash collision
Answer: B – The contract sent ETH before updating its internal balance, allowing the attacker to re-enter the withdraw function repeatedly.

Q7. What is the main advantage of ERC-1155 over ERC-721?
A) More secure B) Cheaper to deploy C) Supports both fungible and non-fungible tokens, enabling batch transfers D) Higher royalties
Answer: C – ERC-1155 is a multi-token standard: one contract handles fungible items (gold coins) and non-fungible items (rare sword) with gas-efficient batch operations.

Q8. Composability (the "money Lego" property of DeFi) creates which systemic risk?
A) Higher gas fees B) A bug in one protocol can cascade through all dependent protocols C) Lower liquidity D) Slower block times
Answer: B – When protocols are chained together, an exploit in any one layer can drain value from all dependent protocols simultaneously.

Q9. After the DAO hack, Ethereum hard-forked to return funds. What did this reveal?
A) Smart contracts are perfectly safe B) Immutability is absolute C) Even "code is law" communities can override the rules when stakes are high enough D) The EVM had a bug
Answer: C – The hard fork showed that social consensus can override protocol rules — "code is law" is a norm, not an absolute guarantee.

Q10. A contract offers 20% annual yield funded by new deposits. Which of your 5 questions immediately identifies the fatal flaw?
A) Question 1 (audited?) B) Question 3 (admin keys?) C) Question 4 (oracle?) D) Question 5 (worst-case loss?)

Quiz — Questions 6–10

Q6. What was the root cause of the DAO hack reentrancy bug?
A) A broken private key B) Withdraw was called recursively before the balance updated C) The EVM crashed D) Hash collision
Answer: B – The contract sent ETH before updating its internal balance, allowing the attacker to re-enter the withdraw function repeatedly.

Q7. What is the main advantage of ERC-1155 over ERC-721?
A) More secure B) Cheaper to deploy C) Supports both fungible and non-fungible tokens, enabling batch transfers D) Higher royalties
Answer: C – ERC-1155 is a multi-token standard: one contract handles fungible items (gold coins) and non-fungible items (rare sword) with gas-efficient batch operations.

Q8. Composability (the "money Lego" property of DeFi) creates which systemic risk?
A) Higher gas fees B) A bug in one protocol can cascade through all dependent protocols C) Lower liquidity D) Slower block times
Answer: B – When protocols are chained together, an exploit in any one layer can drain value from all dependent protocols simultaneously.

Q9. After the DAO hack, Ethereum hard-forked to return funds. What did this reveal?
A) Smart contracts are perfectly safe B) Immutability is absolute C) Even "code is law" communities can override the rules when stakes are high enough D) The EVM had a bug
Answer: C – The hard fork showed that social consensus can override protocol rules — "code is law" is a norm, not an absolute guarantee.

Q10. A contract offers 20% annual yield funded by new deposits. Which of your 5 questions immediately identifies the fatal flaw?
A) Question 1 (audited?) B) Question 3 (admin keys?) C) Question 4 (oracle?) D) Question 5 (worst-case loss?)
Answer: D – Question 5 reveals a Ponzi: if new deposits stop, existing depositors lose 100%. There is no productive yield source.

Challenge: Questions 9–10 require you to synthesize multiple concepts into a judgment.