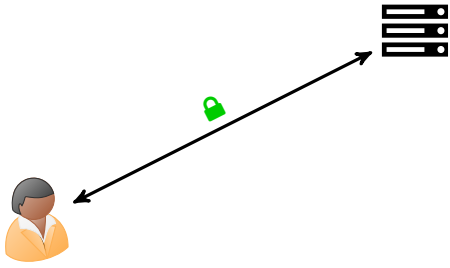
TLS-N: Non-repudiation over TLS
Enabling Ubiquitous Content Signing

Hubert Ritzdorf, **Karl Wüst**, Arthur Gervais, Guillaume Felley, Srdjan Čapkun

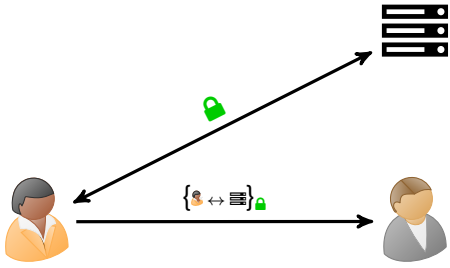
ETH Zurich

TLS

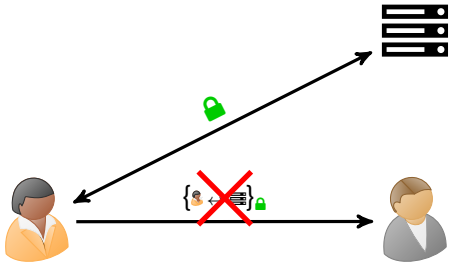
TLS



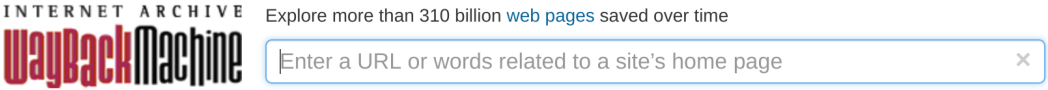
TLS



TLS



Web Archives



This is Google's cache of https://www.ndss-symposium.org/. It is a snapshot of the page as it appeared on 18 Feb 2018 22:09:23 GMT. The current page could have changed in the meantime. Learn more

Full version Text-only version View source

How can we get reliable data into the blockchain?

Blockchain

World

How can we get reliable data into the blockchain?

Blockchain

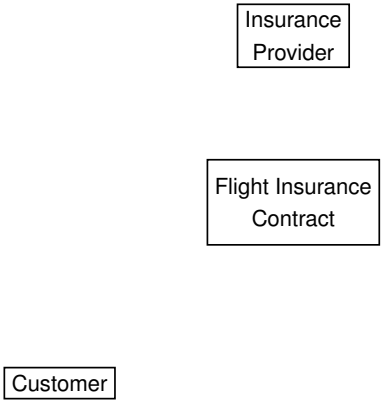
Oracle

World

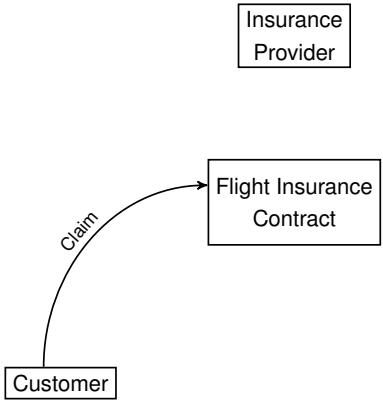
How can we get reliable data into the blockchain?

How can we get reliable data into the blockchain?

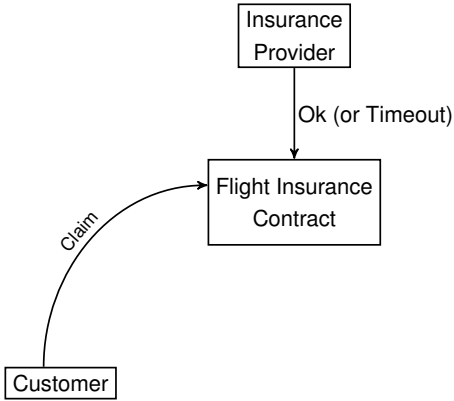
Example: Flight Insurance



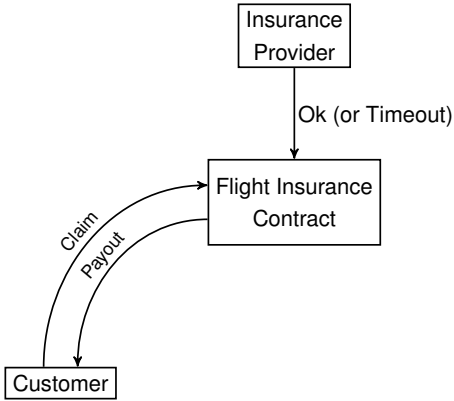
Example: Flight Insurance



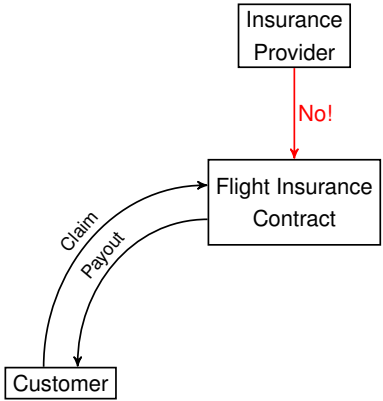
Example: Flight Insurance



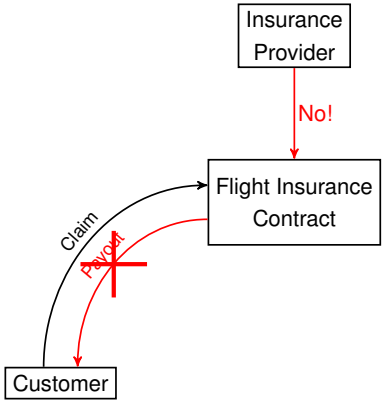
Example: Flight Insurance



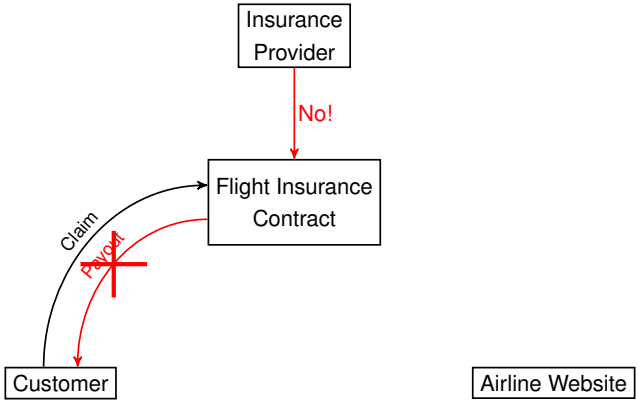
Example: Flight Insurance



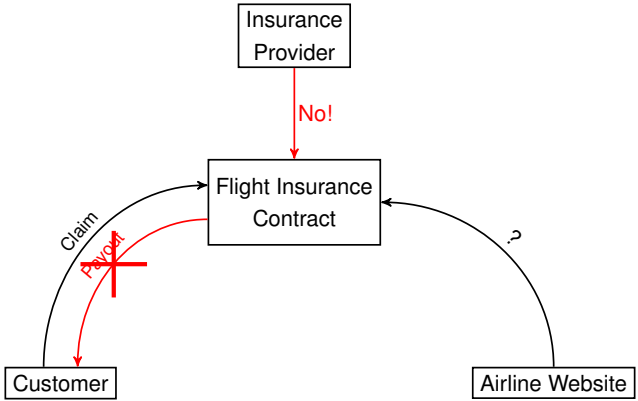
Example: Flight Insurance



Example: Flight Insurance



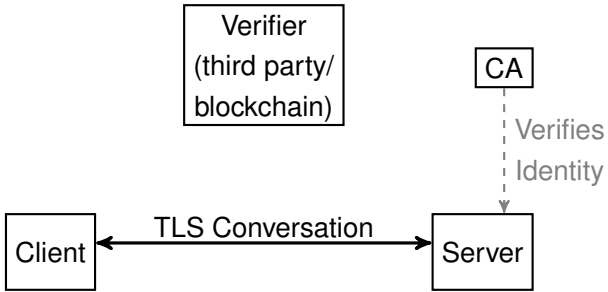
Example: Flight Insurance



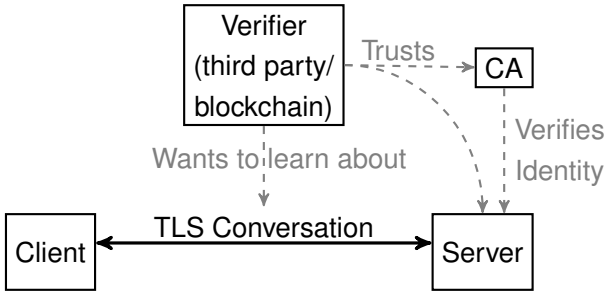
Contributions

- First secure TLS extension for non-repudiation
- Decentralized Blockchain Oracle
- Implementation using the NSS library
- Ethereum library for proof verification

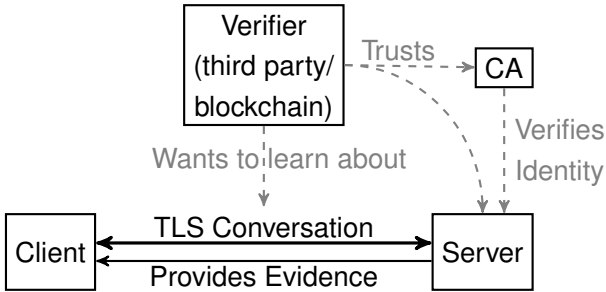
Non-Repudiation for TLS



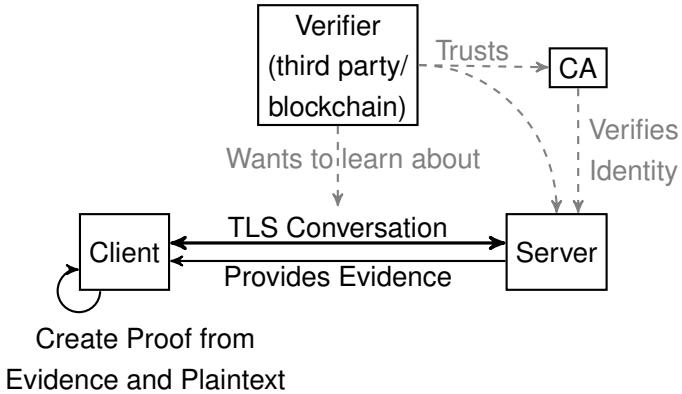
Non-Repudiation for TLS



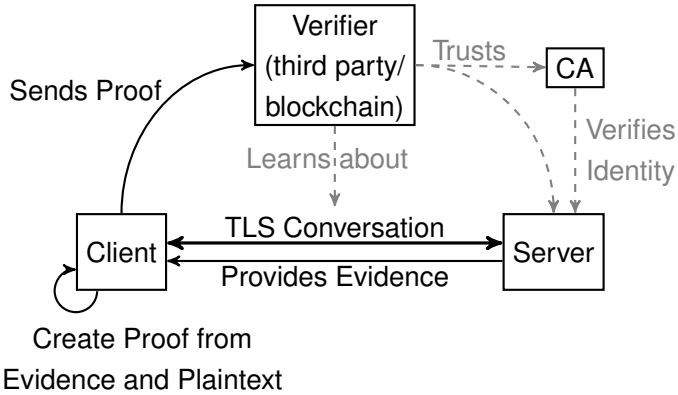
Non-Repudiation for TLS



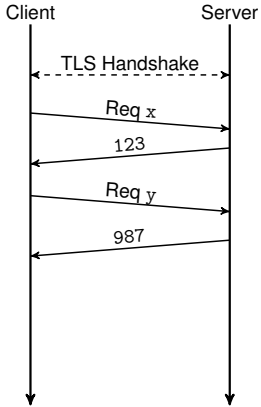
Non-Repudiation for TLS



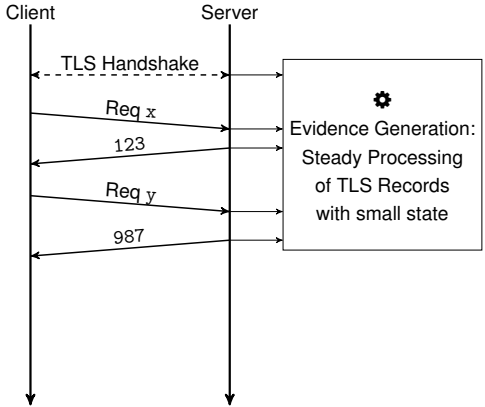
Non-Repudiation for TLS



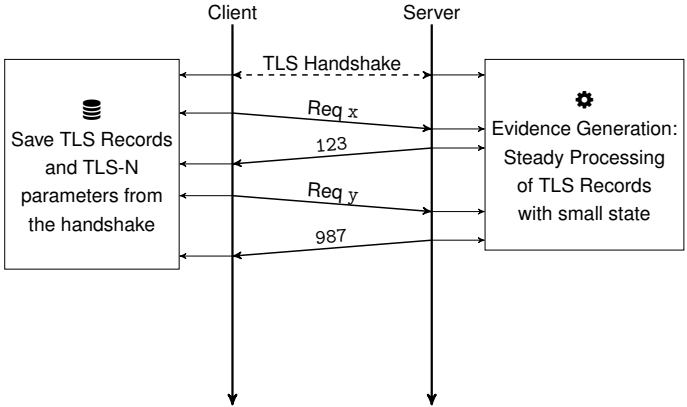
TLS-N Overview



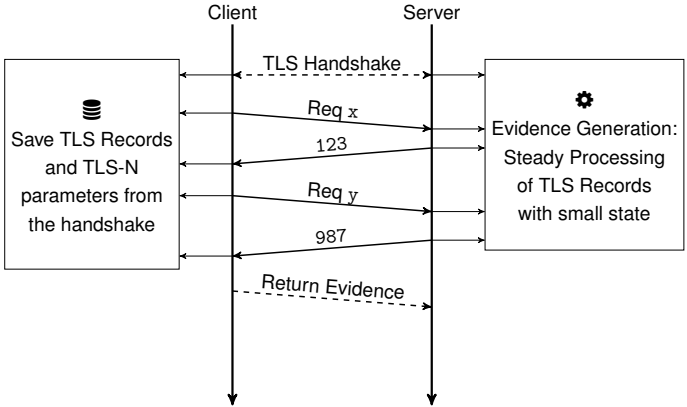
TLS-N Overview



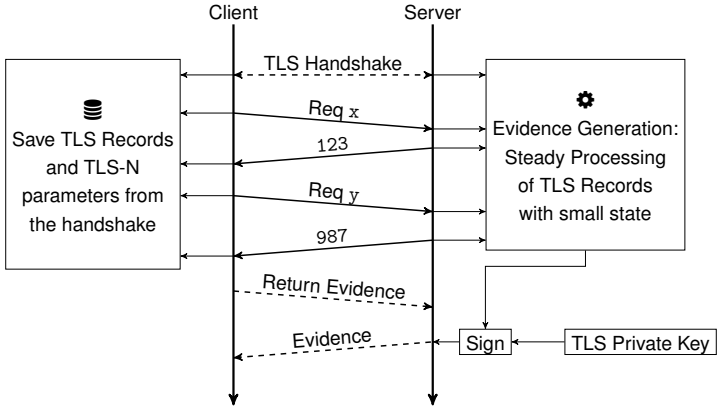
TLS-N Overview



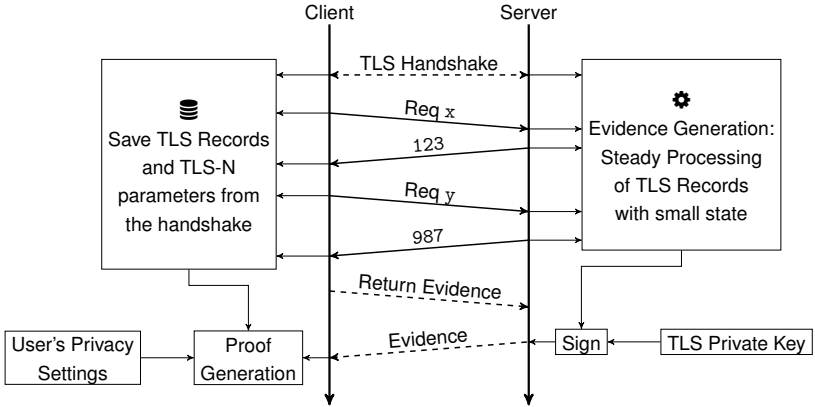
TLS-N Overview



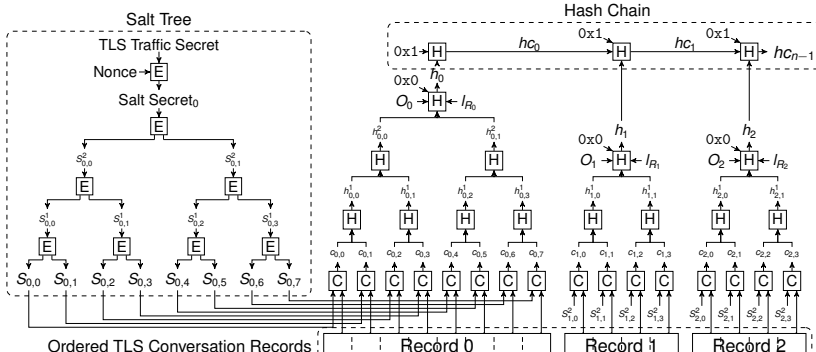
TLS-N Overview



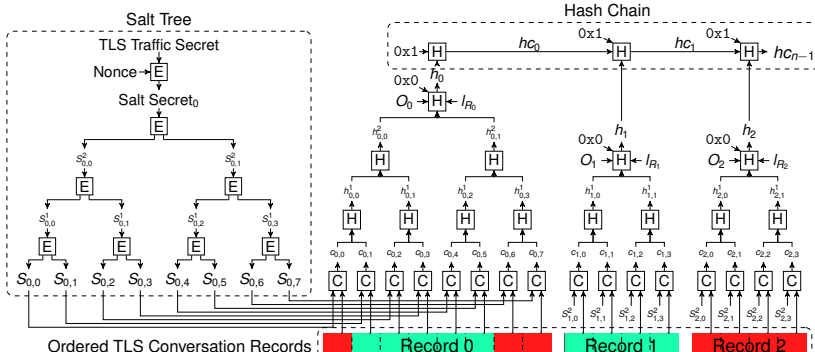
TLS-N Overview



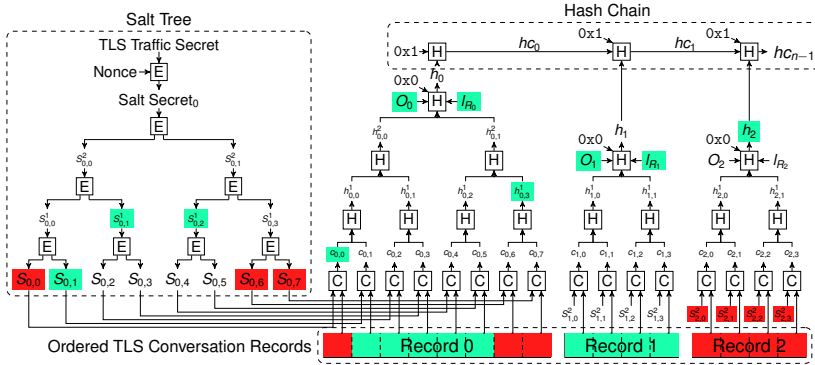
Chunk Level Privacy Protection



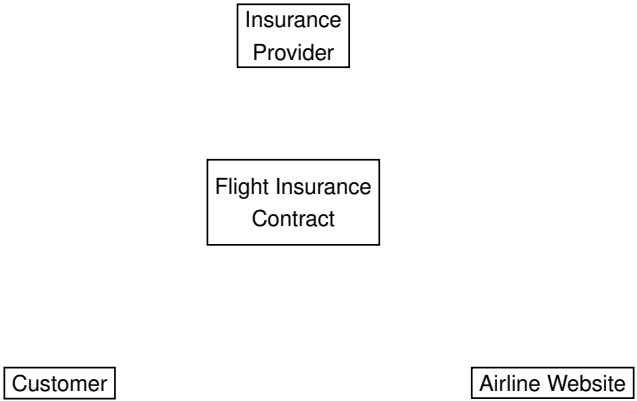
Chunk Level Privacy Protection



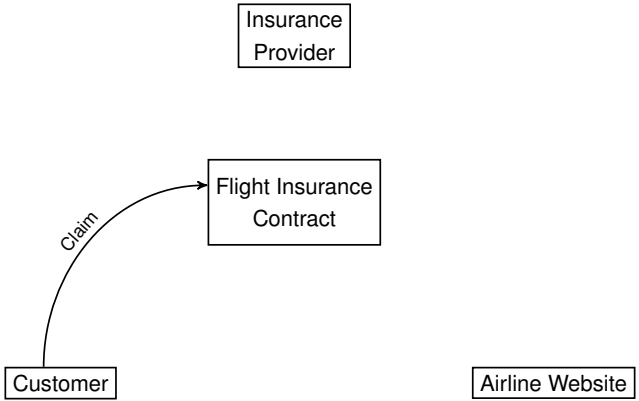
Chunk Level Privacy Protection



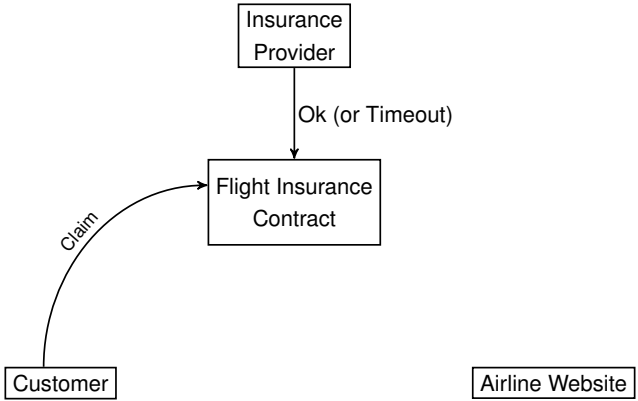
Flight Insurance (1)



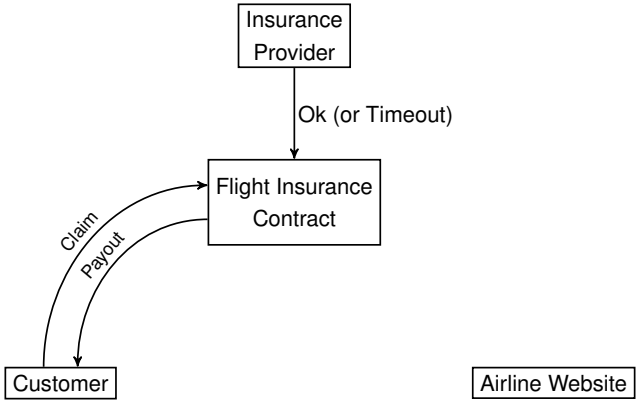
Flight Insurance (1)



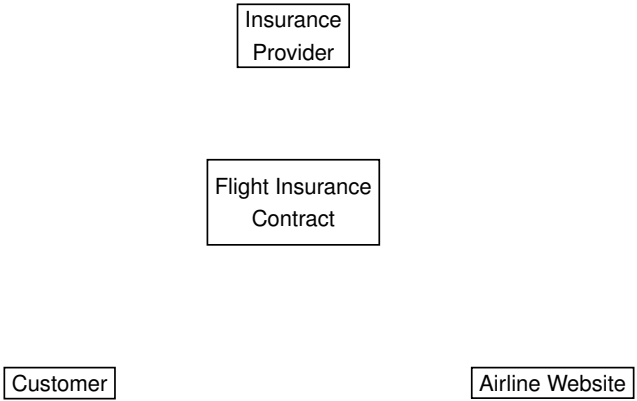
Flight Insurance (1)



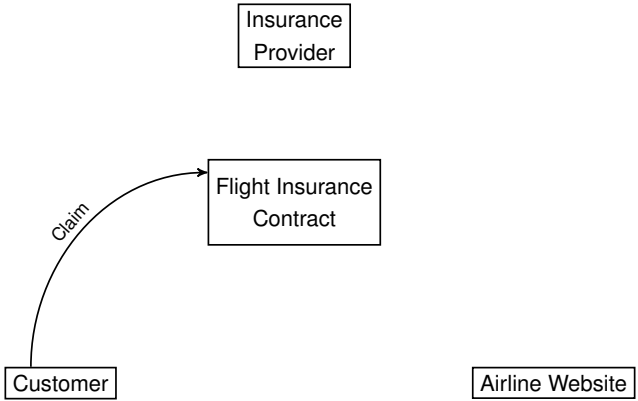
Flight Insurance (1)



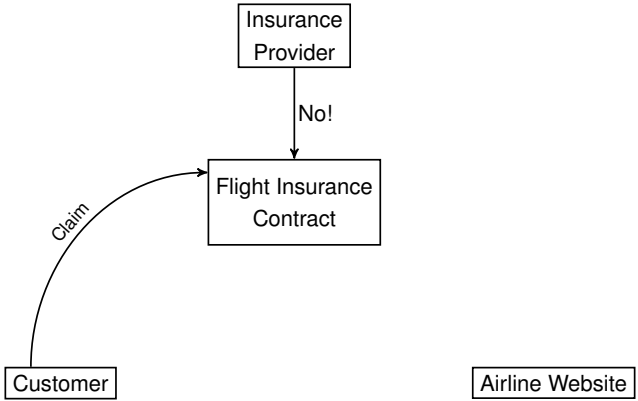
Flight Insurance (2)



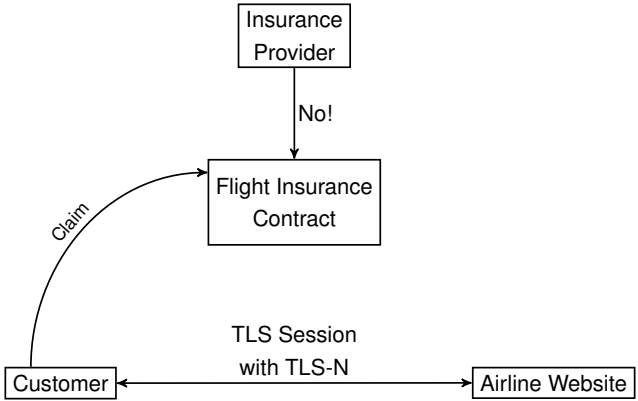
Flight Insurance (2)



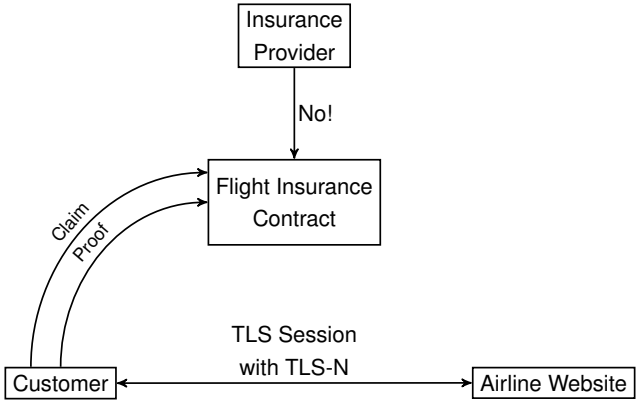
Flight Insurance (2)



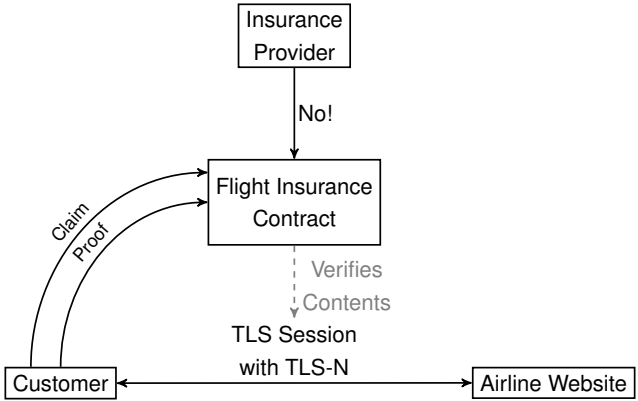
Flight Insurance (2)



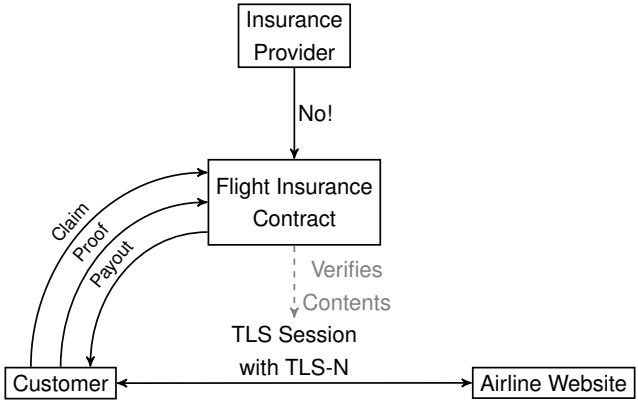
Flight Insurance (2)



Flight Insurance (2)



Flight Insurance (2)



Conclusions

TLS extension for non-repudiation

Conclusions

TLS extension for non-repudiation

- Privacy Preserving

Conclusions

TLS extension for non-repudiation

- Privacy Preserving
- Redactions are visible to verifiers

Conclusions

TLS extension for non-repudiation

- Privacy Preserving
- Redactions are visible to verifiers
- Efficient

Conclusions

TLS extension for non-repudiation

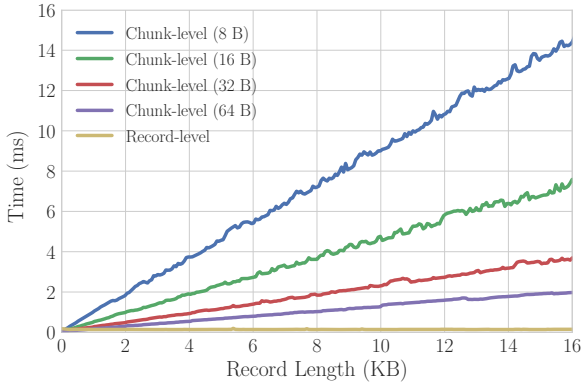
- Privacy Preserving
- Redactions are visible to verifiers
- Efficient
- Acts as decentralized Blockchain Oracle

Try it out: `https://tls-n.org`

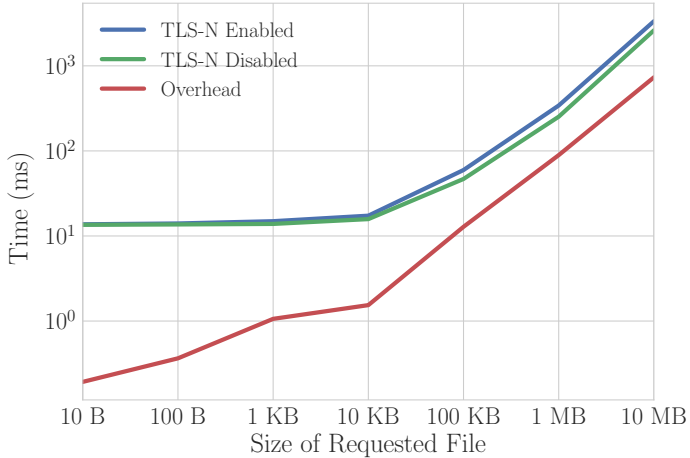
- Interactive Proof Generation
- Code for the TLS extension (NSS library)
- Smart Contract Library
- Example Smart Contract

Questions?

Overhead - Processing Time



Overhead - Requesting a File

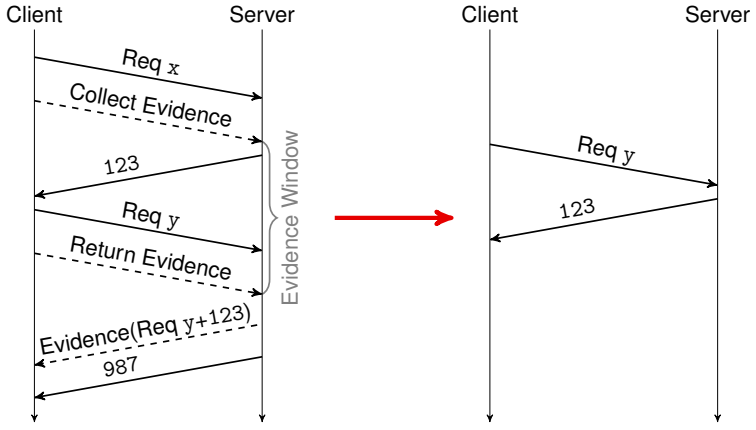


Smart Contract Costs

Costs (2018-01-23)

	Conversation Size			
	1 KB		10 KB	
	secp256r1	secp256k1	secp256r1	secp256k1
Basic Gas	119,758		737,159	
Total Gas	1,284,723	131,286	1,938,872	782,219
Ether	0.0434	0.0044	0.0655	0.0264
USD	41.08	4.20	62.00	25.01

Content Reordering Attack



Privacy

```
GET /me?fields=id&access_token=EAACEdEose0cB...  HTTP/1.1
Host:  graph.facebook.com
```

Privacy

```
GET /me?fields=id&access_token=EAACEdEose0cB...  HTTP/1.1
Host:  graph.facebook.com
```