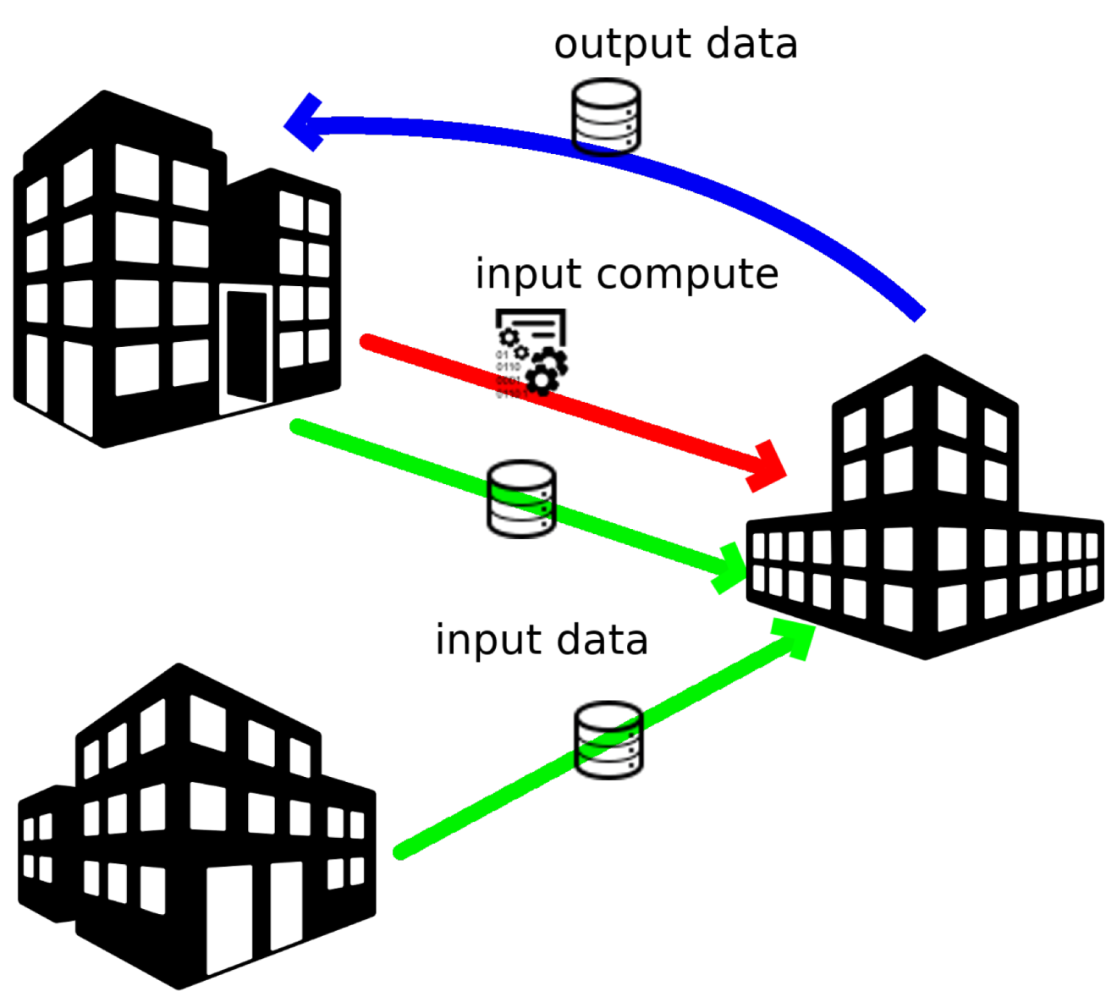
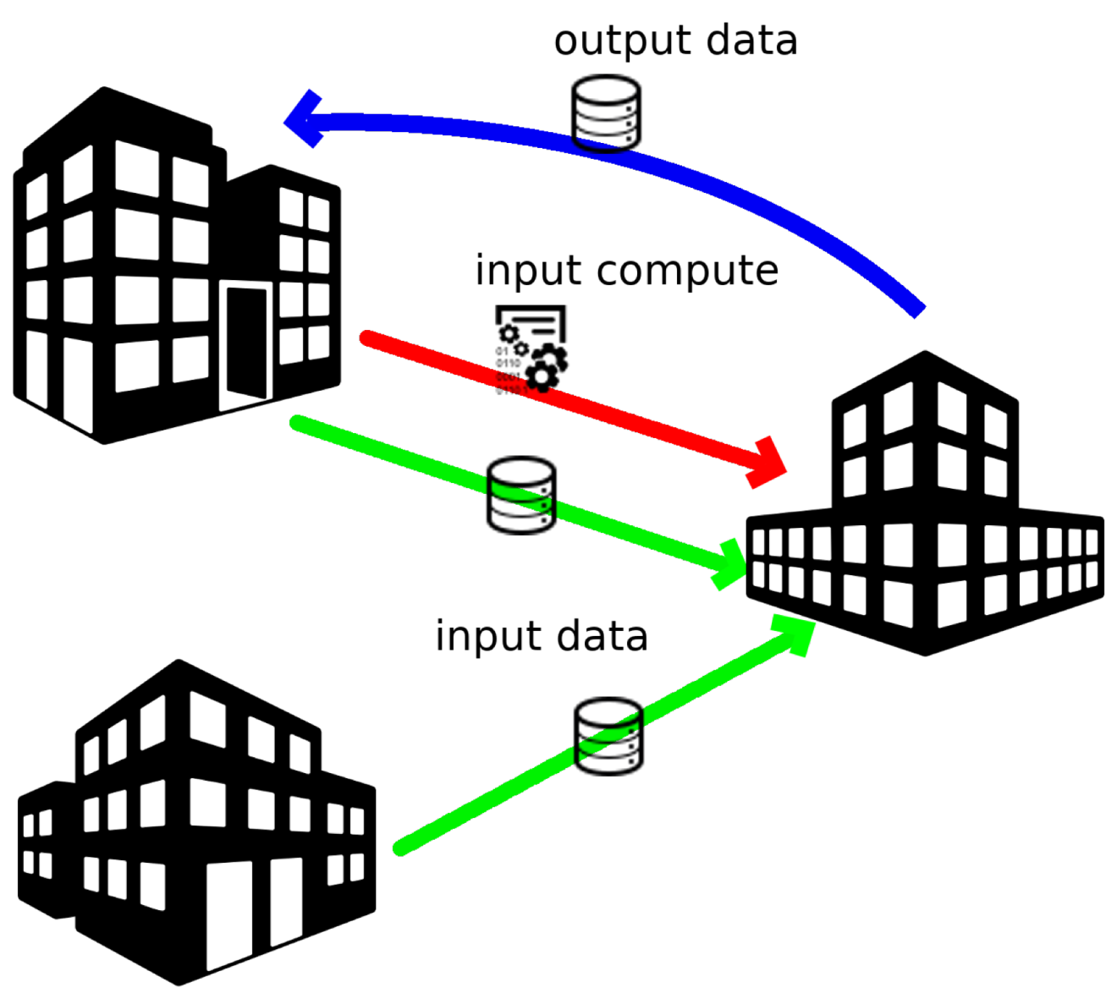
# A secure network overlay for tracking and enforcement of data transaction rules.

**Ralph Koning, Reginald Cushing Lu Zhang, Cees de Laat, Paola Grosso, University of Amsterdam**



Competing companies can, together, generate value from collaborating on data and compute. Examples include airlines industry, ports, healthcare.

Clearly this poses a challenge of how to facilitate such collaborations through technology. Here we look at one piece of the puzzle i.e. setting up distributed multi-domain infrastructures between such parties to facilitate the running of applications.

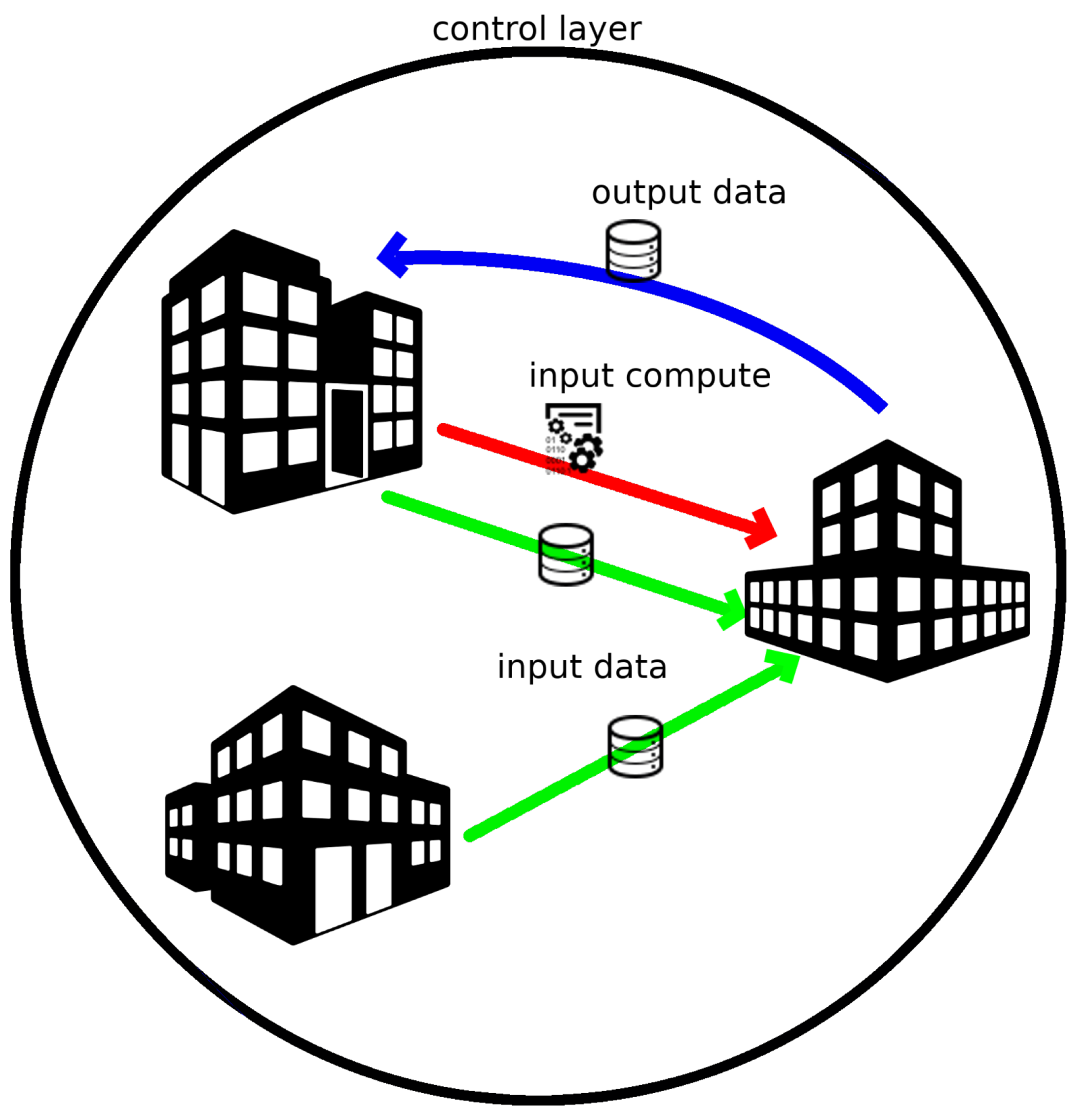


**Motivation**

- Multi-domain distributed applications need to share data and compute under different policies.

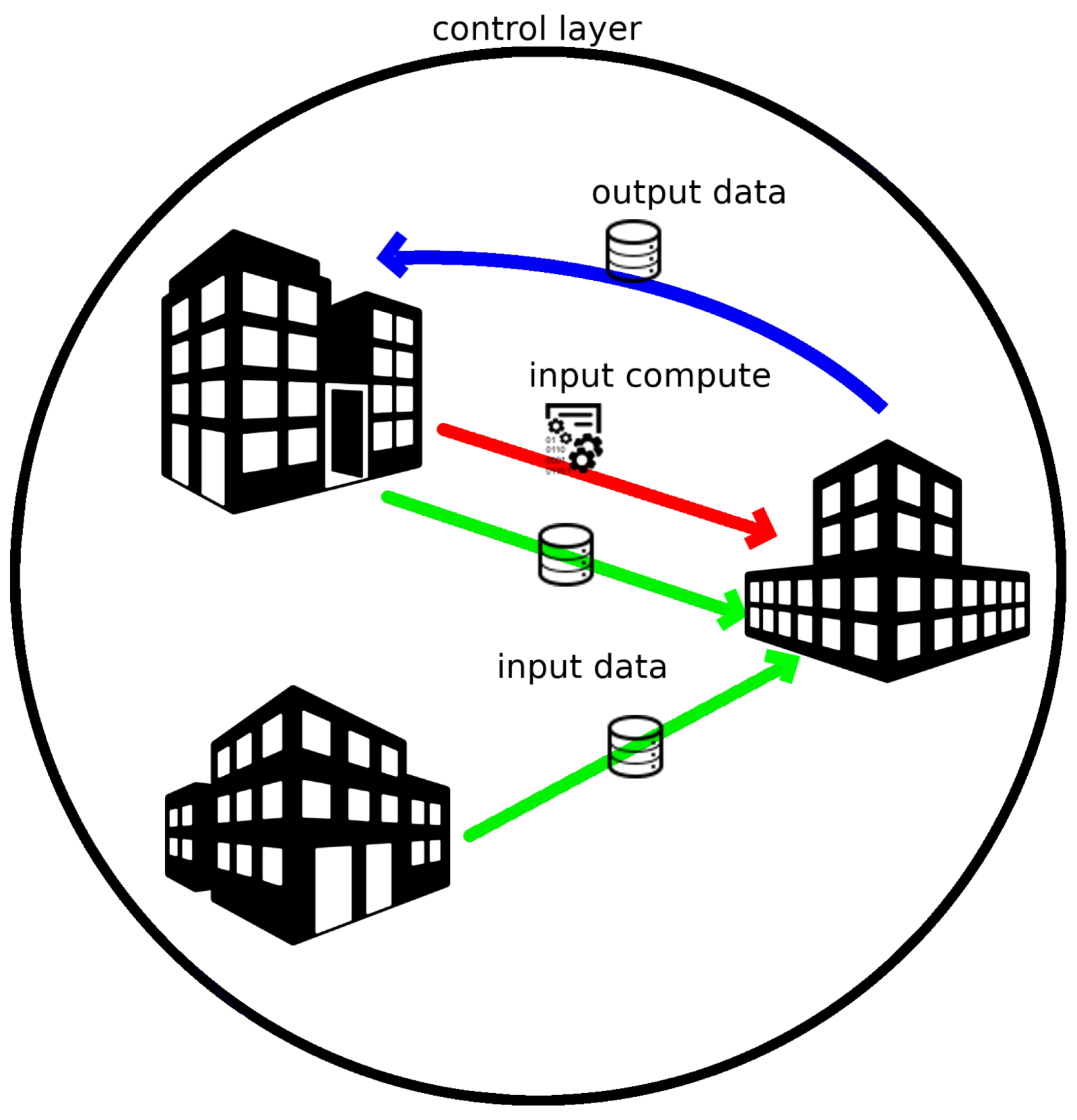
**Challenges**

- Map data sharing policies to infrastructure.
- Build an infrastructure that facilitates these applications.
- Control sharing of data and compute.
- Audit activity of the network.
- Minimize risk of policy/security breaches.



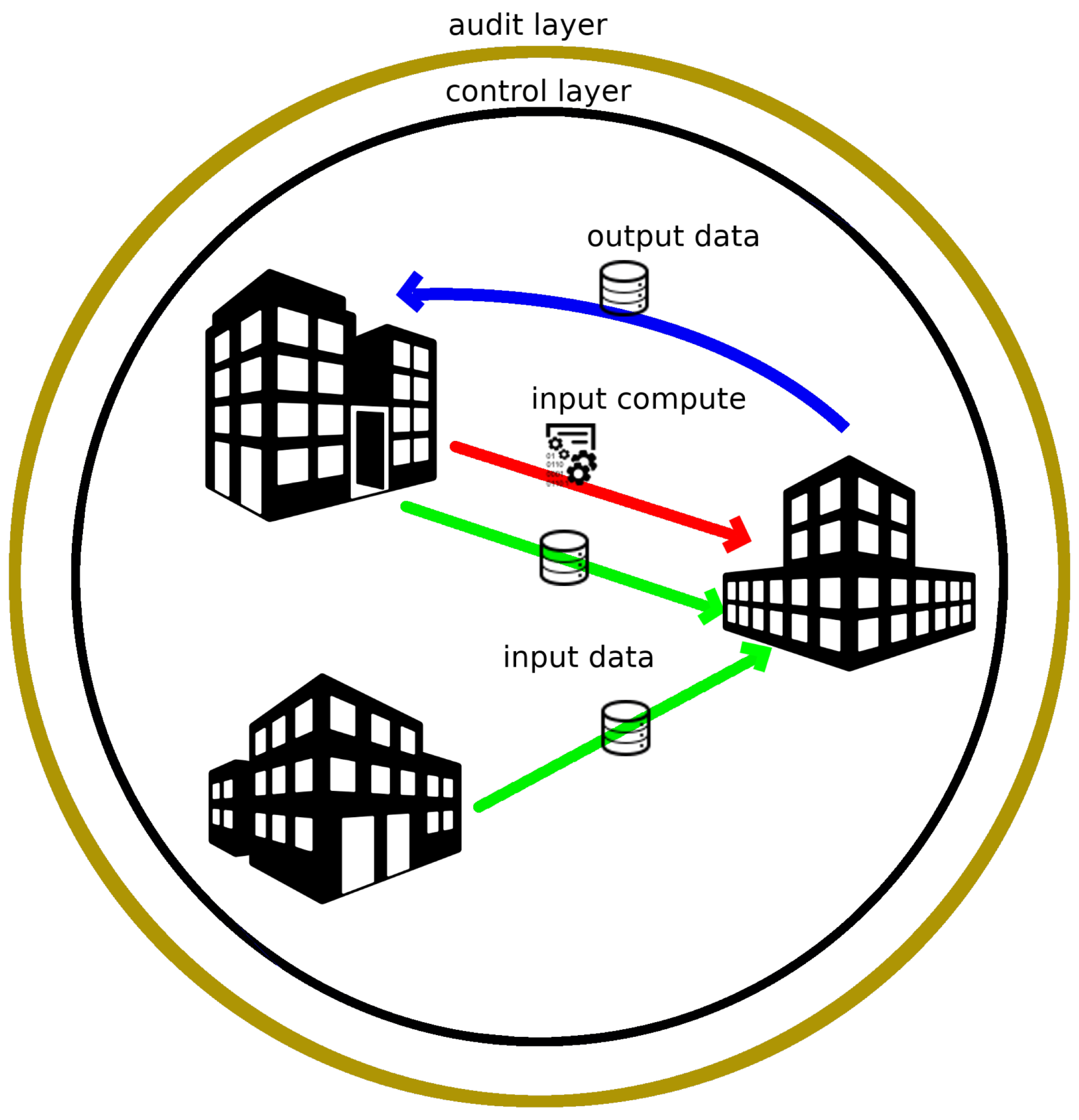
**Overlay**

- Nodes on the network are addressed using their public key.
- Nodes include: domain controllers, data buckets, auditors, application planners, users.
- Keys create chains of trust and verification through cryptographic signature trails.
- Applications are decomposed to a set of transactions.
- Transactions drive the overlay.



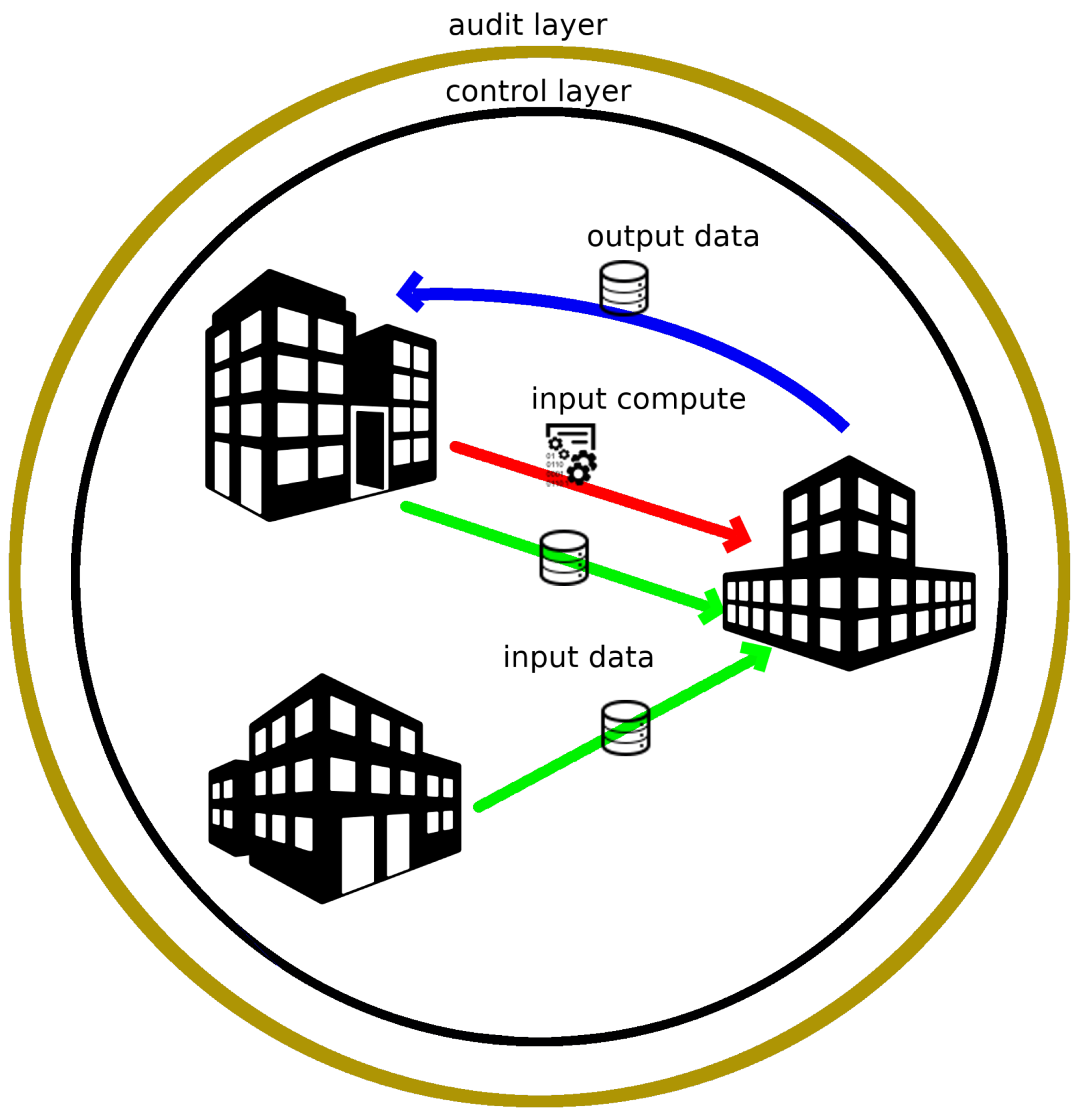
**Control functions**

- Securing bucket-to-bucket communication through transaction specific VPNs.
- Bucket node key address used as VPN keys.
- Opening connection endpoints on audit signatures.
- Network interfaces created on demand. Bucket containers have no network interface. Interfaces are only created and attached per signed transaction.



**Network of Auditors**

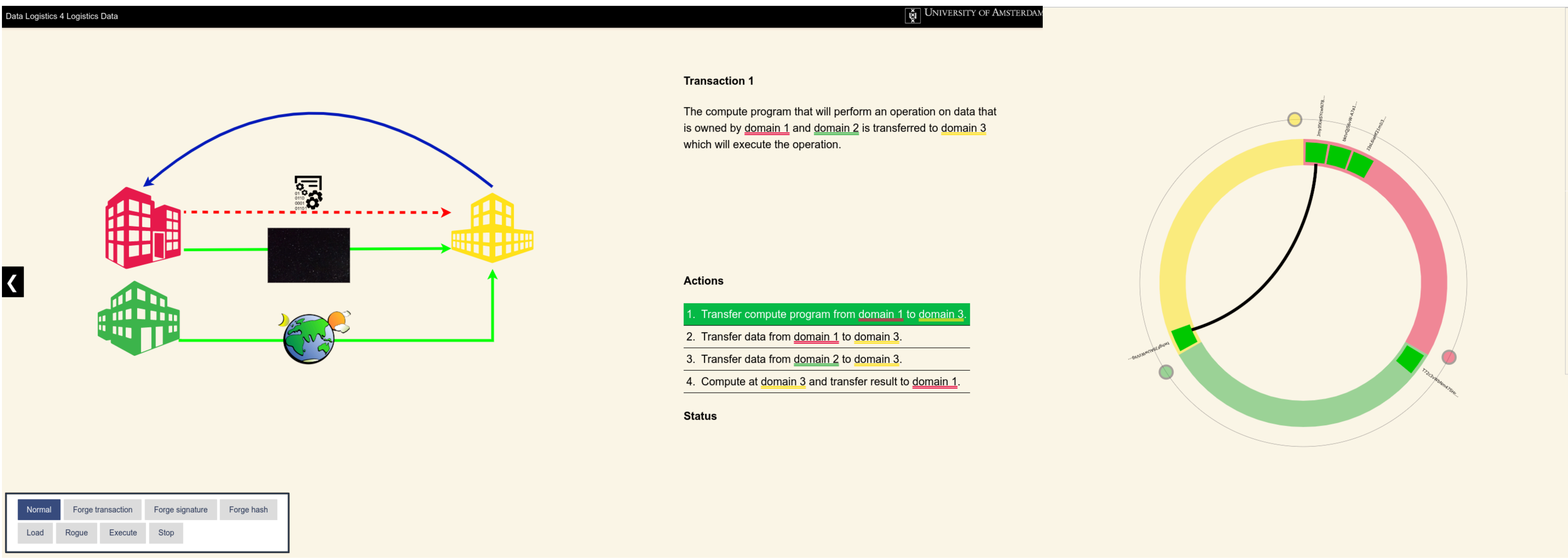
- Auditor nodes on the network provide a signing and verification layer that is checked by the control layer.
- Auditors sign network actions based on their internal policy.
- Auditors are independent of each other.
- The more number of signatures an action gets (e.g. transaction) the more confident the control layer is.
- Auditors cross-verify each other's logs to minimize log tempering.



**In short..**.

- Overlay allows for a distributed infrastructure.
- Key-based addressing allows for node signature trails and trust chains.
- Network of auditors provide *rubber-stamping* of actions/transactions
- Control layer enforces security using inputs from auditors and minimizes attack vectors on data transfers.

## Proof of Concept, see https://dl4ld.nl/



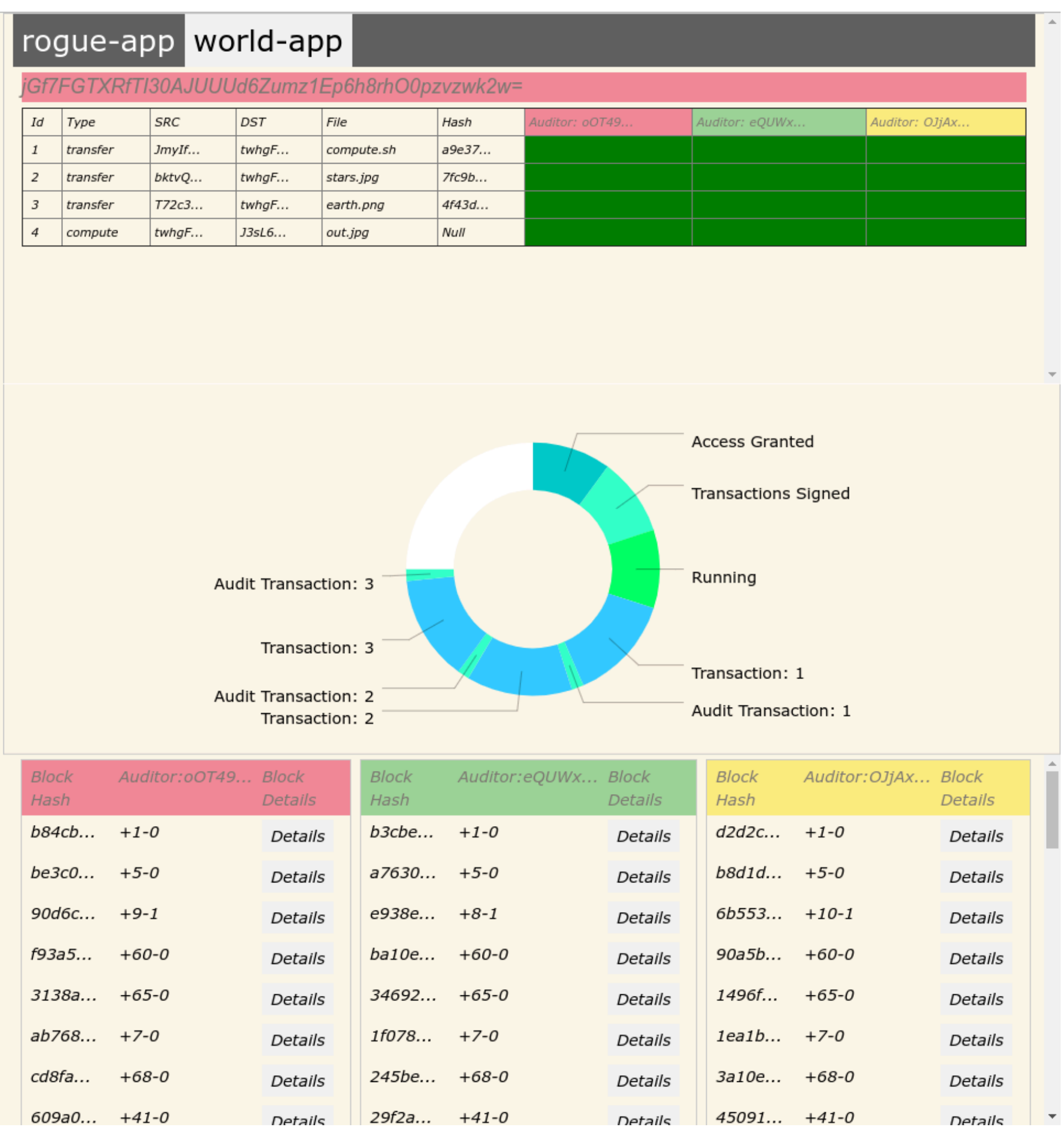
**Transaction 1**

The compute program that will perform an operation on data that is owned by domain 1 and domain 2 is transferred to domain 3 which will execute the operation.

**Actions**

1. Transfer compute program from domain 1 to domain 3.
2. Transfer data from domain 1 to domain 3.
3. Transfer data from domain 2 to domain 3.
4. Compute at domain 3 and transfer result to domain 1.

**Status**



jGf7FGTXRfTI30AJUUUd6Zumz1Ep6h8rhO0pzvzwk2w=

| Id | Type | SRC | DST | File | Hash | Auditor: oOT49... | Auditor: eQUWx... | Auditor: OJjAx... |
|---|---|---|---|---|---|---|---|---|
| 1 | transfer | JmyIf... | twhgF... | compute.sh | a9e37... | 🟩 | 🟩 | 🟩 |
| 2 | transfer | bktvQ... | twhgF... | stars.jpg | 7fc9b... | 🟩 | 🟩 | 🟩 |
| 3 | transfer | T72c3... | twhgF... | earth.png | 4f43d... | 🟩 | 🟩 | 🟩 |
| 4 | compute | twhgF... | J3sL6... | out.jpg | Null | 🟩 | 🟩 | 🟩 |

| Block Hash | Auditor:oOT49... | Block Details |
|---|---|---|
| b84cb... | +1-0 | Details |
| be3c0... | +5-0 | Details |
| 90d6c... | +9-1 | Details |
| f93a5... | +60-0 | Details |
| 3138a... | +65-0 | Details |
| ab768... | +7-0 | Details |
| cd8fa... | +68-0 | Details |
| 609a0... | +41-0 | Details |

| Block Hash | Auditor:eQUWx... | Block Details |
|---|---|---|
| b3cbe... | +1-0 | Details |
| a7630... | +5-0 | Details |
| e938e... | +8-1 | Details |
| ba10e... | +60-0 | Details |
| 34692... | +65-0 | Details |
| 1f078... | +7-0 | Details |
| 245be... | +68-0 | Details |
| 29f2a... | +41-0 | Details |

| Block Hash | Auditor:OJjAx... | Block Details |
|---|---|---|
| d2d2c... | +1-0 | Details |
| b8d1d... | +5-0 | Details |
| 6b553... | +10-1 | Details |
| 90a5b... | +60-0 | Details |
| 1496f... | +65-0 | Details |
| 1ea1b... | +7-0 | Details |
| 3a10e... | +68-0 | Details |
| 45091... | +41-0 | Details |

This research is funded by the Dutch Science Foundation in the Commit2Data program (grant no: 628.001.001) and by Equinix.