ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Extending the web-frontend for the cothority-framework

DEDIS - June 2017

Student: Gaylor Bosson
Supervisor: Linus Gasser

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Outline

- **Goals**
- Cothority
- Technologies
- Architecture
- Website Inliner
- Conclusion

Goals

1. Modularity + Extensibility
2. Previous features and more
    a. Keep all the previous features
    b. Use new services (skip-chain)
3. Libraries for mobile application
    a. Crypto
    b. Protobuf
4. Cross-site integration

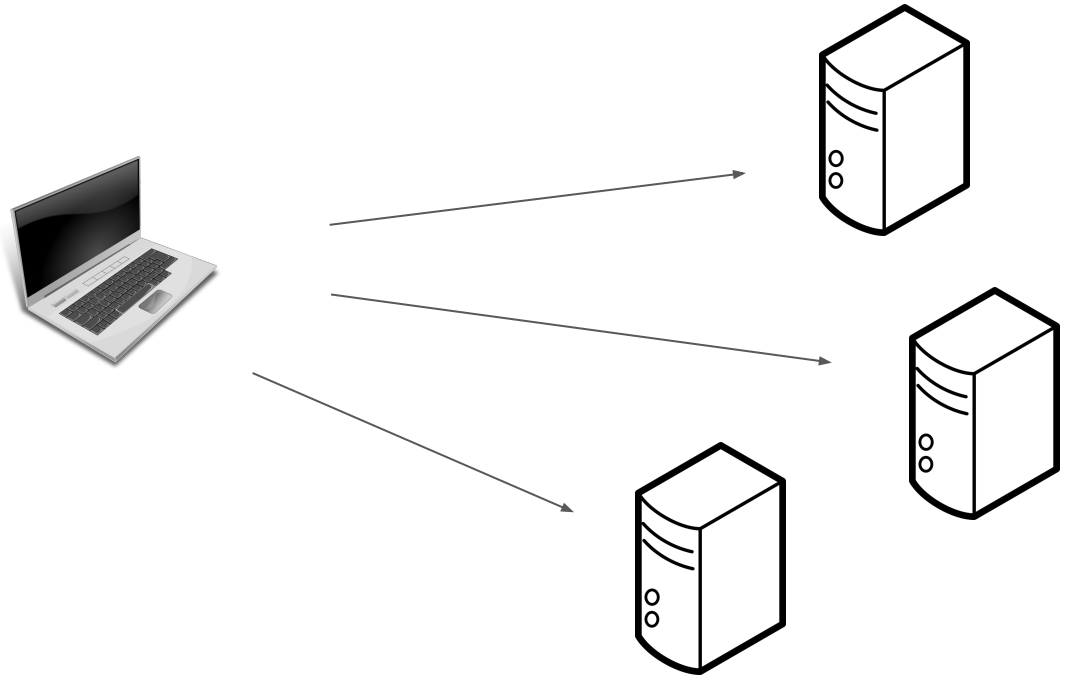
ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Outline

- Goals
- **Cothority**
- Technologies
- Architecture
- Website Inliner
- Conclusion

Cothority - Status

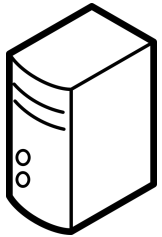
Each node provide a status service to get information about itself



Cothority - CoSi

Given a hash and roster, it provides a sign and verify process

```
message SignatureRequest {
   required bytes message = 1;
   required Roster roster = 2;
}
```



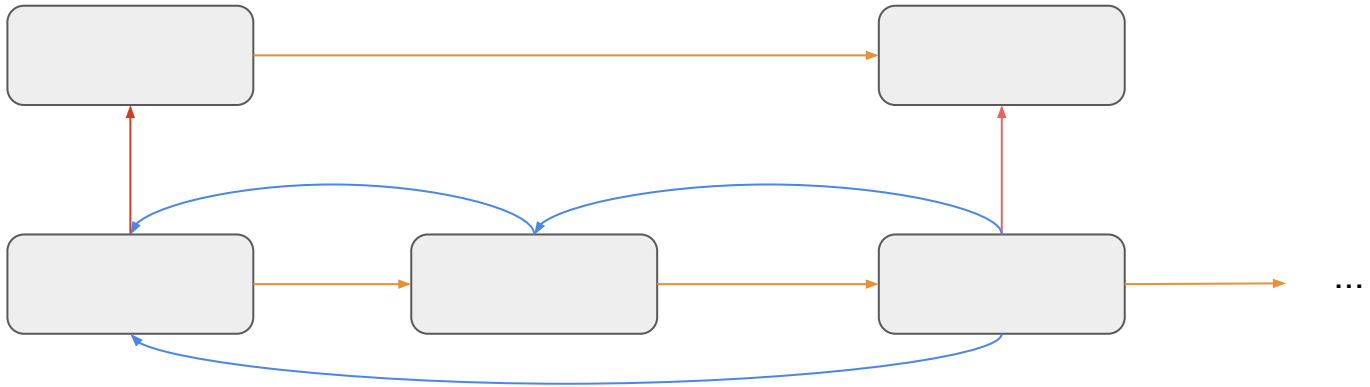
```
message SignatureResponse {
   required bytes hash = 1;
   required bytes signature = 2;
}
```

```
{
    "filename": "7378e468ad6e24925f61560829ca1205.jpg",
    "signature": "134f07469307fc3e4...",
    "hash": "38ab97d8e44...",
    "genesisID": "32bf04100...",
    "blockID": "32bf04100...",
    "offlineServers": [
        "192.33.210.8:7005"
    ]
}
```

Cothority - Skip-chain

It can be used in many ways but we are interested in:

1. Roster
2. HTML content in the data field

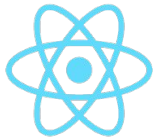


ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Outline

- Goals
- Cothority
- **Technologies**
- Architecture
- Website Inliner
- Conclusion

Technologies



React

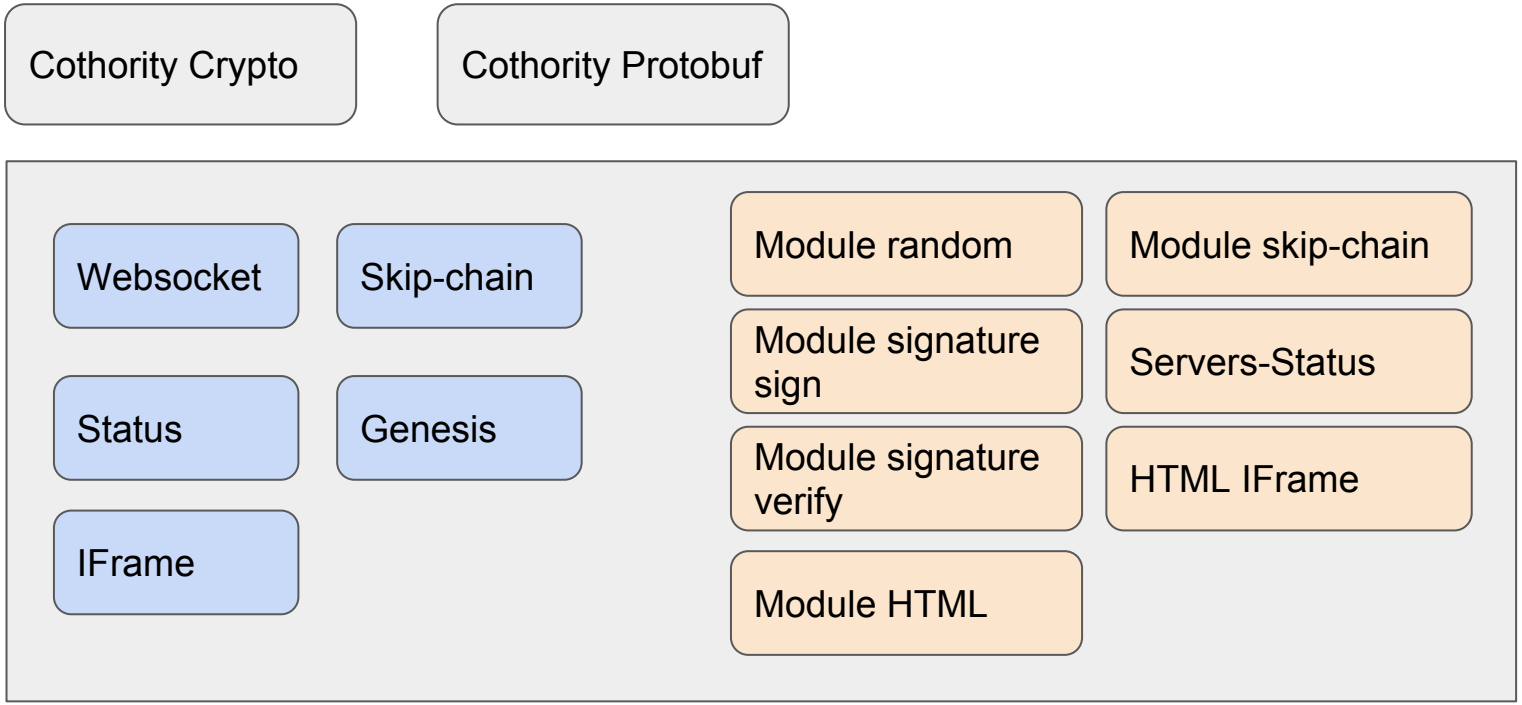
- Create React App
- React Router
- Font Awesome
- Moment
- Reactstrap
- Jest + Enzyme + Faker

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

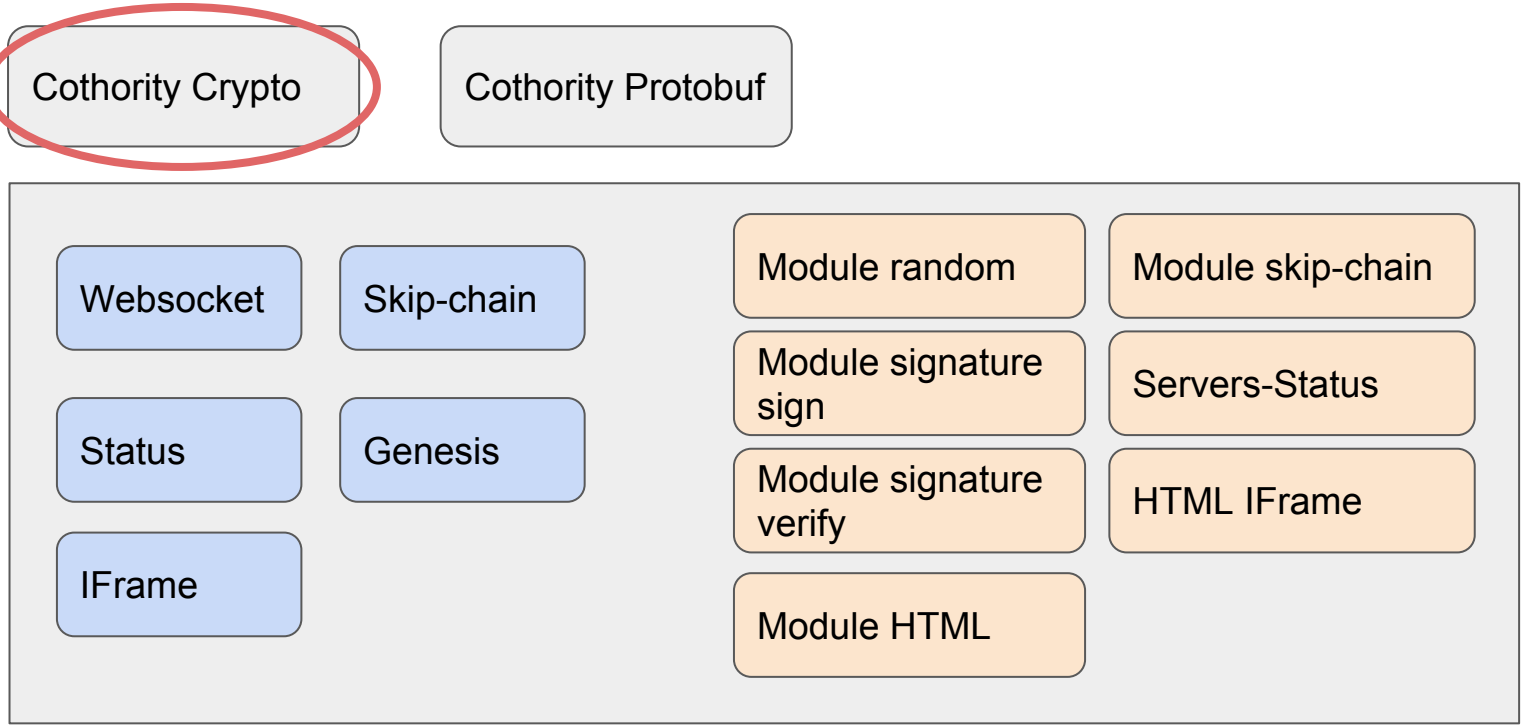
Outline

- Goals
- Cothority
- Technologies
- **Architecture**
- Website Inliner
- Conclusion

Architecture



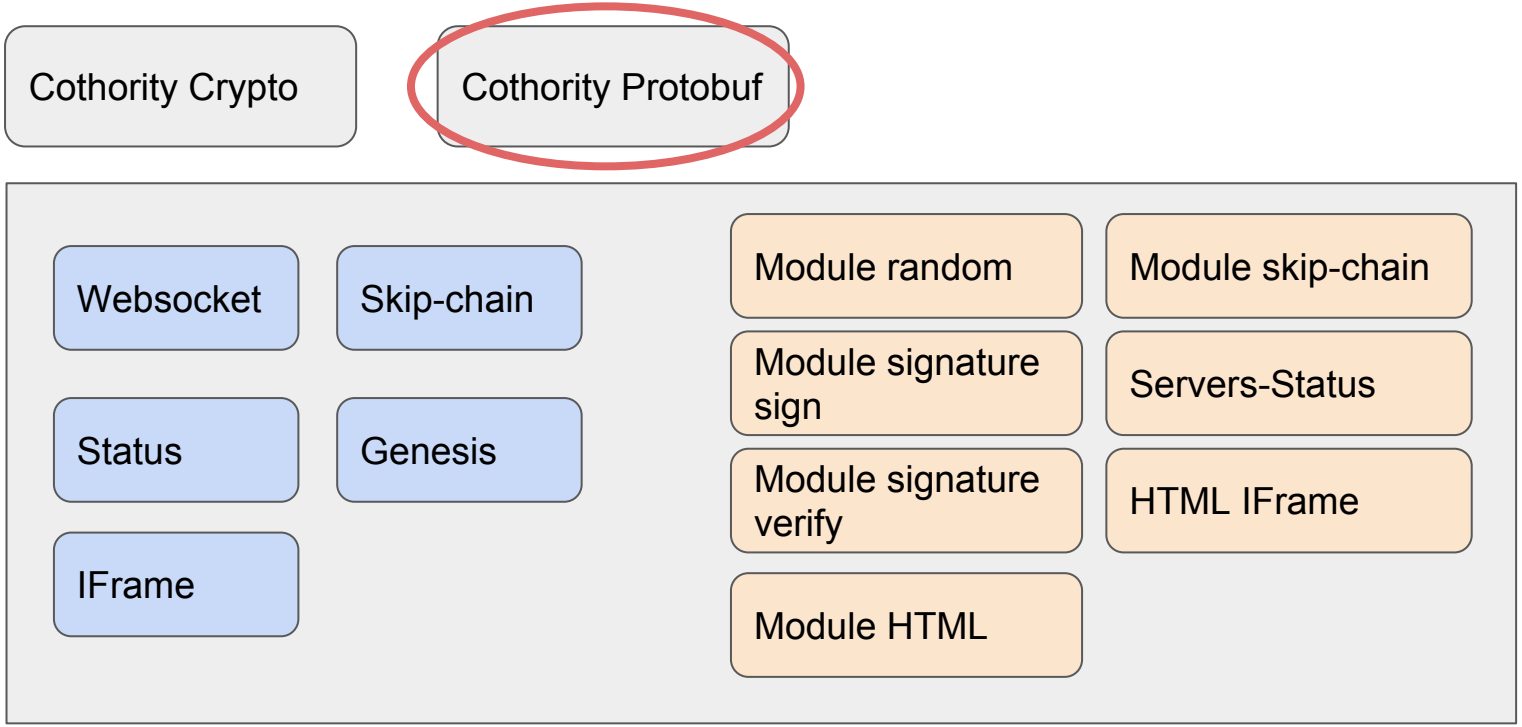
Architecture



Architecture - Cothority Crypto

- GopherJS
- Interface between Go and Javascript
- Primitives
  - Hash
  - Public and Private Keys (i.e. aggregate)
  - Signature
  - Skip-chain

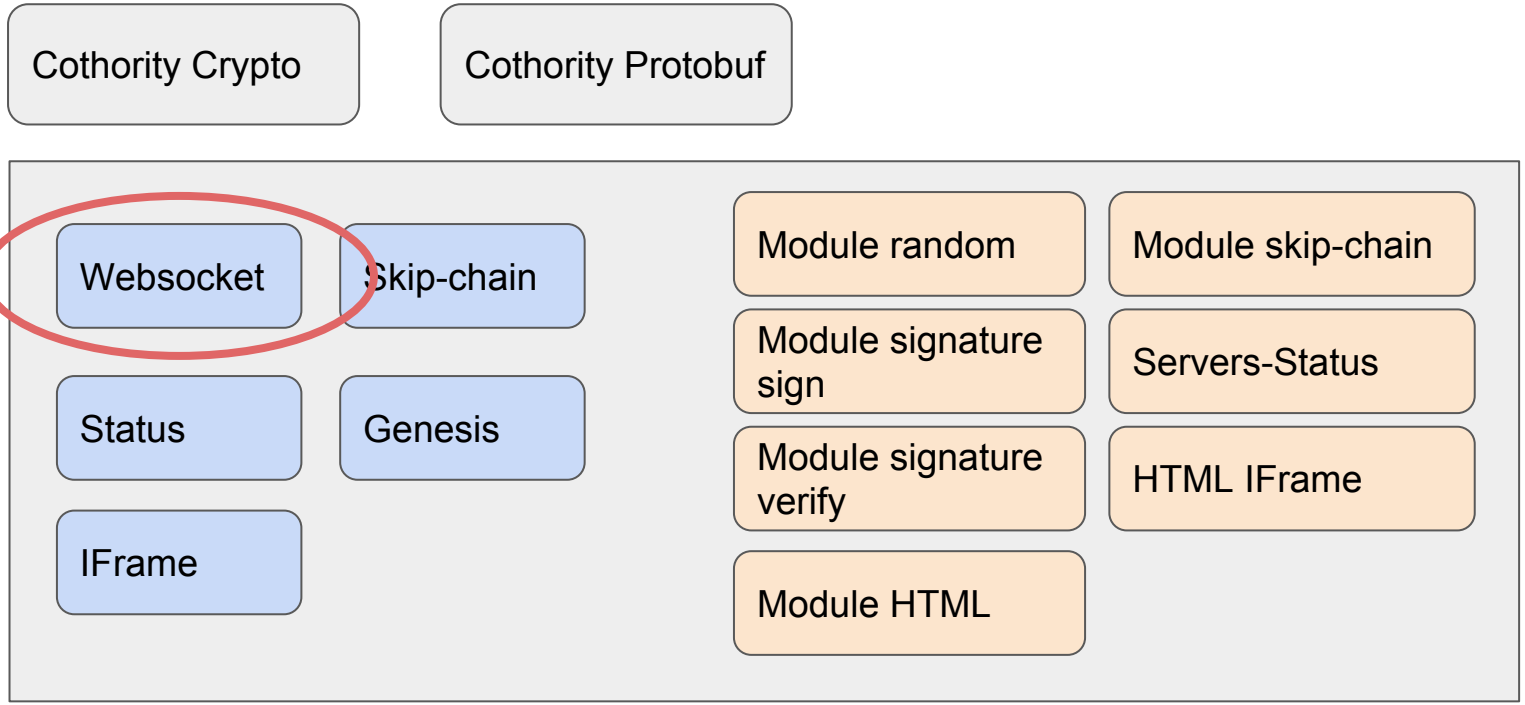
Architecture



Architecture - Cothority Protobuf

- Helper
  - Data types (e.g buffer)
- *.proto definition
- Script to build the .proto files into a javascript file
  - We cannot create a bundle with external .proto files

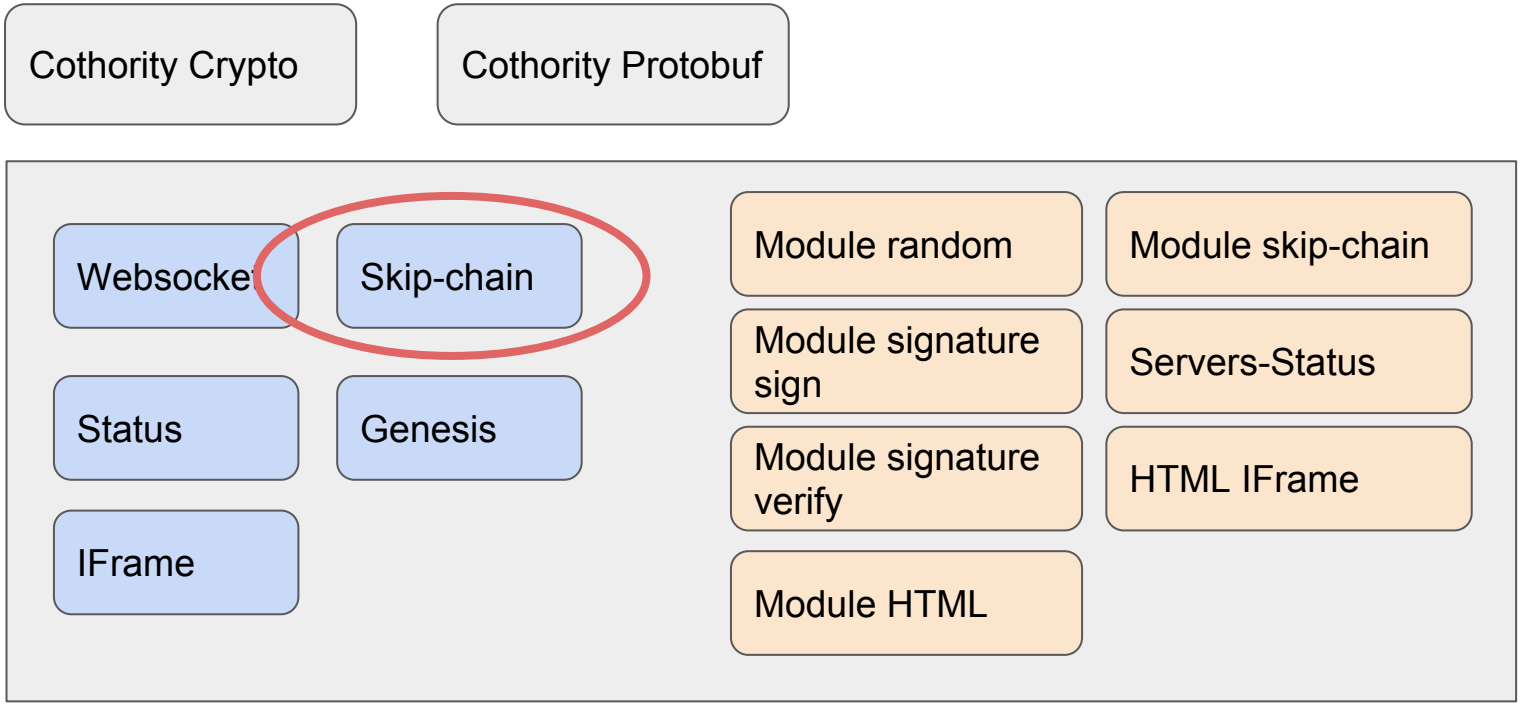
Architecture



Architecture - Websocket service

- Use Cothority Protobuf
- Maintain the websockets
- Provide helpers for the requests to the Cothority

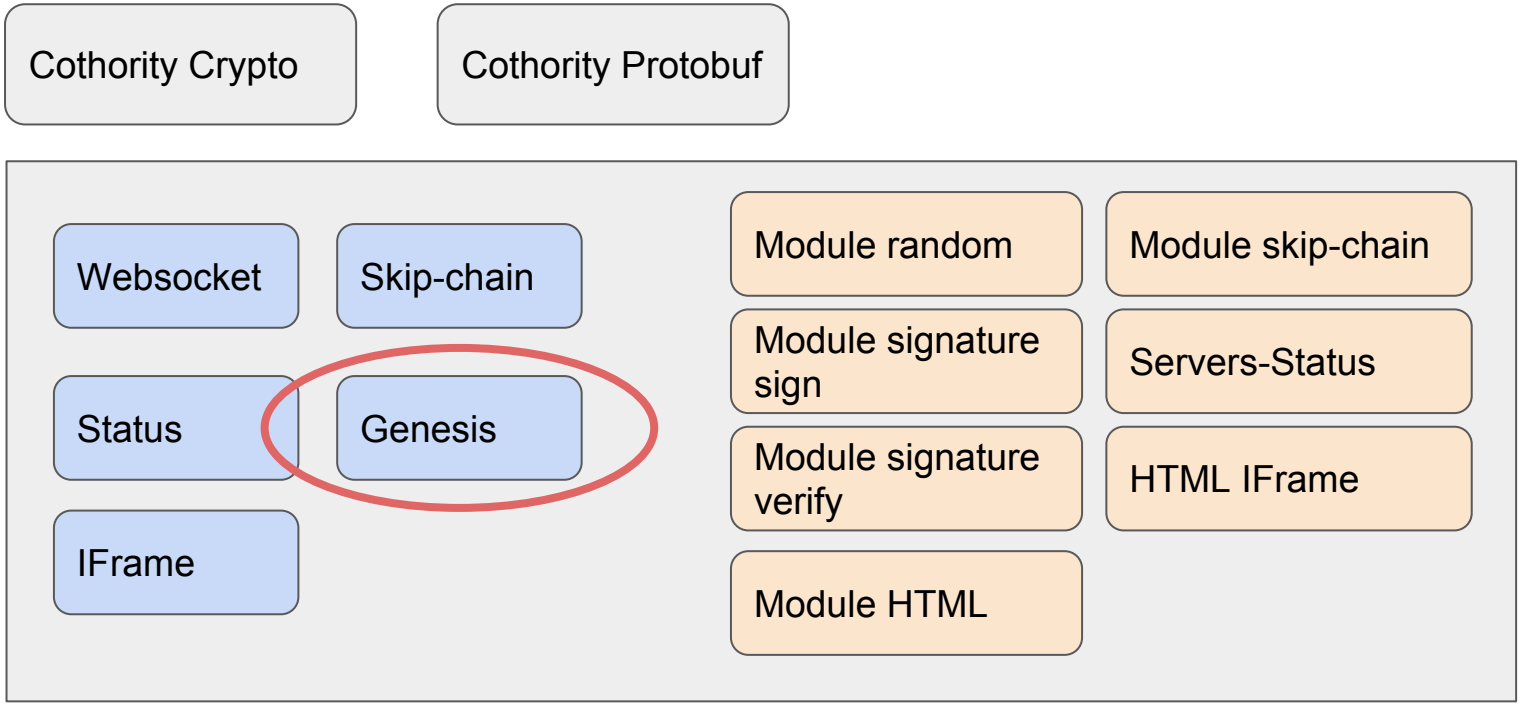
Architecture



Architecture - Skip-chain

- Use the websocket service
- One function => get the skip-chain for a given ID
  - Main role is to verify the integrity of the blocks !

Architecture

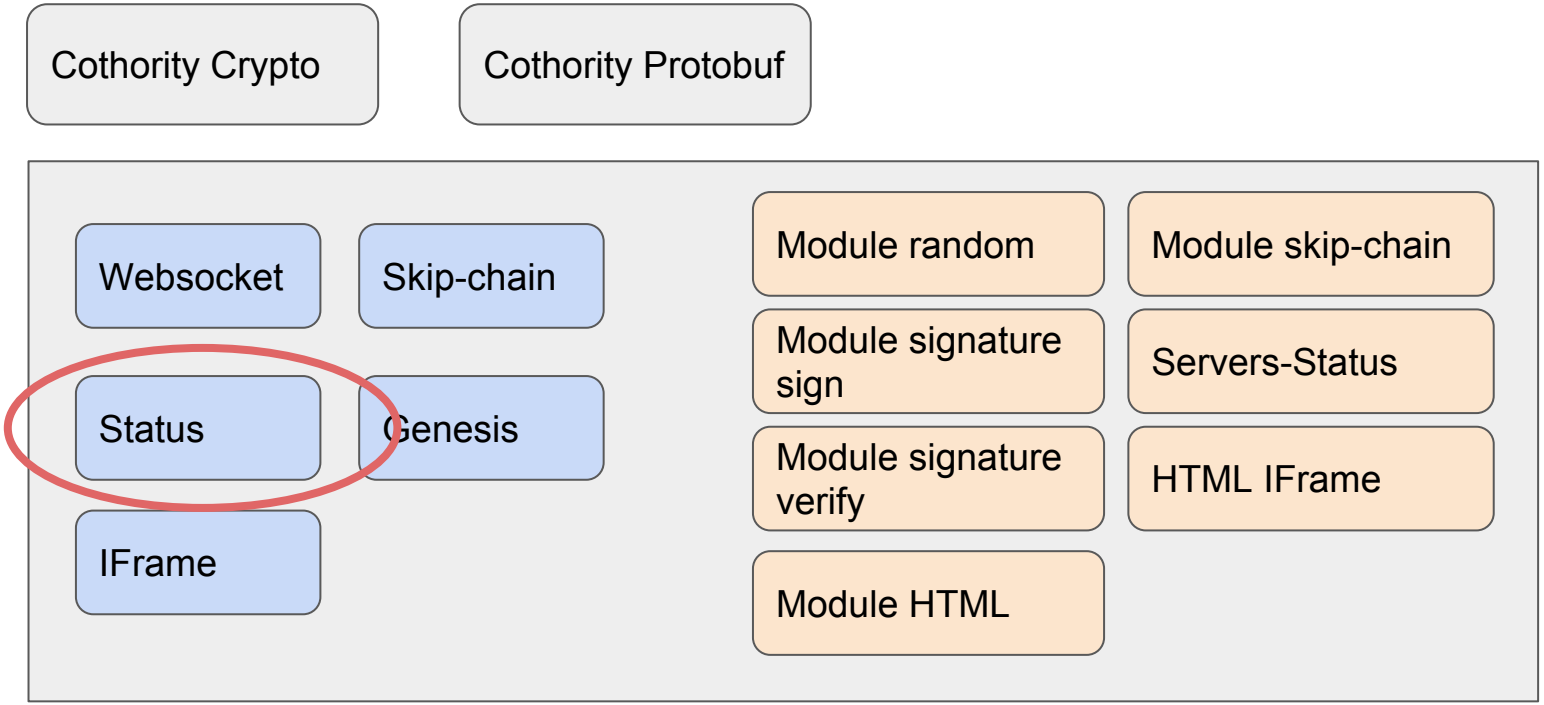


Architecture - Genesis service

- Use the skip-chain service
- Entry point of the app
  - Available skip-chains
  - Current active skip-chain
  - Events for active chain
  - Get a block given a skip-chain ID + block ID

```
https://skipchain.dedis.ch
{
    "Blocks": [{
        "GenesisID": "0b8d24c8d3...",
        "Servers": [
            "192.33.210.8:7002",
            "192.33.210.8:7004",
            "192.33.210.8:7006"
        ],
        "Data": "3c1b8rA7XN66xq/fn3jvQQoA"
    }]
}
```

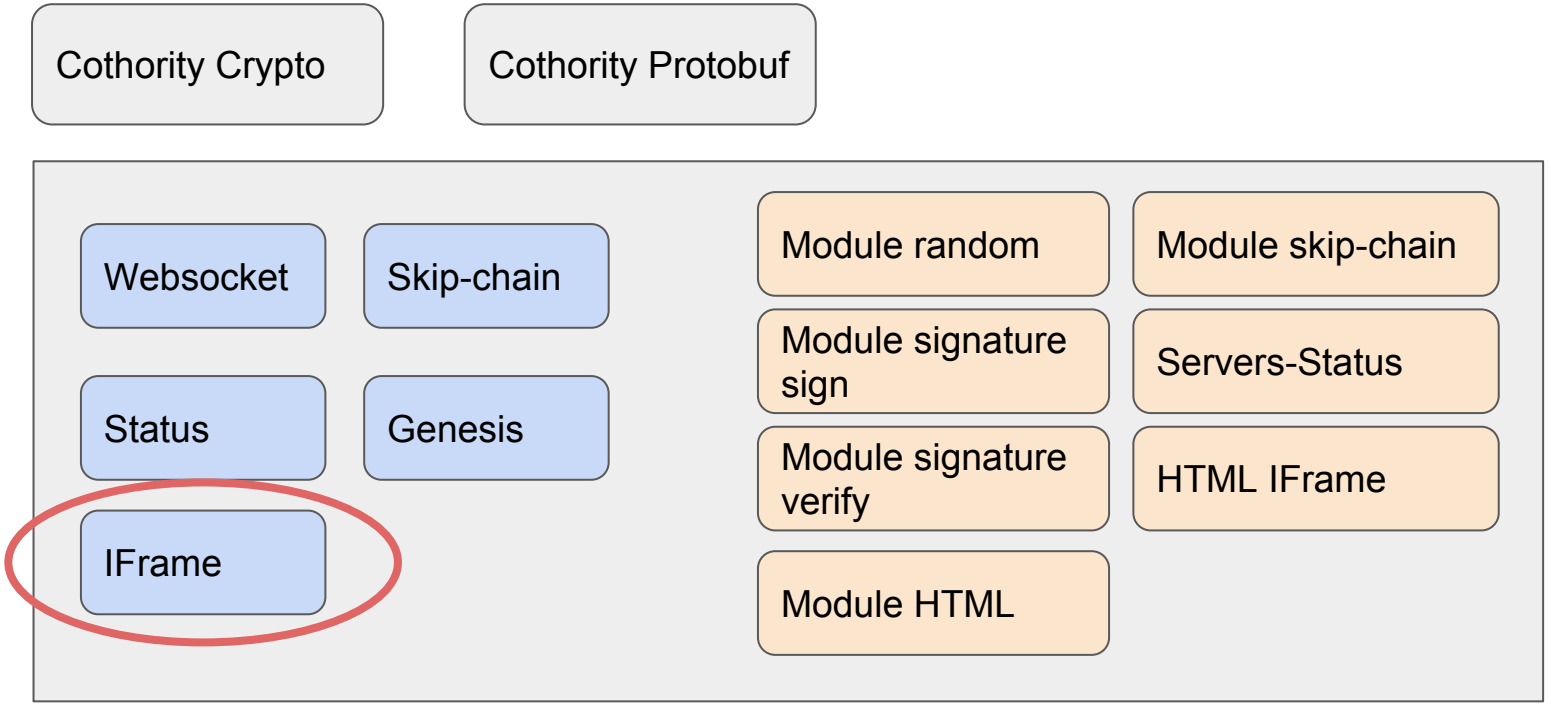
Architecture



Architecture - Status service

- Use Websocket and Genesis services
- Provide the status of the nodes
  - Roster of the active skip-chain
  - Events
- Provide the online/offline roster
  - Important for the signature ! (at least ⅔)

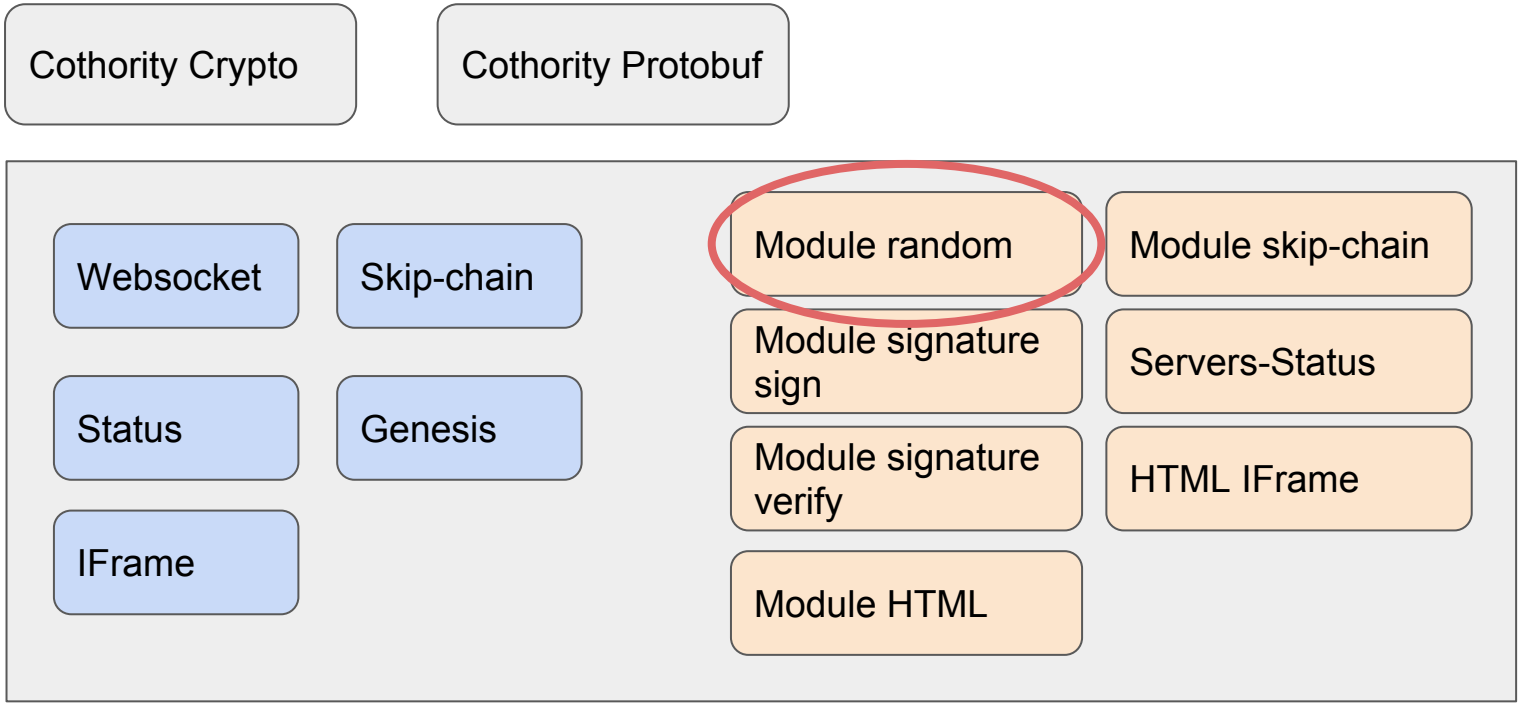
Architecture



Architecture - IFrame service

- Use the Genesis service
- Sync the components to show an HTML skip-chain
  - Events (e.g. open and back)
  - Given a skip-chain ID
- Take care of loading the HTML content
  - Provide it in the open event

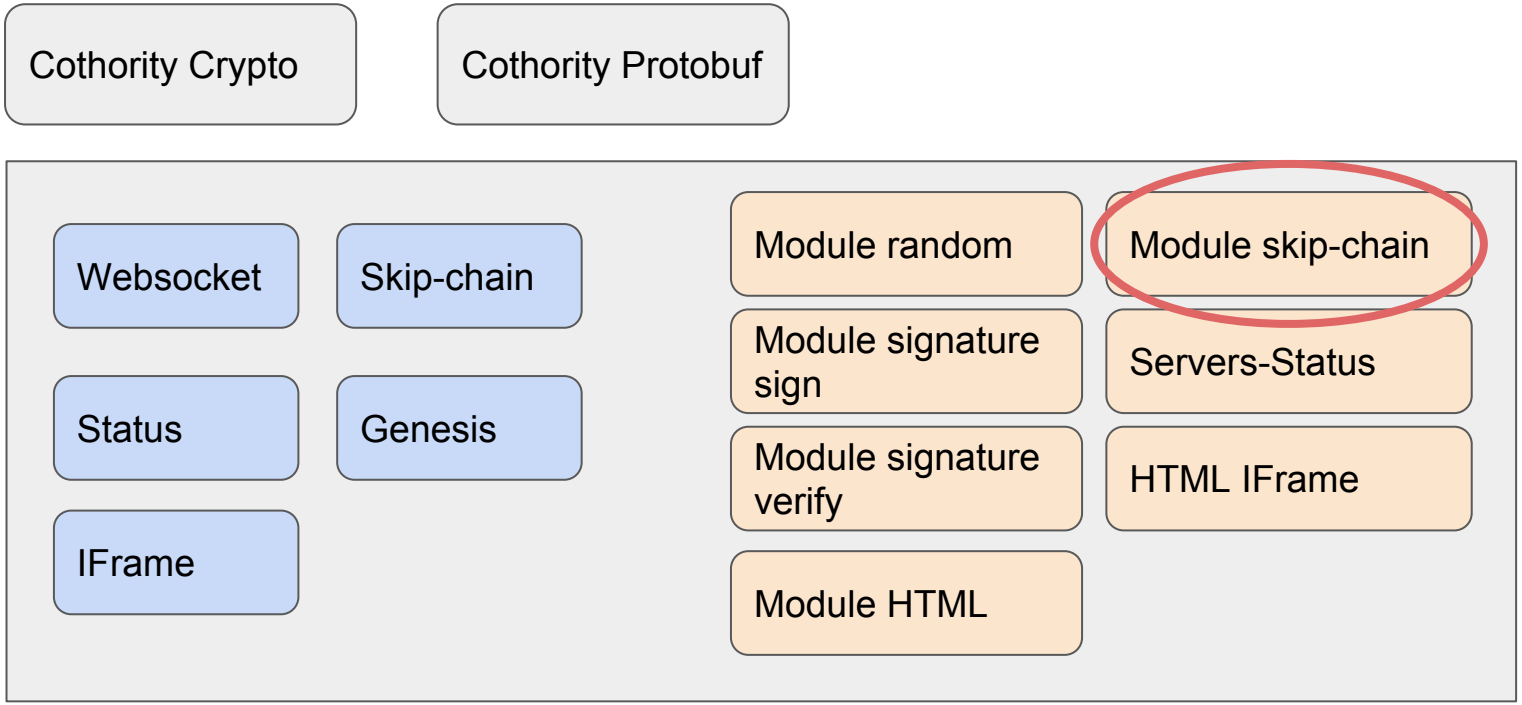
Architecture



Architecture - Module random

- Use the Websocket service
- Display a random number
  - Refresh itself every 30 seconds
  - Makes a request to the random service of a given node (wss://pulsar.dedis.ch:9000)

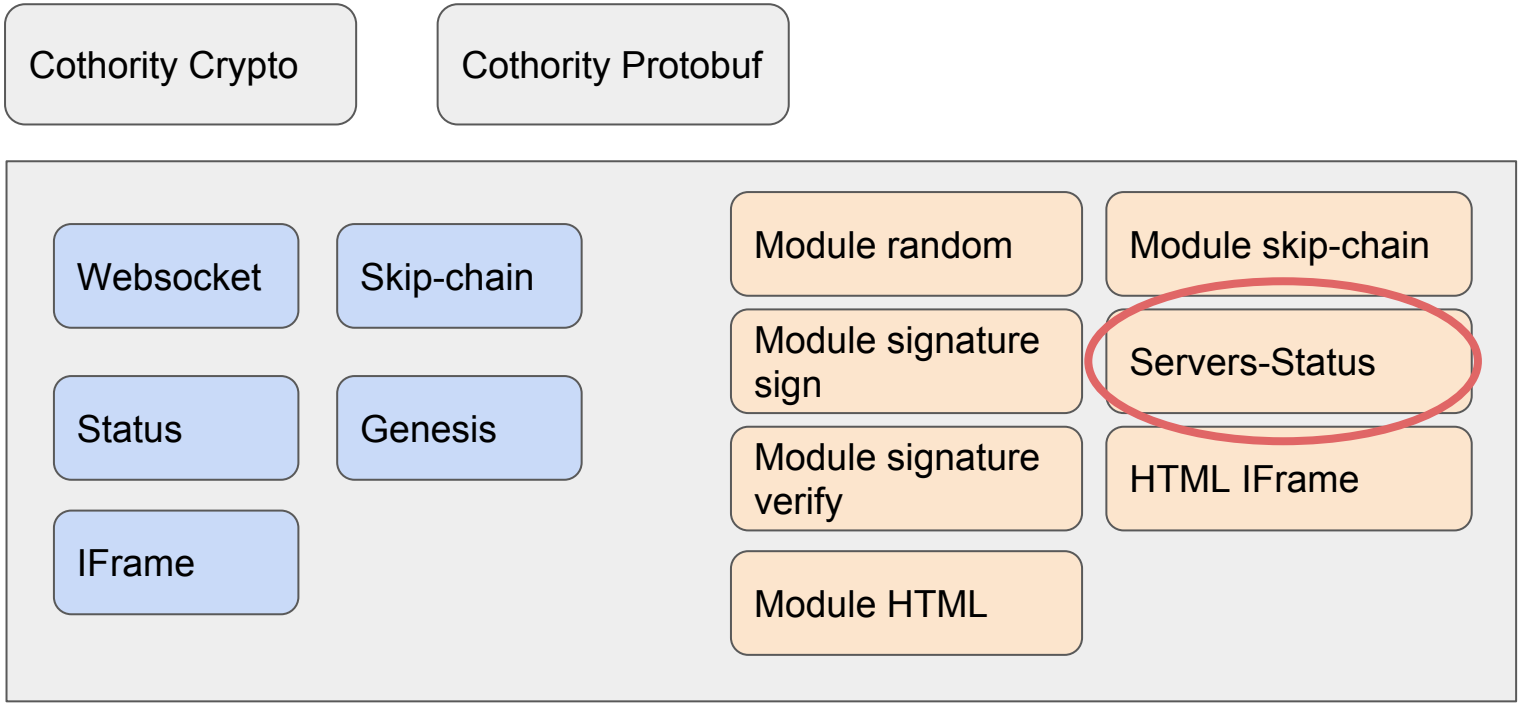
Architecture



Architecture - Module skip-chain

- Use the Genesis service
- Display the list of available skip-chains
  - Highlight the active one
- User can choose the active chain
  - … by clicking

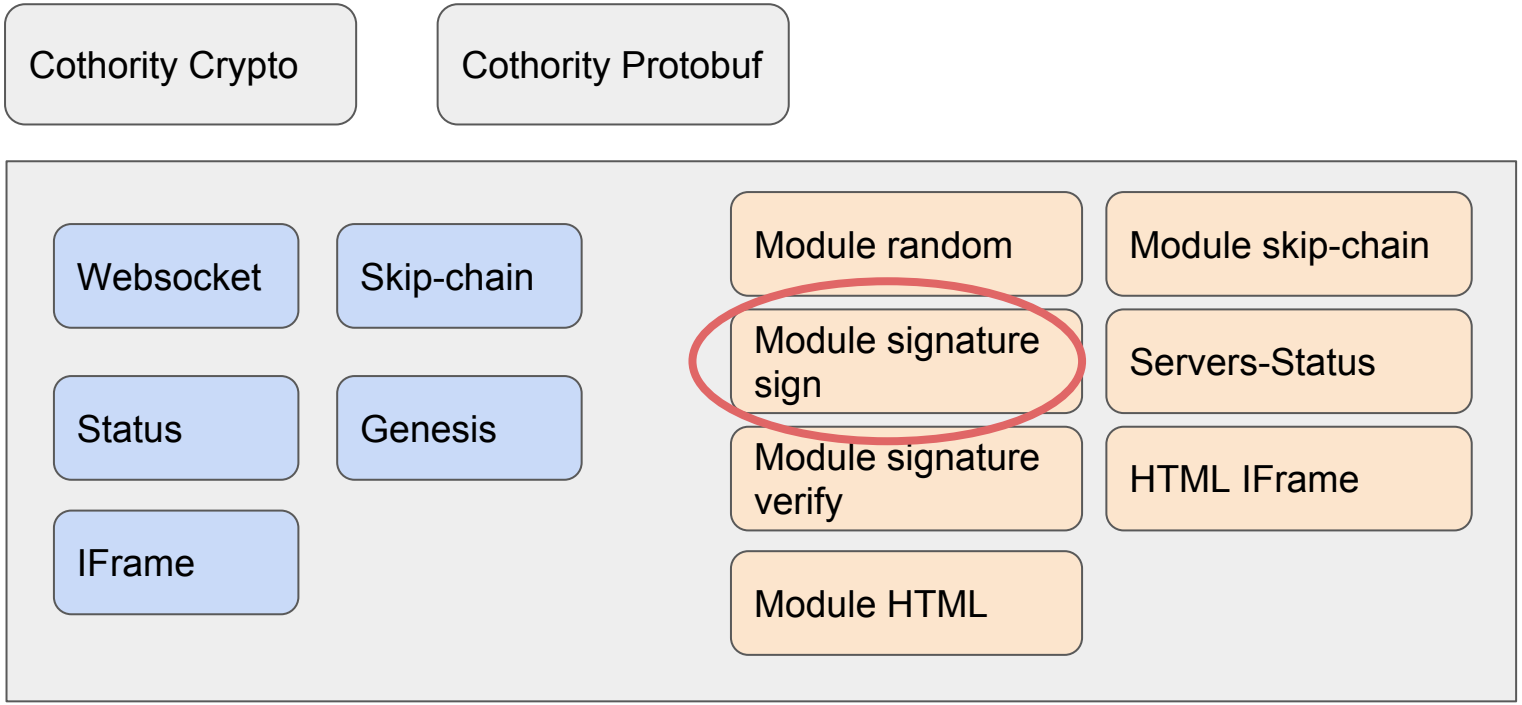
Architecture



Architecture - Servers-Status

- Use the Status service
- Not a module
  - but a table of the nodes
- Display information about the nodes
  - Name, IP, Port, Up-time, Traffic, Services and Version
  - online/offline

Architecture

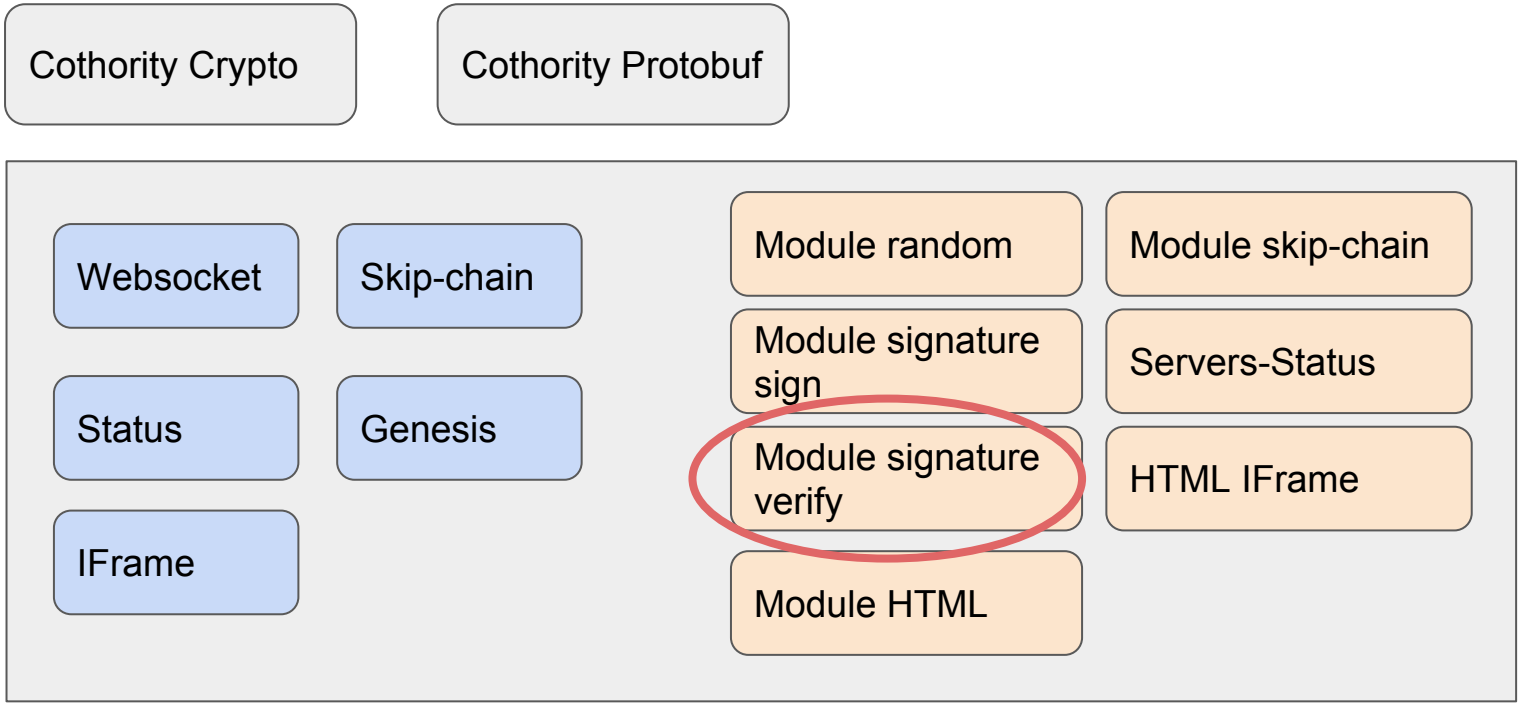


Architecture - Module signature (sign)

- Use the Status and Genesis services
- 2 steps
  a. Dropzone to upload a file
  b. Confirmation to sign
- Require at least ⅔ of the roster (or reject)
- Download a signature file


```
{
    "filename": "7378e468ad6e24925f61560829ca1205.jpg",
    "signature": "134f07469307fc3e4...",
    "hash": "38ab97d8e44...",
    "genesisID": "32bf04100...",
    "blockID": "32bf04100...",
    "offlineServers": [
        "192.33.210.8:7005"
    ]
}
```

Architecture

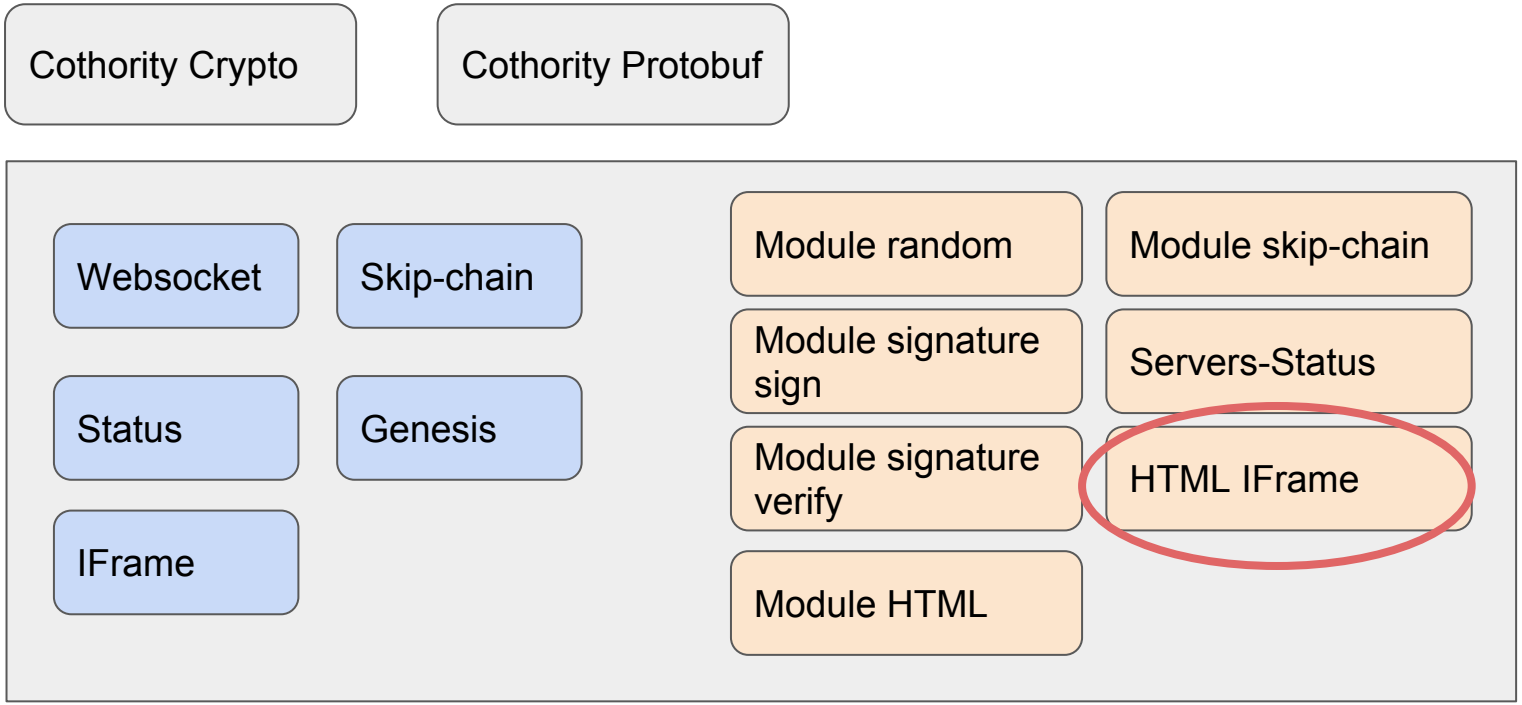


Architecture - Module signature (verify)

- Use the Genesis service
- 2 steps
  a. Dropzone to upload a file
  b. Dropzone to upload the signature file
- Fetch the specific block
- Remove public keys of offline nodes


```
{
    "filename": "7378e468ad6e24925f61560829ca1205.jpg",
    "signature": "134f07469307fc3e4...",
    "hash": "38ab97d8e44...",
    "genesisID": "32bf04100...",
    "blockID": "32bf04100...",
    "offlineServers": [
        "192.33.210.8:7005"
    ]
}
```

Architecture

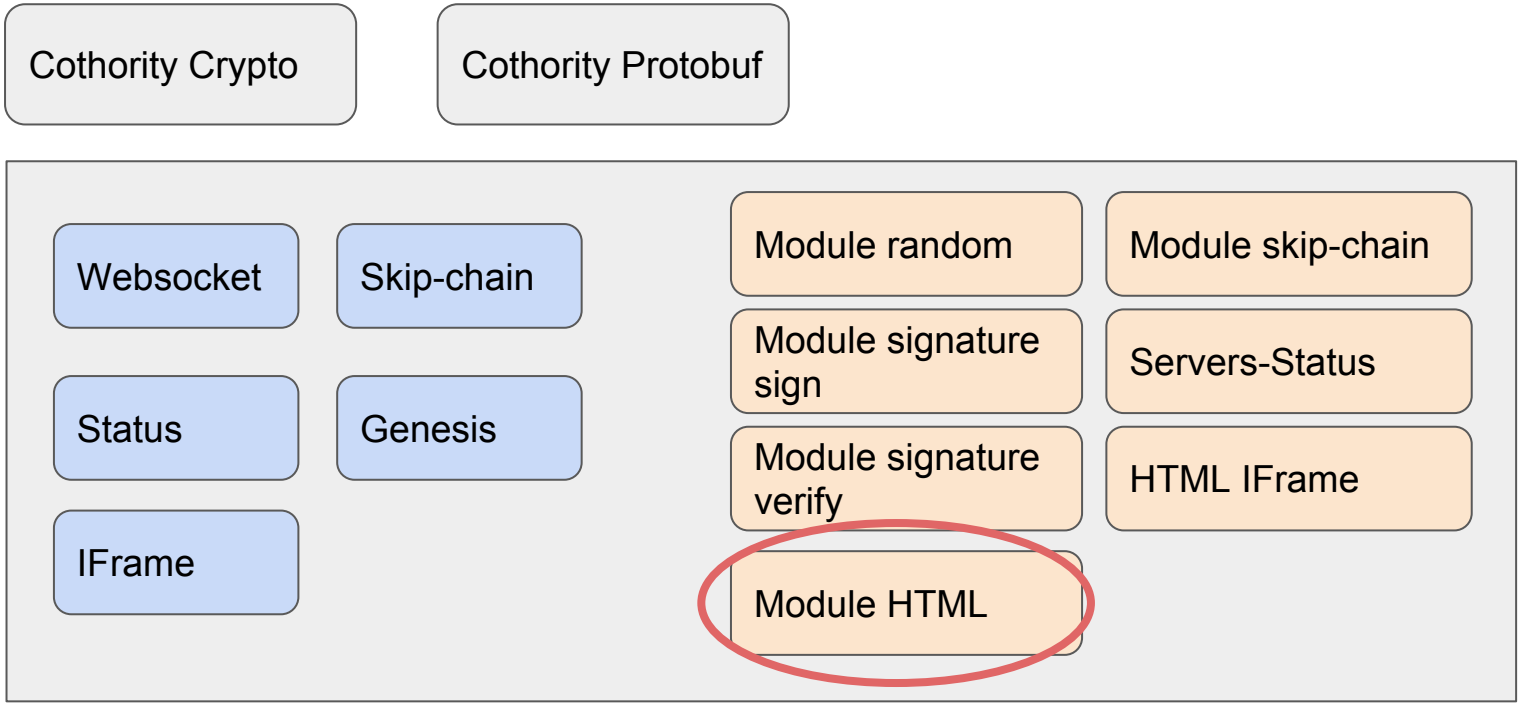


Architecture - HTML IFrame

- Use the IFrame service
- Open
  a. Add an iframe to the html
  b. Populate the iframe with the base64 of the HTML content
- Back
  a. Remove the iframe
- postMessage to tackle the security

```
<a href="javascript:void 0" onclick="window.parent.postMessage('skipchain://0b8d24c8d3d1c323f6eaed455a55b7949cbde5370f32a64c6f9bb3b961fa6d6d', '*')">CoSi Binary </a>
```

Architecture



Architecture - Module HTML

- Use the Genesis and IFrame services
- Display the list of HTML skip-chain
  - Genesis blocks with data field starting with “http://” or “https://”
  - Only the index of websites
- Open the content
  - Ask the IFrame service to fetch the last block

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

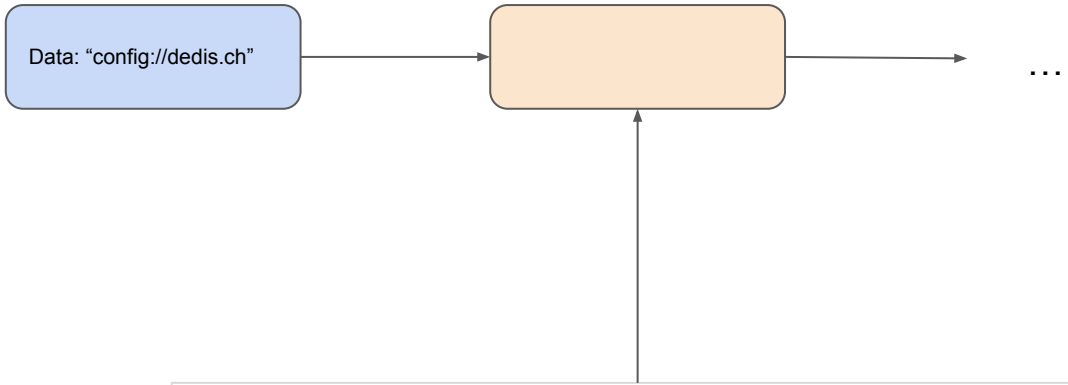
Outline

- Goals
- Cothority
- Technologies
- Architecture
- **Website Inliner**
- Conclusion

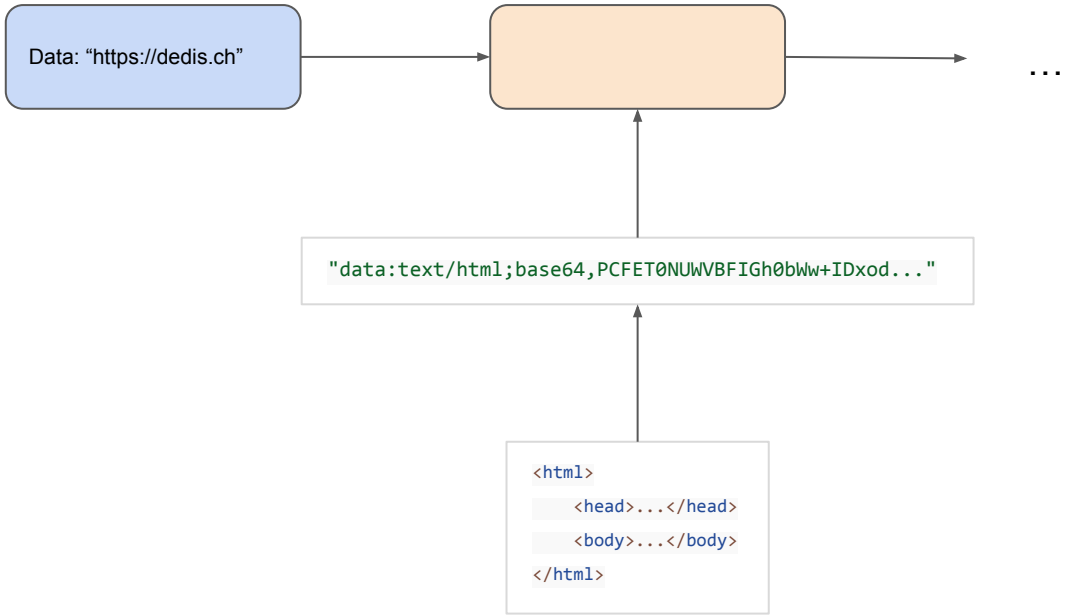
Website Inliner

- NodeJS script
- Use the Inliner node module
- Automatically create and populate the skip-chains
  - One per page
  - Last block of the chain is the latest content
  - Use a public.toml file for the roster
- Create a config skip-chain to keep track of the chains
  - You can provide the the skip-chain ID to update
- Optimize for the DEDIS website...

Website Inliner - Configuration file



Website Inliner - Page skip-chain



ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Outline

- Goals
- Cothority
- Technologies
- Architecture
- Website Inliner
- **Conclusion**

Conclusion

- Code is modular and extensible
- User friendly signature
- Not anymore a static roster
  - we can change it !
- HTML skip-chain
- Tests
- Libraries (simple usage of crypto primitives)

But

- Status is not scalable (require a back-end support)

Thank you for your attention !