Using a Verifiable and Decentralized Ledger as a Basis for Trusting Hospital Endpoints

Matthijs Bartelink

January 2020

Supervisor: Guido van't Noordende

The whitebox infrastructure

- Individual GP's hold patient data

The whitebox infrastructure

- Individual GP's hold patient data
- GP's own a whitebox which controls data access

The whitebox infrastructure

- Individual GP's hold patient data
- GP's own a whitebox which controls data access
- Patient transfers code to establish trust

Research Question

Can we use a blockchain ledger to verify the authenticity of hospital endpoints?

- Can we record trust by whiteboxes in a verifiable way?

Research Question

Can we use a blockchain ledger to verify the authenticity of hospital endpoints?

- Can we record trust by whiteboxes in a verifiable way?
- How can we use this record to identify hospital endpoints?

Research Question

Can we use a blockchain ledger to verify the authenticity of hospital endpoints?

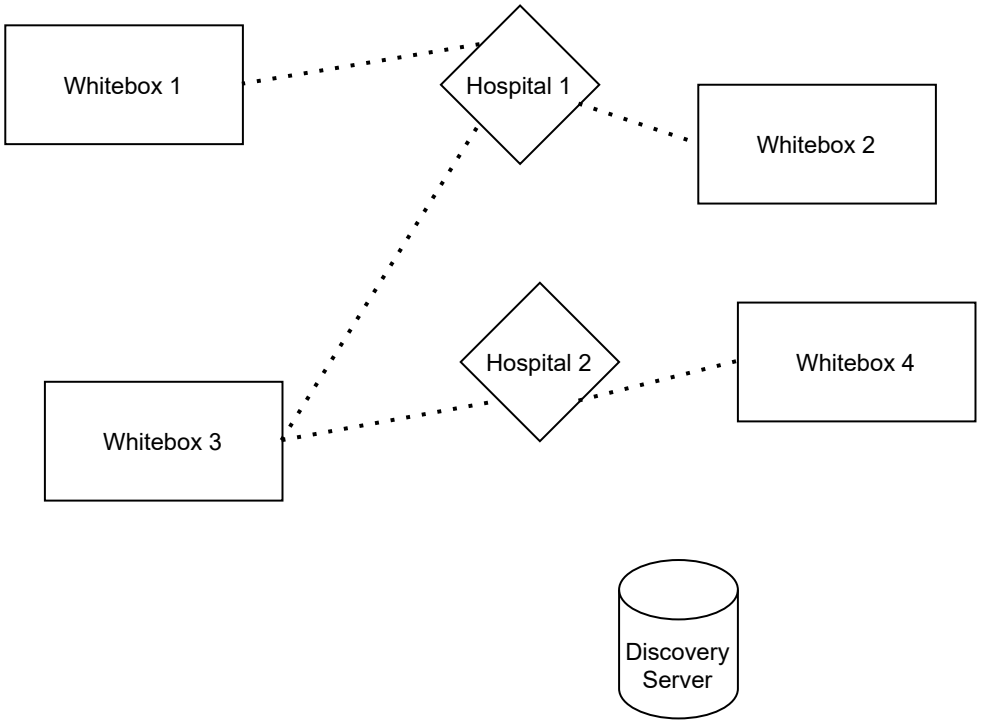
- Can we record trust by whiteboxes in a verifiable way?
- How can we use this record to identify hospital endpoints?
- How do we account for loss of trust?

Research Question

Can we use a blockchain ledger to verify the authenticity of hospital endpoints?

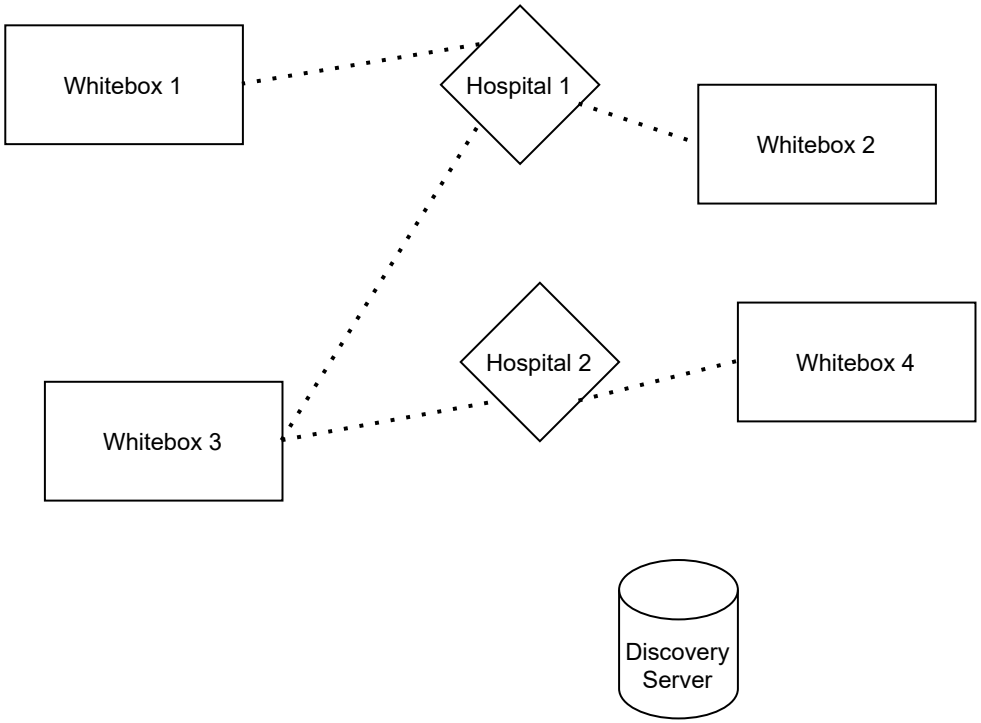
- Can we record trust by whiteboxes in a verifiable way?
- How can we use this record to identify hospital endpoints?
- How do we account for loss of trust?
- Does the proposed system scale efficiently enough?

A Design Overview



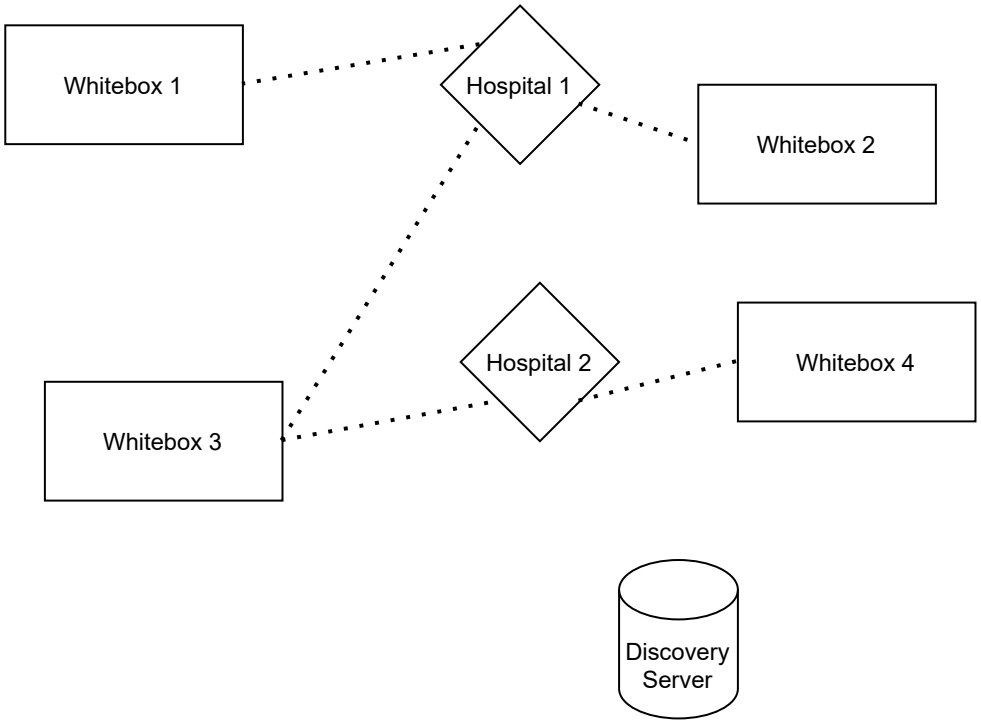
- Record established trust in a decentralized ledger

A Design Overview



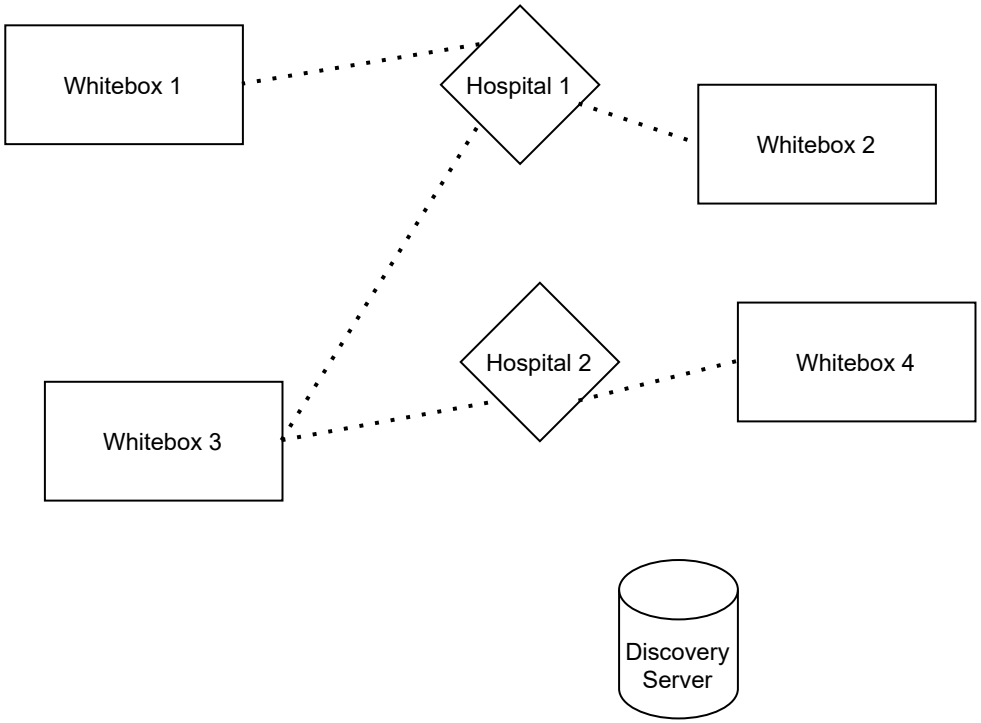
- Record established trust in a decentralized ledger
- Record addition and removal operations to allow for revocation

A Design Overview



- Record established trust in a decentralized ledger
- Record addition and removal operations to allow for revocation
- Allow for negative trust-links

A Design Overview



- Record established trust in a decentralized ledger
- Record addition and removal operations to allow for revocation
- Allow for negative trust-links
- Use proof of authority as consensus algorithm

The Ledger

- A sequence of blocks describing operations

The Ledger

- A sequence of blocks describing operations
- Blocks contain a hash of the previous block, making integrity easy to verify

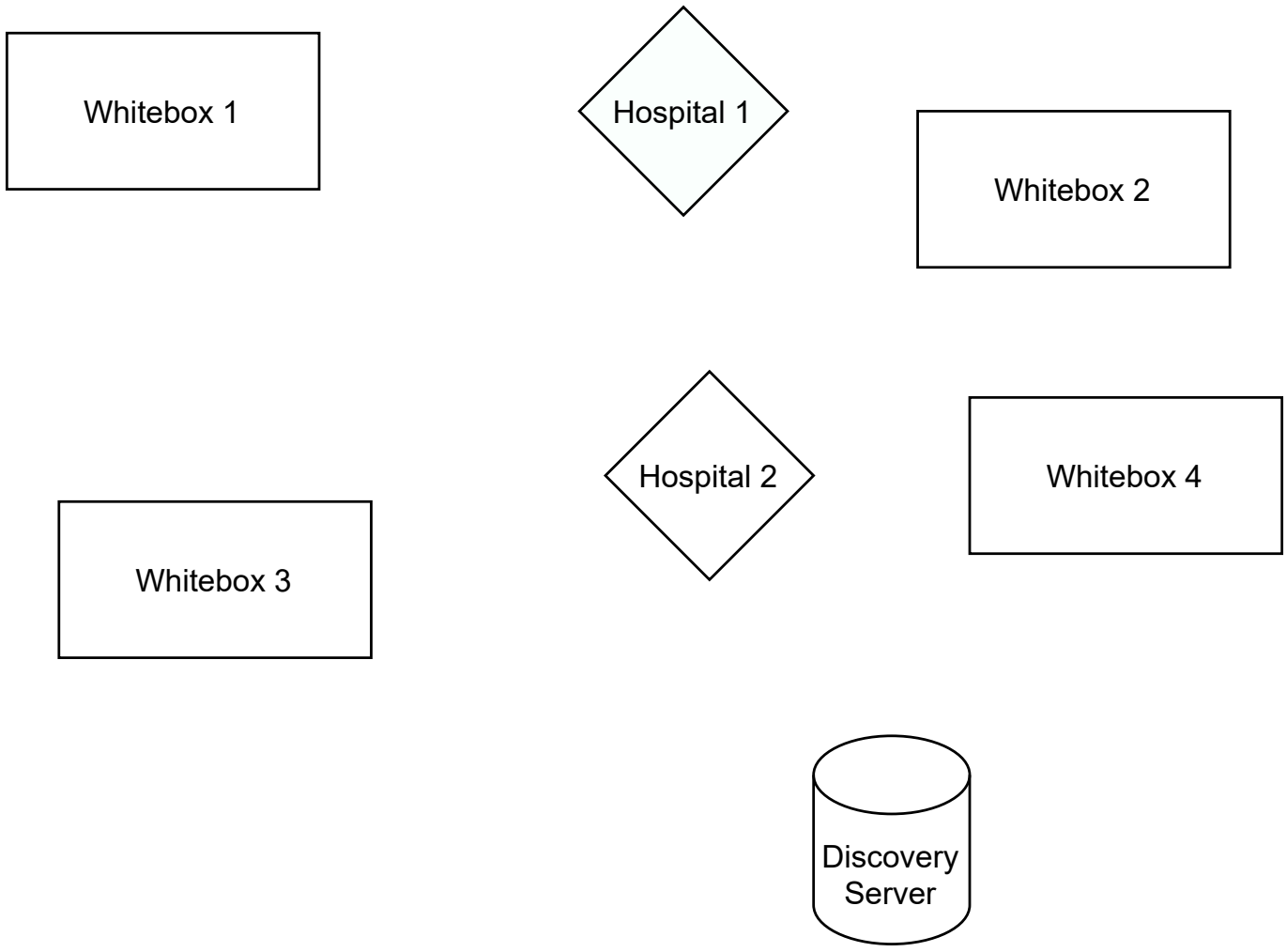
The Ledger

- A sequence of blocks describing operations
- Blocks contain a hash of the previous block, making integrity easy to verify
- Blocks are considered valid when the whitebox they describe agrees

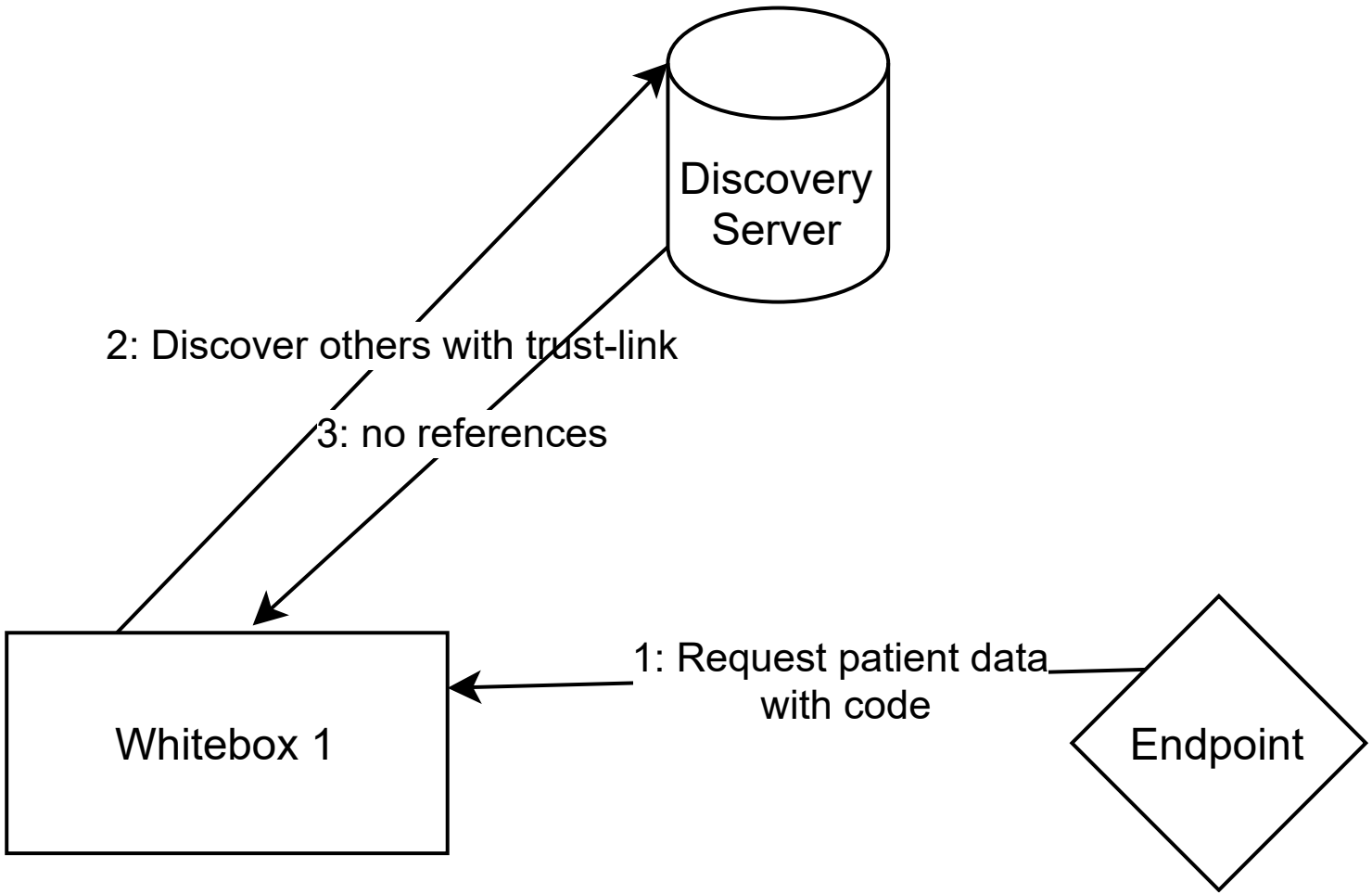
The Ledger

- A sequence of blocks describing operations
- Blocks contain a hash of the previous block, making integrity easy to verify
- Blocks are considered valid when the whitebox they describe agrees
- Timestamp used to determine order

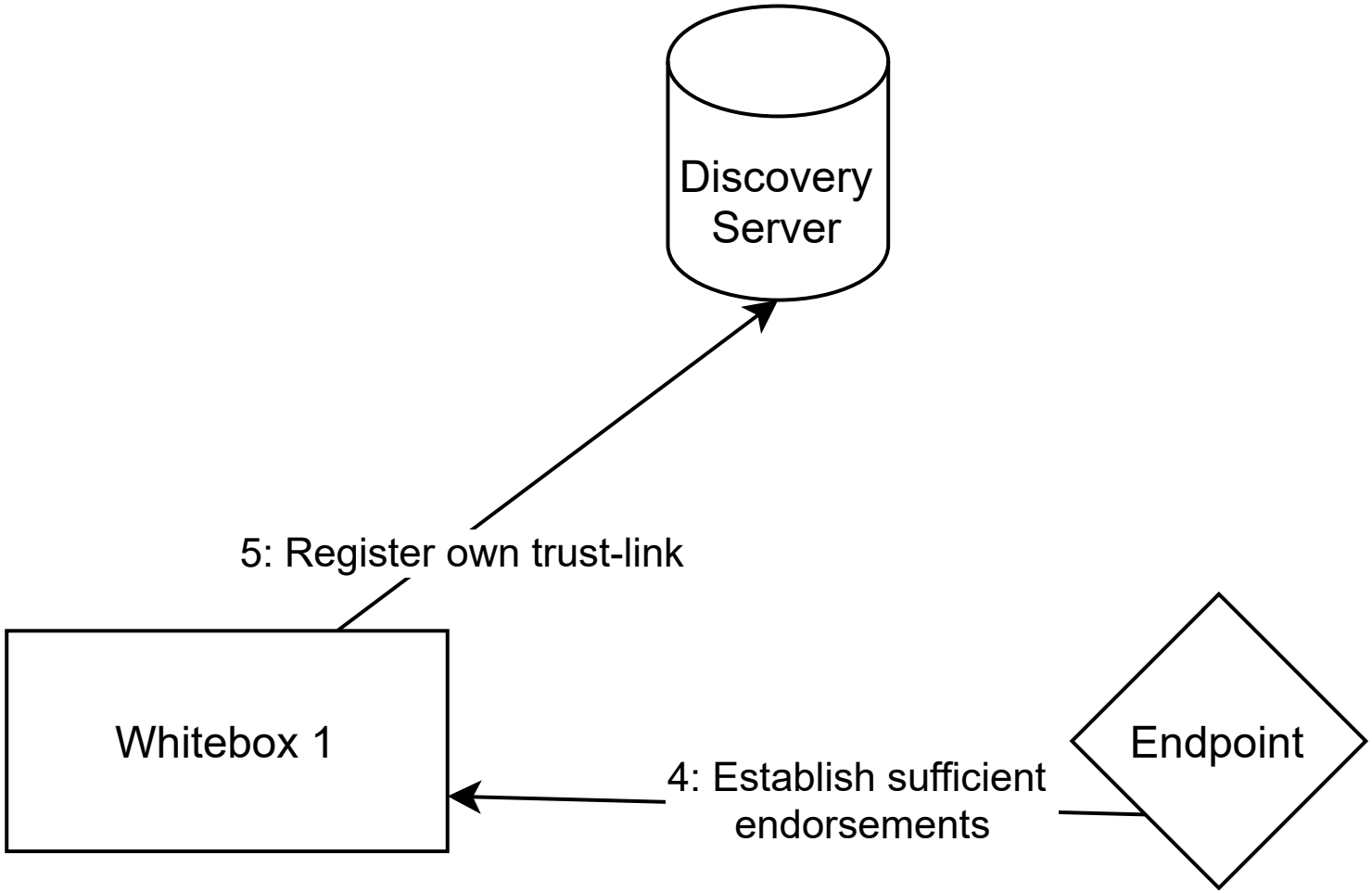
Scenario 1: No trust-links



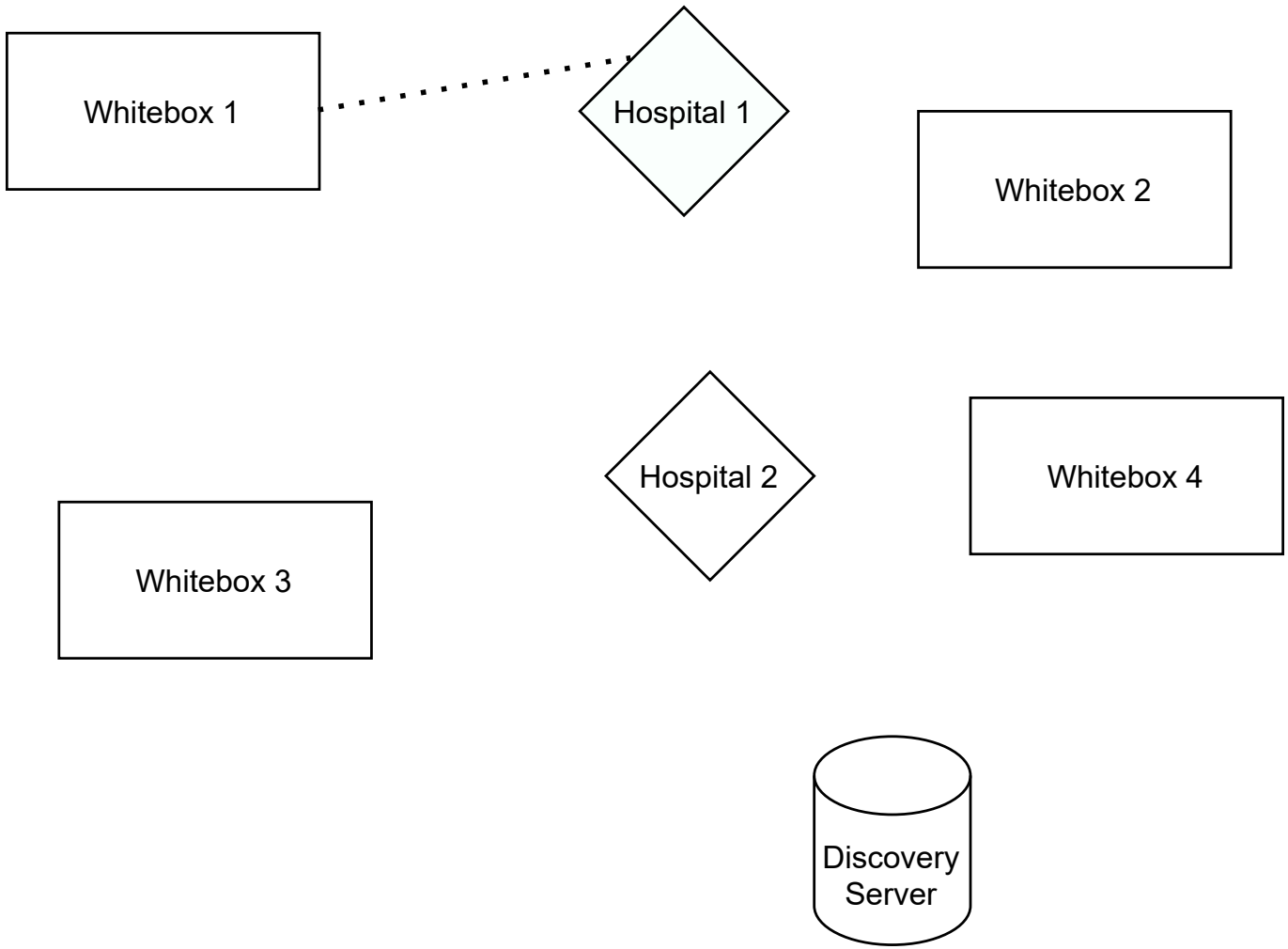
Establishing first trust-link



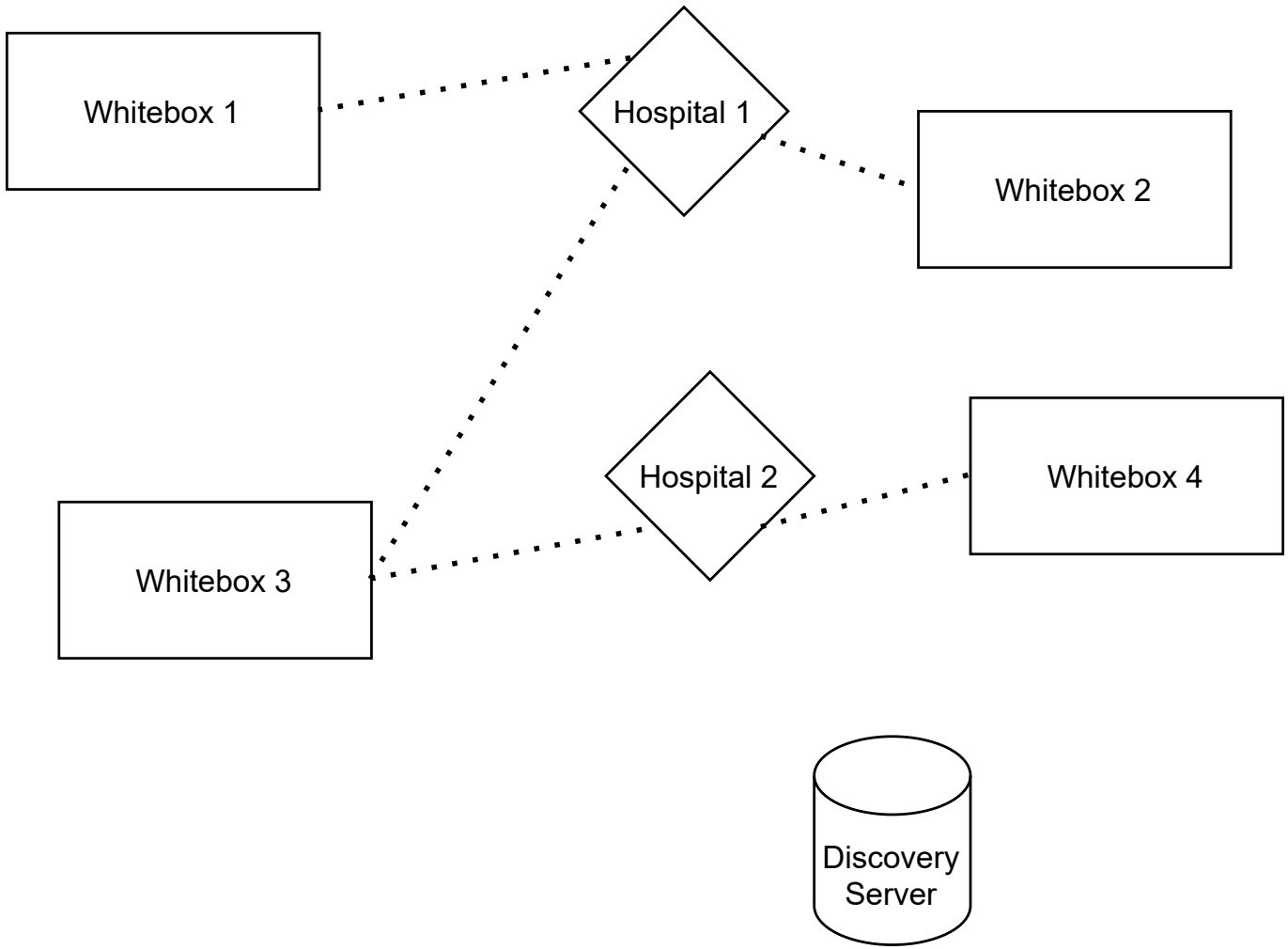
Establishing first trust-link



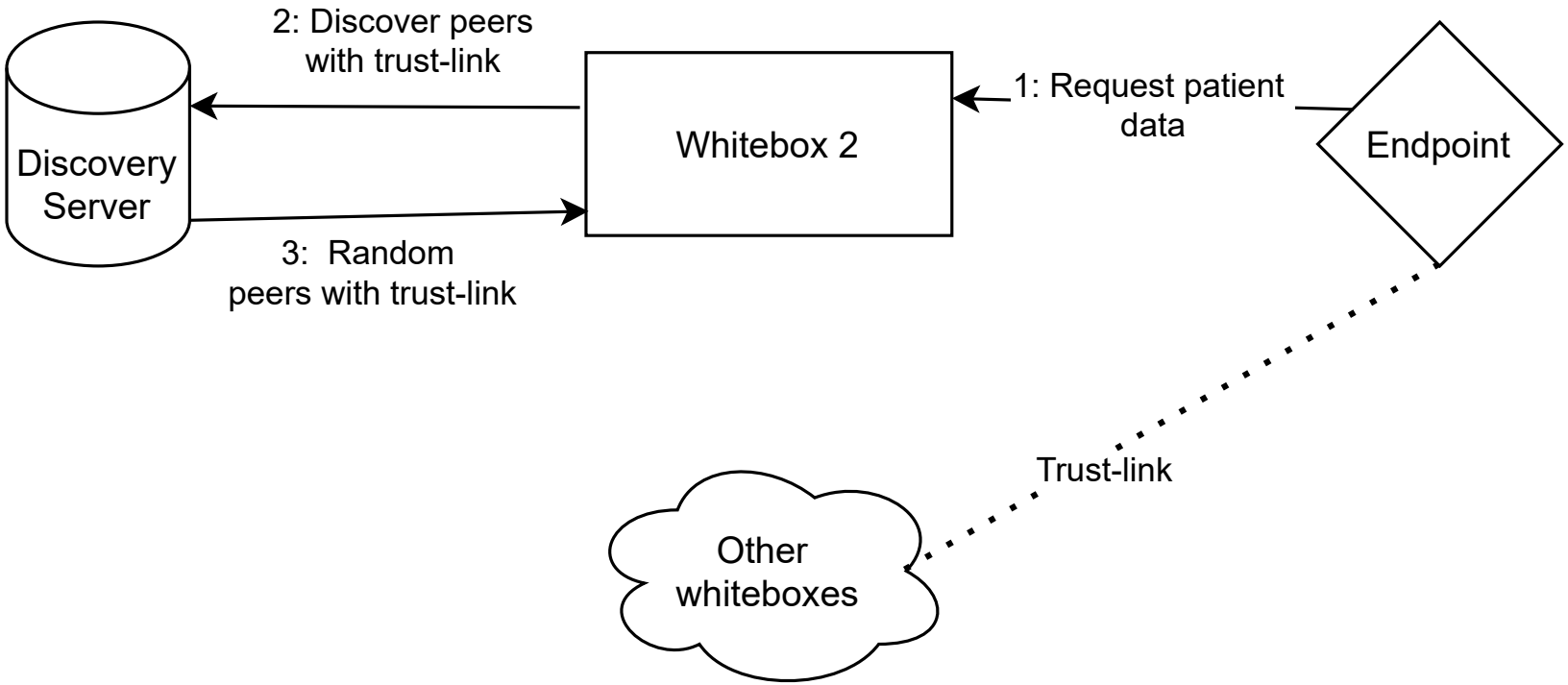
Scenario


Whitebox 1
Hospital 1
Whitebox 2
Hospital 2
Whitebox 4
Whitebox 3
Discovery Server

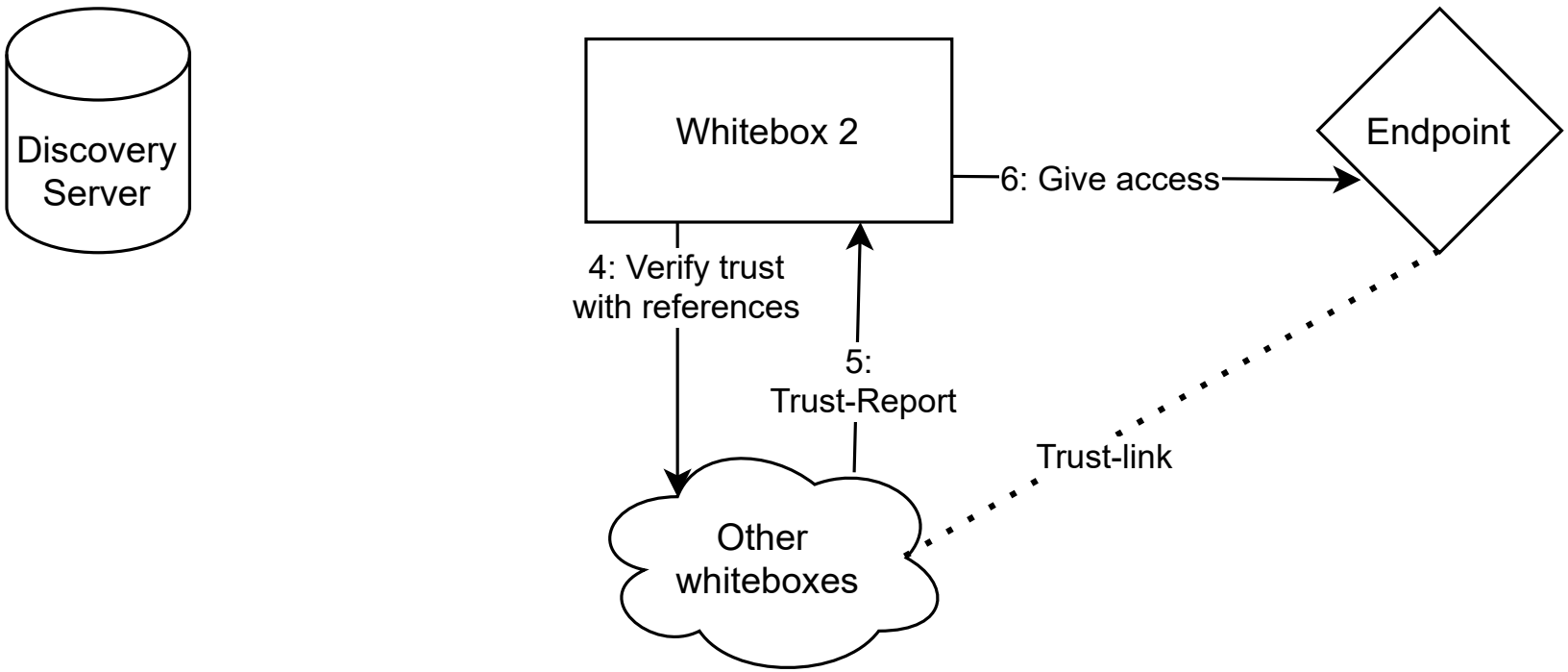
Scenario 2: Trust exists



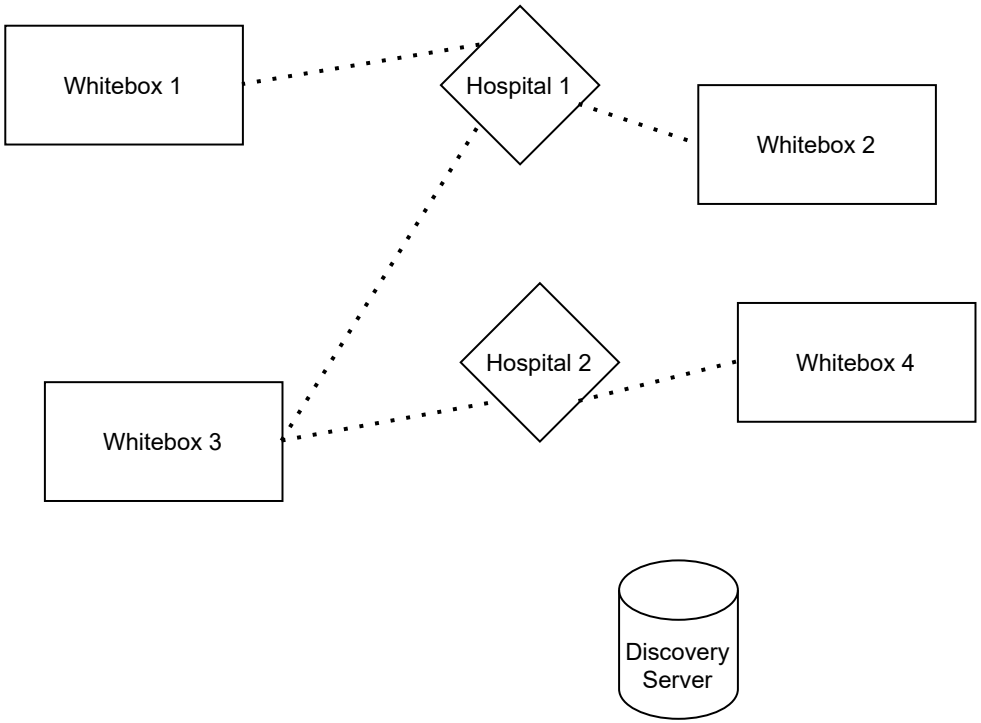
Checking Trust



Checking Trust

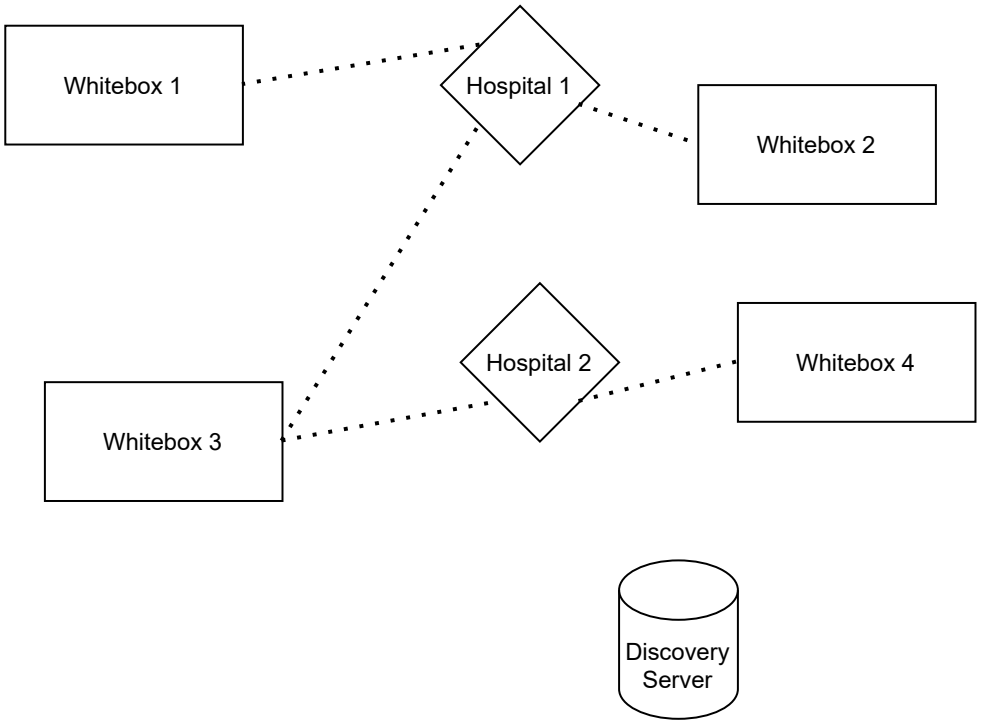


Security Parameter



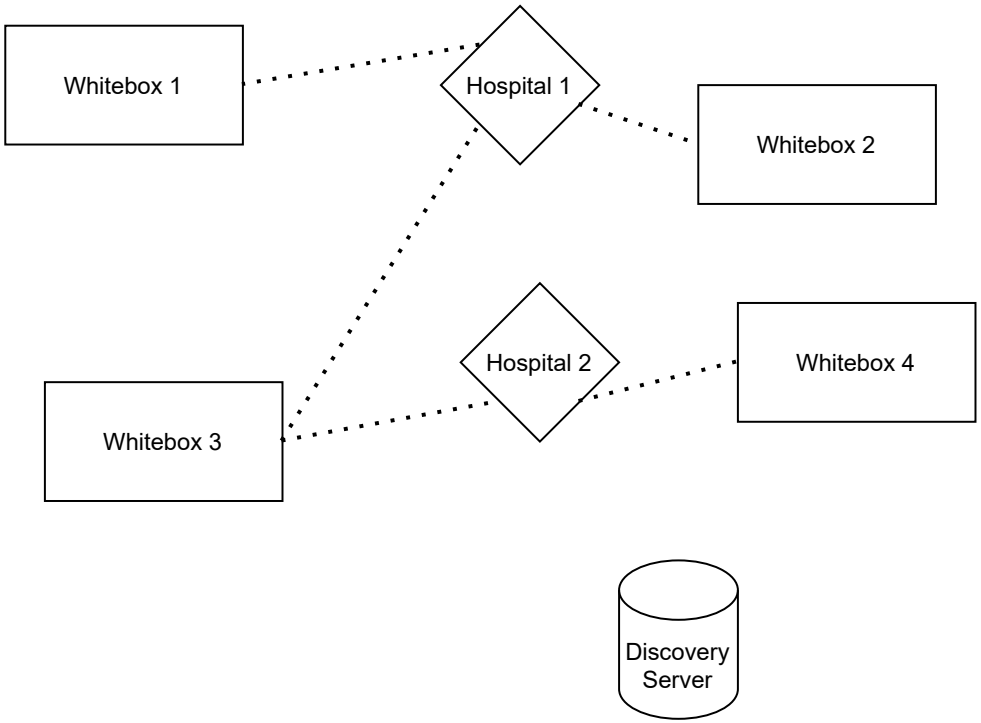
- Security parameter S

Security Parameter



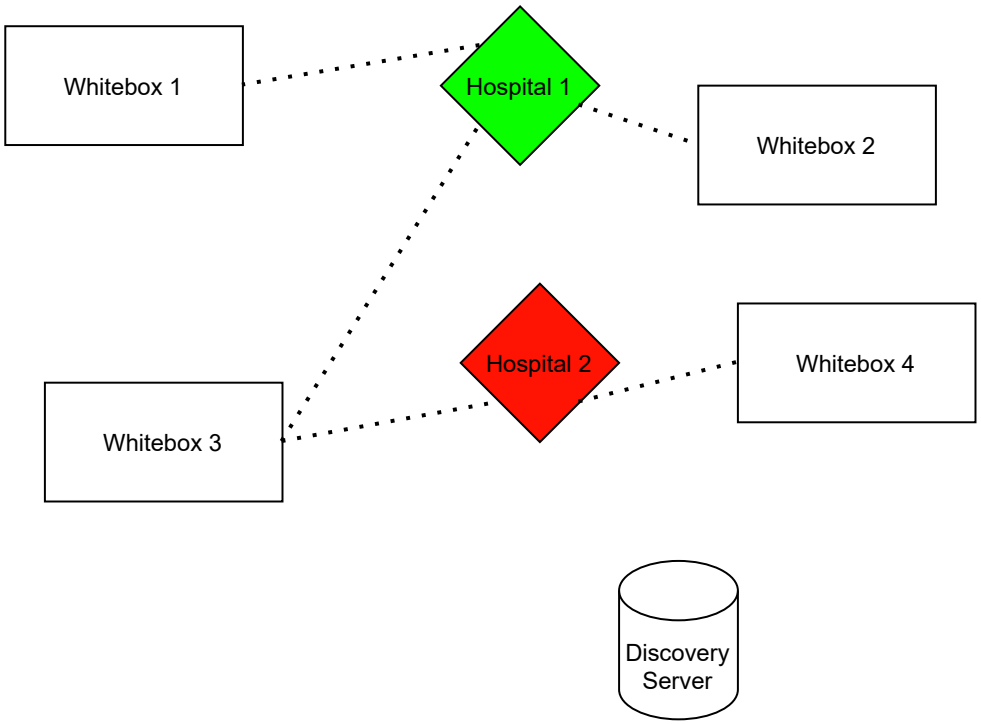
- Security parameter S
- First S whiteboxes use alternative method

Security Parameter



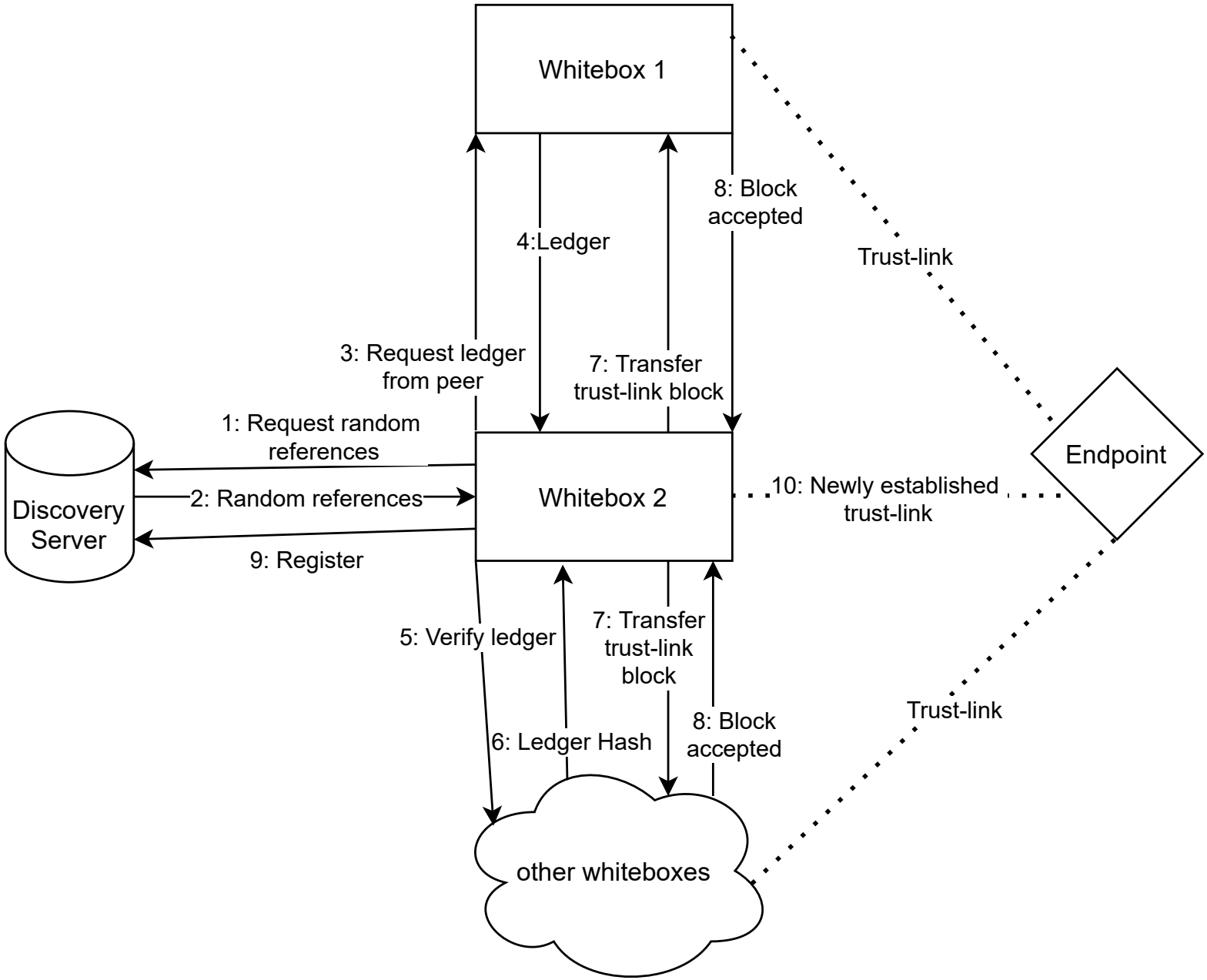
- Security parameter S
- First S whiteboxes use alternative method
- Then rely on previously established trust

Security Parameter

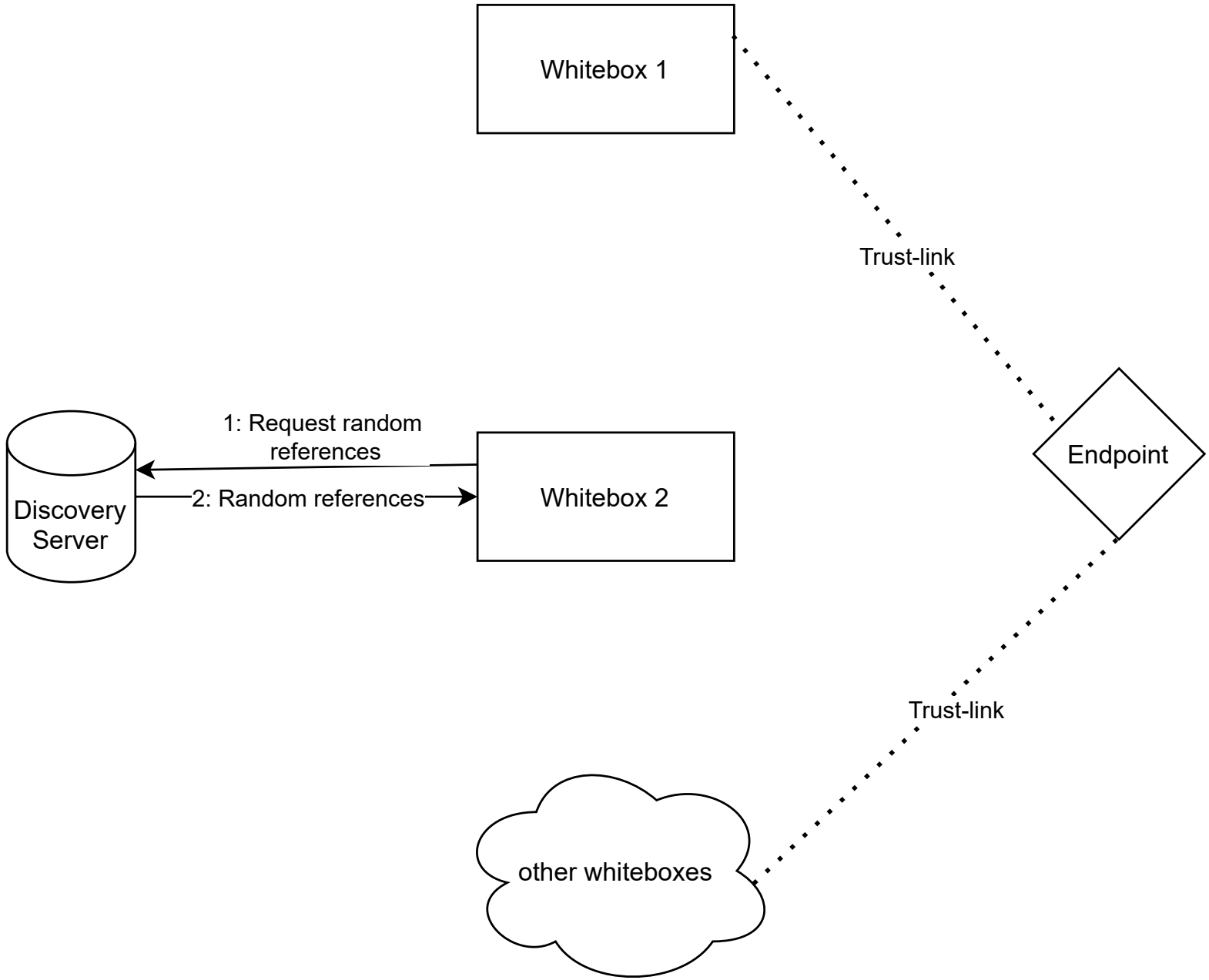


- Security parameter S
- First S whiteboxes use alternative method
- Then rely on previously established trust
- Example: S=3

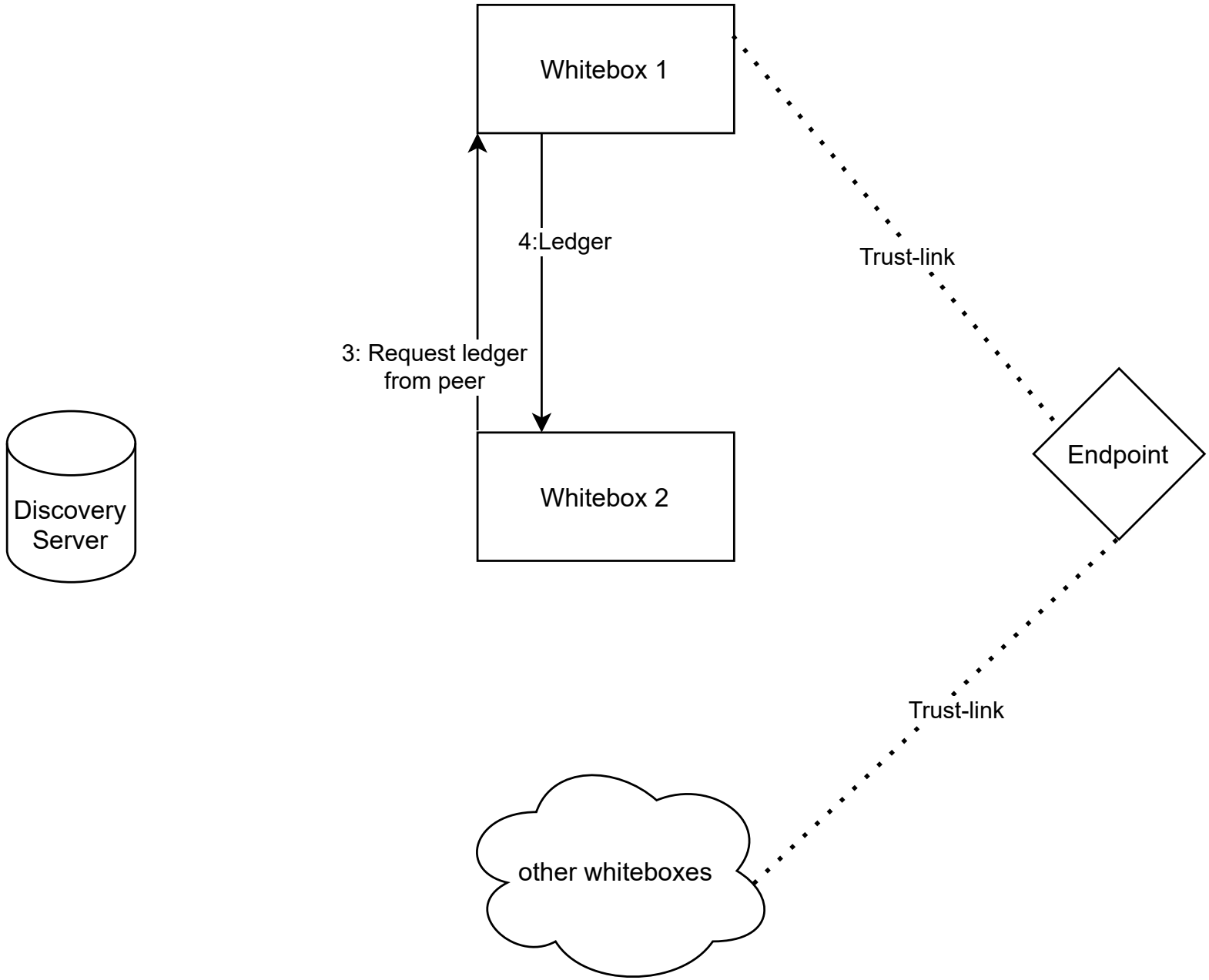
Establishing Trust(2)



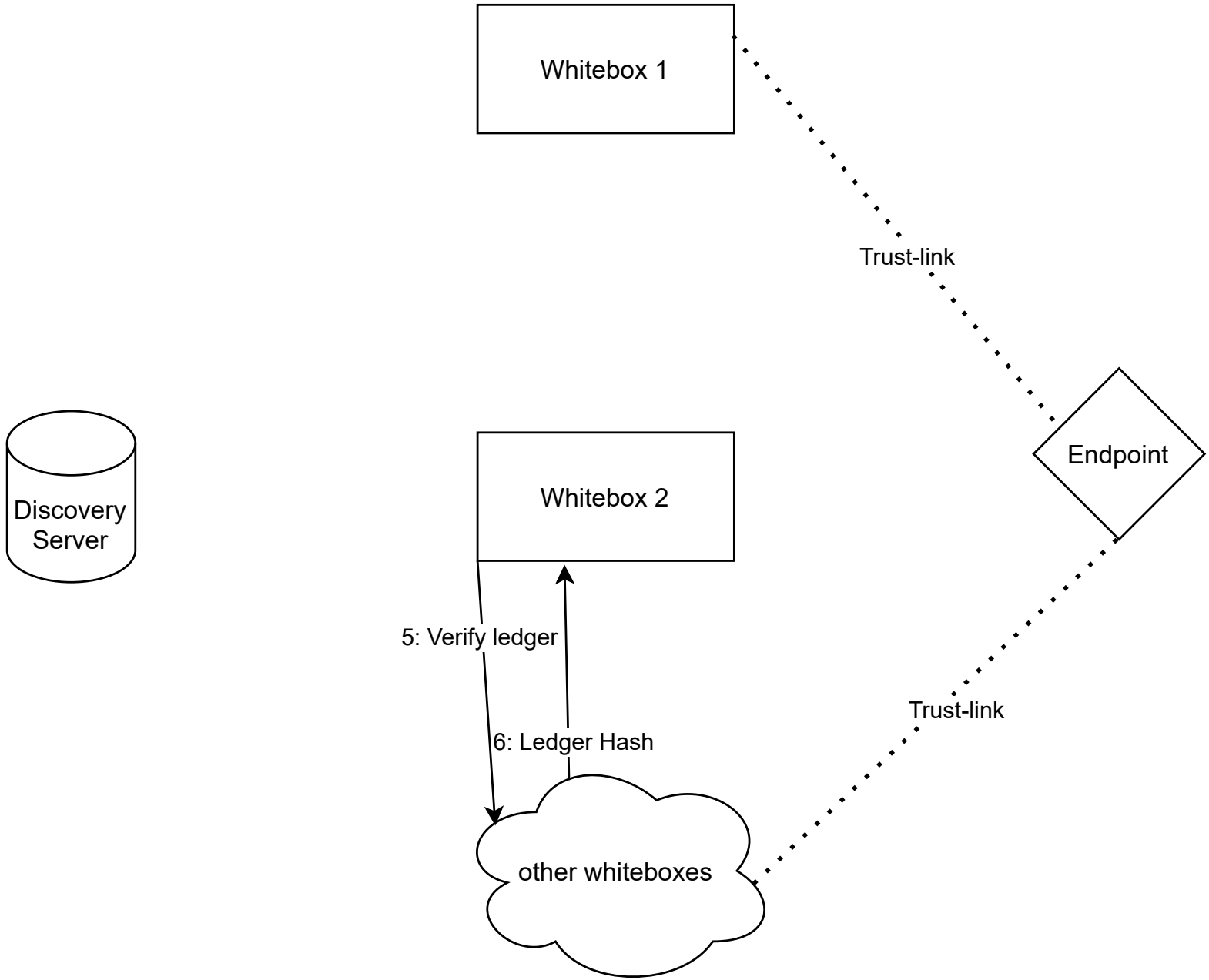
Establishing Trust(2)



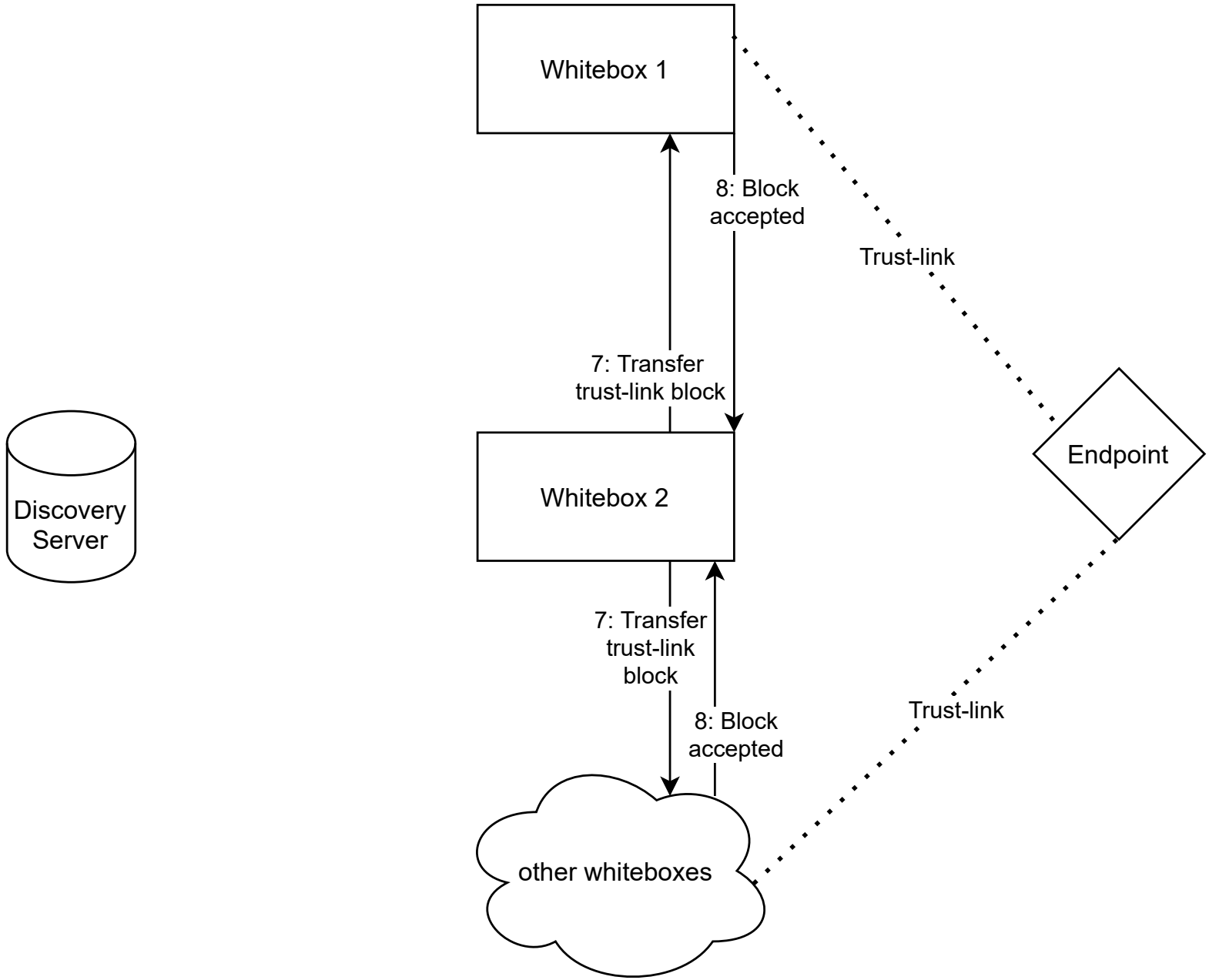
Establishing Trust(2)



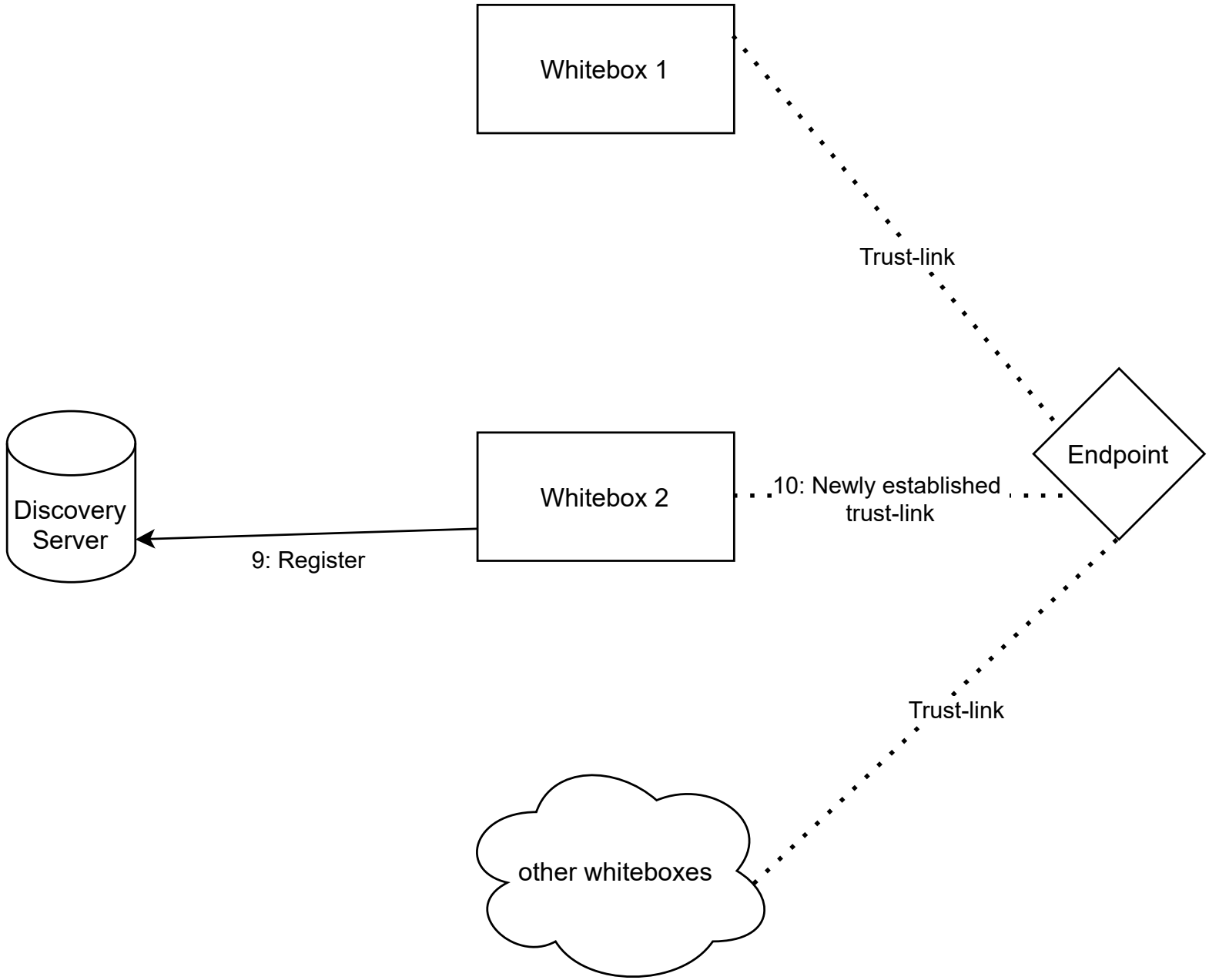
Establishing Trust(2)



Establishing Trust(2)



Establishing Trust(2)



Consensus Algorithm

- Proof of Authority

Consensus Algorithm

- Proof of Authority
- Block publisher is responsible for consensus

Consensus Algorithm

- Proof of Authority
- Block publisher is responsible for consensus
- Discovers and resolves conflicts during publishing

Consensus Algorithm

- Proof of Authority
- Block publisher is responsible for consensus
- Discovers and resolves conflicts during publishing
- Blocks older than one hour become immutable

Consensus Algorithm

- Proof of Authority
- Block publisher is responsible for consensus
- Discovers and resolves conflicts during publishing
- Blocks older than one hour become immutable
- Unless majority disagrees

Threat Models

- Malicious whiteboxes establish an endpoint

Threat Models

- Malicious whiteboxes establish an endpoint
- Denial of service attack on the discovery server

Threat Models

- Malicious whiteboxes establish an endpoint
- Denial of service attack on the discovery server
- Inference attack

Scaling

- Checking trust must be fairly quick
- Other operations are allowed to be slow

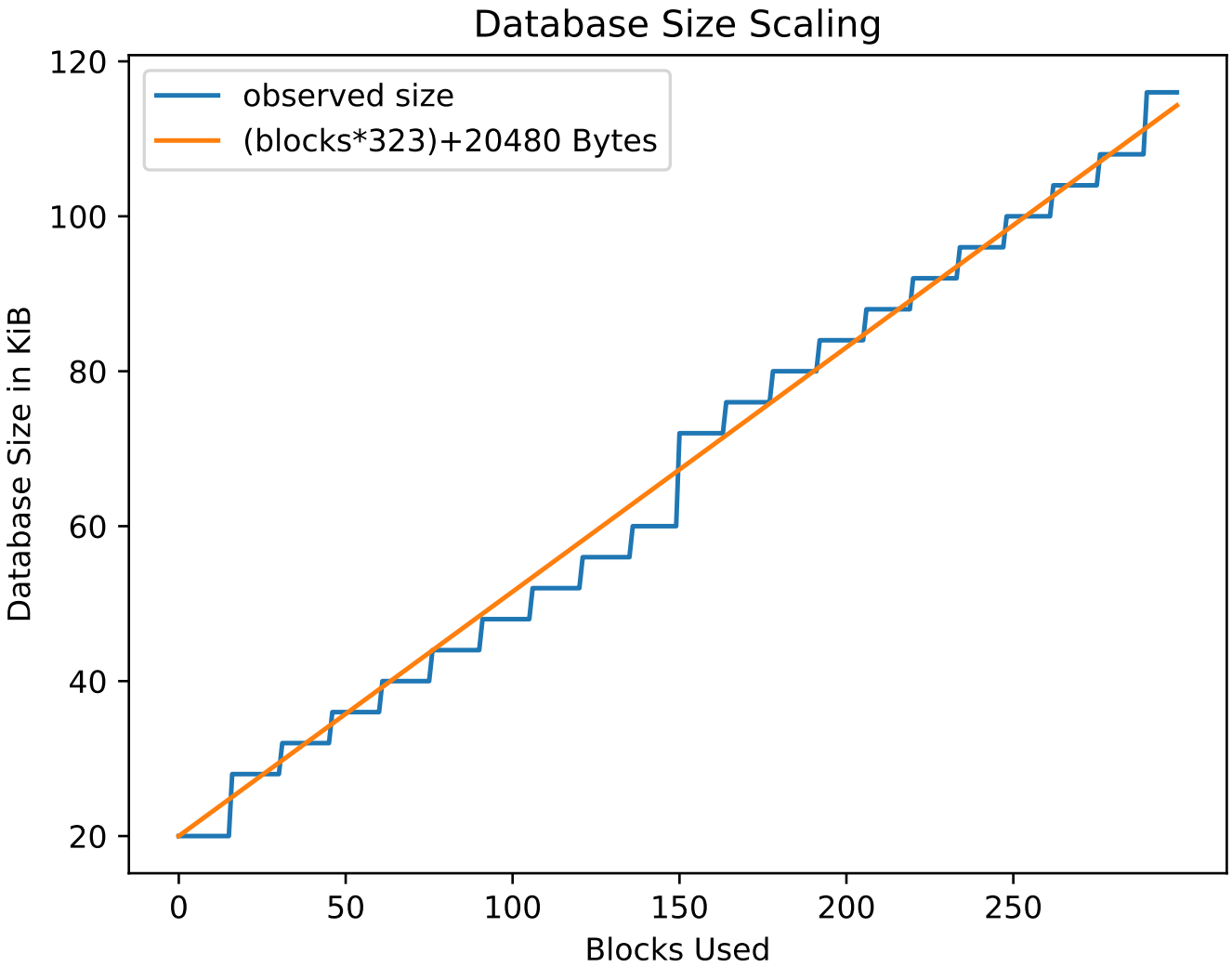
Scaling

- Checking trust must be fairly quick
- Other operations are allowed to be slow
- Storage used should be reasonable

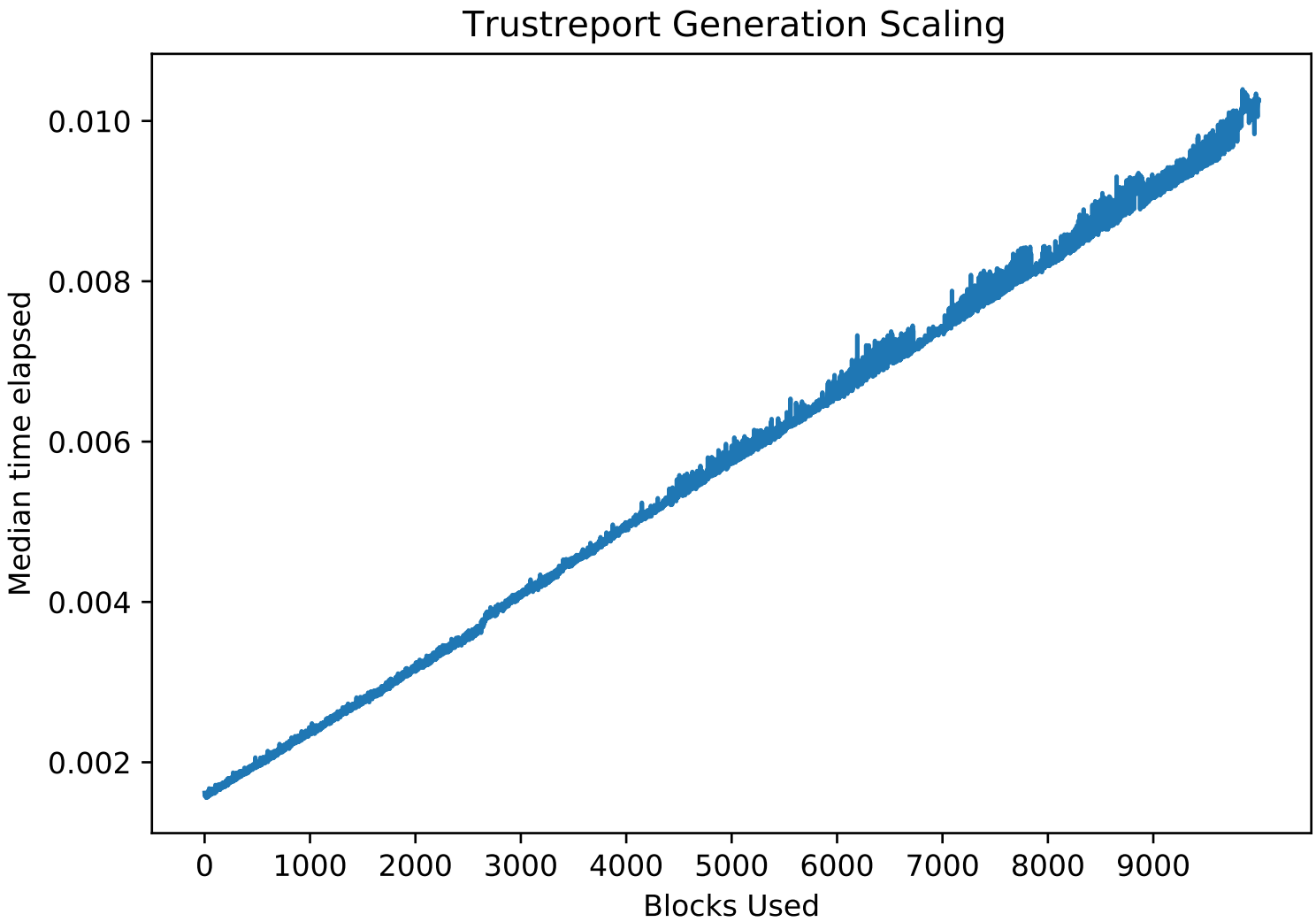
Scaling

- Checking trust must be fairly quick
- Other operations are allowed to be slow
- Storage used should be reasonable
- +-5000 whiteboxes, each with 150 or so ledgers

Scaling(2)


Database Size Scaling
observed size
(blocks*323)+20480 Bytes
Database Size in KiB
120
100
80
60
40
20
0
50
100
150
200
250
Blocks Used

Scaling(3)


Trustreport Generation Scaling
Median time elapsed
0.010
0.008
0.006
0.004
0.002
0
1000
2000
3000
4000
5000
6000
7000
8000
9000
Blocks Used

Conclusion

- Trust ledger is used to verify hospital endpoints

Conclusion

- Trust ledger is used to verify hospital endpoints
- Loss of trust is accounted for by negative trust-links

Conclusion

- Trust ledger is used to verify hospital endpoints
- Loss of trust is accounted for by negative trust-links
- System scales sufficiently

Conclusion

- Trust ledger is used to verify hospital endpoints
- Loss of trust is accounted for by negative trust-links
- System scales sufficiently
- Discovery server is central point of failure

Conclusion

- Trust ledger is used to verify hospital endpoints
- Loss of trust is accounted for by negative trust-links
- System scales sufficiently
- Discovery server is central point of failure
- Whitebox Systems is source of trust for whitebox identification

Future Work

- Implement and improve consensus algorithm

Future Work

- Implement and improve consensus algorithm
- Replace discovery method

Future Work

- Implement and improve consensus algorithm
- Replace discovery method
- Decentralize trust in whiteboxes