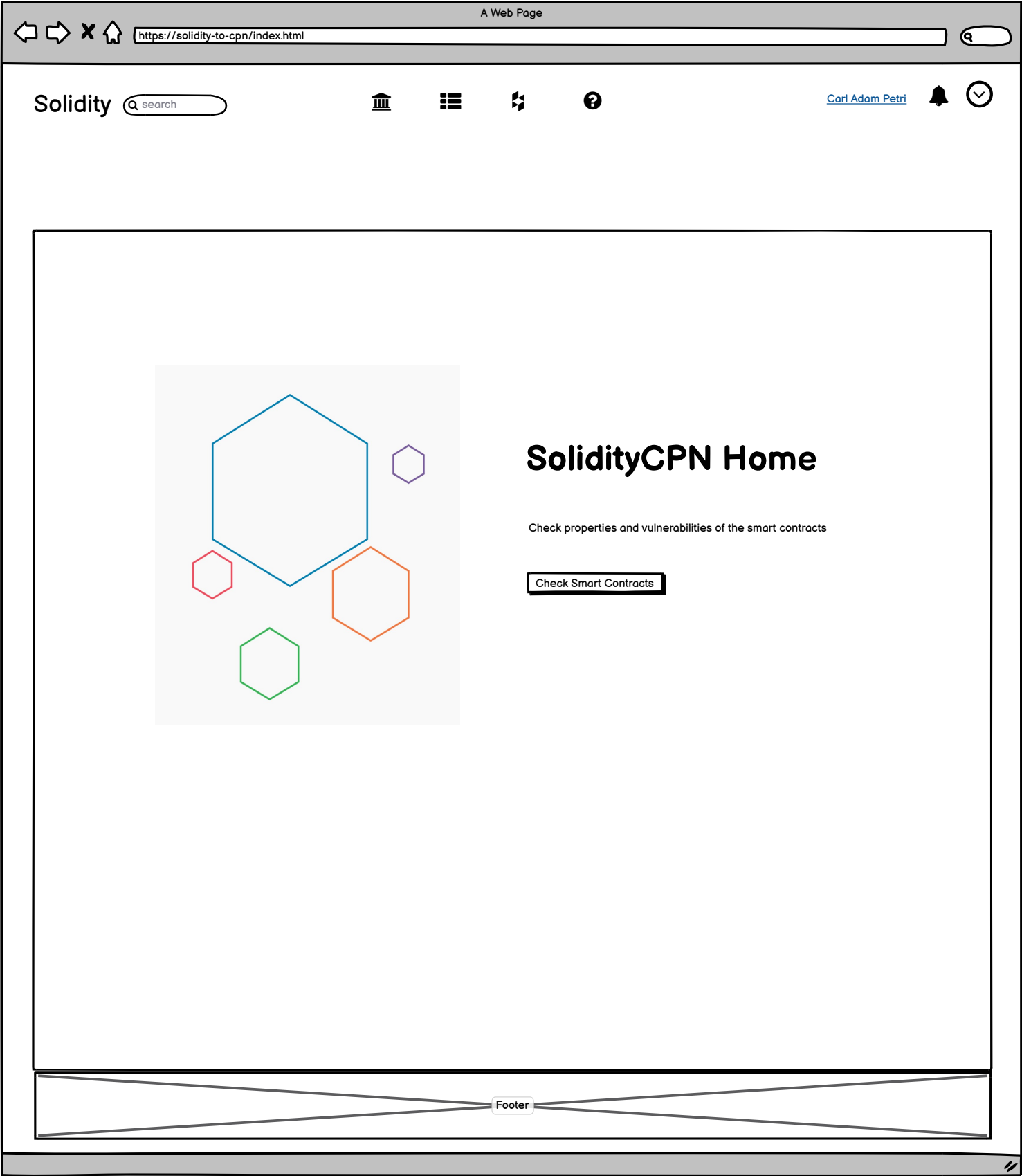
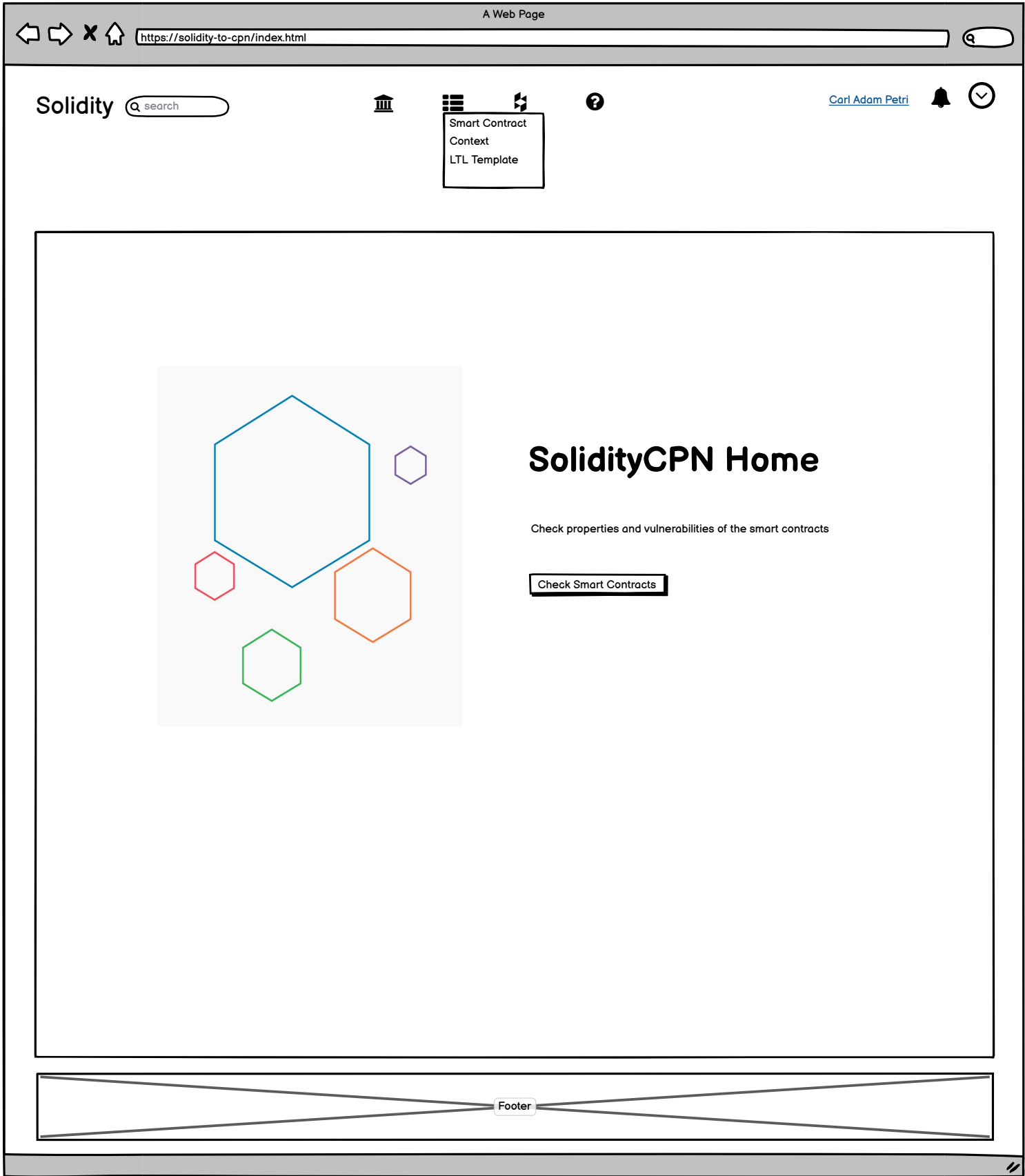


1



1



2

←

→

✕

🏠

https://solidity-to-cpn/select-sc.html

🔍

A Web Page

Solidity

Roadmap

Start

Select Smart Contracts

Select Context

Choose Vulnerability

Generate SC to CPN

Check the SCs

Finished

☰

↺

Checked Smart Contract List

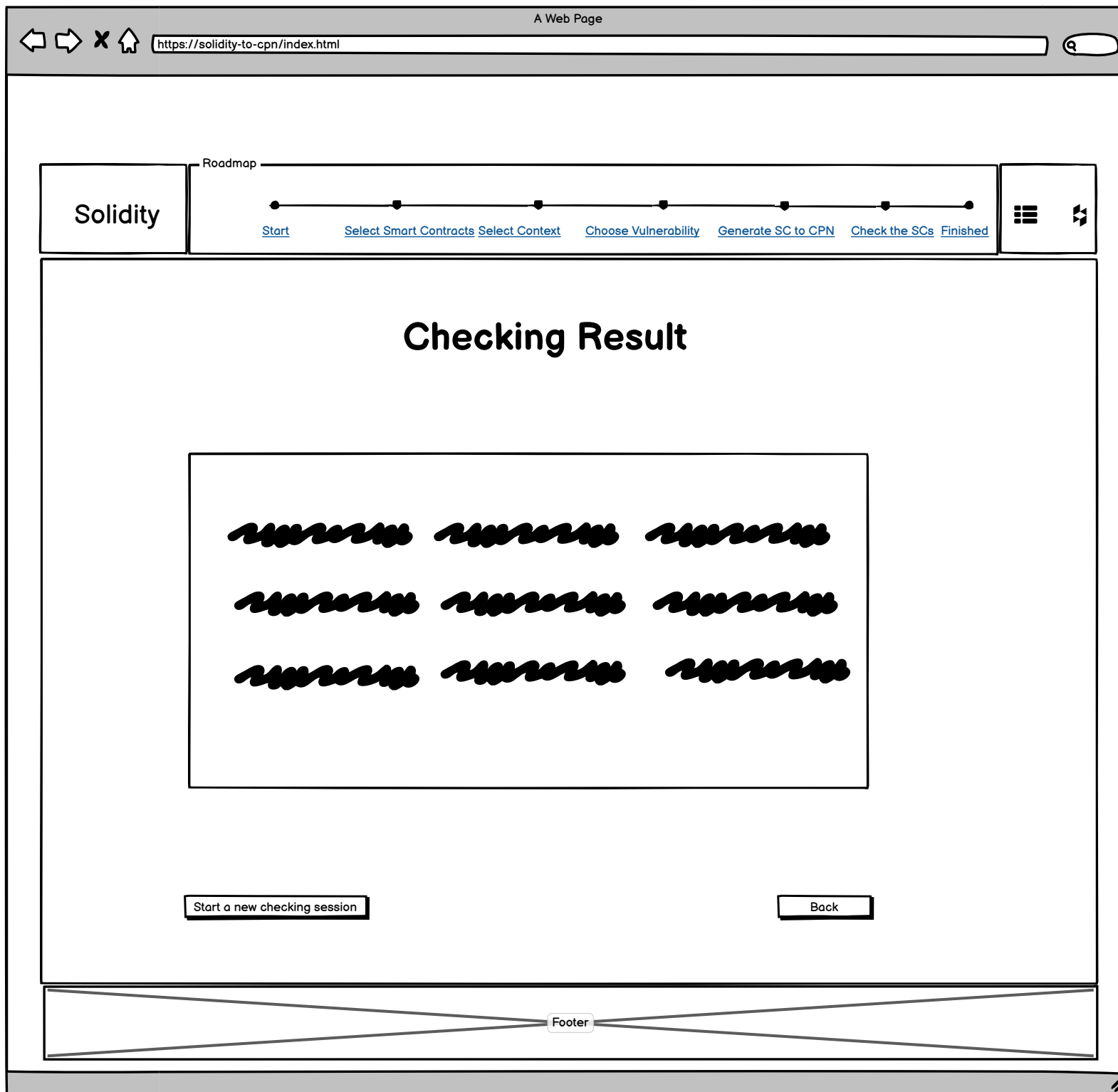
#	Checker	Checked Date	Number of smart contracts
1	David	09/10/2021	3
2	Jaime		
3	Billy		
4	Ikram	06/10/2021	2
5	Thomas	05/10/2021	1
6	Alex	04/10/2021	3
7	Micheal	03/10/2021	1
...	...		

Start a new checking session

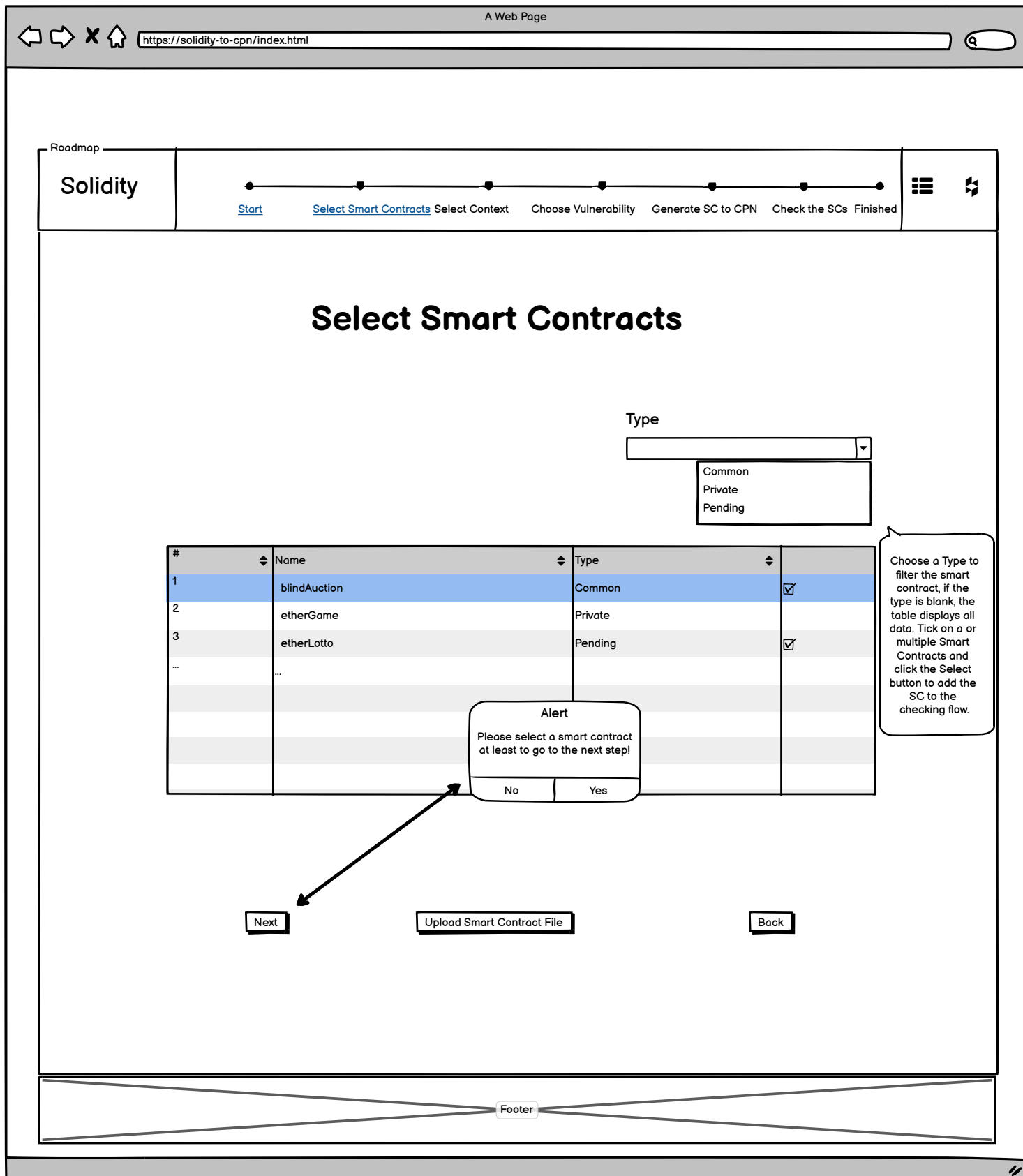
Back

Footer

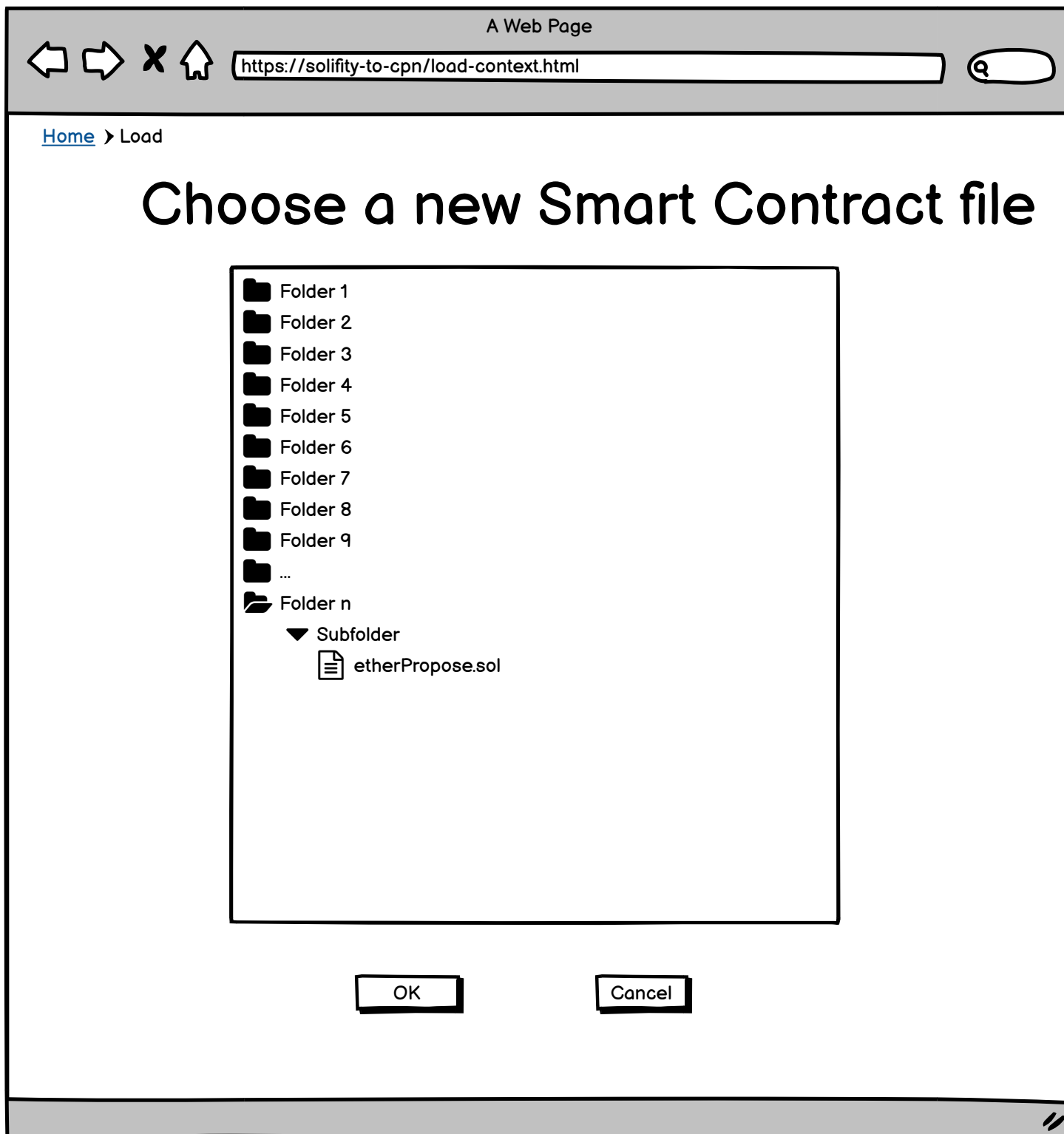
3



4



4a



5

A Web Page

https://solifity-to-cpn/upload-sc.html

Home > Upload





Upload a new Smart Contract code

Name

Smart Contract Type ☐ Pending ☒ Private

Normal user can request to change a private smart contract to become a common one.
Default is Private

B I U

6

←

→

✕

🏠

A Web Page

https://solidity-to-cpn/context.html

🔍

Solidity

Roadmap

Start

Select Smart Contracts

Select Context

Choose Vulnerability

Generate SC to CPN

Check the SCs

Finished

☰

↺

Select Context

Name

Gaming

- Medicine

- Gaming

- ...

- Lotto

Type

DCR

Description

There are several options:

· BPMN: The user will choose the BPMN context by clicking on the "Load a Context" button.

· DCR: The user will choose the DCR context by clicking on the "Load a Context" button.

· ...

· Free

Next

Upload a Context file

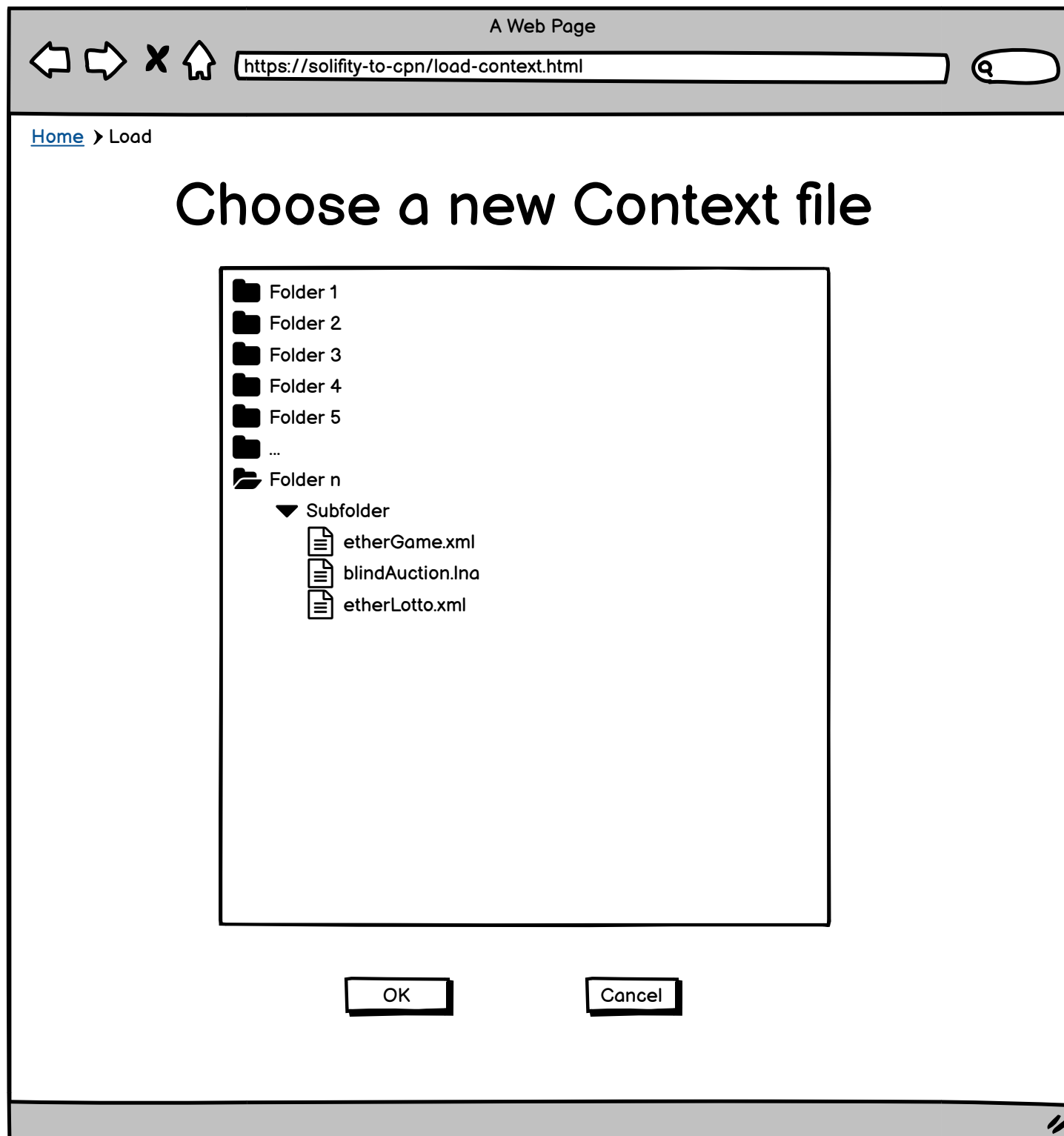
Skip

Back

If the user does not choose a context here, and click Skip, it means the user chooses the free-context

Footer

6a



7

A Web Page

https://solify-to-cpn/upload-sc.html

[Home](#) > Upload

Upload a new Context file

Name

Type

- DCR
- CPN
- ...

If the user chooses the CPN context, it means the CPN file (.lna) will be uploaded (the system does not need to run DCR2CPN tool to convert a xml file to a lna file.)

Content

Description

8

← → × ↗

A Web Page

https://solidity-to-cpn/ltlformula.html

🔍

Solidity

Roadmap

Start

Select Smart Contracts

Select Context

Choose Property

Generate SC to CPN

Check the SCs

Finished

☰ ☲

LTL Checking Options

Please choose your way to check the Smart Contracts:

- Contract-Specific Property: You will choose the functions and using template or non-template to design your LTL formula.
- General Vulnerability: You will select the common vulnerability from the list.

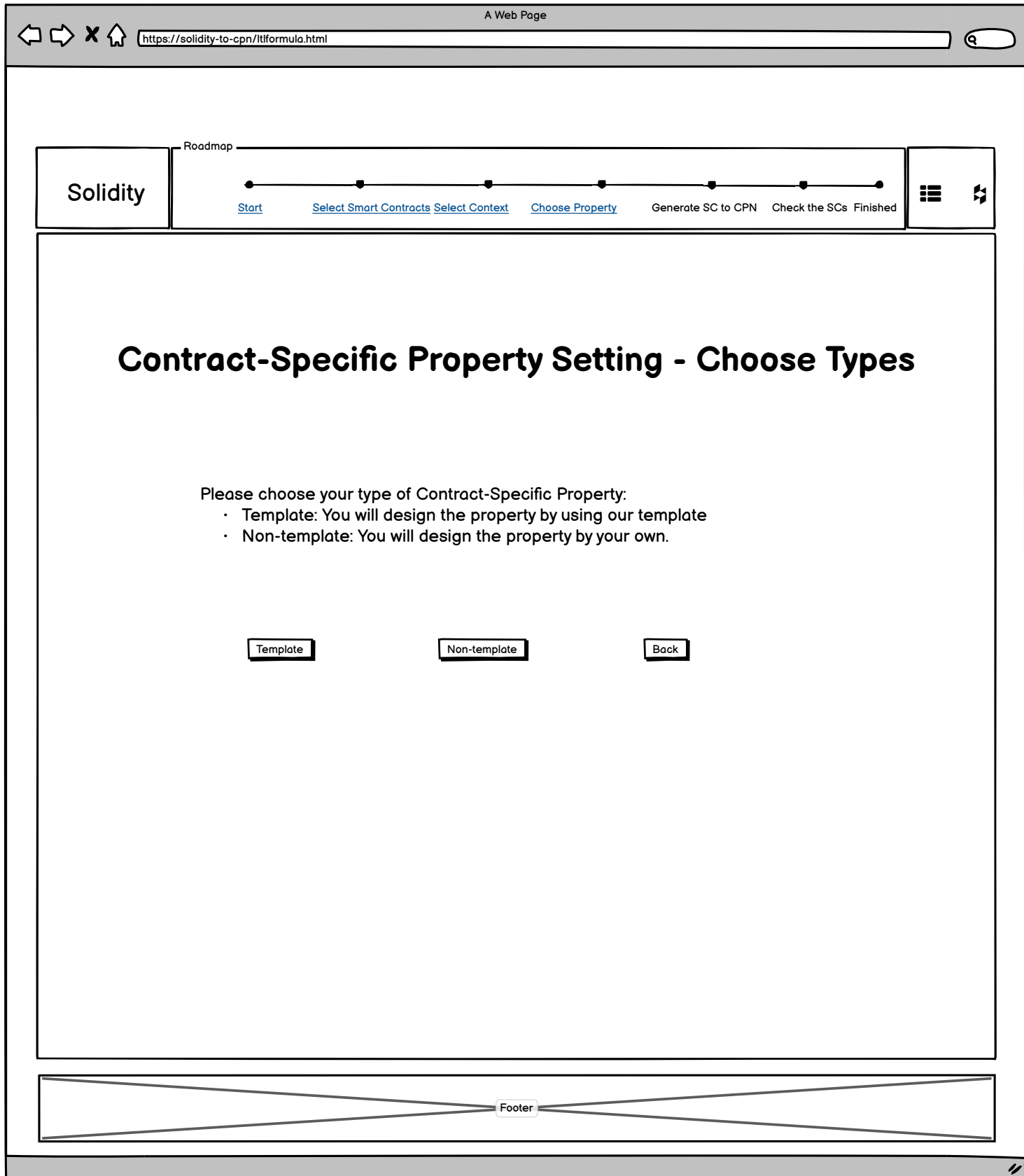
Check a Contract-Specific Property

Check a General Vulnerability

Back

Footer

9



10

←→✕🏠

https://solidity-to-cpn/ltformula.html

🔍

A Web Page

Solidity

Roadmap

Start

Select Smart Contracts

Select Context

Choose Property

Generate SC to CPN

Check the SCs

☰⚡

Contract-Specific Property Setting - Template

Name

Mutual exclusion

Template

Template 1

Template 1

Template 2

Template 3

Template 4

Template 5

...

Others

Formula

After an occurrence of { [local variable 1](#) } there will be at least one occurrence of { [global variable 2](#) }

Click on the [variable](#) or [function](#) or [argument](#) to choose the right one in the smart contract

Description

The users need to click on the keyword {local variable} to choose the proposition for the first logic sentence and then click on {global variable} to choose the second proposition for the second logic sentence.

Next

Back

Footer

11

A Web Page

X

https://solidity-to-cpn/add-segmented-sc.html

Q

[Back to home](#)

Select smart contracts

#	Smart Contract name	Selected
1	Smart Contract 1	<input checked="" type="radio"/>
2	Smart Contract 2	<input type="radio"/>
3	Smart Contract 3	<input type="radio"/>
4	Smart Contract 4	<input type="radio"/>
...		

OK

Cancel

12

A Web Page

https://solidity-to-cpn/add-segmented-sc.html

[Back to home](#)

Select global variables of the smart contract

Smart Contract 1Smart Contract 2Smart Contract 3

#	Global variables	Selected
1	GV1	<input checked="" type="radio"/>
2	GV2	<input type="radio"/>
3	GV3	<input type="radio"/>
4	GV4	<input type="radio"/>
...		

OK

Cancel

13

A Web Page

X

https://solidity-to-cpn/add-segmented-sc.html

Q

[Back to home](#)

Select functions of the smart contract

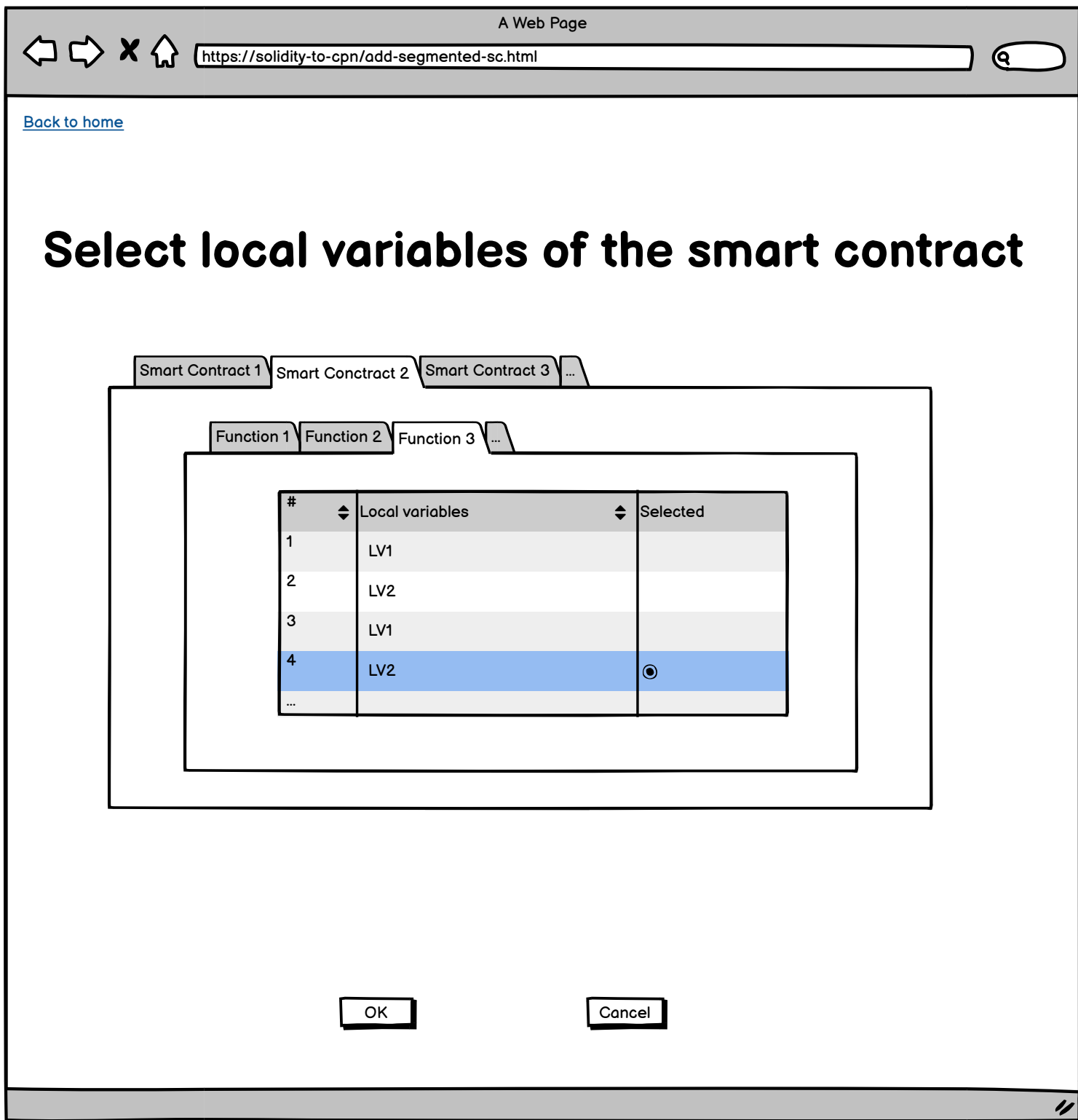
Smart Contract 1Smart Contract 2Smart Contract 3...

#	Functions	Selected
1	Function 1	
2	Function 2	
3	Function 3	
4	Function 4	<input checked="" type="radio"/>
...		

OK

Cancel

14



10a

Mutual exclusion

Template

Template 1

Template 1

Template 2

Template 3

Template 4

Template 5

...

Others

Formula

$$(GF\{\text{local variable 1}\} \wedge GF\{\text{global variable 1}\}) \Rightarrow G(\{\text{local variable 2}\} \Rightarrow F\{\text{smart contract}\})$$

Alert

The variable 2 is missing content. Please choose the right one on the smart contract before you move to the next step.

No

Yes

Description

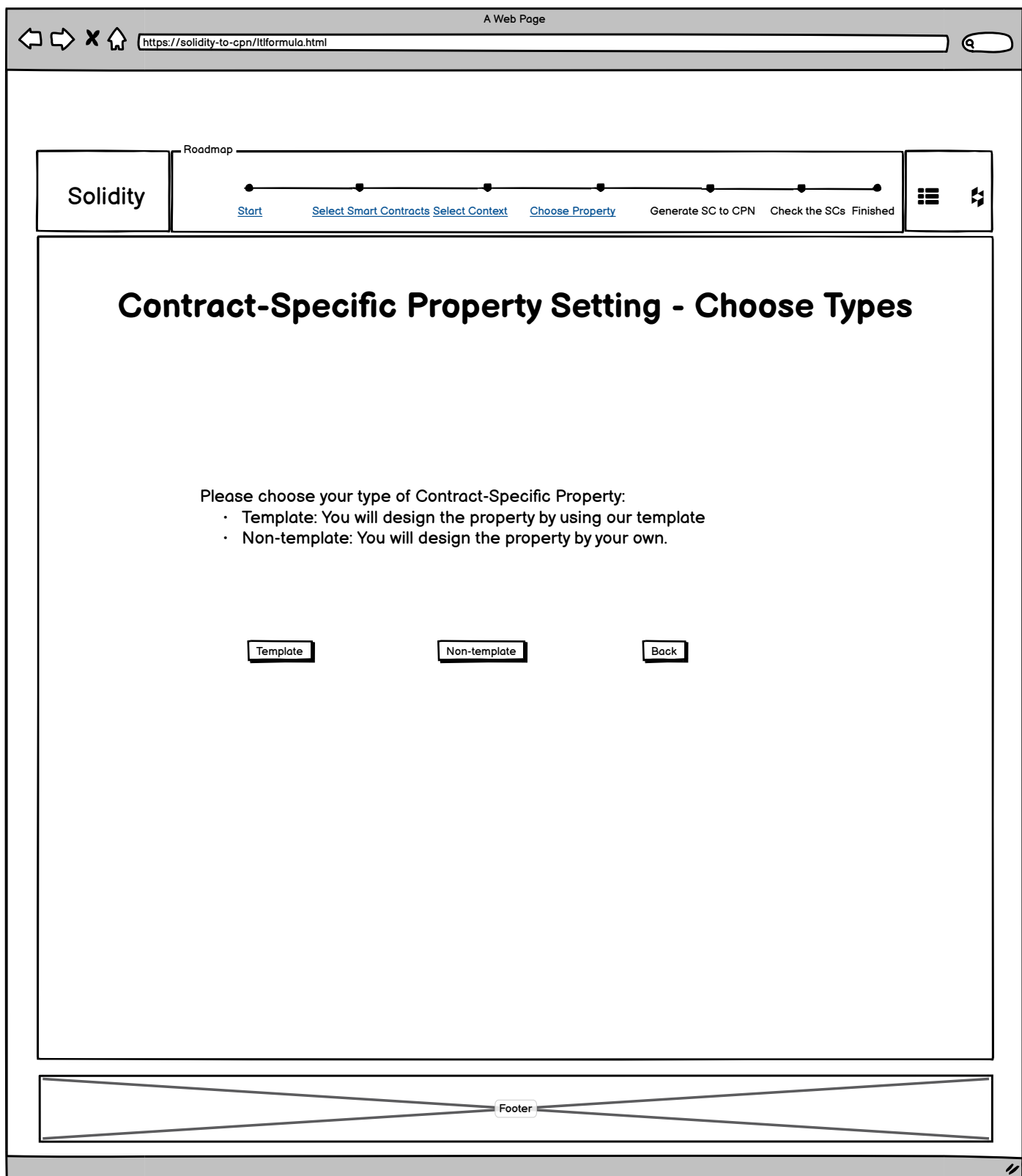
If {variable 1} occurs infinitely often and {variable 2} occurs infinitely often, then each occurrence of {function 3} is followed by an occurrence of {function 4}.

Next

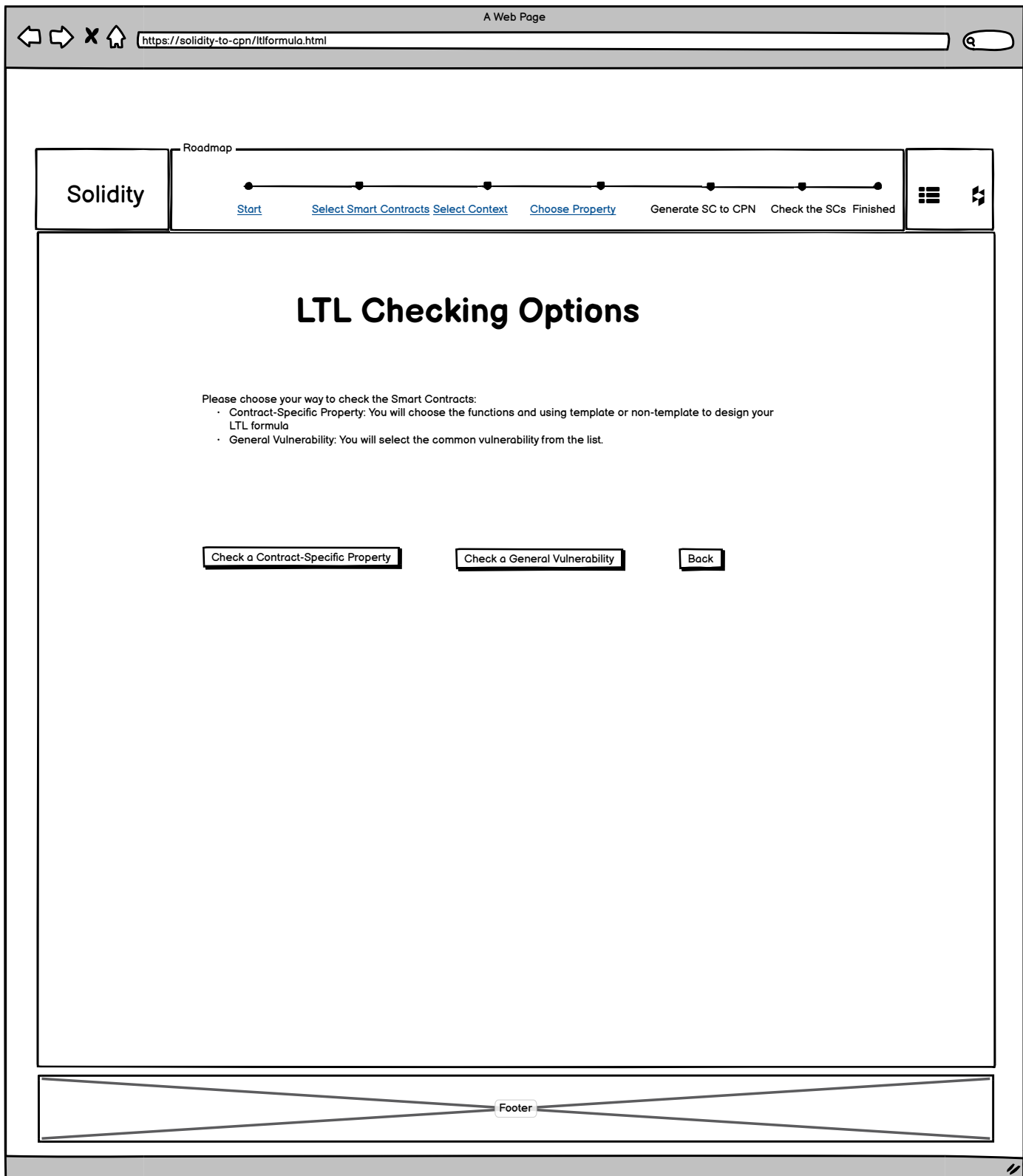
Back

Footer

9a



8a



← → × 🏠

https://solidity-to-cpn/ltformula.html

🔍

A Web Page

Solidity

Roadmap

Start

Select Smart Contracts

Select Context

Choose Property

Generate SC to CPN

Check the SCs

Finished

☰ ⏮

General Vulnerability Setting

Vulnerability

Integer Overflow/Underflow

If the user choose Integer Overflow/Underflow or Unitialized Storage Literal the system will display a windows for the user to choose a variable to insert to the formula

Integer Overflow/Underflow

Reentrancy

Self-destruction

Timestamp Dependence

Skip Empty String Literal

Uninitialized Storage Variable

Others

Description

outOfRange(x) = (x < minThreshold) V (x > maxThreshold)

Next

Back

Footer

← → × ↗

https://solidity-to-cpn/ltformula.html

🔍

A Web Page

Solidity

Roadmap

Start

Select Smart Contracts

Select Context

Choose Property

Generate SC to CPN

Check the SCs

Finished

☰ ☲

Select variables of the function

Smart Contract 1

Smart Contract 2

Smart Contract 3

...

#	Global variables	Selected
1	GV1	
2	GV2	
3	GV3	
4	GV4	<input checked="" type="radio"/>
...		

Function 1

Function 2

...

#	Local variables	Selected
1	LV1	
2	LV2	
3	LV3	
4	LV4	
...		

Next

Back

Footer

16a

←

→

✕

🏠

https://solidity-to-cpn/ltformula.html

🔍

A Web Page

Solidity

Roadmap

Start

Select Smart Contracts

Select Context

Choose Property

Generate SC to CPN

Check the SCs

Finished

☰

↺

General Vulnerability Setting

Vulnerability

Reentrancy

Integer Overflow/Underflow

Reentrancy

Self-destruction

Timestamp Dependence

Skip Empty String Literal

Uninitialized Storage Variable

Others

Description

There are two options for the reentrancy vulnerability:

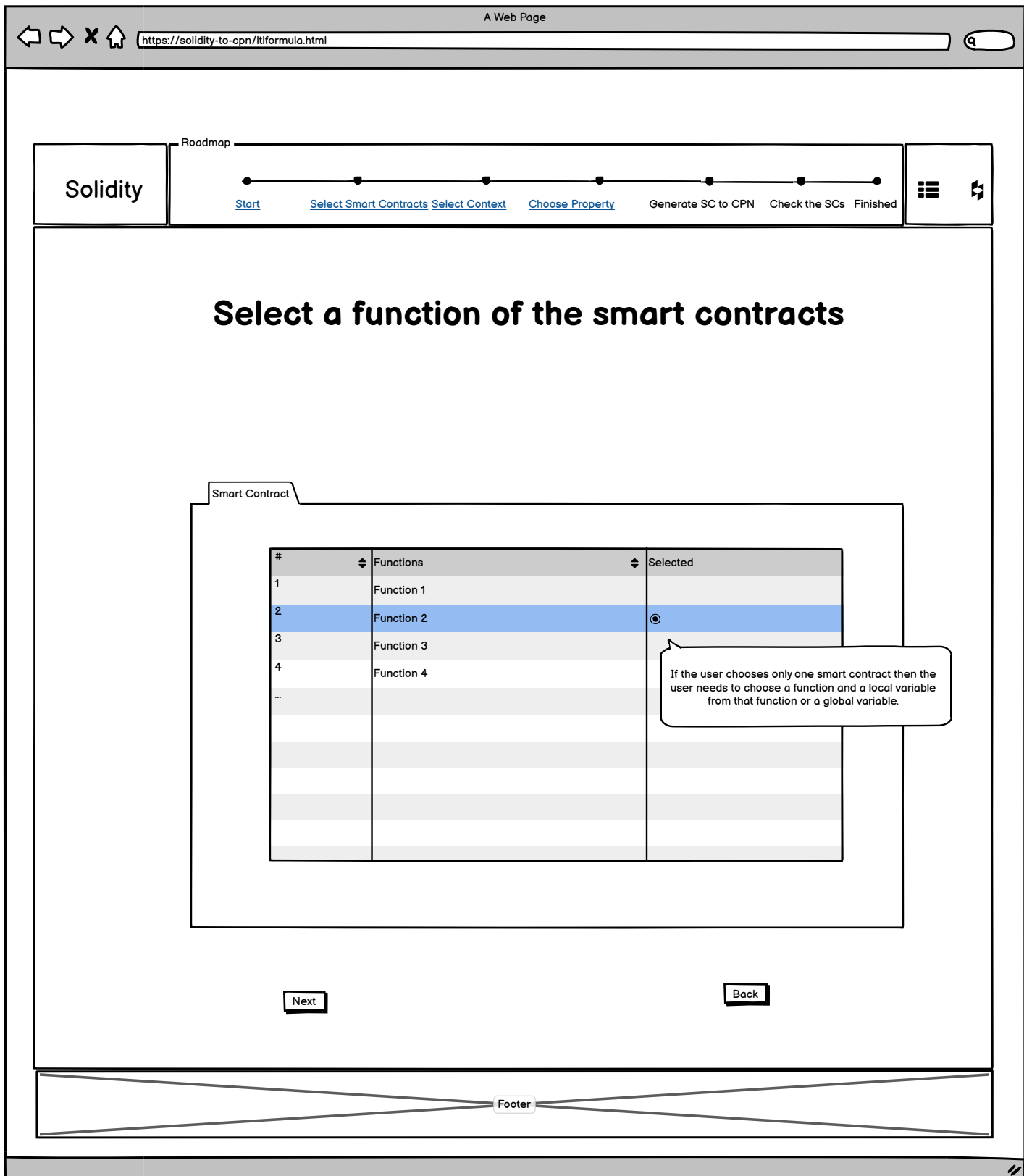
• If the user chooses only one smart contract then the user needs to choose a function and a local variable from that function or a global variable.

• If the user chooses more than one smart contract, then the user needs to choose a smart contract S_i , a function F_i from that smart contract S_i . If he knows which smart contract S_j , will be interacting with, he selects it. If he doesn't, he needs to choose a local variable from the function he had selected F_i or a global variable from S_i .

Next

Back

Footer



← → × ↗

A Web Page

https://solidity-to-cpn/ltformula.html

🔍

Solidity

Roadmap

Start

Select Smart Contracts

Select Context

Choose Property

Generate SC to CPN

Check the SCs

Finished

☰

↺

Select variables of the selected function

#	Global variable	Selected
1	Global Variable 1	
2	Global Variable 2	<input checked="" type="radio"/>
3	Global Variable 3	
4	Global Variable 4	

Function 2

#	Local variable	Selected
1	Local Variable 1	
2	Local Variable 2	
...		

Next

Back

Footer

Select functions of the smart contracts

Smart Contract 1Smart Contract 2...

#	Functions	Selected
1	Function 1	
2	Function 2	<input checked="" type="radio"/>
3	Function 3	
4	Function 4	
...		

If the user chooses more than one smart contract, then the user needs to choose a smart contract S_i , a function F_i from that smart contract S_i . If he knows which smart contract S_j , will be interacting with, he selects it. If he doesn't, he needs to choose a local variable from the function he had selected F_i or a global variable from S_i .

Select a smart contract

Select a variable from the selected function

Back

21

A Web Page

https://solidity-to-cpn/select-sc.html

Q

[Back to home](#)

Select smart contracts

#	Smart Contract name	Selected
1	Smart Contract 2	<input checked="" type="radio"/>
2	Smart Contract 3	<input type="radio"/>
...		

Next

Skip

Back

←→✕🏠

https://solidity-to-cpn/ltlformula.html

🔍

A Web Page

Solidity

Roadmap

[Start](#) [Select Smart Contracts](#) [Select Context](#) [Choose Property](#) [Generate SC to CPN](#) [Check the SCs](#) [Finished](#)

☰

↺

Select a variable of the selected function

#	Global variable	Selected
1	Global Variable 1	
2	Global Variable 2	
3	Global Variable 3	
...		

Function 2

#	Local variable	Selected
1	Local Variable 1	
2	Local Variable 2	<input checked="" type="radio"/>
...		

Next

Back

Footer

22

16b

←

→

✕

🏠

https://solidity-to-cpn/ltformula.html

🔍

A Web Page

Solidity

Roadmap

●

●

●

●

●

●

●

[Start](#)

[Select Smart Contracts](#)

[Select Context](#)

[Choose Property](#)

Generate SC to CPN

Check the SCs

Finished

☰

🔄

General Vulnerabilty Setting

Vulnerability

Timestamp Dependence

If the user chooses Timestamp Dependence, Skip Empty String Literal then the system will display the functions for the users to choose

Integer Overflow/Underflow

Reentrancy

Self-destruction

Timestamp Dependence

Skip Empty String Literal

Uninitialized Storage Variable

Others

Description

Since the execution on a Blockchain needs to be deterministic for all the miners to get the same results and reach a consensus, users usually resort to block-related variables such as timestamp as a source of entropy.

Next

Back

Footer

Solidity

Roadmap

[Start](#) [Select Smart Contracts](#) [Select Context](#) [Choose Property](#) [Generate SC to CPN](#) [Check the SCs](#) [Finished](#)

Select functions of the smart contracts

Smart Contract 1 Smart Contract 2 ...

#	Functions	Selected
1	Function 1	
2	Function 2	<input checked="" type="radio"/>
3	Function 3	
4	Function 4	
...		

Next

Back

Footer

16c

←

→

✕

🏠

A Web Page

https://solidity-to-cpn/ltformula.html

🔍

Solidity

Roadmap

[Start](#)

[Select Smart Contracts](#)

[Select Context](#)

[Choose Property](#)

Generate SC to CPN

Check the SCs

Finished

☰

⚡

General Vulnerability Setting

Vulnerability

Self-Destruction

Integer Overflow/Underflow

Reentrancy

Self-destruction

Timestamp Dependence

Skip Empty String Literal

Uninitialized Storage Variable

Others

Description

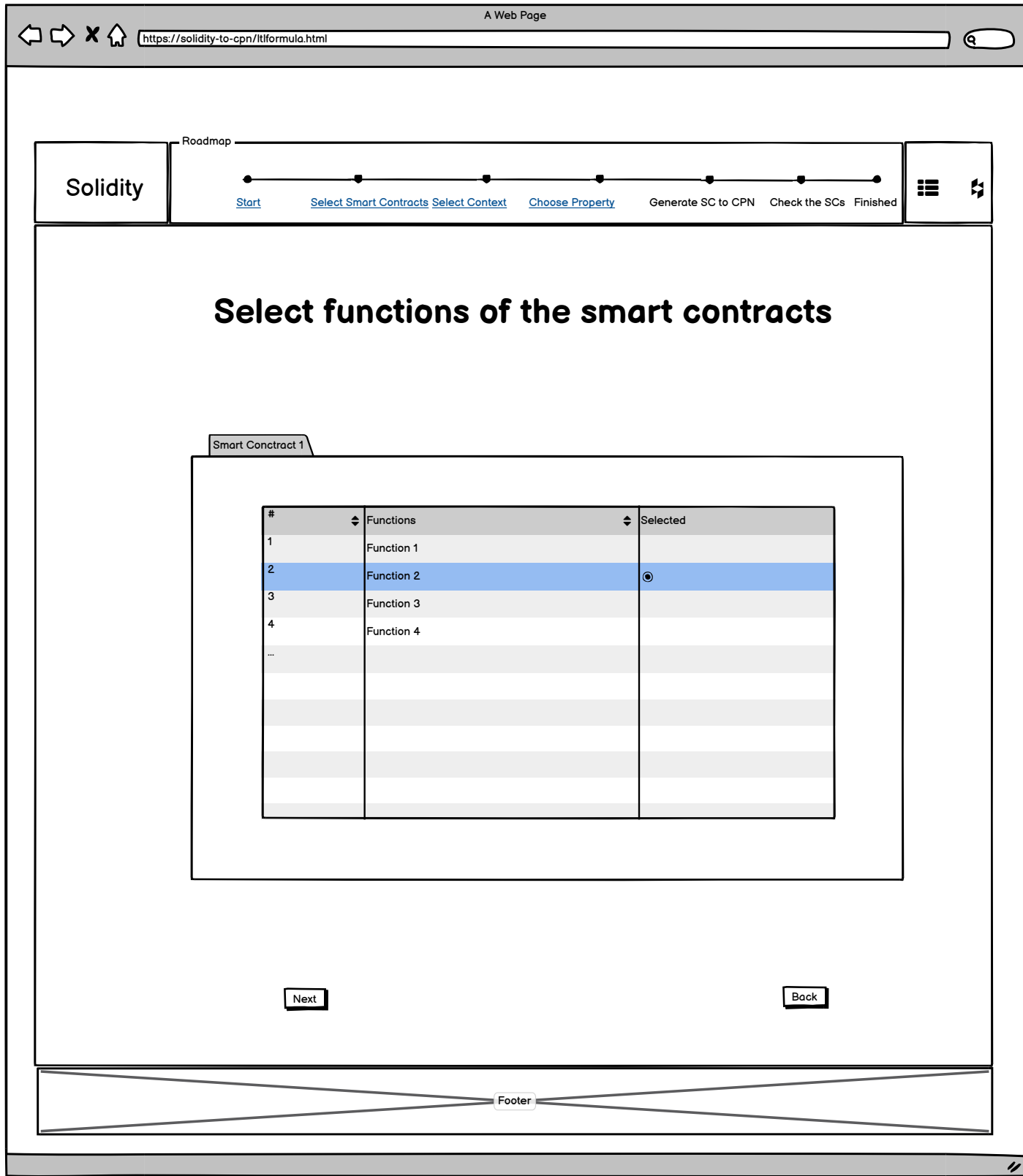
There are 2 options:

- The user chooses only one smart contract then the user needs to choose a function in the smart contract for the vulnerability.
- If the user chooses more than one smart contract and after choosing a function in the first one the user chooses another smart contract, the system will go to option 2 of Self-destruction (2 functions). If the user does not choose any function, the system goes to option 1 (only one function is chosen)

Next

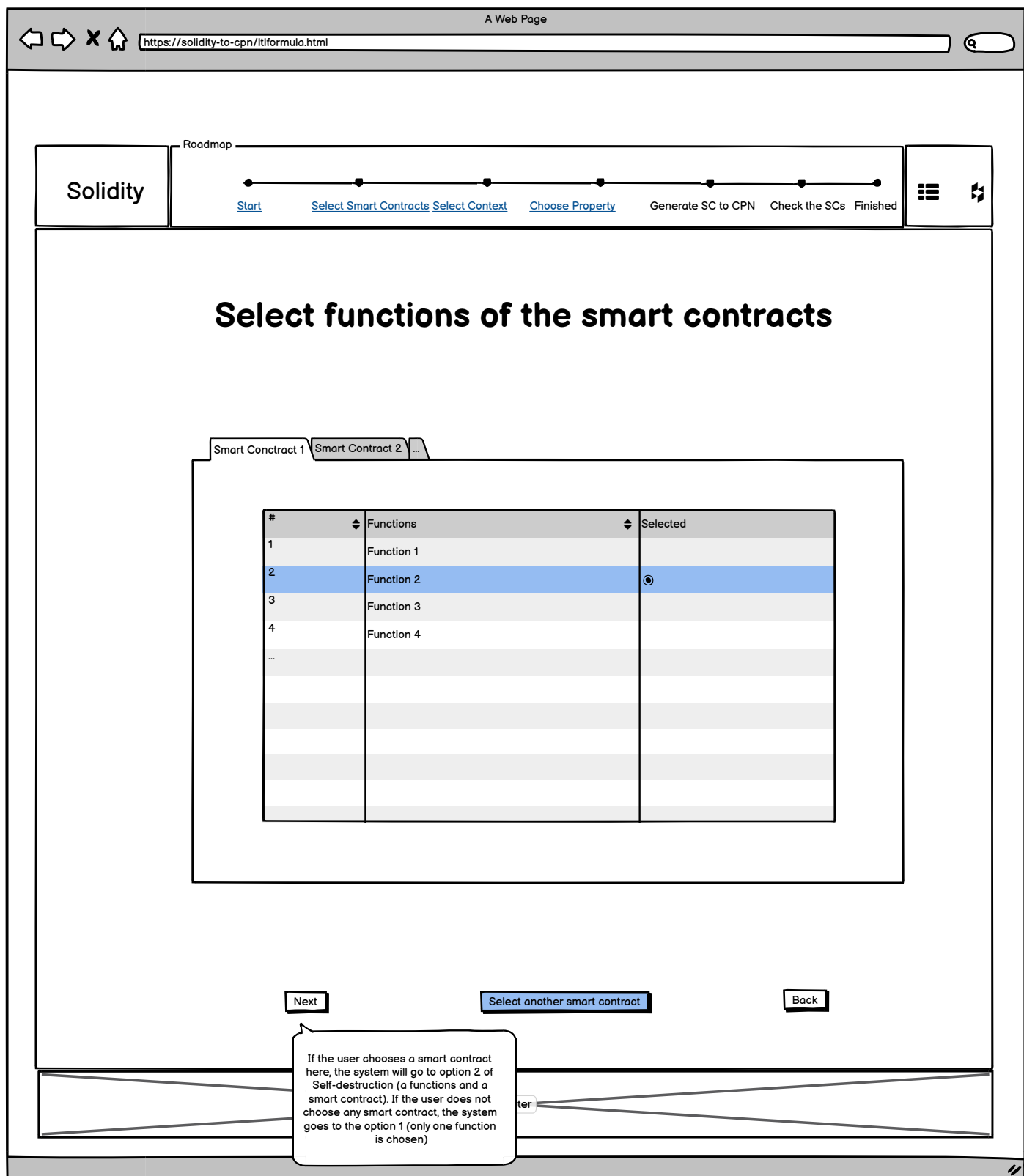
Back

Footer



24a

24b



←→✕🏠

https://solidity-to-cpn/ltlformula.html

🔍

Solidity

Roadmap

[Start](#)[Select Smart Contracts](#)[Select Context](#)[Choose Property](#)Generate SC to CPNCheck the SCsFinished

☰↺

Select smart contracts

#	Smart Contract Name	Selected
1	Smart Contract 2	
2	Smart Contract 3	
3	Smart Contract 4	<input checked="" type="radio"/>
...		

Next

Back

Footer

25

A Web Page

https://solidity-to-cpn/initialmarking.html

🏠

🔍

Solidity

Roadmap

Start

Select Smart Contracts

Select Context

Choose Property

Generate SC to CPN

Check the SCs

Finished

☰

🔄

Configuration

Number of users

5

☒ Fixed

☐ Random

☐ Map

Balance

10

Smart Contract 1Smart Contract 2Smart Contract 3...

Function parameters

#	Functions	Arguments
1	Function 1	Input Params
2	Function 2	Input Params
3	Function 3	Input Params
4	Function 4	Input Params
...		

Next

Back

Footer

26a

←

→

✕

🏠

https://solidity-to-cpn/initialmarking.html

🔍

A Web Page

Solidity

Roadmap

[Start](#)

[Select Smart Contracts](#)

[Select Context](#)

[Choose Property](#)

Generate SC to CPN

Check the SCs

Finished

☰⚡

Configuration

Number of users

☐ Fixed

☒ Random

☐ Map

Balance

From

To

Function parameters

Smart Contract 1Smart Contract 2Smart Contract 3...

#	Functions	Arguments
1	Function 1	Input Params
2	Function 2	Input Params
3	Function 3	Input Params
4	Function 4	Input Params
...		

Next

Back

Footer

26b

A Web Page

https://solidity-to-cpn/initialmarking.html

Solidity

Roadmap

Start

Select Smart Contracts

Select Context

Choose Property

Generate SC to CPN

Check the SCs

Finished

Configuration

Number of users

5

☐ Fixed ☐ Random ☒ Map

Balance

1,2,3,4,5

Function parameters

Smart Contract 1Smart Contract 2Smart Contract 3...

#	Functions	Arguments
1	Function 1	Input Params
2	Function 2	Input Params
3	Function 3	Input Params
4	Function 4	Input Params
...		

Next

Back

Footer

27

←

→

✕

🏠

https://solidity-to-cpn/initialmarking.html

🔍

A Web Page

Solidity

Roadmap

●

●

●

●

●

●

●

[Start](#)

[Select Smart Contracts](#)

[Select Context](#)

[Choose Property](#)

Generate SC to CPN

Check the SCs

Finished

☰

↔

Input Parameters

Sender value

2

To

10

#	Parameters	Range
1	Argument 1	<div><div>1</div></div> To <div><div>5</div></div>
2	Argument 2	<div><div>1</div></div> To <div><div>5</div></div>
...		

Next

Back

Footer

26c

←

→

✕

🏠

https://solidity-to-cpn/initialmarking.html

🔍

A Web Page

Solidity

Roadmap

Start

Select Smart Contracts

Select Context

Choose Property

Generate SC to CPN

Check the SCs

Finished

☰

↺

Configuration

Type

☐ Fixed

☐ Random

☒ Map

User parameters

#	User	Balance
1	User 1	1
2	User 2	3
3	User 3	2
4	User 4	5
5	User 5	4
...		

Function parameters

Smart Contract 1

Smart Contract 2

Smart Contract 3

...

Function 1

Function 2

...

Sender value

2

To

10

#	Argument	Value
1	Argument 1	3
2	Argument 2	5
...		

Back

Footer

← → × ↗

https://solidity-to-cpn/index.html

🔍

A Web Page

Solidity

Roadmap

[Start](#) [Select Smart Contracts](#) [Select Context](#) [Choose Property](#) [Generate SC to CPN](#) [Check the SCs](#) [Finished](#)

☰

↺

Generating CPN Model

Smart Contracts

#	Contract Name
1	blindAuction
2	etherLotto
3	etherGame
4	...

Context

Gaming

LTL Property

Integer Overflow

Configuration

[Link to the setting configuration](#)

The smart contract is generating...

Generate

Back

When the user clicks on this button, the system will call the DCR2CPN tool to generate the context file, and then call the unfolding tool to generate the HCPN file to add atomic proposition to the HCPN file and create the property file (the input for Helena tool)

← → × ↶

A Web Page

https://solidity-to-cpn/index.html

🔍

Solidity

Roadmap

●

●

●

●

●

●

●

[Start](#) [Select Smart Contracts](#) [Select Context](#) [Choose Property](#) [Generate SC to CPN](#) [Check the SCs](#) [Finished](#)

☰ ⚡

Generating CPN Model

Smart Contracts

#	Contract Name
1	blindAuction
2	etherLotto
3	etherGame
4	...

Context

Gaming

LTL Property

Integer Overflow

Configuration

[Link to the setting configuration](#)

The generating process completed successfully

Next

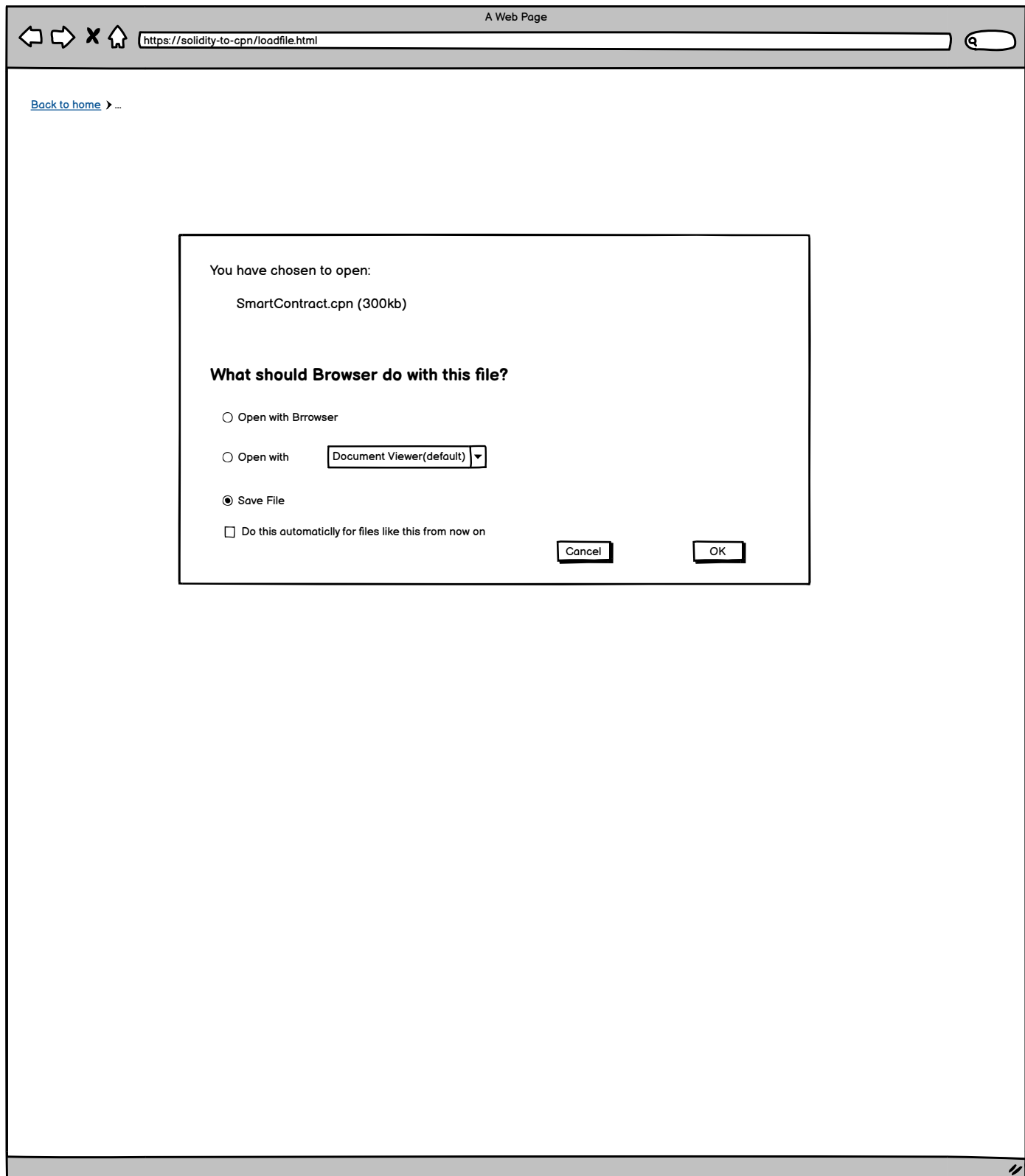
Download

Back

Click on "Download" button to download the CPN generated files

Footer

29a



← → × 🏠

A Web Page

https://solidity-to-cpn/index.html

🔍

Solidity

Roadmap

Start

Select Smart Contracts

Select Context

Choose Property

Generate SC to CPN

Check the SCs

Finished

☰ ⚡

Checking Smart Contracts

Smart Contracts

#	Contract Name
1	blindAuction
2	etherLotto
3	etherGame
4	...

Context

Gaming

LTL Property

Integer Overflow

Configuration

[Link to the setting configuration](#)

Check

Back

Footer

30a

← → × 🏠

A Web Page

https://solidity-to-cpn/index.html

🔍

Solidity

Roadmap

Start

Select Smart Contracts

Select Context

Choose Vulnerability

Generate SC to CPN

Check the SCs

Finished

☰ ⚡

Checking Smart Contracts

Smart Contracts

#	Contract Name
1	blindAuction
2	etherLotto
3	etherGame
4	...

Context

Gaming

LTL Property

Integer Overflow

Configuration

[Link to the setting configuration](#)

The smart contract is checking...

Check

Back

When the user clicks on this button, the system will call the Helena tool to check the CPN file generated by tools in the previous steps and get the result from the Helena tool to show on the screen for the user.

Footer

30b

← → × ↗

A Web Page

https://solidity-to-cpn/index.html

🔍

Solidity

Roadmap

Start

Select Smart Contracts

Select Context

Choose Vulnerability

Generate SC to CPN

Check the SCs

Finished

☰ ☲

Checking Smart Contracts

Smart Contracts

#	Contract Name
1	blindAuction
2	etherLotto
3	etherGame
4	...

Context

Gaming

LTL Property

Integer Overflow

Configuration

[Link to the setting configuration](#)

The checking process completed successfully

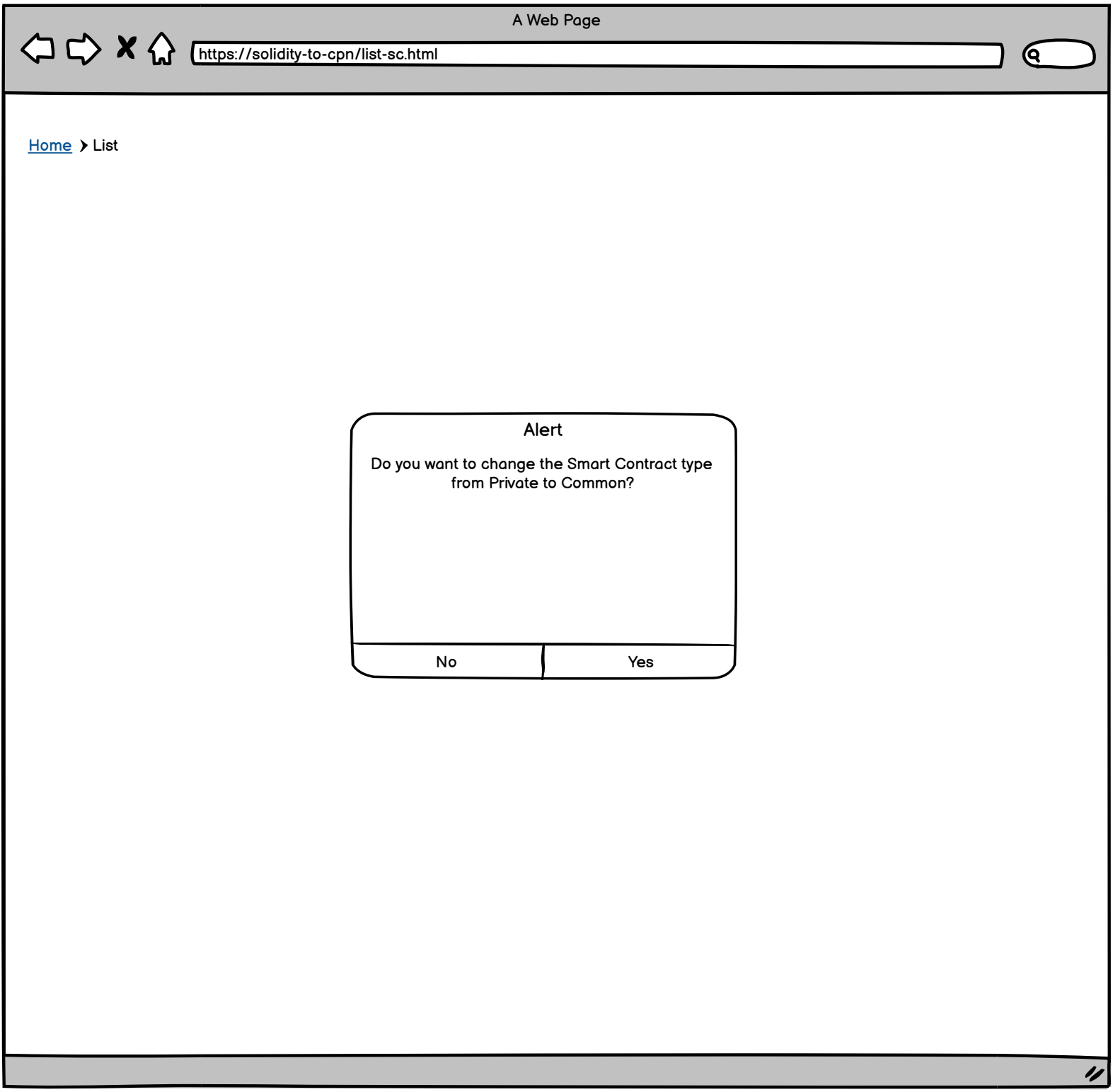
Check

Back

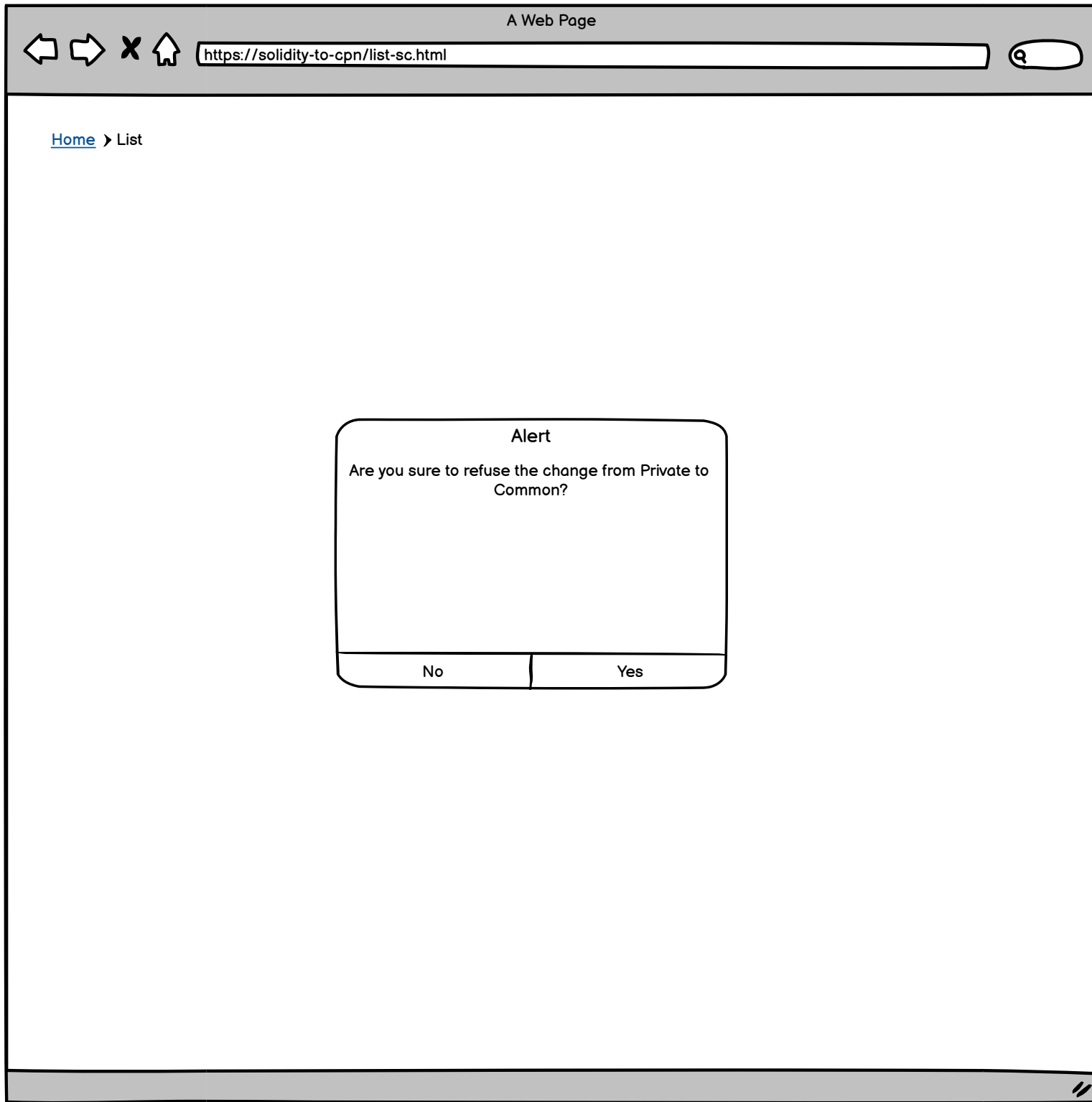
Footer

11

32a



32b



33

A Web Page






https://solify-to-cpn/add-sc.html


Create a new Smart Contract code


Name


Smart Contract Type


- Common
- Private
- Pending

B I U S *style*     









Admin can create a new smart contract type in any types

A Web Page

https://solidity-to-cpn/edit-sc.html

Smart contract 1

Smart Contract Type

Common

Common

Private

Pending

Content

B I U style

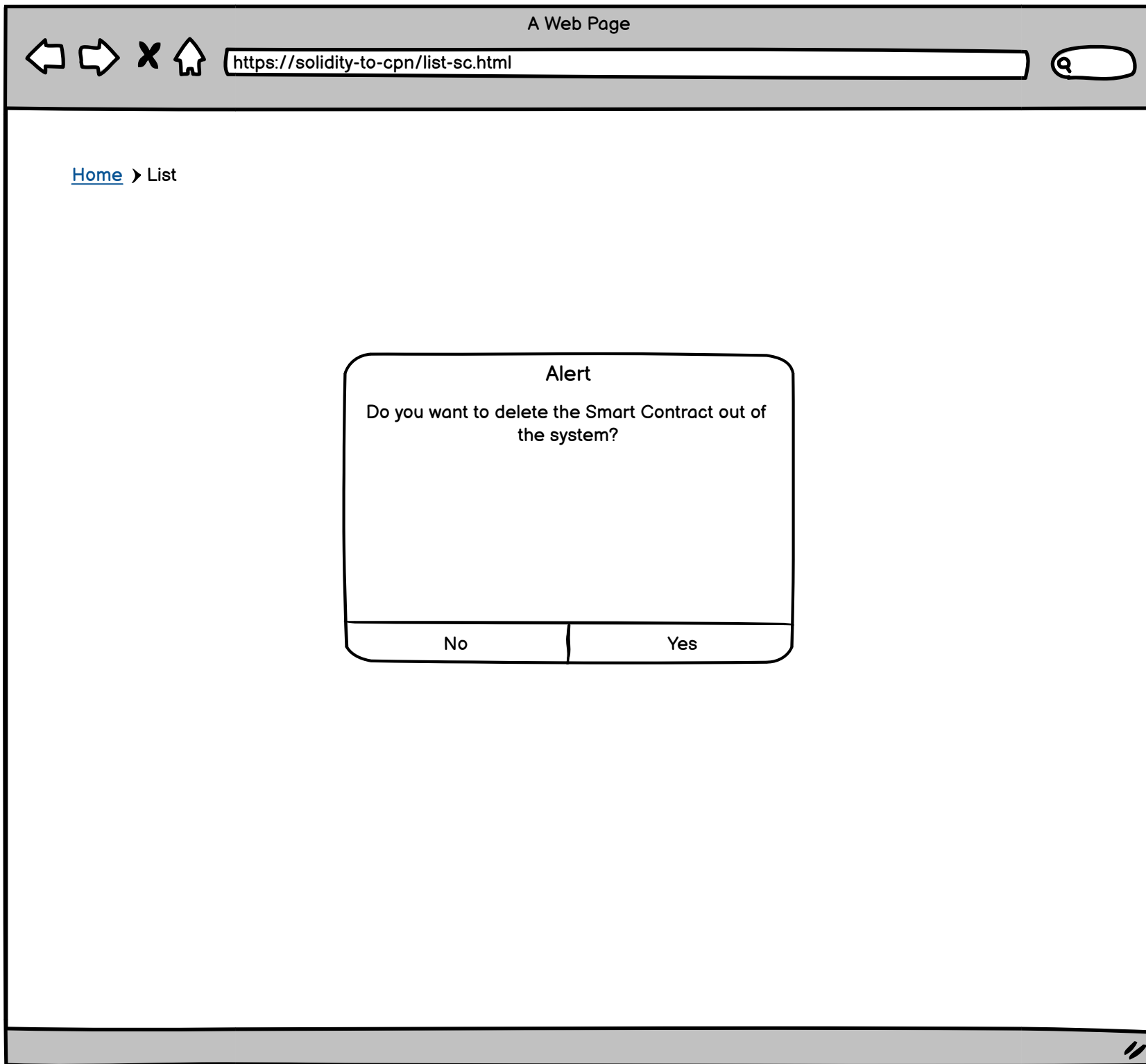
Description

Save

Cancel

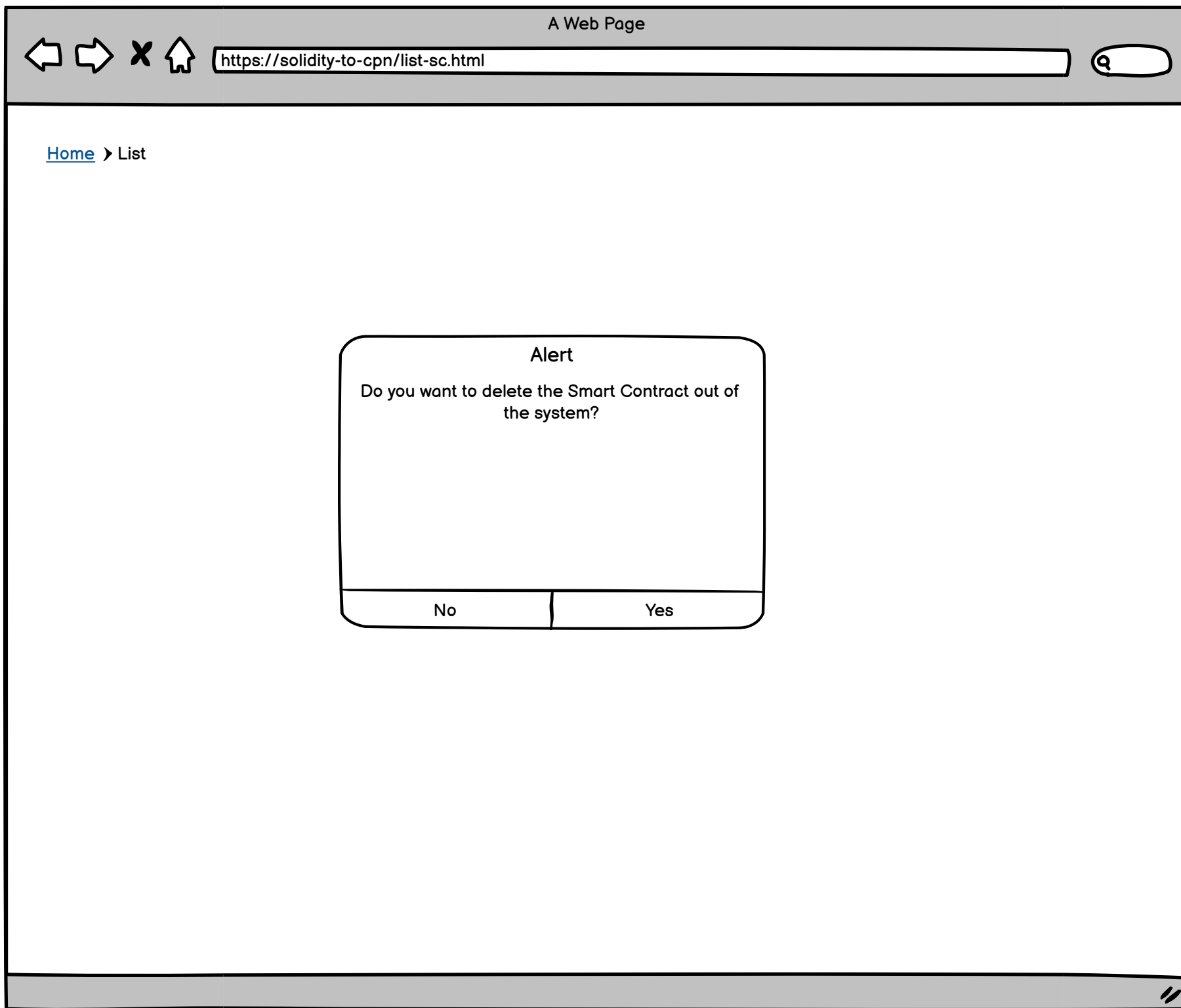
Admin can change the smart contract type from private to common
If user requested to change the SC type from private to common, the type will be Pending

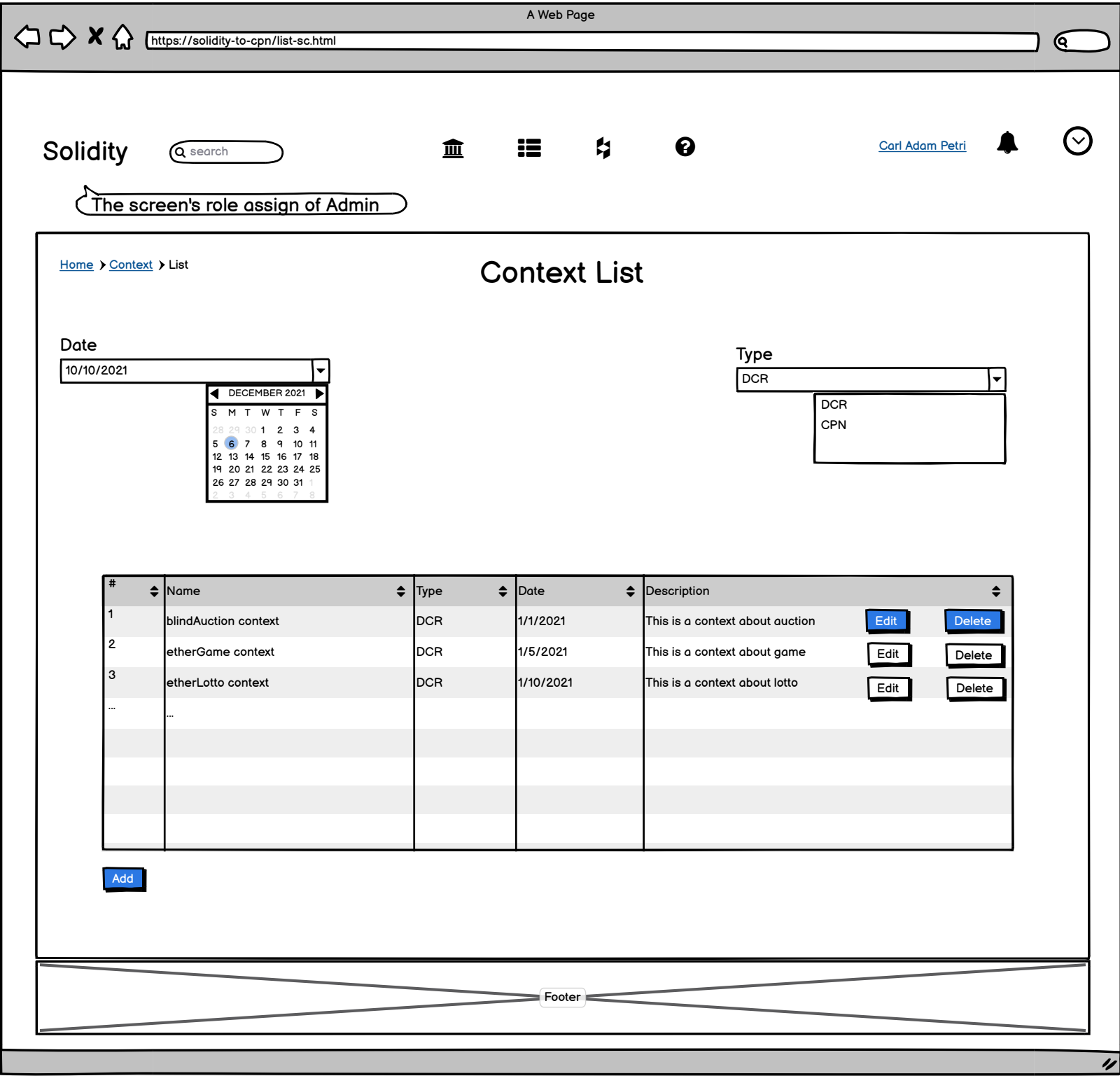
32c



Cancel

35a





39

A Web Page


https://solify-to-cpn/add-context.html

Create a new Context

Name

Type

Description



Content

```
test(N := 2) {  
  type boolean : range 0 .. 1;  
  type count : range 0 .. N;  
  function cvalue (marking_value mv, vchange lc) ->  
    marking_value{  
      marking_value m := empty;  
      for(v in mv){  
        m := m & v;  
      }  
      for(v in lc){  
        m[v.id] := v.vl;  
      }  
      return m;  
    }  
}
```

A Web Page


https://solify-to-cpn/edit-context.html

Update the Context

Name

Type

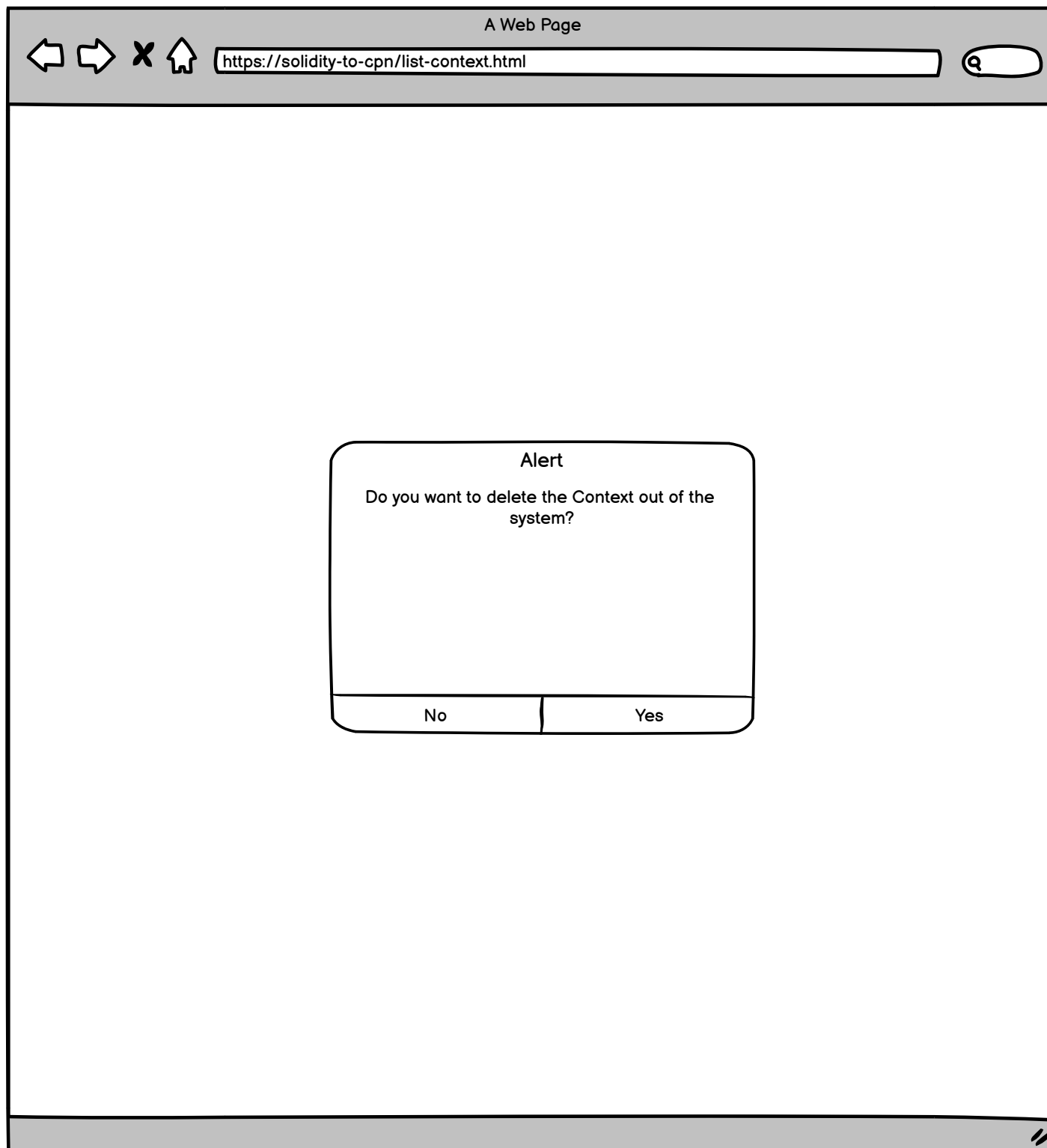
Description



Content

```
test(N := 2) {  
  type boolean : range 0 .. 1;  
  type count : range 0 .. N;  
  function cvalue (marking_value mv, vchange lc) ->  
  marking_value{  
    marking_value m := empty;  
    for(v in mv){  
      m := m & v;  
    }  
    for(v in lc){  
      m[v.id] := v.vi;  
    }  
    return m;  
  }  
}
```

38a



41

A Web Page

https://solidity-to-cpn/list-ltl.html

Solidity

search

[Carl Adam Petri](#)

The screen's role assign of Admin

Home

LTL

List

LTL Property Template List

Date

10/10/2021

DECEMBER 2021

S

M

T

W

T

F

S

28

29

30

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

1

2

3

4

5

6

7

8

Type

CSP

CSP

Vulnerability

#	Name	Type	Date	Description
1	LTL property 1	CSP	1/1/2021	bla bla
2	LTL property 2	CSP	1/5/2021	bla bla
3	LTL property 3	CSP	1/10/2021	bla bla
...	...			

Add

Footer

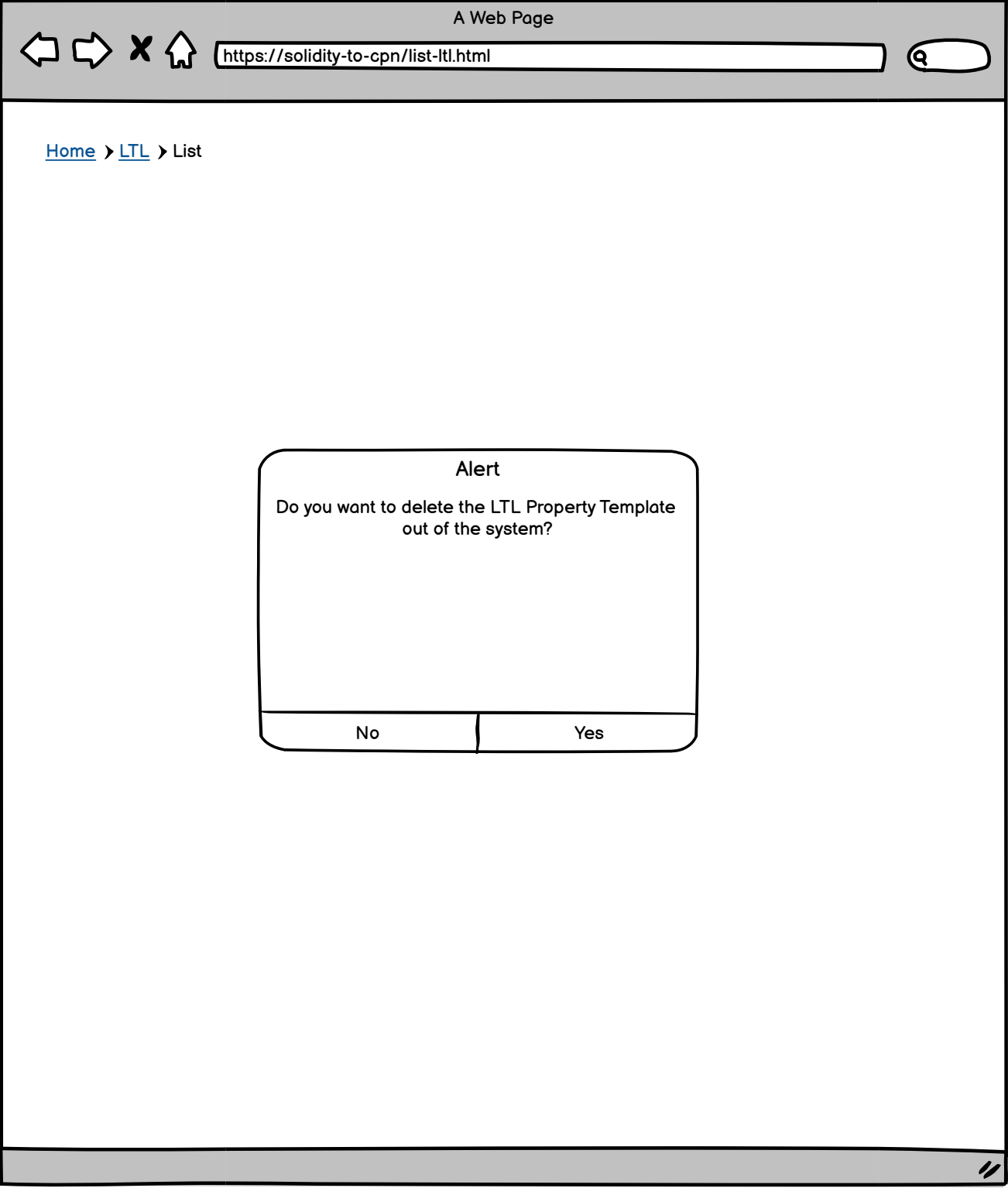
Livello

$$G(\{ \text{local variable} \}) \Rightarrow F \{ \text{global variable} \}$$

After an occurrence of { local variable 1 } there will be at least one occurrence of { global variable 2 }

Cancel

41a



Starts

Select Smart Contracts

Select Context

Choose Contract-Specific Property or Vulnerability

[Generate Smart Contract to CPN](#)

Check Smart Contracts

Finished

The result is displayed on the screen for viewing. If there is any counter-example, the user can have a look at them in the smart contracts.