X509 Certificate Transparency using fabric

August, 2019

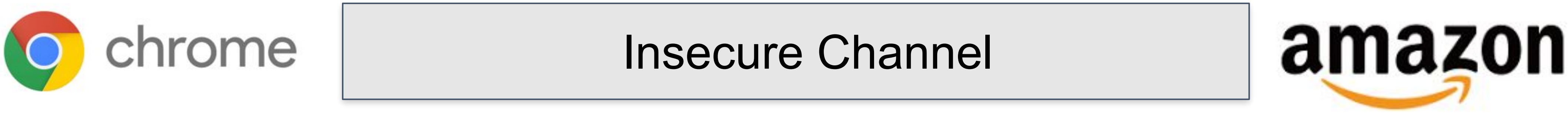
HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

X509 Certificate Transparency using fabric

- Introduction
  - **Name**: Harsh Jain
  - **Location**: India
  - **University**: Indian Institute Of Technology, Roorkee
  - **Mentor(s):** Mahavir Jhawar, Deva Madala
  - **Hyperledger project**: Fabric, blockchain-explorer, caliper

X.509 Certificate Transparency using Blockchain

- **Project Description:** Secure Communication over Internet

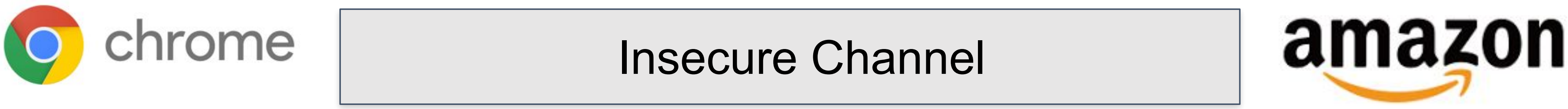


Insecure Channel

X.509 Certificate Transparency using Blockchain

- **Project Description:** Secure Communication over Internet

(pk_A) $(\mathsf{pk}_A, \mathsf{sk}_A)$

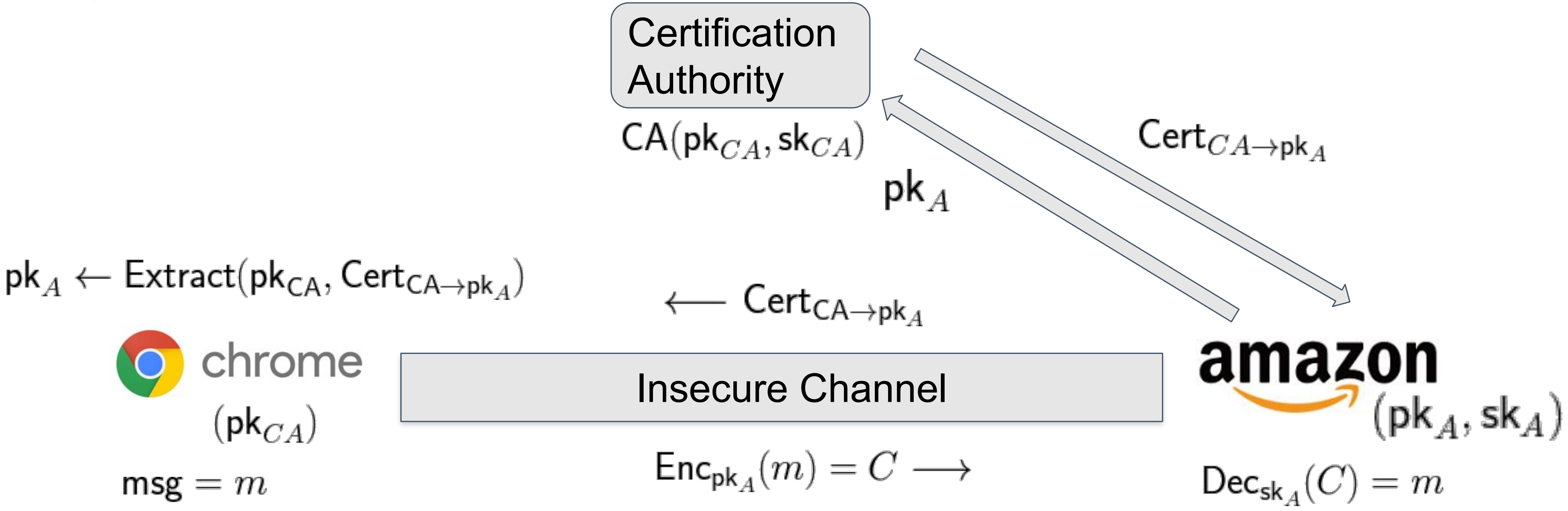


$\mathsf{msg} = m$ $\mathsf{Enc}_{\mathsf{pk}_A}(m) = C \longrightarrow$ $\mathsf{Dec}_{\mathsf{sk}_A}(C) = m$

Assumption: $\textit{Amazon's public key is } \mathsf{pk}_A$

X.509 Certificate Transparency using Blockchain

- **Project Description**: Secure Communication over Internet



Certification Authority

$\mathsf{CA}(\mathsf{pk}_{CA}, \mathsf{sk}_{CA})$

pk_A

$\mathsf{Cert}_{CA \to \mathsf{pk}_A}$

$\mathsf{pk}_A \leftarrow \mathsf{Extract}(\mathsf{pk}_{\mathsf{CA}}, \mathsf{Cert}_{\mathsf{CA} \to \mathsf{pk}_A})$

$\longleftarrow \mathsf{Cert}_{\mathsf{CA} \to \mathsf{pk}_A}$

chrome

(pk_{CA})

$\mathsf{msg} = m$

Insecure Channel

$\mathsf{Enc}_{\mathsf{pk}_A}(m) = C \longrightarrow$

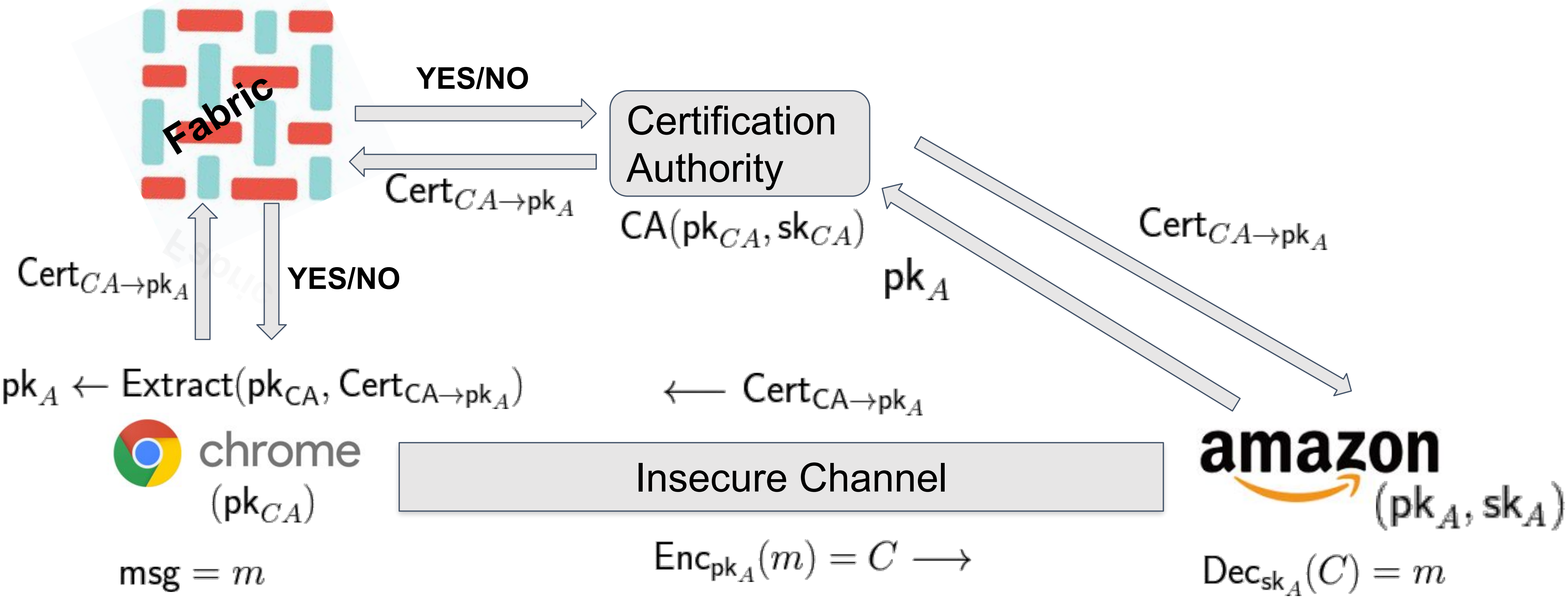
amazon

$(\mathsf{pk}_A, \mathsf{sk}_A)$

$\mathsf{Dec}_{\mathsf{sk}_A}(C) = m$

Assumption: *We must trust CA's*

X.509 Certificate Transparency using Blockchain



Fabric

YES/NO

Certification Authority

$\mathsf{Cert}_{CA\to \mathsf{pk}_A}$

$\mathsf{CA}(\mathsf{pk}_{CA}, \mathsf{sk}_{CA})$

$\mathsf{Cert}_{CA\to \mathsf{pk}_A}$

YES/NO

pk_A

$\mathsf{Cert}_{CA\to \mathsf{pk}_A}$

$\mathsf{pk}_A \leftarrow \mathsf{Extract}(\mathsf{pk}_{\mathsf{CA}}, \mathsf{Cert}_{\mathsf{CA}\to \mathsf{pk}_A})$

$\longleftarrow \mathsf{Cert}_{\mathsf{CA}\to \mathsf{pk}_A}$

chrome

(pk_{CA})

Insecure Channel

amazon

$(\mathsf{pk}_A, \mathsf{sk}_A)$

$\mathsf{msg} = m$

$\mathsf{Enc}_{\mathsf{pk}_A}(m) = C \longrightarrow$

$\mathsf{Dec}_{\mathsf{sk}_A}(C) = m$

~~**Assumption:** *We must trust CA's*~~

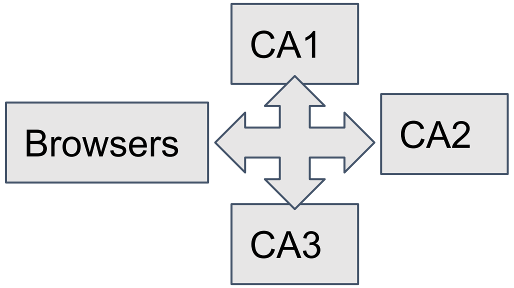
Blockchain ensures CA accountability

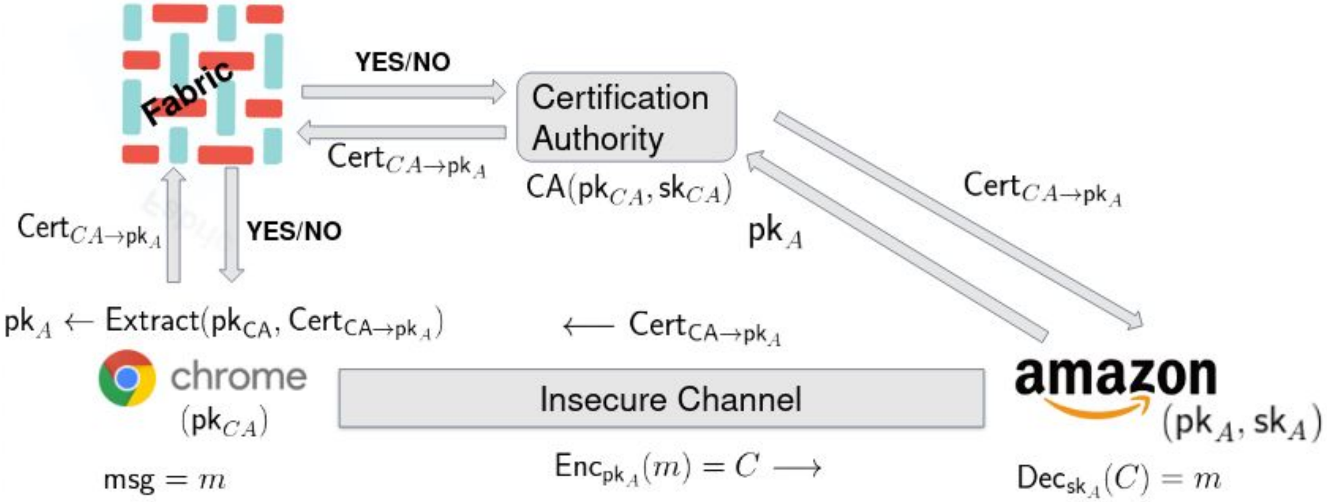
X509 Certificate Transparency using fabric

- **Project Objectives**:
  - Development of client application for Certificate Authority organisation
  - Setting up the CTB over cloud.
  - Browser extension for client side validation of certificates.
  - Benchmarking CTB-assisted SSL/TLS handshake duration

X509 Certificate Transparency using fabric

- **Project Deliverables:** Demo
  - CTB has CAs and browsers as its peers

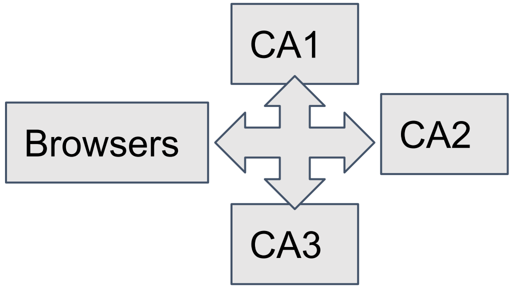


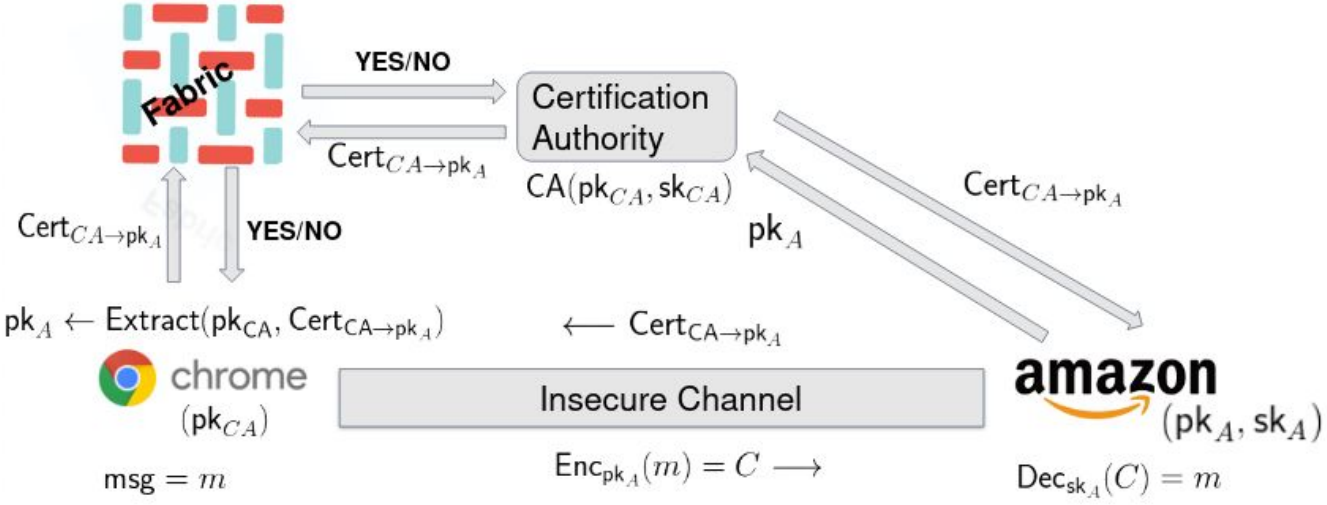

Fabric
YES/NO
Certification Authority
$\mathsf{Cert}_{CA\to \mathsf{pk}_A}$
$\mathsf{CA}(\mathsf{pk}_{CA}, \mathsf{sk}_{CA})$
$\mathsf{Cert}_{CA\to \mathsf{pk}_A}$
YES/NO
pk_A
$\mathsf{Cert}_{CA\to \mathsf{pk}_A}$
$\mathsf{pk}_A \leftarrow \mathsf{Extract}(\mathsf{pk}_{\mathsf{CA}}, \mathsf{Cert}_{\mathsf{CA}\to \mathsf{pk}_A})$
$\longleftarrow \mathsf{Cert}_{\mathsf{CA}\to \mathsf{pk}_A}$
chrome
(pk_{CA})
Insecure Channel
amazon
$(\mathsf{pk}_A, \mathsf{sk}_A)$
$\mathsf{msg} = m$
$\mathsf{Enc}_{\mathsf{pk}_A}(m) = C \longrightarrow$
$\mathsf{Dec}_{\mathsf{sk}_A}(C) = m$

- CAs can submit certificates (that they issue to different domain owners) to CTB
- Browsers can query certificates (that they receive from domain owners over https connections) to CTB

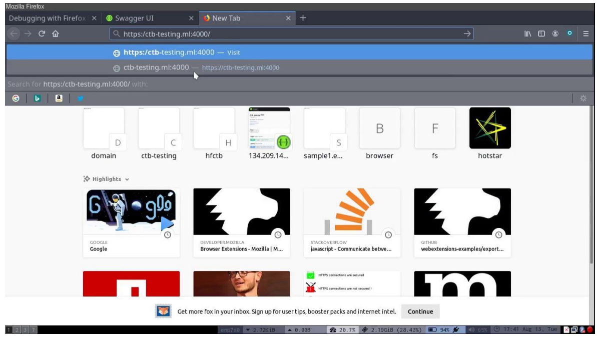
X509 Certificate Transparency using fabric

- **Project Deliverables:** Demo
  - CTB has CAs and browsers as its peers




Fabric
YES/NO
Certification Authority
$\mathsf{Cert}_{CA\to\mathsf{pk}_A}$
$\mathsf{CA}(\mathsf{pk}_{CA}, \mathsf{sk}_{CA})$
$\mathsf{Cert}_{CA\to\mathsf{pk}_A}$
YES/NO
pk_A
$\mathsf{Cert}_{CA\to\mathsf{pk}_A}$
$\mathsf{pk}_A \leftarrow \mathsf{Extract}(\mathsf{pk}_{\mathsf{CA}}, \mathsf{Cert}_{\mathsf{CA}\to\mathsf{pk}_A})$
$\longleftarrow \mathsf{Cert}_{\mathsf{CA}\to\mathsf{pk}_A}$
chrome
(pk_{CA})
Insecure Channel
amazon
$(\mathsf{pk}_A, \mathsf{sk}_A)$
$\mathsf{msg} = m$
$\mathsf{Enc}_{\mathsf{pk}_A}(m) = C \longrightarrow$
$\mathsf{Dec}_{\mathsf{sk}_A}(C) = m$

- CAs can submit certificates (that they issue to different domain owners) to CTB
- Browsers can query certificates (that they receive from domain owners over https connections) to CTB
- Demo 1
  - **CA submitting the certificate to CTB**
  - **Exhibit Client-server connection = firefox connecting to ctb-testing.ml**



https:/ctb-testing.ml:4000/

https:/ctb-testing.ml:4000 — Visit

ctb-testing.ml:4000 — https://ctb-testing.ml:4000

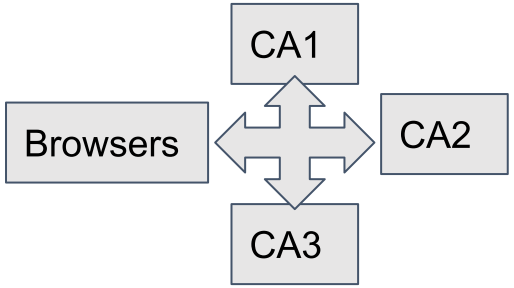
Search for https:/ctb-testing.ml:4000/ with:

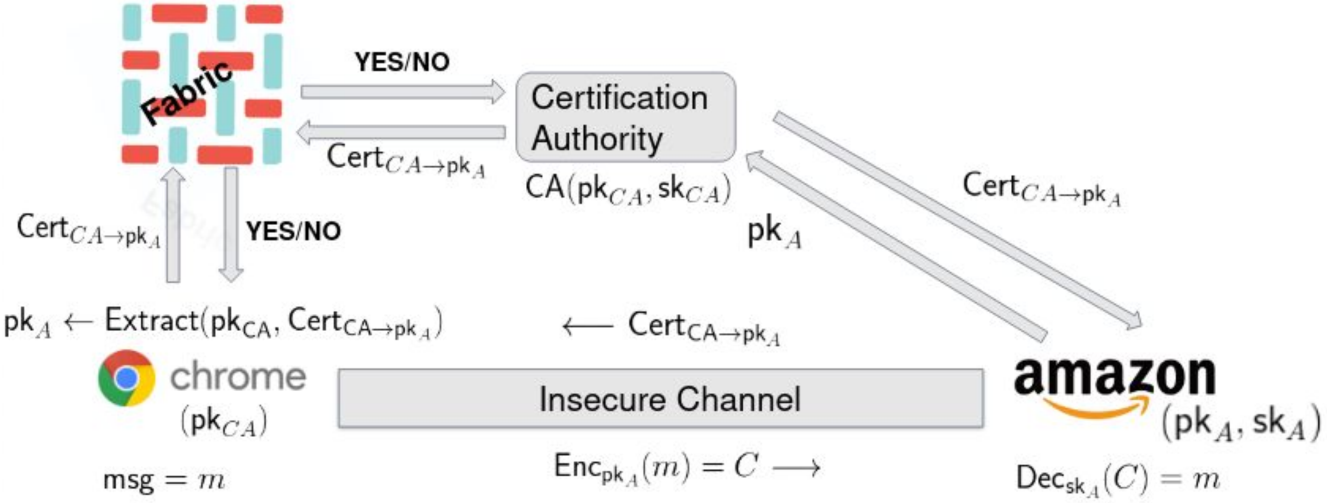
Get more fox in your inbox. Sign up for user tips, booster packs and internet intel.

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

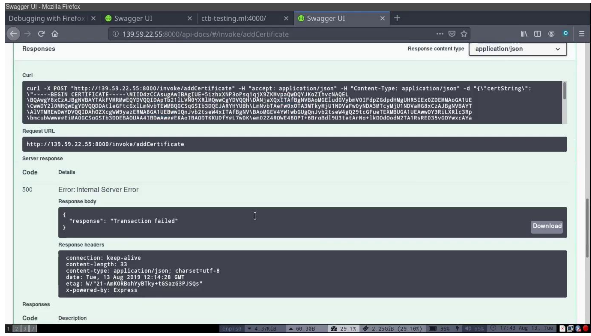
X509 Certificate Transparency using fabric

- **Project Deliverables:** Demo
  - CTB has CAs and browsers as its peers




Fabric
YES/NO
Certification Authority
$\text{Cert}_{CA \to \text{pk}_A}$
$\text{CA}(\text{pk}_{CA}, \text{sk}_{CA})$
$\text{Cert}_{CA \to \text{pk}_A}$
$\text{Cert}_{CA \to \text{pk}_A}$
YES/NO
pk_A
$\text{pk}_A \leftarrow \text{Extract}(\text{pk}_{\text{CA}}, \text{Cert}_{\text{CA} \to \text{pk}_A})$
$\longleftarrow \text{Cert}_{\text{CA} \to \text{pk}_A}$
chrome
(pk_{CA})
Insecure Channel
amazon
$(\text{pk}_A, \text{sk}_A)$
$\text{msg} = m$
$\text{Enc}_{\text{pk}_A}(m) = C \longrightarrow$
$\text{Dec}_{\text{sk}_A}(C) = m$

- CAs can submit certificates (that they issue to different domain owners) to CTB
- Browsers can query certificates (that they receive from domain owners over https connections) to CTB
- Demo 2
  - **Another CA issuing certificate for ctb-testing.ml and show that it will not be allowed**
  - **Pick another domain: google.com for which the certificate is not available at CTB**
  - **Exhibit the firefox failing to connect to google.com**



Curl

```
curl -X POST "http://139.59.22.55:8000/invoke/addCertificate" -H "accept: application/json" -H "Content-Type: application/json" -d "{\"certString\":
\"-----BEGIN CERTIFICATE-----\MIID4zCCAsugAwIBAgIUE+5izhxXNP3oPsq1qjX9ZKMvpaQwDQYJKoZIhvcNAQEL
\BQAwgY8xCzAJBgNVBAYTAkFVMRMwEQYDVQQIDApTb21lLVN0YXRlMQwwCgYDVQQH\DANjaXQxITAfBgNVBAoMGEludGVybmV0IFdpZGdpdHMgUHR5IEx0ZDEMMAoGA1UE
\CwwDY2l0MRQwEgYDVQQDDAtleGFtcGxlLmNvbTEWMBQGCSqGSIb3DQEJARYHYUBh\LmNvbTAeFw0xOTA3MTkyMjU1NDVaFw0yNDA3MTcyMjU1NDVaMG8xCzAJBgNVBAYT
\AlVTMREwDwYDVQQIDAhOZXcgWW9yazERMA8GA1UEBwwIQnJvb2tseW4xITAfBgNV\BAoMGEV4YW1wbGUgQnJvb2tseW4gQ29tcGFueTEXMBUGA1UEAwwOY3RiLXRlc3Rp
\bmcubWwwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDTKKUDfYgL7w0K\em02Z4ROWE48OPI+6BrgBdl9U3tetArNq+lkDOdOodN2TA1RsRE035vGOYwxcAYa
```

Request URL

```
http://139.59.22.55:8000/invoke/addCertificate
```

Server response

Code	Details
500	Error: Internal Server Error

Response body

```
{
  "response": "Transaction failed"
}
```

Response headers

```
connection: keep-alive
content-length: 33
content-type: application/json; charset=utf-8
date: Tue, 13 Aug 2019 12:14:28 GMT
etag: W/"21-AmKORBohYyBTky+tGSazG3PJSQs"
x-powered-by: Express
```

Responses

Code	Description

```
1 2 3 7    enp7s0  ▾ 4.37KiB  ▴ 60.30B  29.1%  2.25GiB (29.10%)  95%  65%  17:43 Aug 13, Tue
```

Implementation details of chaincode are available [Paper]

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

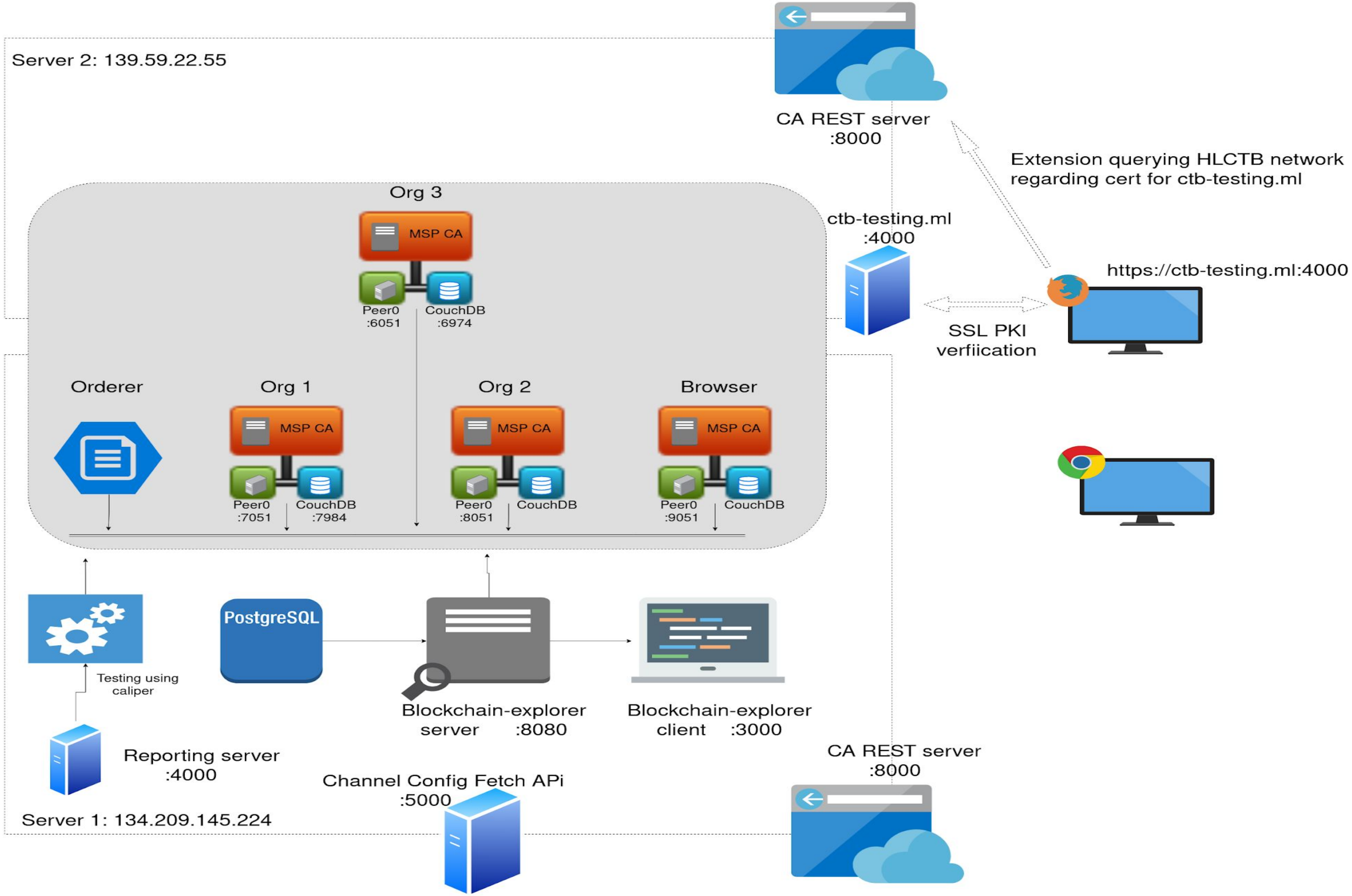
X509 Certificate Transparency using fabric

- **Project Deliverables:**

- Implementing CA REST server
- Firefox extension for certificate verification
- Deployment of CTB^{hf} to digitalocean
- Documentation of every step involved
- Testing fabric@1.4 for TPS and how to scaling it for multiple CAs
- Code and all the configuring are available @https://github.com/harsh-98/ctb

X509 Certificate Transparency using fabric

Architecture of CTB^{hf} network:



HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

X509 Certificate Transparency using fabric

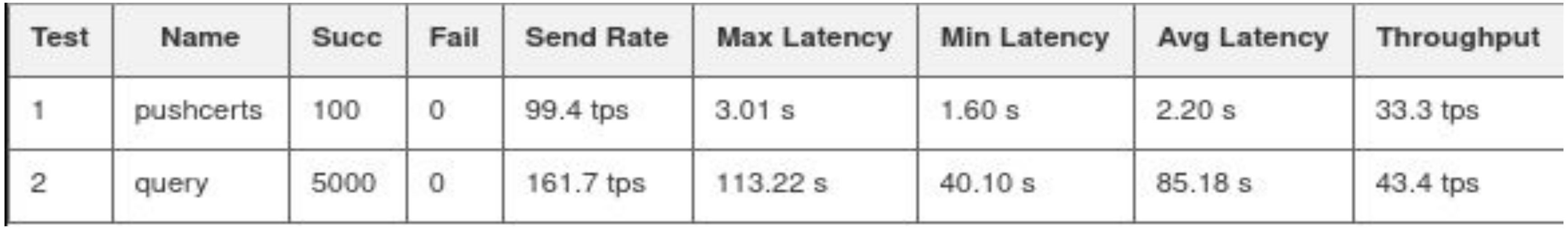
Testing:

We have tested our fabric network spread over two servers, running in docker environment. Fabric@1.4 is used.

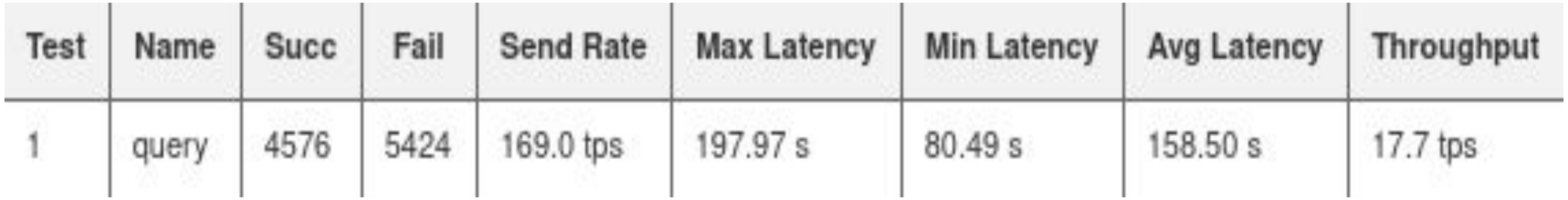
Caliper was used for testing two types of transactions:

Pushcerts: addition of certificates to fabric

Query: Getting certificate for a particular domain



Test	Name	Succ	Fail	Send Rate	Max Latency	Min Latency	Avg Latency	Throughput
1	pushcerts	100	0	99.4 tps	3.01 s	1.60 s	2.20 s	33.3 tps
2	query	5000	0	161.7 tps	113.22 s	40.10 s	85.18 s	43.4 tps



Test	Name	Succ	Fail	Send Rate	Max Latency	Min Latency	Avg Latency	Throughput
1	query	4576	5424	169.0 tps	197.97 s	80.49 s	158.50 s	17.7 tps

We have gone through some of the papers on scaling hyperledger upto 20000 TPS.. LINK

This requires new features which are planned to be implemented in fabric@2.0.

X509 Certificate Transparency using fabric

Project Execution & Accomplishments:

- List of completed tasks are available on hyerpledger wiki.
- Adding a new org to live CTB^{hf} network and modifying certificate for IP SANs
- Testing the network required working and maintaining multiple machines.
- I have been active on chat.hyperledger.org, mainly caliper, fabric and fabric-kubernetes channels.
- Jira platform has been very useful. I usually got a response on the issue within 2-3 hrs. Link Link

X509 Certificate Transparency using fabric

› **Recommendations for future work:**

› Currently, we are working on revocation part of certificate in more detail. Going through CRL, OCSP and OCSP stapling.

› Chrome extension: currently chrome is missing API through which extension can get SSL data. Once it is available, we plan to build chrome extension too.

› We plan to test our configuring on more servers with different number of CA orgs.

THANK YOU

Any questions?

You can find me at: @harsh-98 harshjniitr@gmail.com