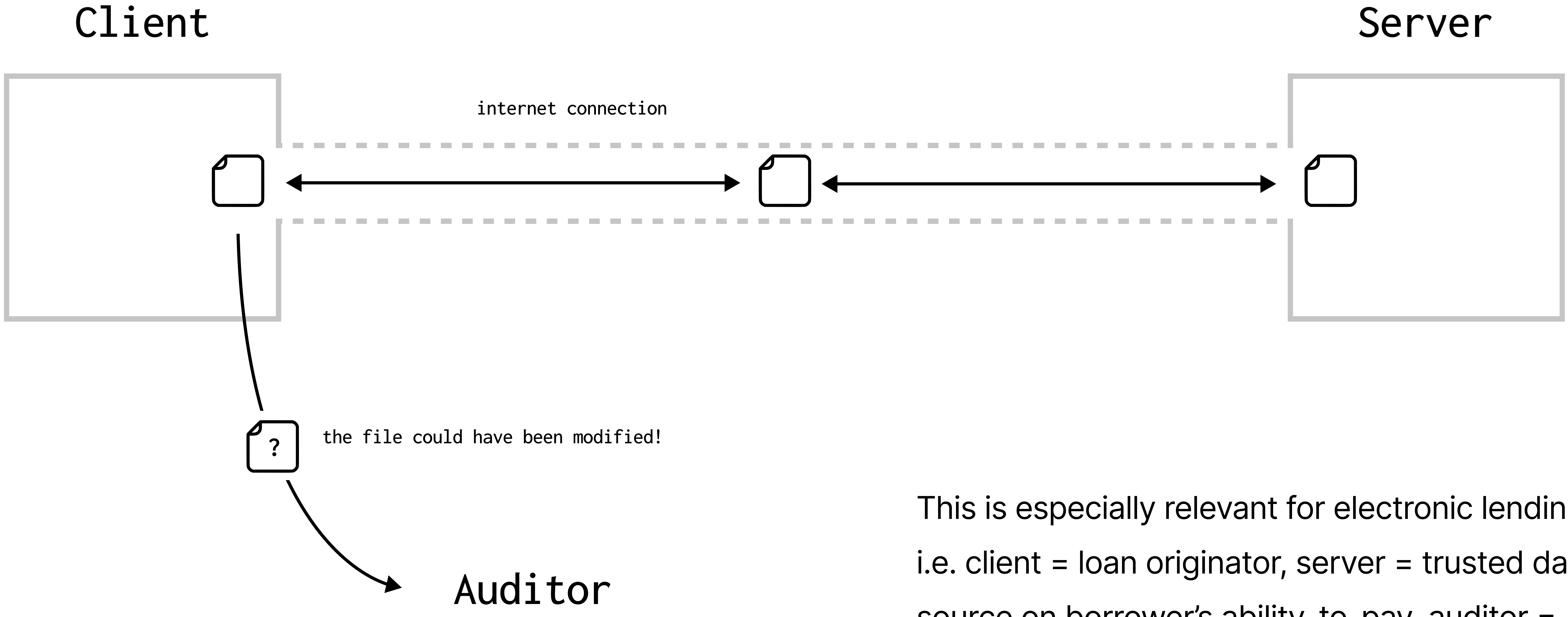
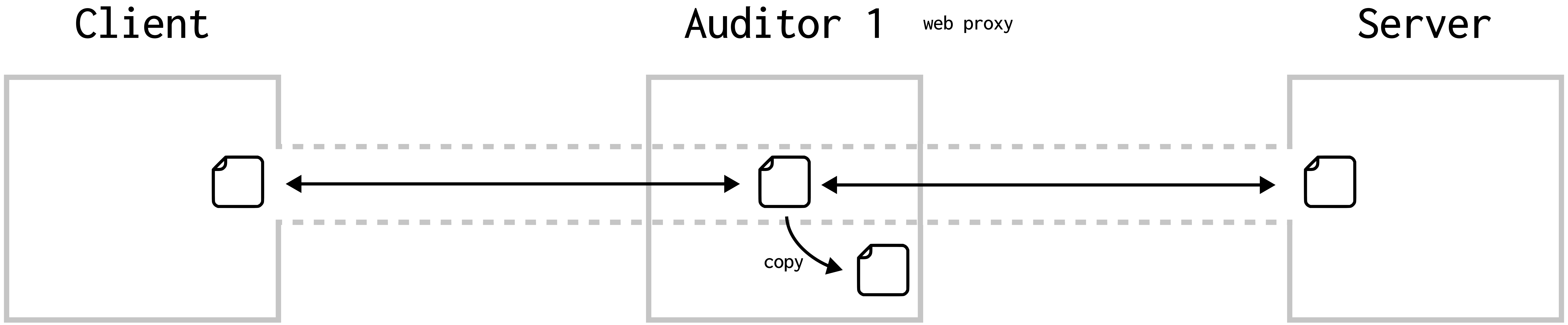
Problem: A web client cannot prove to a third-party auditor that specific data was transferred to/from a web server.

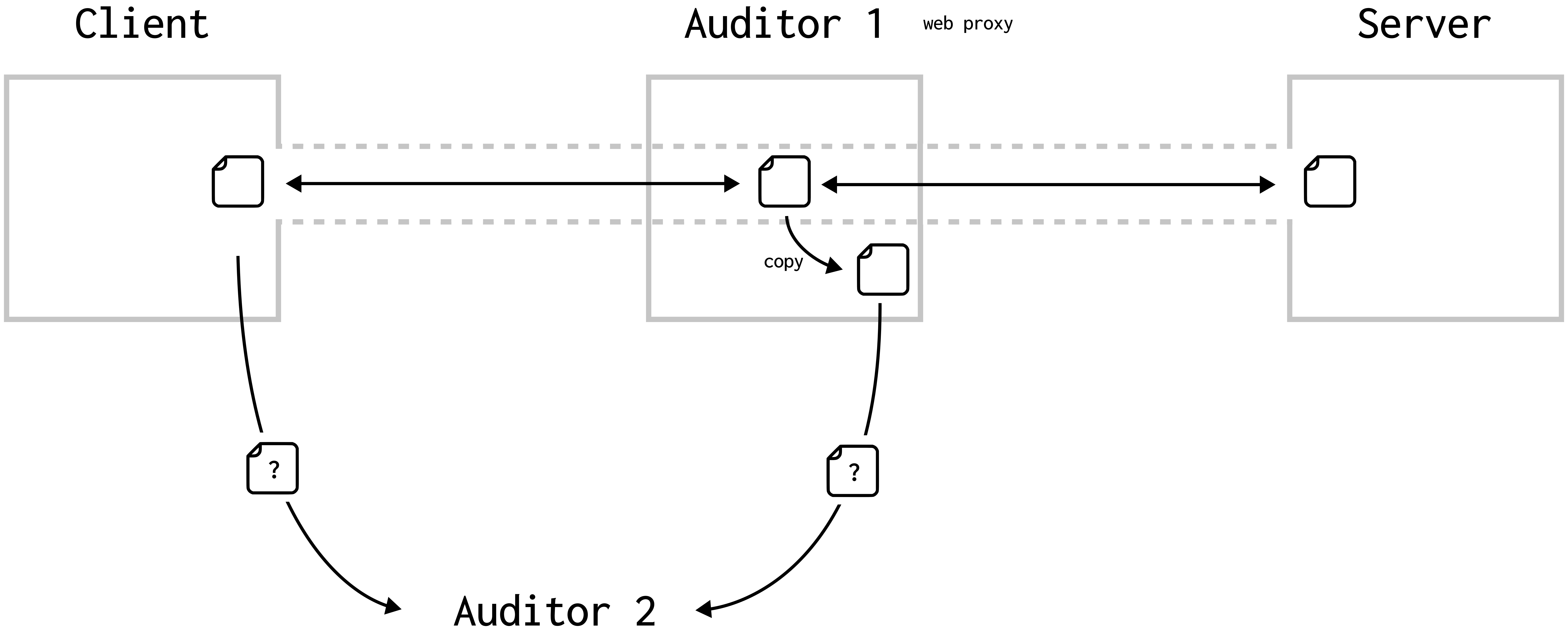


This is especially relevant for electronic lending, i.e. client = loan originator, server = trusted data source on borrower’s ability-to-pay, auditor = regulator or loan purchaser

The auditor can act as a web proxy between client and server, allowing them to monitor the traffic.

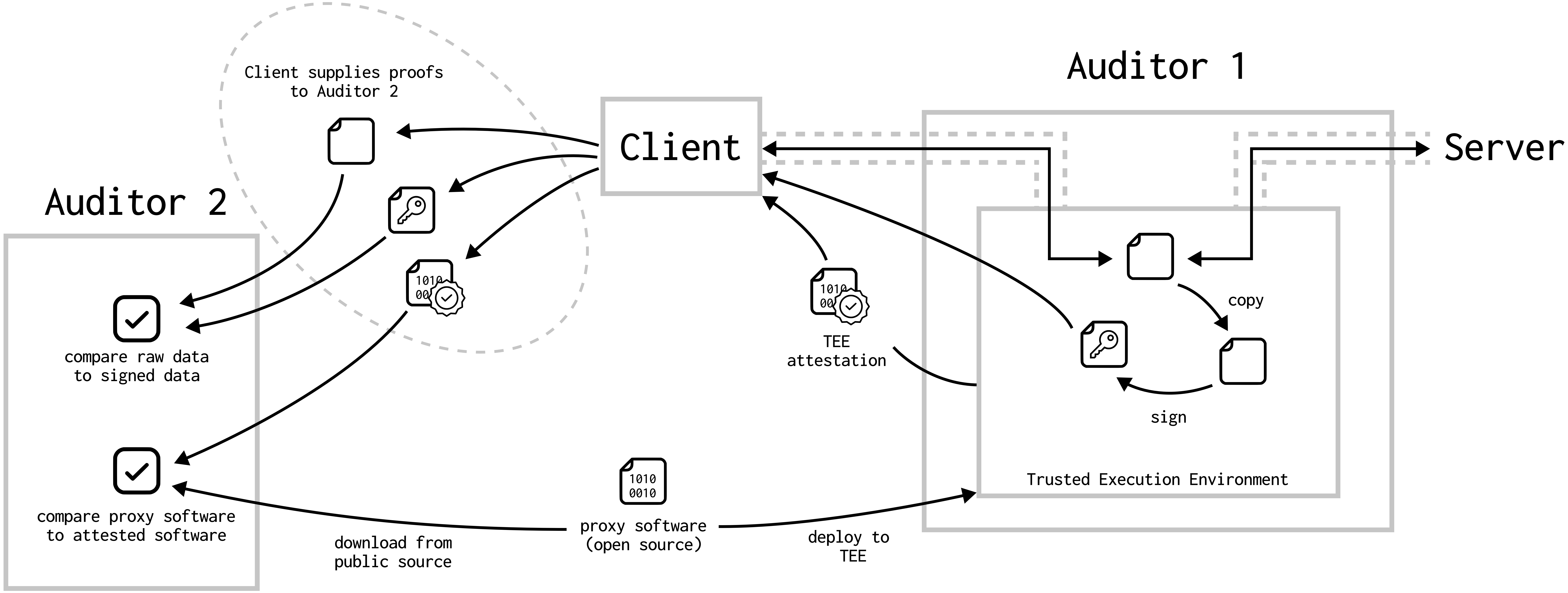


However, other auditors face the original dilemma -- they can't know for sure what data was transferred unless they also participate as a proxy (impractical).



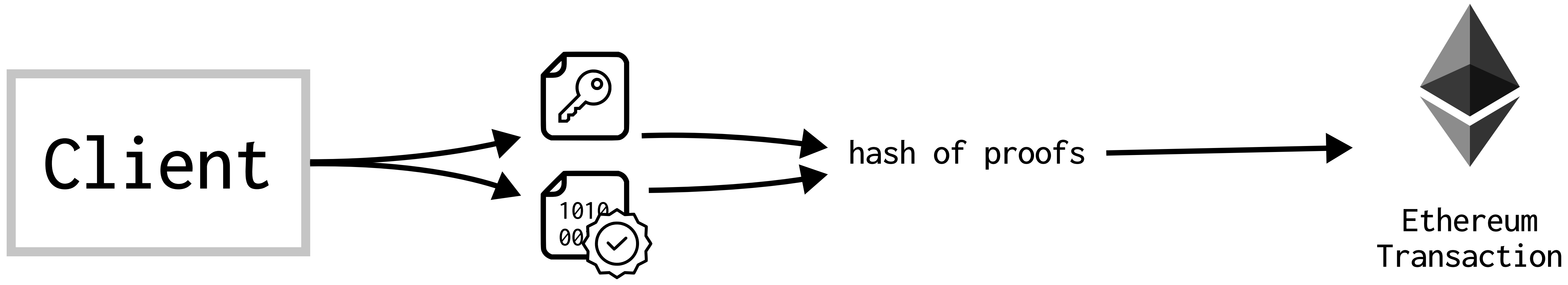
Auditors can deploy proxy software into a “Trusted Execution Environment” (TEE), allowing other auditors to verify its software and authenticate data copies signed by it.

TEEs can provide a cryptographic “attestation” that proves which software they are running. This can be used to mathematically prove the data it outputs by cryptographically signing it (using a cryptographic key within by the TEE).


Client supplies proofs to Auditor 2
Auditor 1
Client
Server
Auditor 2
1010 00
1010 00
compare raw data to signed data
TEE attestation
copy
sign
Trusted Execution Environment
compare proxy software to attested software
1010 0010
proxy software (open source)
download from public source
deploy to TEE

The only remaining issue is that TEEs cannot reliably report clock time. This is an issue because it may allow Clients to cheat by backdating data prior to when it was received.

This can be solved with Clients publishing the proofs to a public blockchain (e.g. Ethereum), allowing it to serve as a global tamper-proof ledger proving when specific data was obtained.



Alternatively: if desiring independence from existing public blockchains, a new blockchain can be created to store these data verification proofs and incentivize a **public decentralized permissionless network of "auditing web proxies"**. Auditors can join into a network, be paid by Clients to perform audits, and create a single shared ledger of proofs.