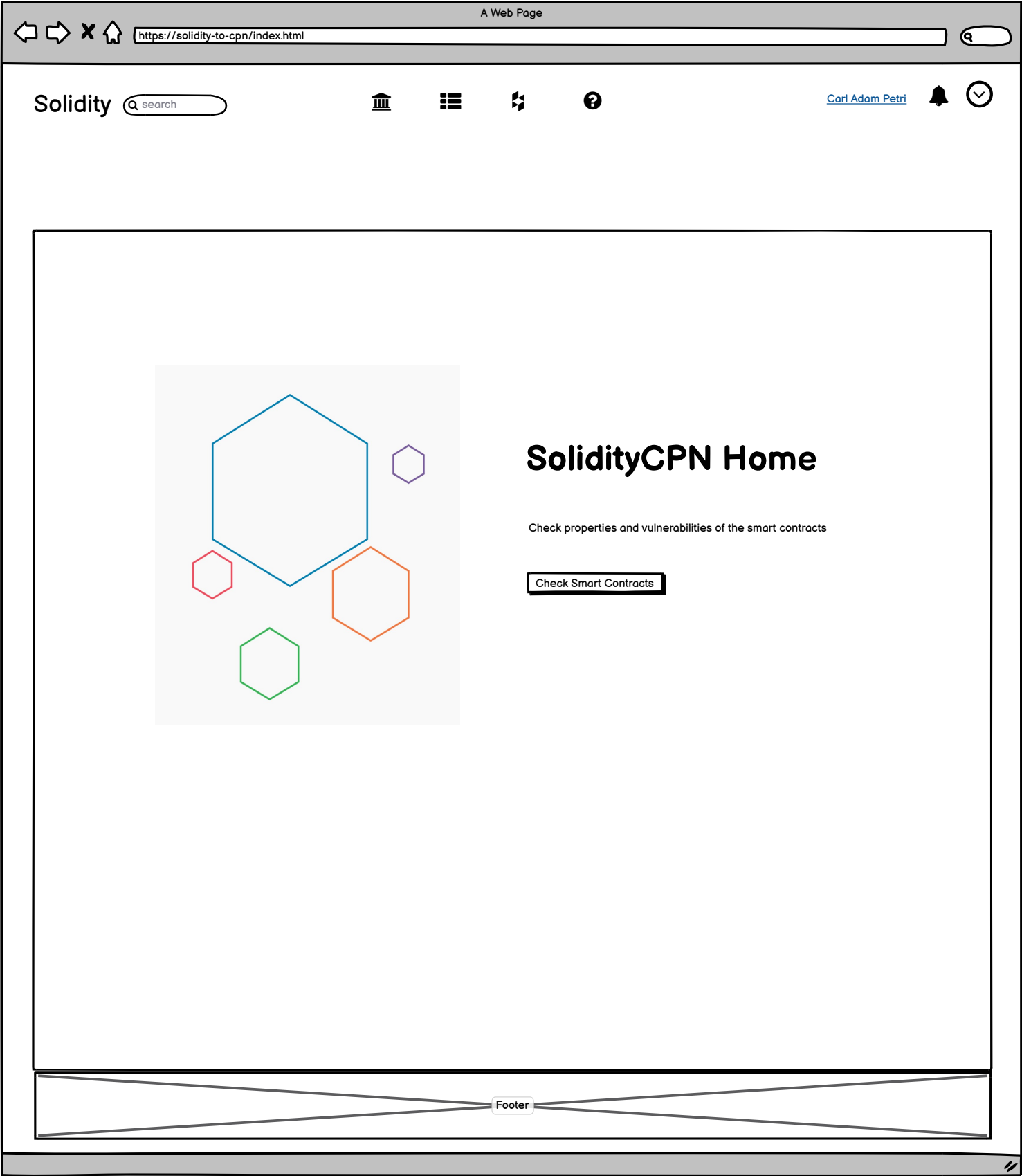
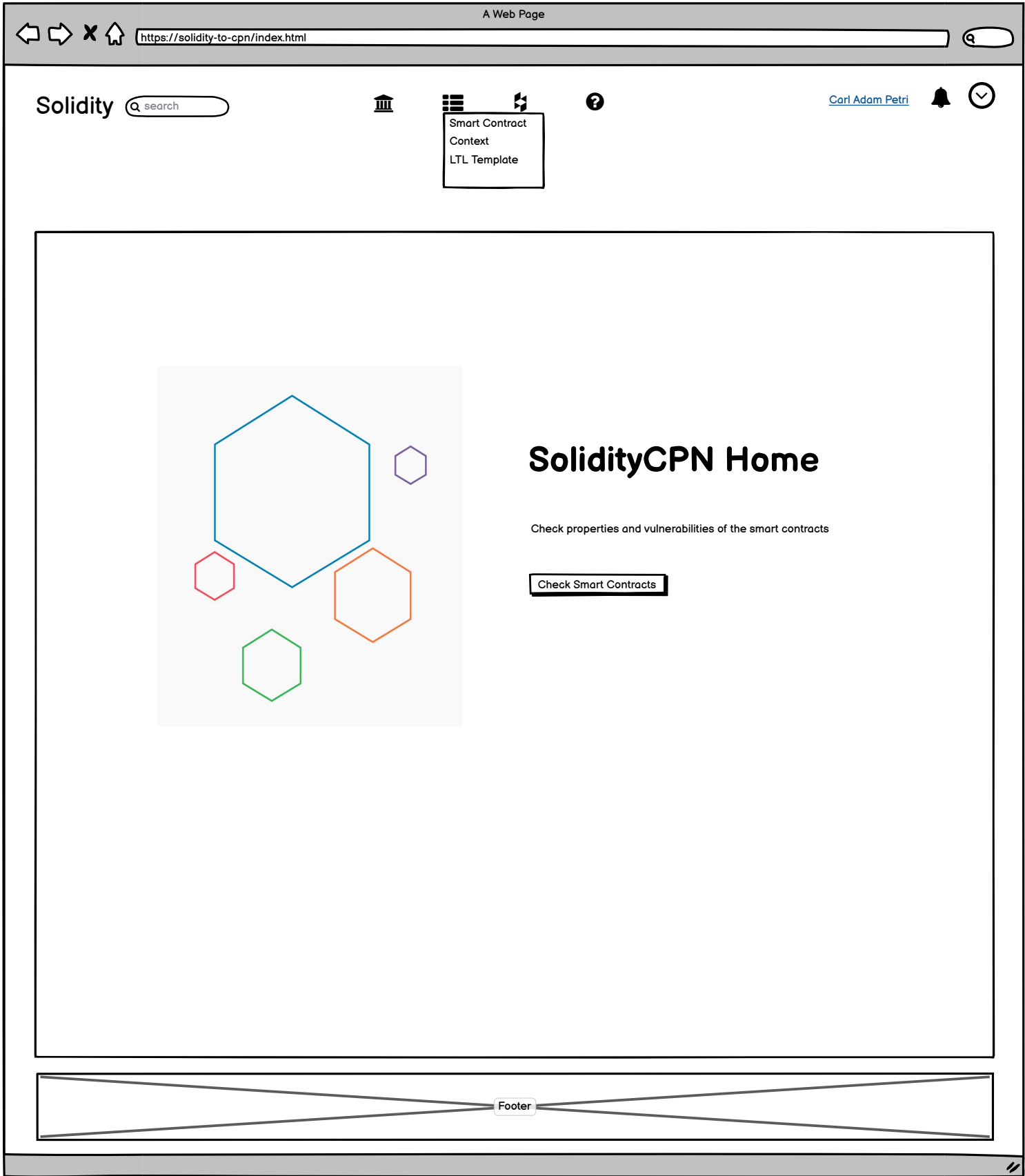


1



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

←→✕🏠

A Web Page

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

🔍

Solidity

Roadmap

Start

Select Smart Contracts

Select Context

Choose Vulnerability

Generate SC to CPN

Check the SCs

Finished

☰⌂

Smart Contract Detailed Information

#	Smart Contract Name	Context	LTL	Status	Date	Result
1	etherLottor					
	etherGame	context 1	LTL name 1	True	9/10/2021	Successfully
	blindAuction					
...	...					

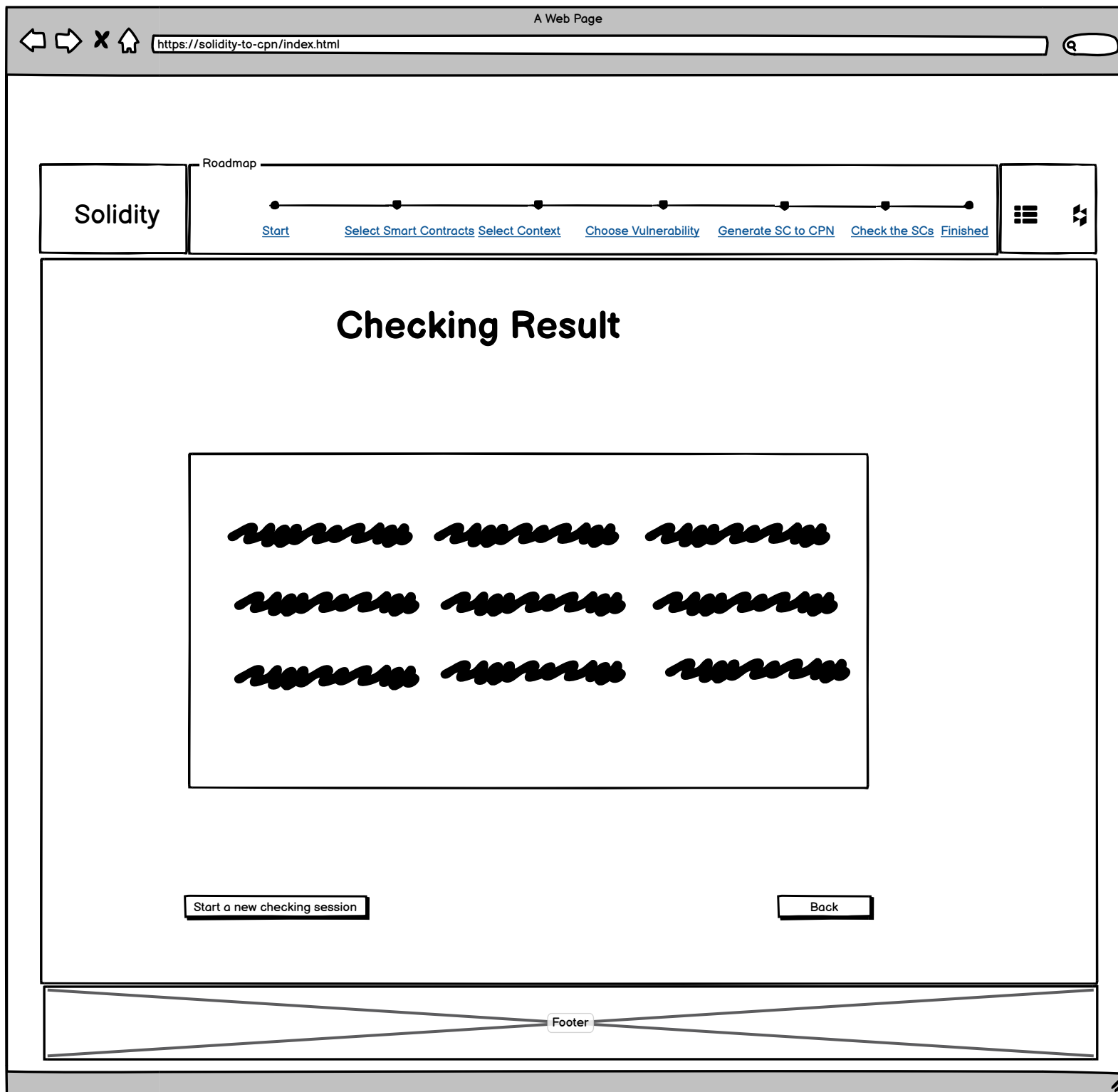
The user click here to go to the detail results

Start a new checking session

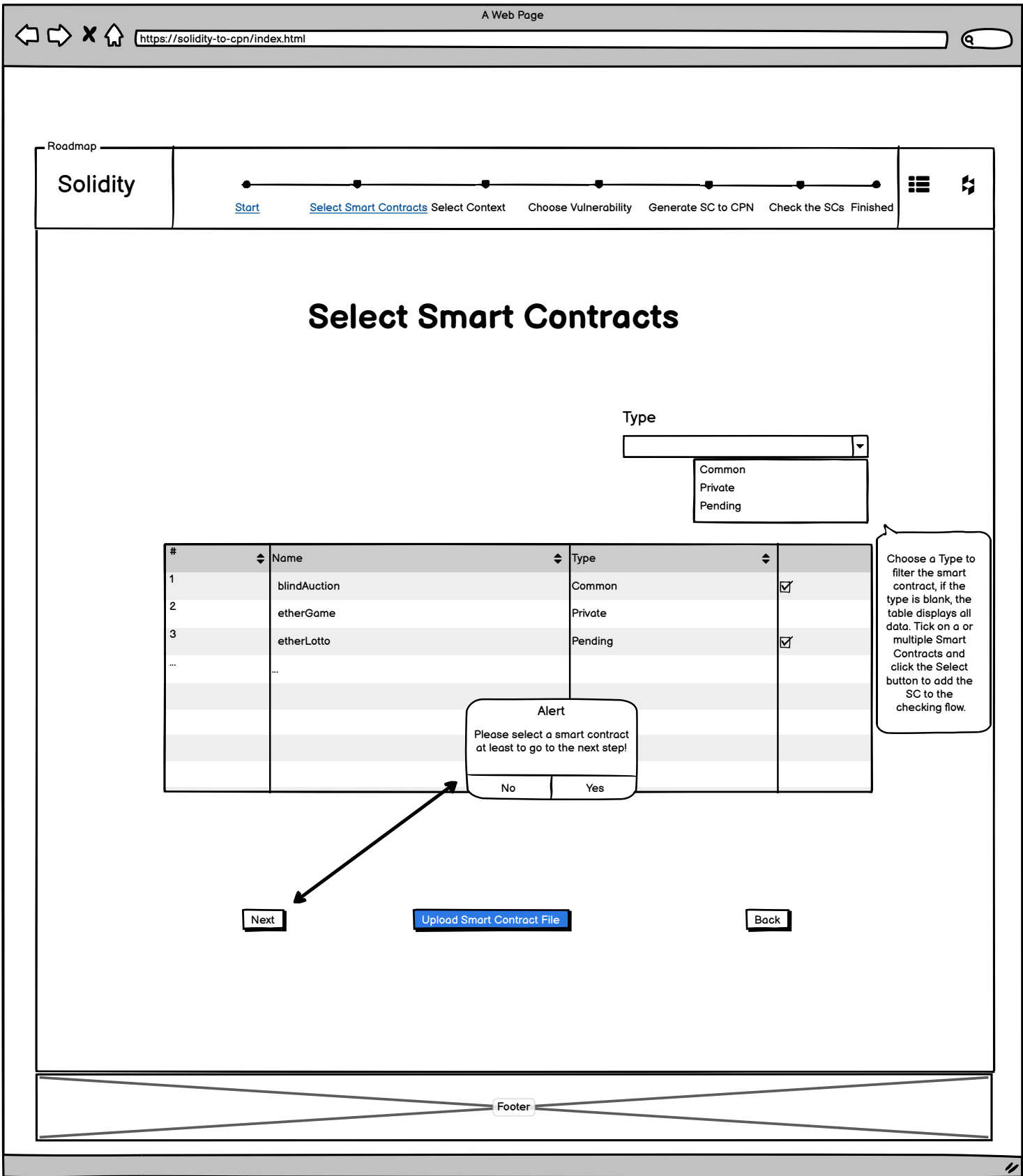
Back

Footer

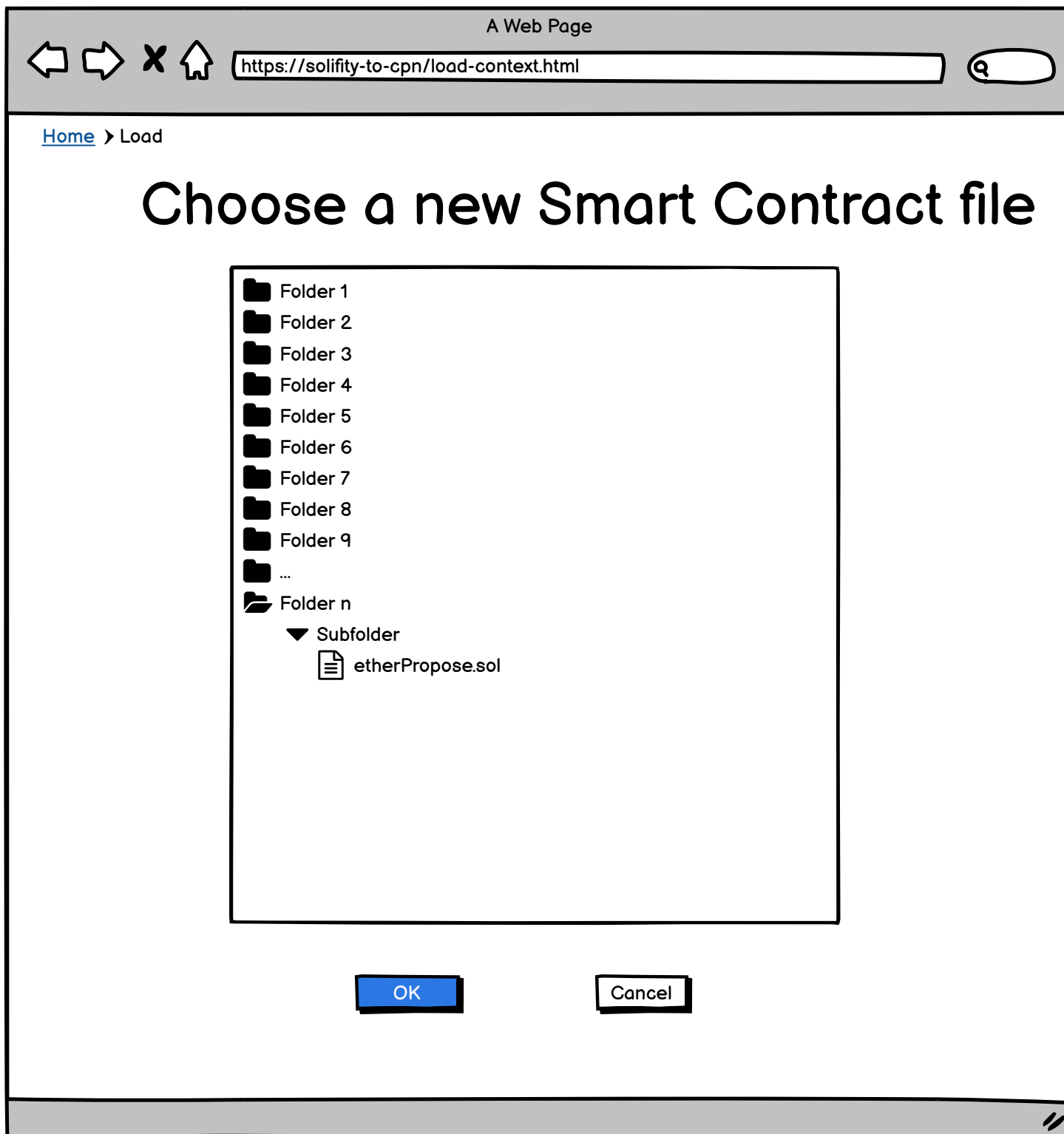
4



5



5a



6

A Web Page

X

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

Q

[Home](#) > Upload

Upload a new Smart Contract code

Name

etherPropose

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

~~~~~

~~~~~

~~~~~

~~~~~

Save

Cancel

7

←

→

✕

🏠

A Web Page

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

🔍

Solidity

Roadmap

●

●

●

●

●

●

●

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

☰⏮

Select Context

Name

Lotto

- Medicine

- Game

- ...

- 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

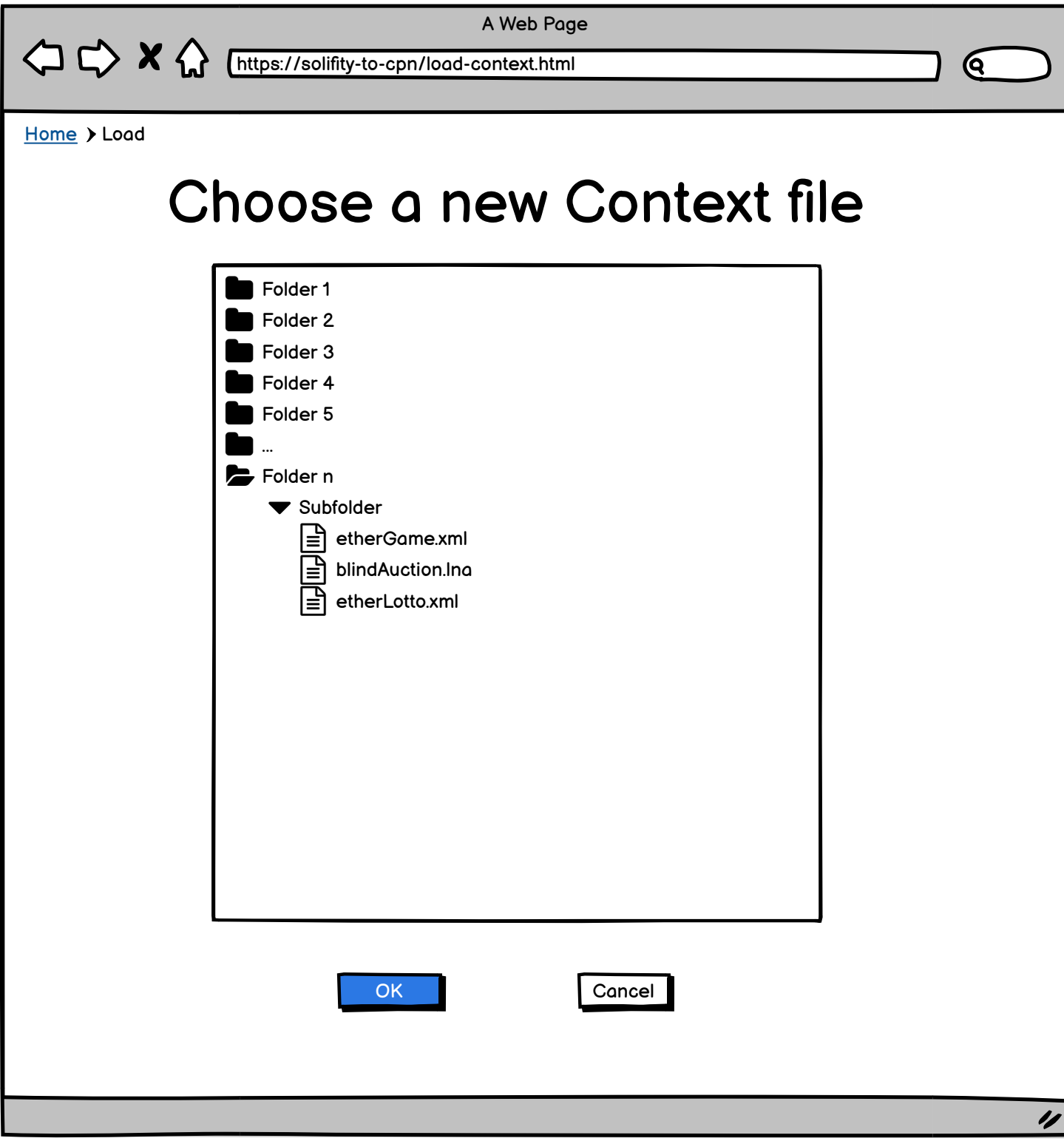
Skip

Back

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

Footer

7a



8

A Web Page

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

[Home](#) > Upload

Upload a new Context file

Name

Type

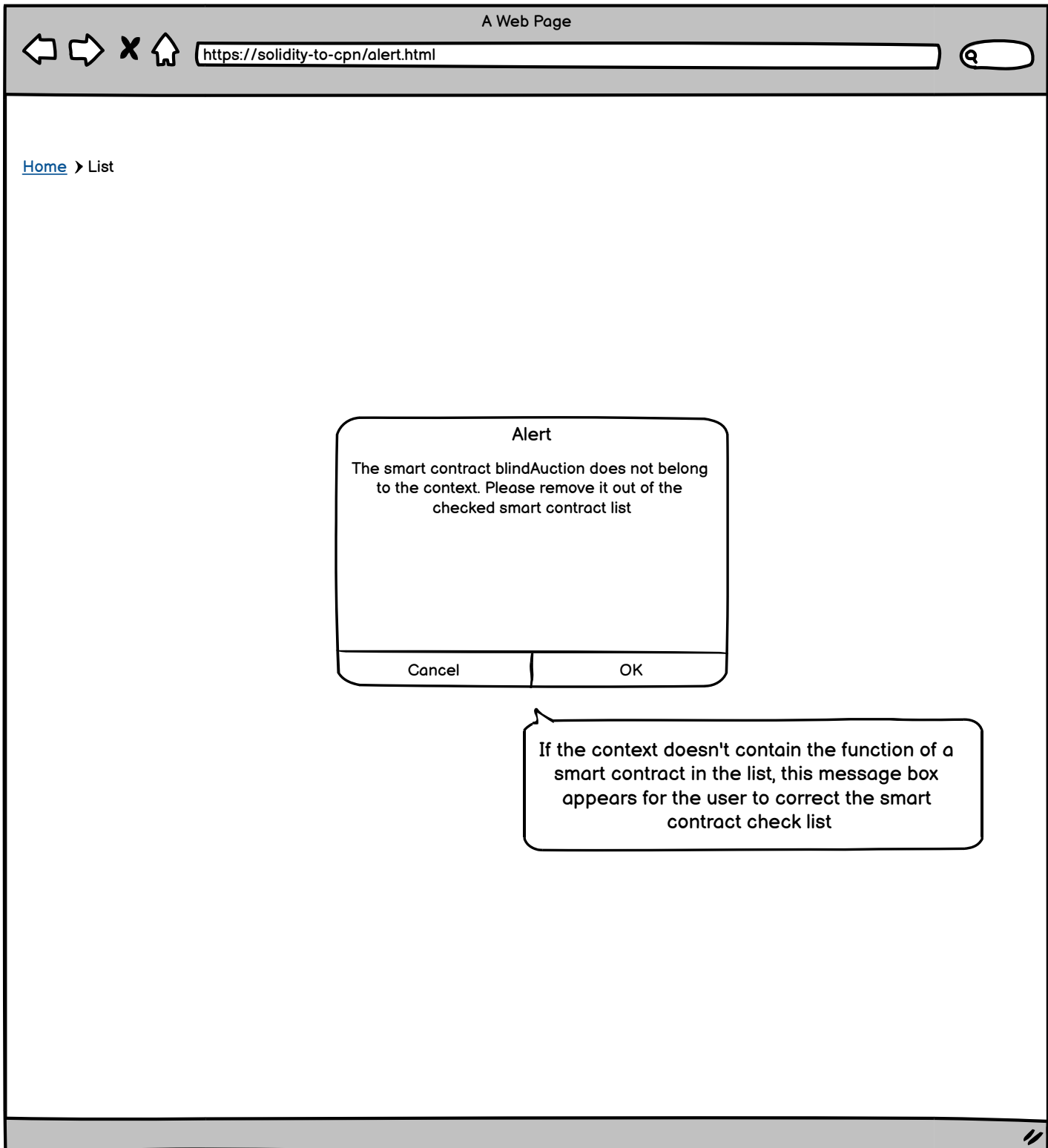
- DCR
- CPN
- ...

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.)

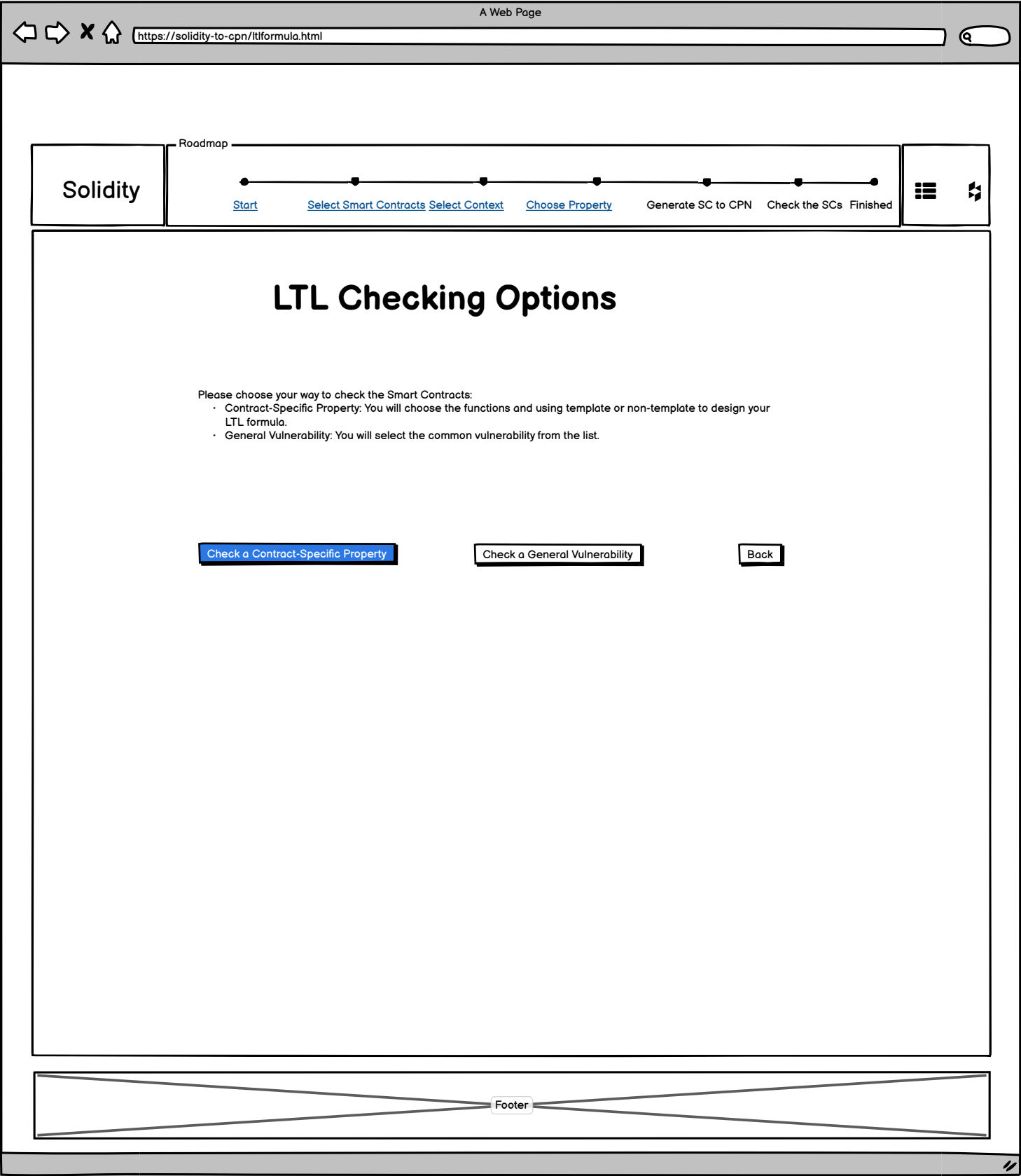
Content

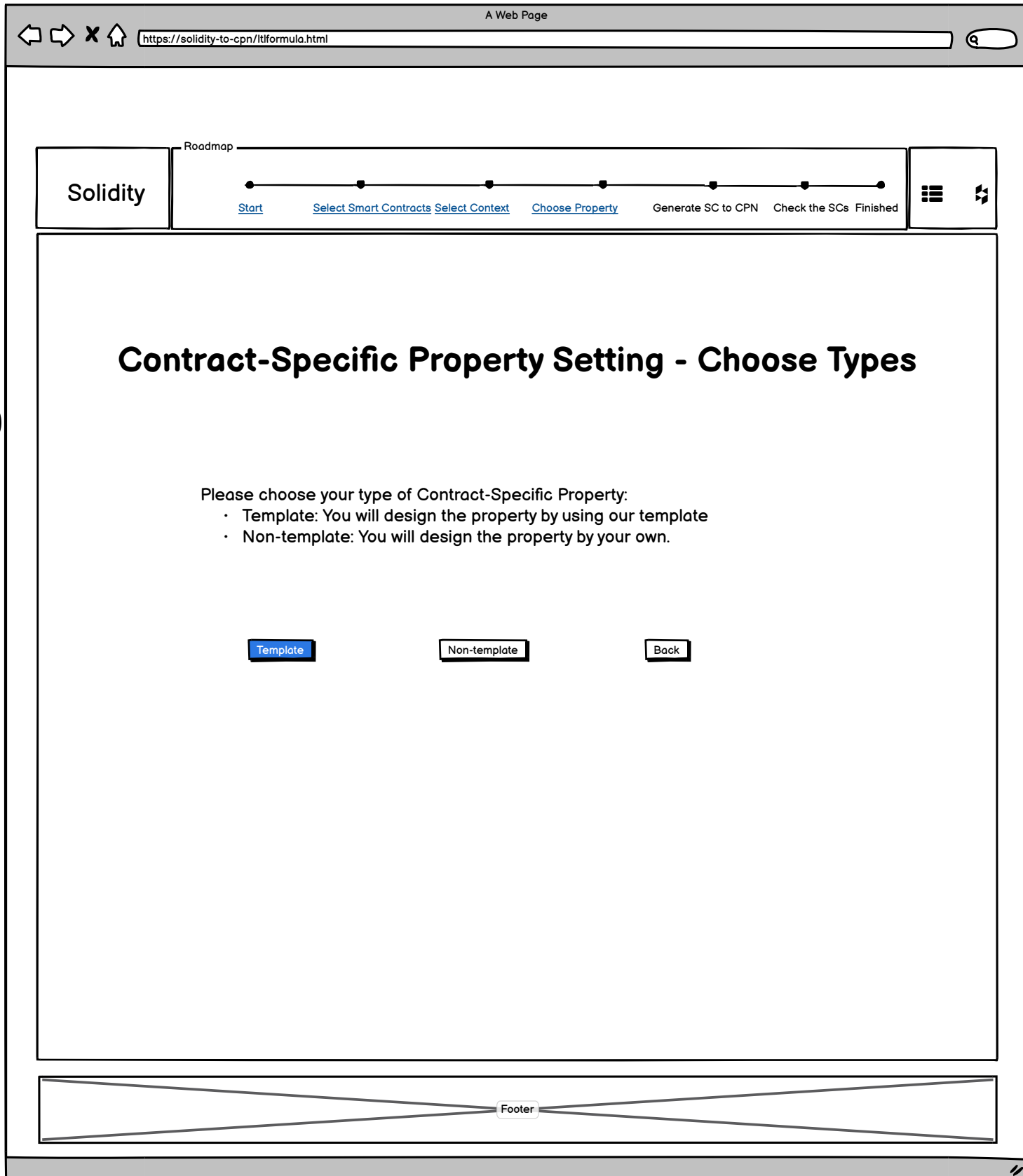
Description

7b



9





11

←

→

✕

🏠

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 Template - Setting

Name

Mutual exclusion

Template

Template 1

Template 1

Template 2

Template 3

Template 4

Template 5

...

Others

Formula

(GF{ local variable 1 } ^ GF{ global variable 2 }) => G({ local variable 2 }=> F{ global variable 2 })

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

Description

If [variable 1](#) occurs infinitely often and [variable 2](#) occurs infinitely often, then each occurrence of [function3](#) is followed by an occurrence of [function 4](#)

Select

Back

Footer

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 All []
1	GV1	<input checked="" type="checkbox"/>
2	GV2	<input type="checkbox"/>
3	GV3	<input type="checkbox"/>
4	GV4	<input type="checkbox"/>
...		

Save

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 All []
1	Function 1	
2	Function 2	
3	Function 3	
4	Function 4	<input checked="" type="checkbox"/>
...		

Save

Cancel

14

A Web Page

X

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

Q

[Back to home](#)

Select local variables of the smart contract

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

Function 1Function 2Function 3...

#	Local variables	Selected All []
1	LV1	
2	LV2	
3	LV1	
4	LV2	<input checked="" type="checkbox"/>
...		

Save

Cancel

← → × 🏠

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 Template - Setting

Name

Mutual exclusion

Template

Template 1

Template 1

Template 2

Template 3

Template 4

Template 5

...

Others

Formula

(GF{ [local variable 1](#) } ^ GF{ [global variable 1](#) }) => G({ [local variable 2](#) }=> F{ [global variable 2](#) })

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

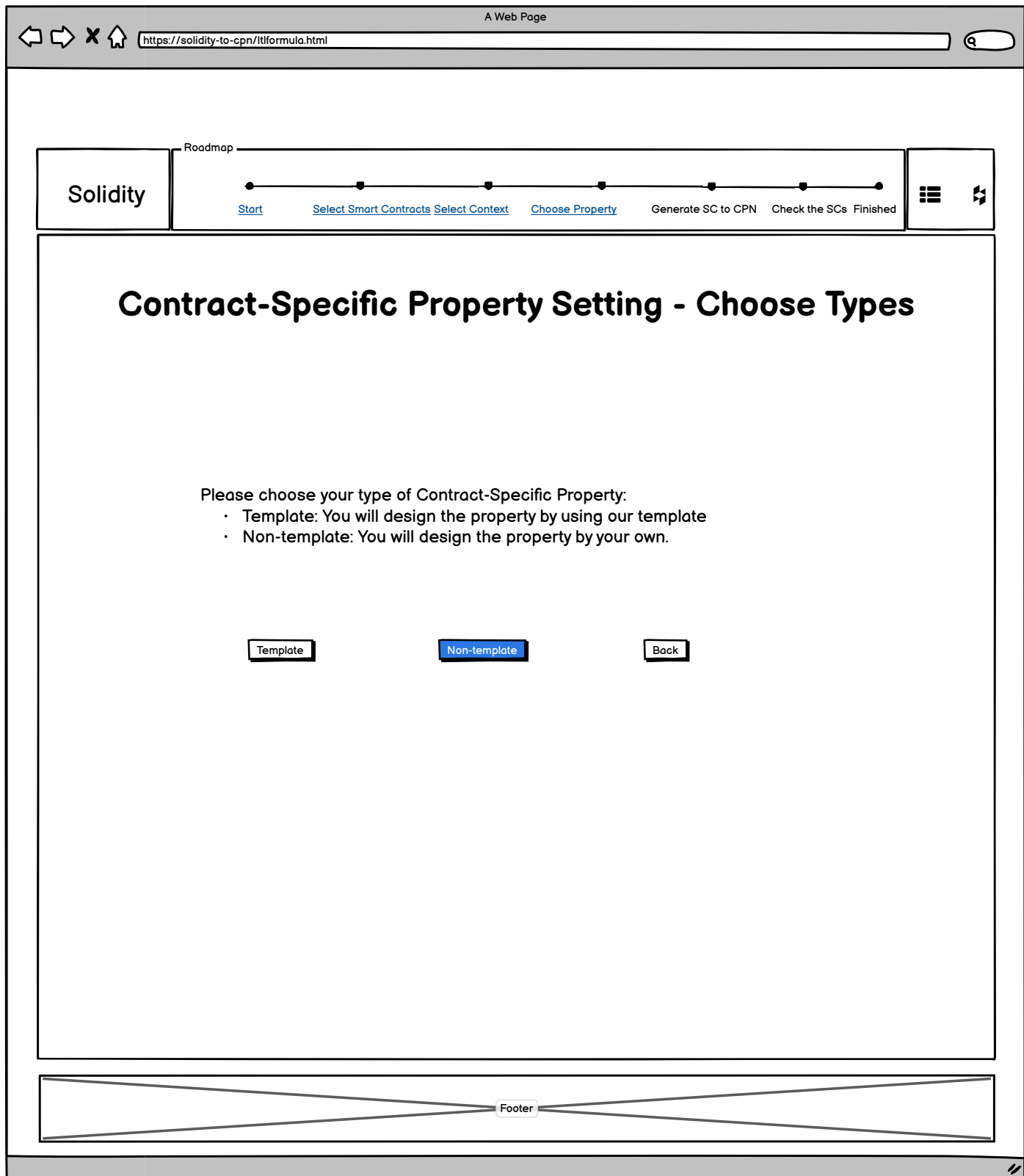
If [{variable 1}](#) occurs infinitely often and [{variable 2}](#) occurs infinitely often, then each occurrence of [{function 3}](#) is followed by an occurrence of [{function 4}](#)

Select

Back

Footer

10a



←

→

✕

🏠

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

Contract-Specific Property Setting - Non Template

Name

Check payment

Formula

B I U S style

G ({ function 1 }=> (~{ function 2 } U { function 3 })))

The users will write the formula by themselves. If the formula is invalid the tool will show an error when reading.

Description

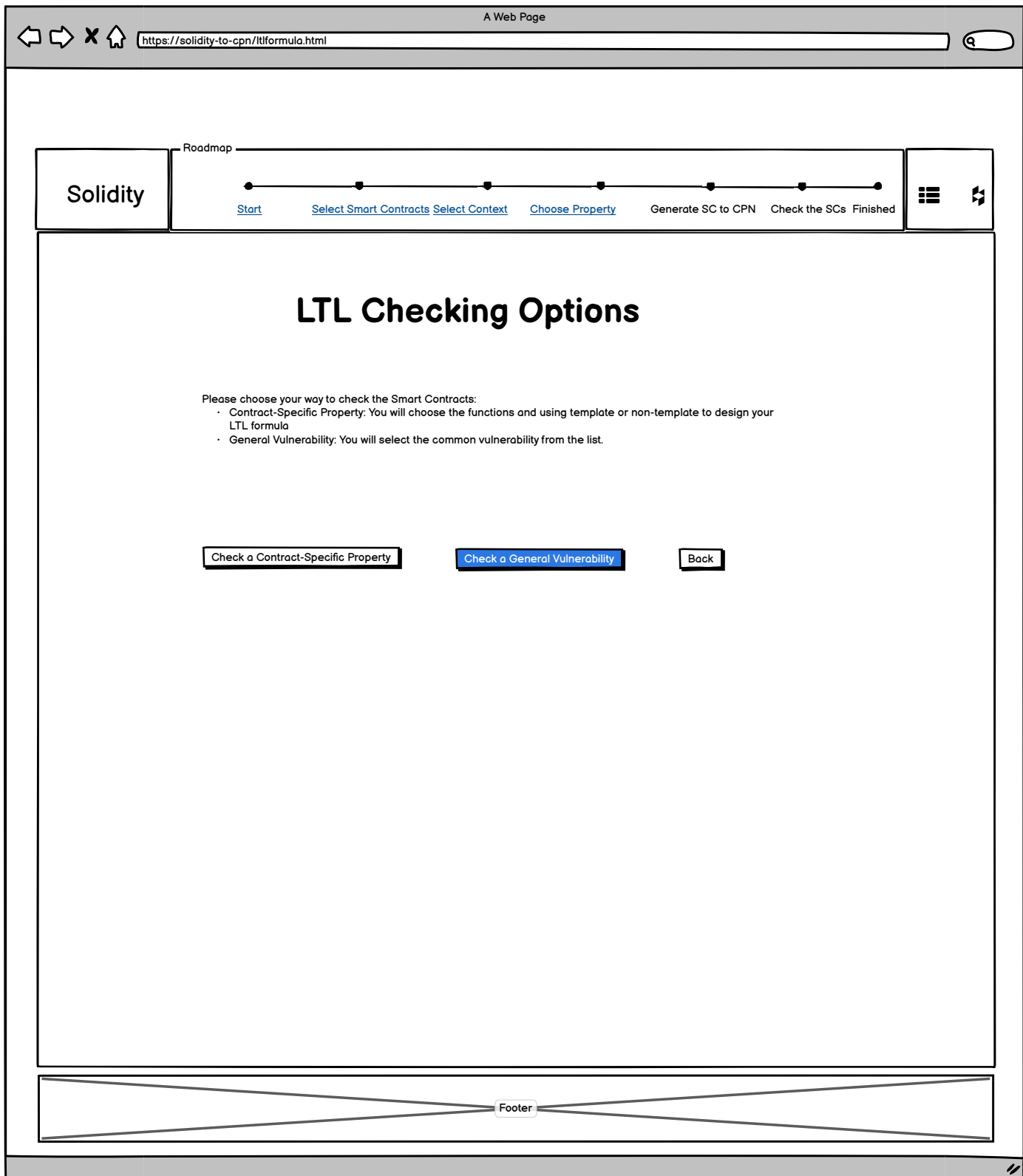
No other function 1 orders are accepted between the function 2 of the amount due and the function 3

Select

Back

Footer

9a



←

→

✕

🏠

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)

Select

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 global variables of the smart contracts

Smart Contract 1

Smart Contract 2

Smart Contract 3

...

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

Function 1

Function 2

...

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

Next

Back

Footer

16a

←

→

✕

🏠

A Web Page

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

🔍

Solidity

Roadmap

●

●

●

●

●

●

●

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

☰

↺

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:

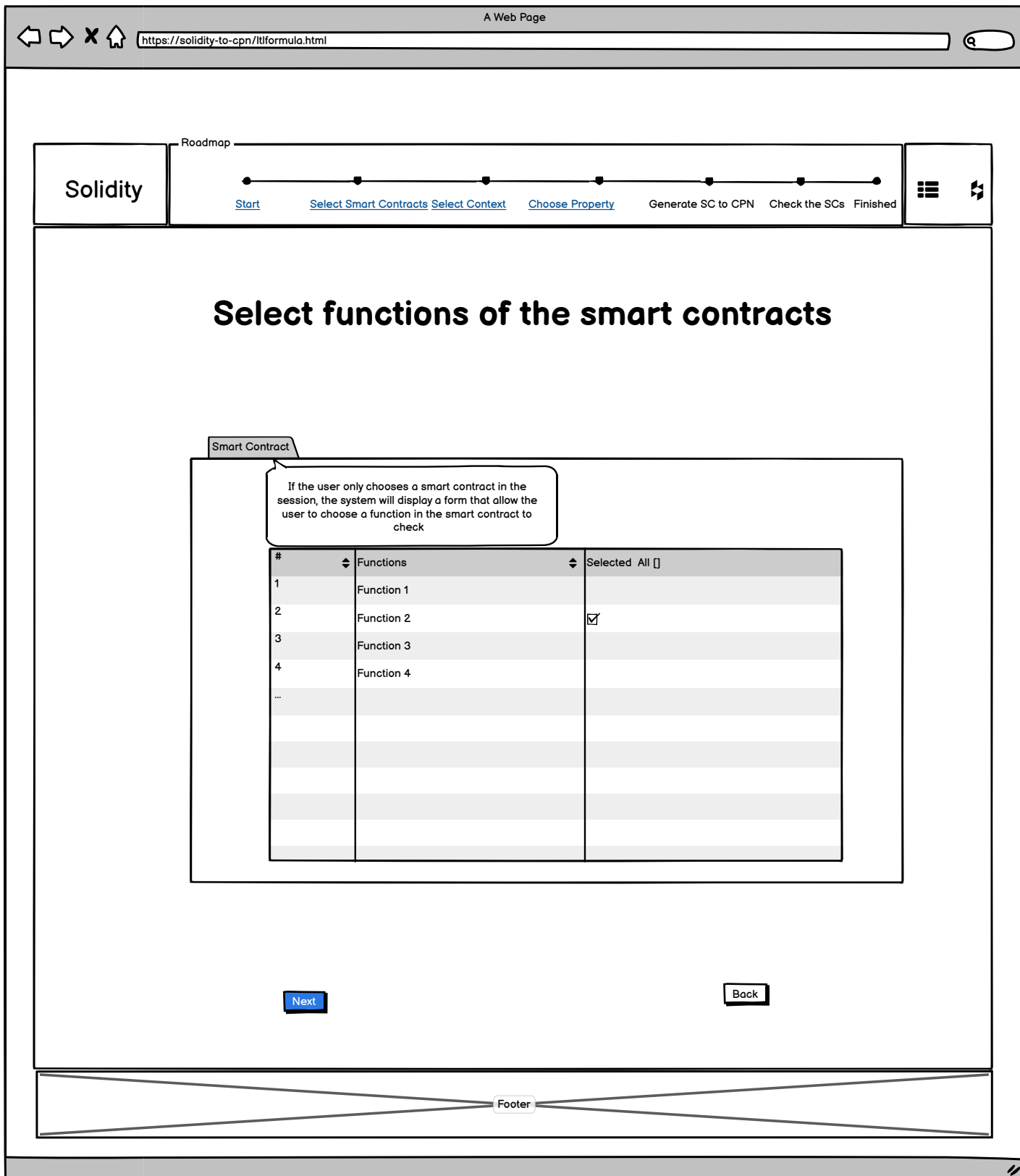
• If the user choose only one smart contract then the user only need to choose a function

• If the user chooses more than one smart contract, then the user can choose a function and another variable

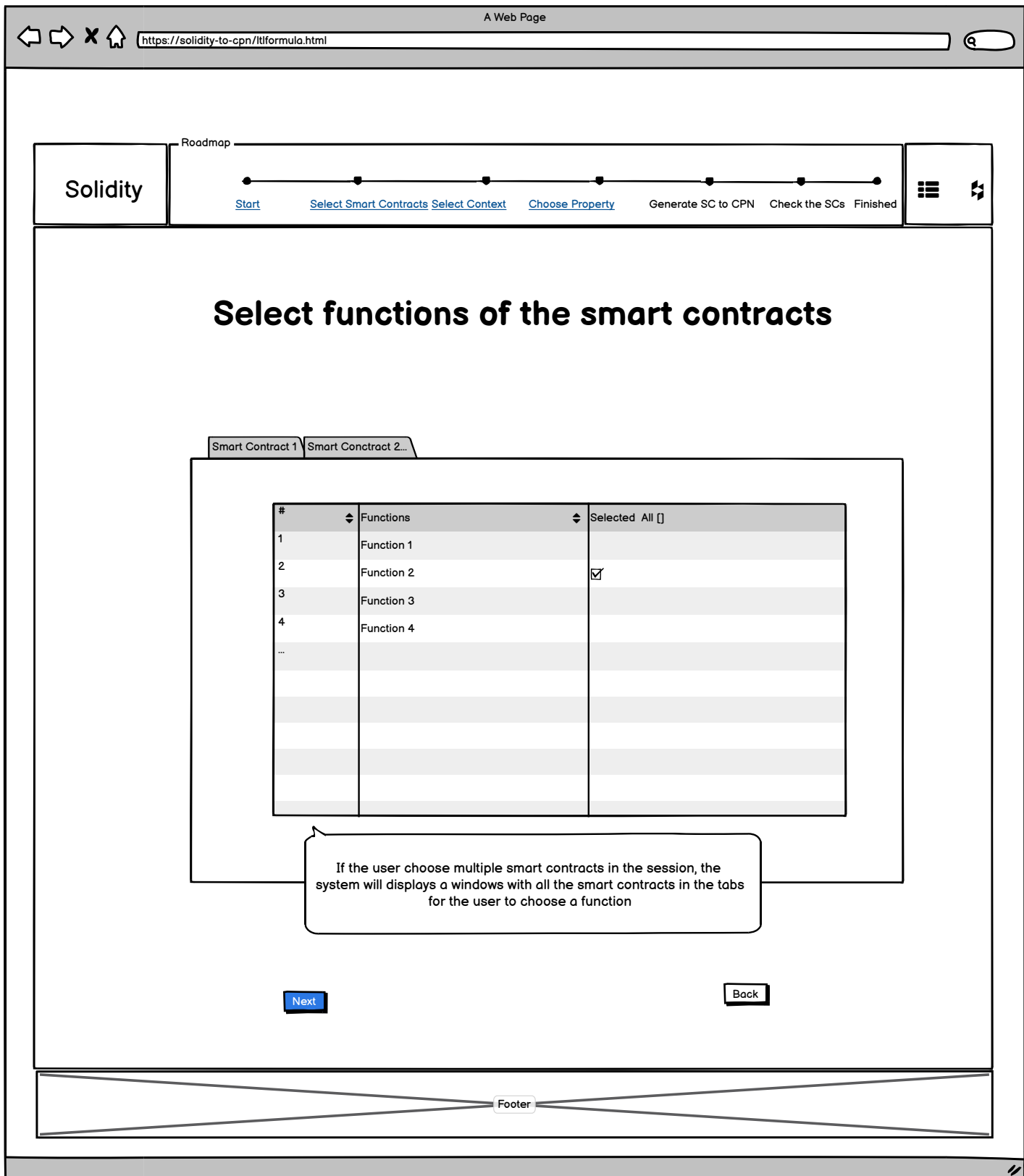
Select

Back

Footer



18a



17a

← → × ↗

A Web Page

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

Q

Solidity

Roadmap

●

●

●

●

●

●

●

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

☰

⚡

Select variables of the smart contracts

Smart Contract 2

Smart Contract 3

...

And then the system will display a windows with the remaining smart contracts for the user to choose a variable. If the user do not choose any variable, the system will go back to the option 1

#	Global variables	Selected	All []
1	LV1	<input checked="" type="checkbox"/>	
2	LV2	<input type="checkbox"/>	
3	LV3	<input type="checkbox"/>	
4	LV4	<input type="checkbox"/>	
...			

Function 1

Function 2

...

#	Local variables	Selected	All []
1	LV1	<input type="checkbox"/>	
2	LV2	<input type="checkbox"/>	
3	LV3	<input type="checkbox"/>	
4	LV4	<input type="checkbox"/>	
...			

Next

Back

Footer

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 Vulnerability 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

There are two options for the reentrancy vulnerability:

- If the user choose only one smart contract then the user only need to choose a function
- If the user chooses more than one smart contract, then the user can choose a function and another variable

Select

Back

Footer

18c

←→✕🏠

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

☰

↺

Select functions of the smart contracts

Smart Contract 1Smart Contract 2...

#	Functions	Selected All <input type="checkbox"/>
1	Function 1	
2	Function 2	<input checked="" type="checkbox"/>
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 two options for the reentrancy vulnerability:

- If the user choose only one smart contract then the user only need to choose a function
- If the user chooses more than one smart contract, then the user can choose a function and another variable

Select

Back

Footer

18b

←→✕🏠

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

☰

↺

Select functions of the smart contracts

Smart Contract 1

Smart Contract 2

...

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

Next

Back

Footer

18c

...

If the user chooses a function in 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 the option 1 (only one function is chosen)

Back

←

→

✕

🏠

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

☒ Fixed ☐ Random ☐ Map

Balance

Function parameters

Smart Contract 1

Smart Contract 2

Smart Contract 3

...

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

Add

Back

Footer

19a

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

From

To

1

10

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
...		

Add

Back

Footer

19b

← → × ↗

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 1

Smart Contract 2

Smart Contract 3

...

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

Add

Back

Footer

20

← → × 🏠

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>
...		

Save

Back

Footer

17a

← → × ↗

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

context name

LTL Property

#	LTL Property Name	Variable	Type
1	Integer Overflow	currentBalance	Vulnerability

Configuration

#	User	Balance	Parameters
1	user 1	3	2
2	user 2	2	1
3	...		
...			

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)

17b

← → × ↶

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

blindAuction-DCR

LTL Property

#	LTL Property Name	Variable	Type
1	Integer Overflow	currentBalance	Vulnerability

Configuration

#	User	Balance	Parameters
1	user 1	3	2
2	user 2	2	1
3	..		
...			

The generating process completed successfully

Next

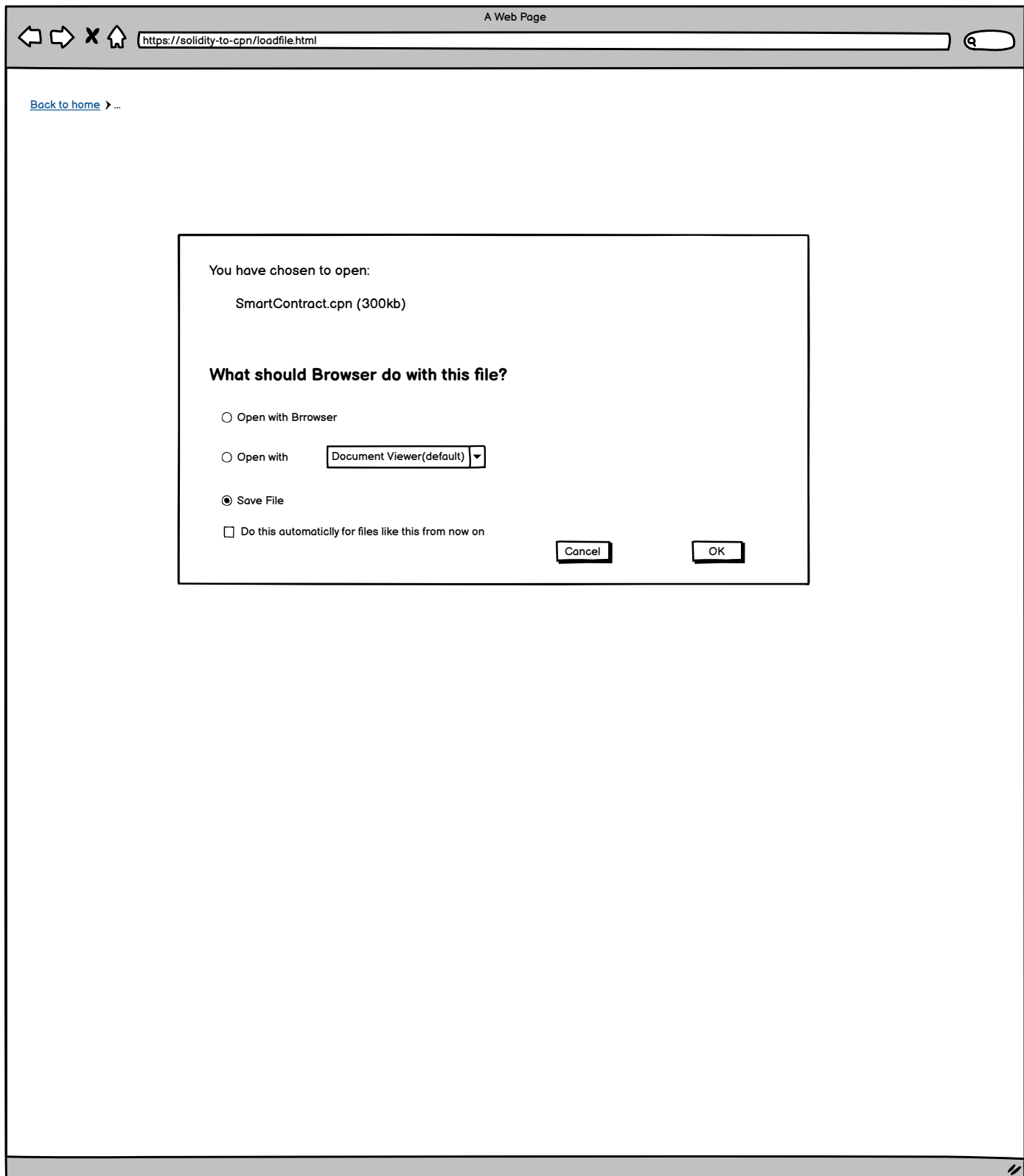
Download

Back

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

Footer

17b



23a

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

blindAuction-DCR

LTL Property

#	LTL Property Name	Type
1	Integer Overflow	Vulnerability
...		

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

23b

← → × ↗

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

blindAuction-DCR

LTL Property

#	LTL Property Name	Type
1	Integer Overflow	Vulnerability
...		

The checking process completed successfully

Check

Back

Footer

24

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 Result

#	Smart Contract Name	Context	LTL	Status	Date	Result
1	etherLotto					
	etherGame	context 1	LTL name 1	True	9/10/2021	Successfully
	blindAuction					
...	...					

When the user clicks on this link, the result will be displayed

Checking with the same LTL property and different configuration

Checking with different LTL property

Start a new checking session

Back

Footer

//

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

Solidity

search

[Carl Adam Petri](#)

The smart contract CRUD page of Admin

Home > List

Smart Contracts Lists

Date

10/10/2021

OCTOBER 2021

S

M

T

W

T

F

S

26

27

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

Type

Pending

Common

Private

Pending

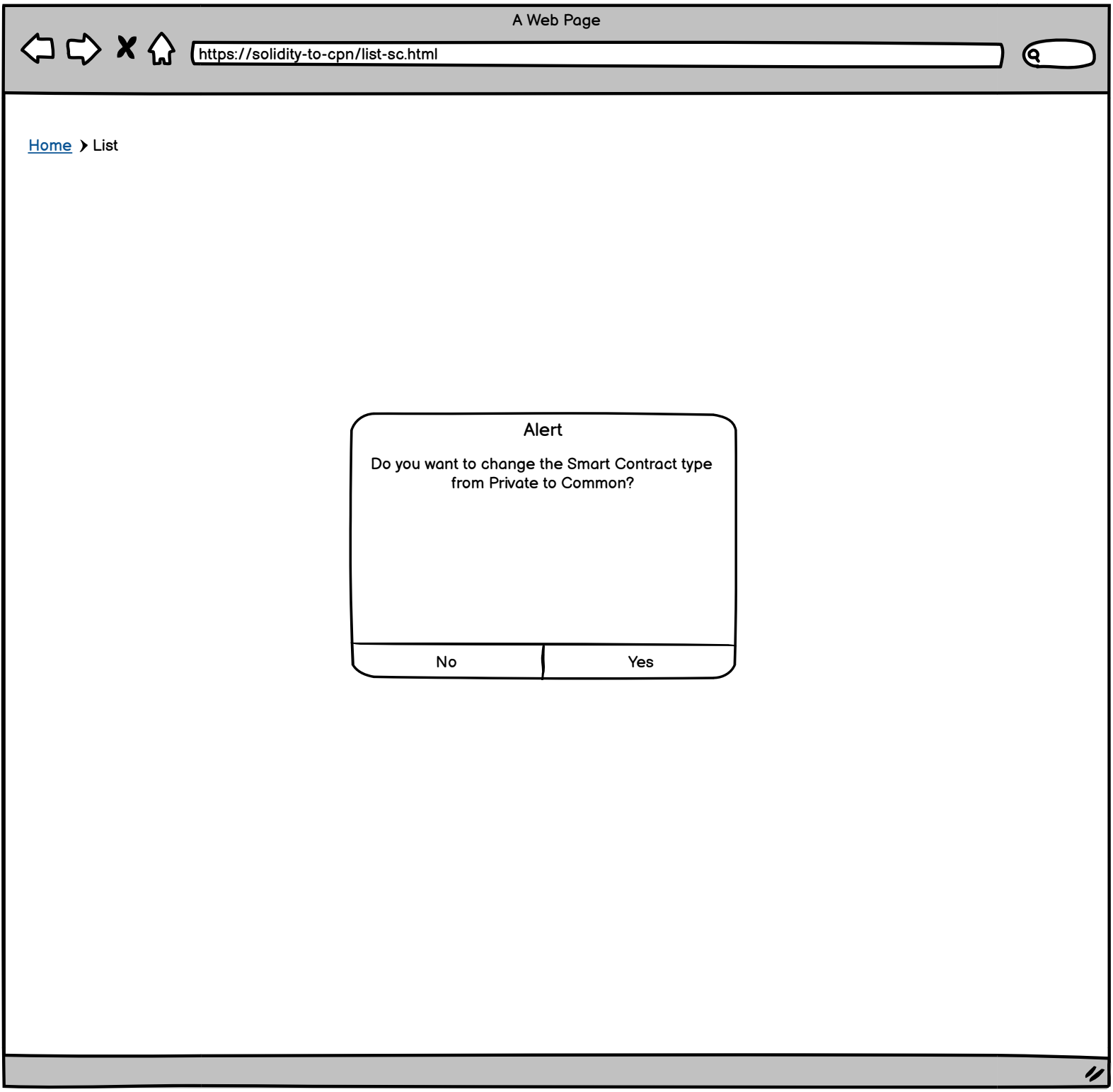
Only Admin can see the private smart contracts that are requested to be common ones (Pending)

#	Name	Type	Date	Description	
1	blindAuction	Pending	1/1/2021	This is a smart contract about auction	<div>EditDeleteAcceptRefuse</div>
2	etherGame	Pending	1/5/2021	This is a smart contract about game	<div>EditDeleteAcceptRefuse</div>
3	etherLotto	Pending	1/10/2021	This is a smart contract about lotto	<div>EditDeleteAcceptRefuse</div>
...	...				

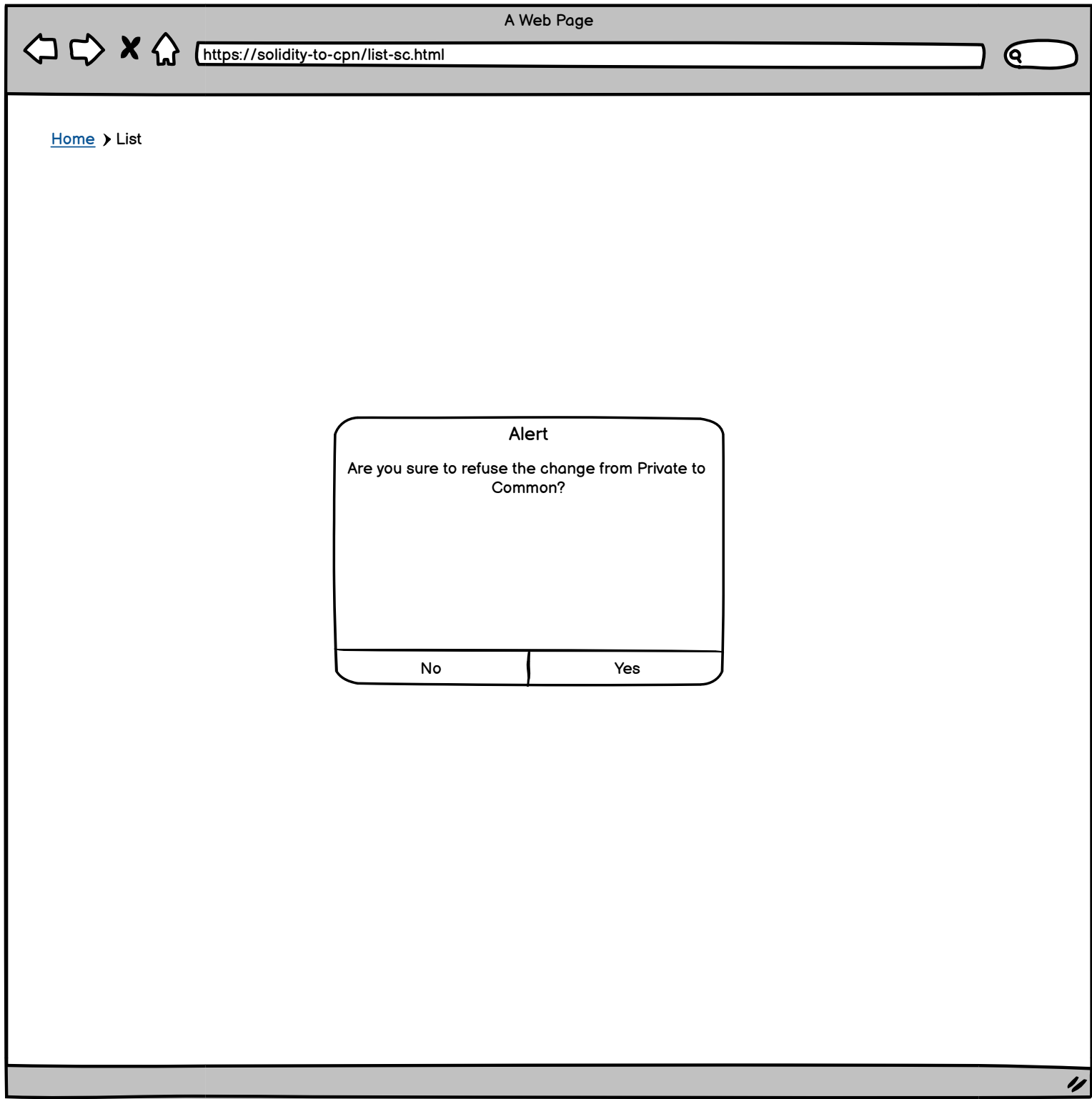
Add

Footer

26a



26b



27

A Web Page

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

[Home](#) > Add

Create a new Smart Contract code

Name

Smart Contract Type

- Common
- Private
- Pending

B I U S *style*

[Redacted content]

Admin can create a new smart contract type in any types

Edit the Smart Contract code


Smart contract 1

Common

Common
Private
Pending

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

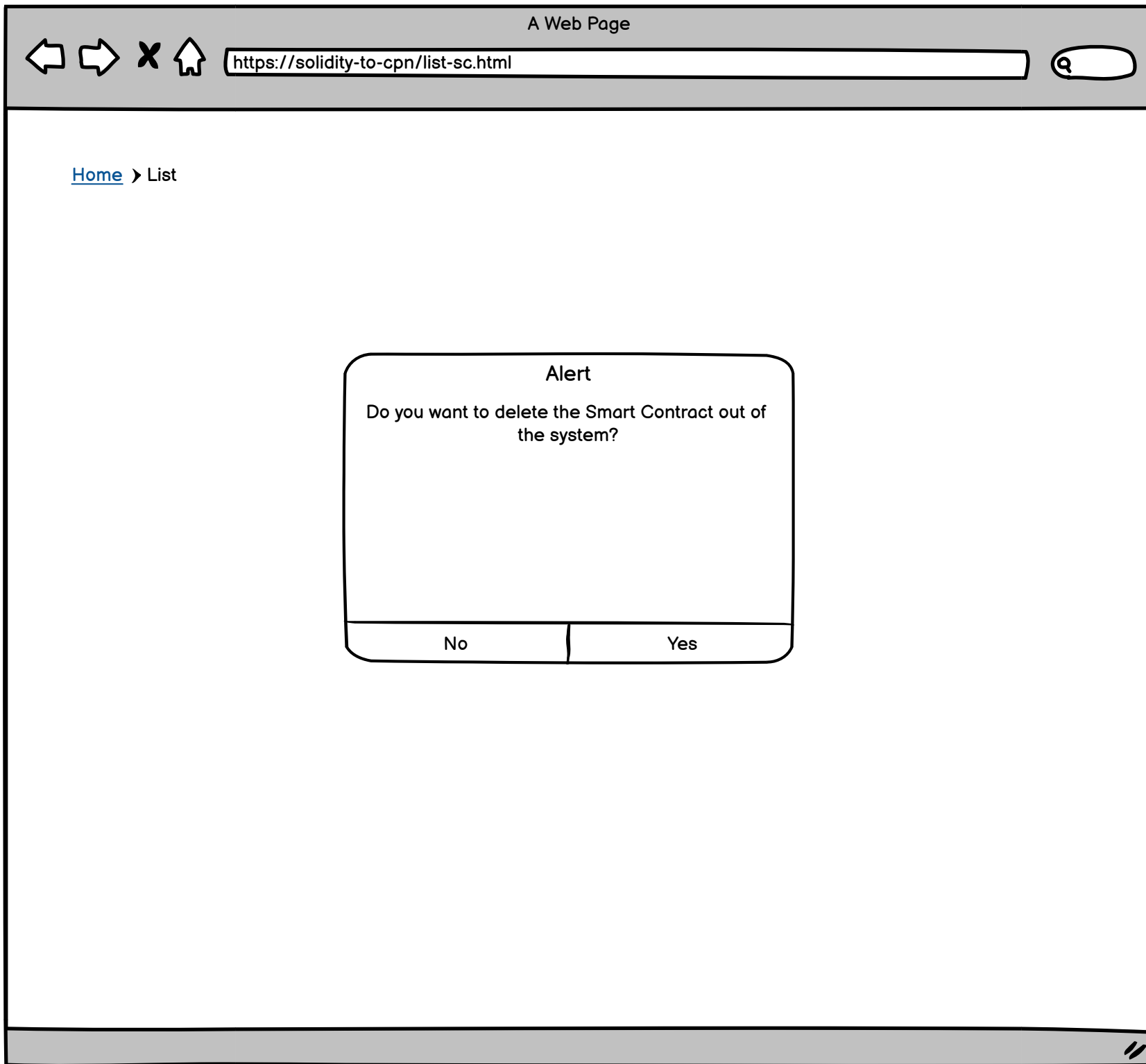
B I U S style ▼



Save

Cancel

26c



29

A Web Page

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

Solidity

Q

search

[Carl Adam Petri](#)

The smart contract CRUD page of normal user

Home

>

List

Smart Contracts Lists

Date

10/10/2021

OCTOBER 2021

S

M

T

W

T

F

S

26

27

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

Type

Private

Private

Pending

Normal users can only manage the private and pending smart contracts.

#	Name	Type	Date	Description		
1	blindAuction	Private	1/1/2021	This is a smart contract about auction	Edit	Delete
2	etherGame	Private	1/5/2021	This is a smart contract about game	Edit	Delete
3	etherLotto	Private	1/10/2021	This is a smart contract about lotto	Edit	Delete
...	...					

Add

Footer

A Web Page

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

Q

[Home](#) > Add

Create a new Smart Contract code

Name

Smart contract 1

Smart Contract Type

☐ Pending

☒ Private

Content

B I U S style

Description

Save

Cancel

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

[Home](#) ➤ [Edit](#)

Smart contract 1

© Private

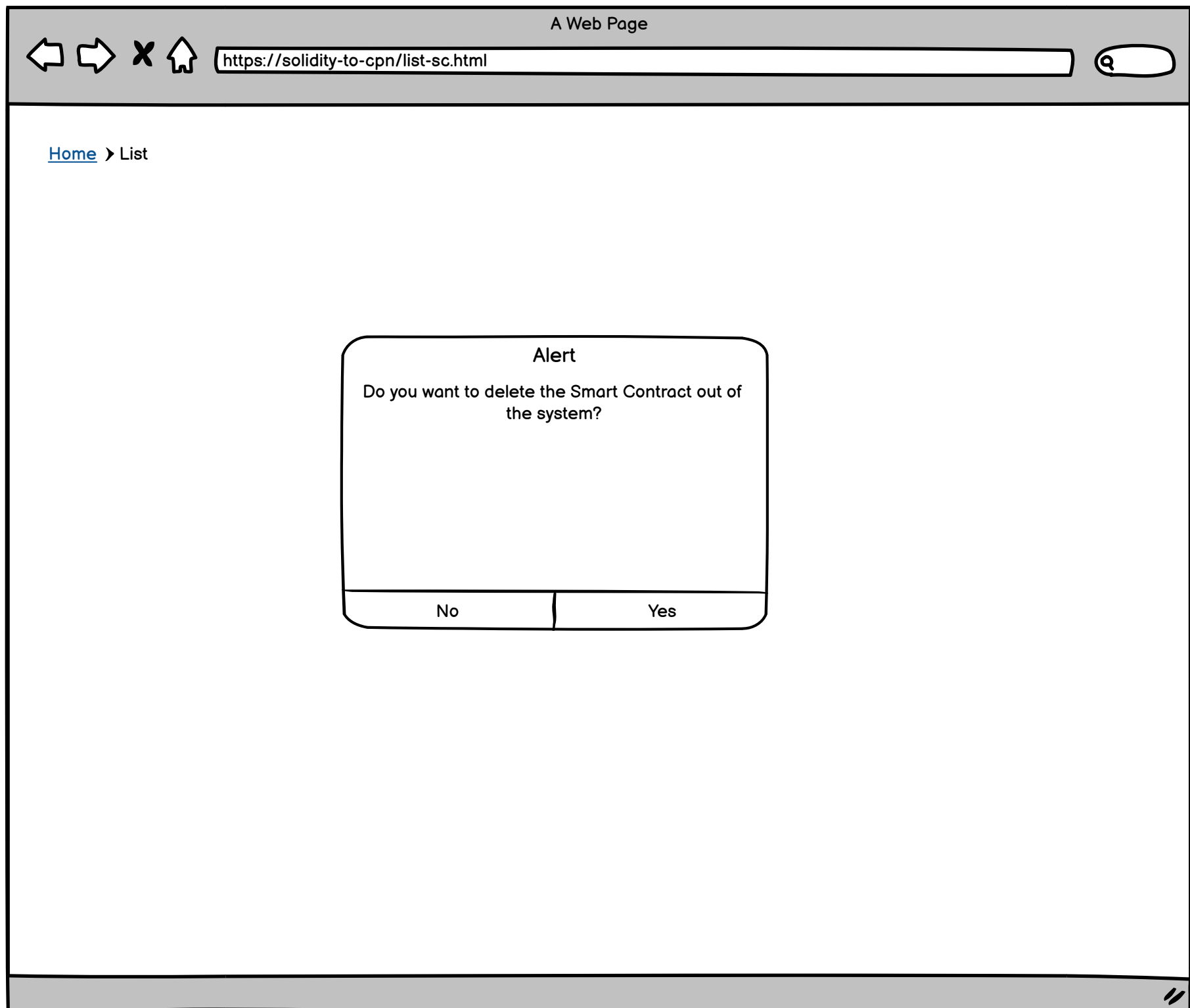
B I U S style ▼ ≡ ≡ ↺ ↻ 🖼️ 😊

~~XXXXXXXXXXXX~~

~~XXXXXXXXXXXX~~

Cancel

29a



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

Solidity

Q

search

Carl Adam Petri

The screen's role assign of Admin

Home

Context

List

Context List

Date

10/10/2021

OCTOBER 2021

S

M

T

W

T

F

S

26

27

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

Type

DCR

DCR

CPN

#	Name	Type	Date	Description		
1	blindAuction context	DCR	1/1/2021	This is a context about auction	Edit	Delete
2	etherGame context	DCR	1/5/2021	This is a context about game	Edit	Delete
3	etherLotto context	DCR	1/10/2021	This is a context about lotto	Edit	Delete
...	...					

Add

Footer

33

A Web Page

X

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

Q

[Home](#) > Add

Create a new Context

Name

Context ABC

Type

DCR

DCR

BPMN

Description

Content

C:/abc/xyz/Context.xml

Save

Cancel

34

A Web Page

X

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

Q

[Home](#) > Edit

Update the Context

Name

Context ABC

Type

DCR

DCR

BPMN

Description

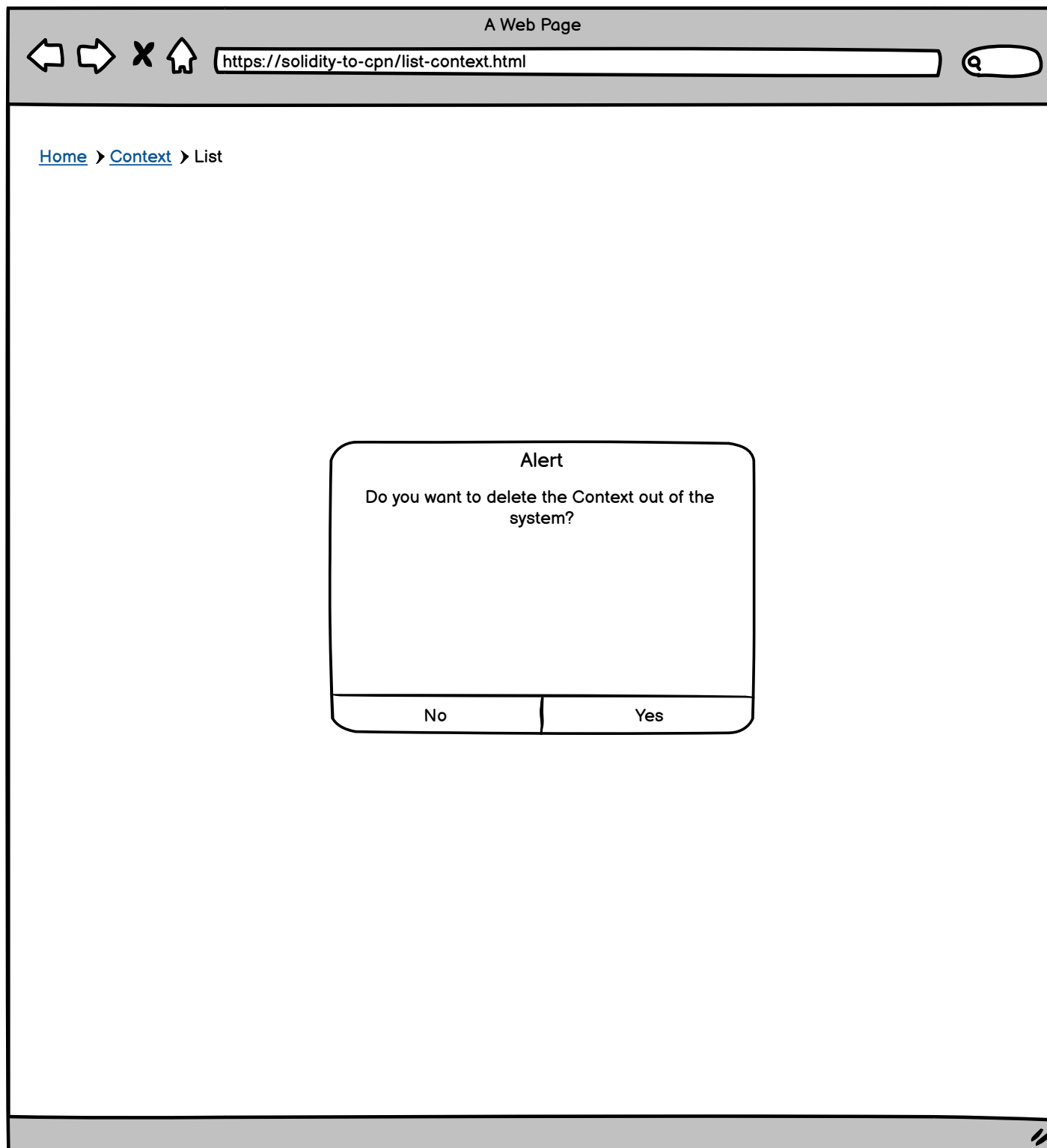
Content

C:/abc/xyz/Context.xml

Save

Cancel

32a



35

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

OCTOBER 2021

S

M

T

W

T

F

S

26

27

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

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

36

A Web Page










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



Home > LTL > Add

Create a new LTL Property Template




Name

Formula

B I U         

Description

Cancel

35

