Seminar Preparation: Impact Considerations

Focus: Smart Contracts with Cryptographic Verification

Lorenzo Deflorian

February 3, 2026

1 Technology Selection

1.1 What it is

Smart contracts are programs stored on a blockchain—Ethereum being a common example—that execute automatically when certain conditions are met. Rather than relying on a central authority to enforce an agreement, the code itself becomes the enforcer through the network's consensus mechanism. Cryptographic signatures ensure only authorised parties can trigger the contract.

1.2 What it is used for

The range of applications is quite broad. In finance, they power decentralised lending platforms and peer-to-peer exchanges. Supply chains use them to track goods and trigger payments on delivery. Real estate deals can be settled by tokenising ownership and releasing funds when conditions are met. Voting systems benefit from the immutability and transparency they offer. Essentially, anywhere you need a contract enforced without trusting a middleman, smart contracts can reduce friction and costs.

1.3 How it works

When someone wants to execute a smart contract, they sign the transaction with their private key. Network participants verify this signature using the sender's public key, confirming that person actually authorised the transaction. If the signature is valid, the network runs the contract code. Once confirmed, the transaction becomes part of a block, which is hashed and cryptographically linked to the previous block. Tampering with any past transaction would break this chain and immediately reveal the fraud.

2 Notes

2.1 What it is

At a deeper level, a smart contract is not just code, but logic embedded into a distributed system. Its behaviour is deterministic and enforced collectively by the network rather than by any single authority.

- Code is deployed to the blockchain at a specific address. Once live, the logic remains fixed unless the original design explicitly allows upgrades under controlled conditions.

- Unlike traditional software, execution is automatic: when predefined conditions occur—such as time passing, data arriving from an oracle, or a call from another contract—the code runs without human intervention.
- Cryptography underpins trust. ECDSA signatures prove transaction authorisation, while cryptographic hashes link blocks together so any alteration to history is detectable.
- No single party controls execution or can unilaterally cancel the contract. Enforcement is distributed across thousands of nodes.

2.2 What it is used for

Because smart contracts remove the need for trusted intermediaries, they are particularly effective in environments where trust is expensive or difficult to establish.

- **Finance**: Platforms such as Aave and Compound enable decentralised lending and borrowing. Decentralised exchanges allow peer-to-peer trading, and stablecoins maintain value through algorithmic rules.
- **Supply chains**: Product histories can be recorded on-chain, with payments released automatically when delivery is confirmed via an external oracle.
- **Real estate**: Ownership is represented by digital tokens. When contractual conditions are met, ownership transfers automatically.
- **Voting**: Votes are recorded immutably on-chain. Cryptographic techniques can preserve voter privacy while allowing public verification of results.
- **Other uses**: Automated insurance claims, royalty payments on resale of digital assets, and verifiable professional credentials.

2.3 How it works

From a technical standpoint, smart contracts combine standard cryptographic primitives with a consensus mechanism that ensures all network participants agree on execution outcomes.

- **Signing the transaction**: A user constructs a transaction request and signs it using their private key, typically via ECDSA.
- **Verification by the network**: Nodes verify the signature and confirm message integrity using the sender's public key.
- **Running the code**: Validators execute the contract in a virtual machine and reach consensus on the resulting state.
- **Recording in the blockchain**: The transaction is included in a block that is cryptographically linked to previous blocks.
- **Cost and incentives**: Users pay gas fees to compensate validators and prevent spam or abuse of the network.