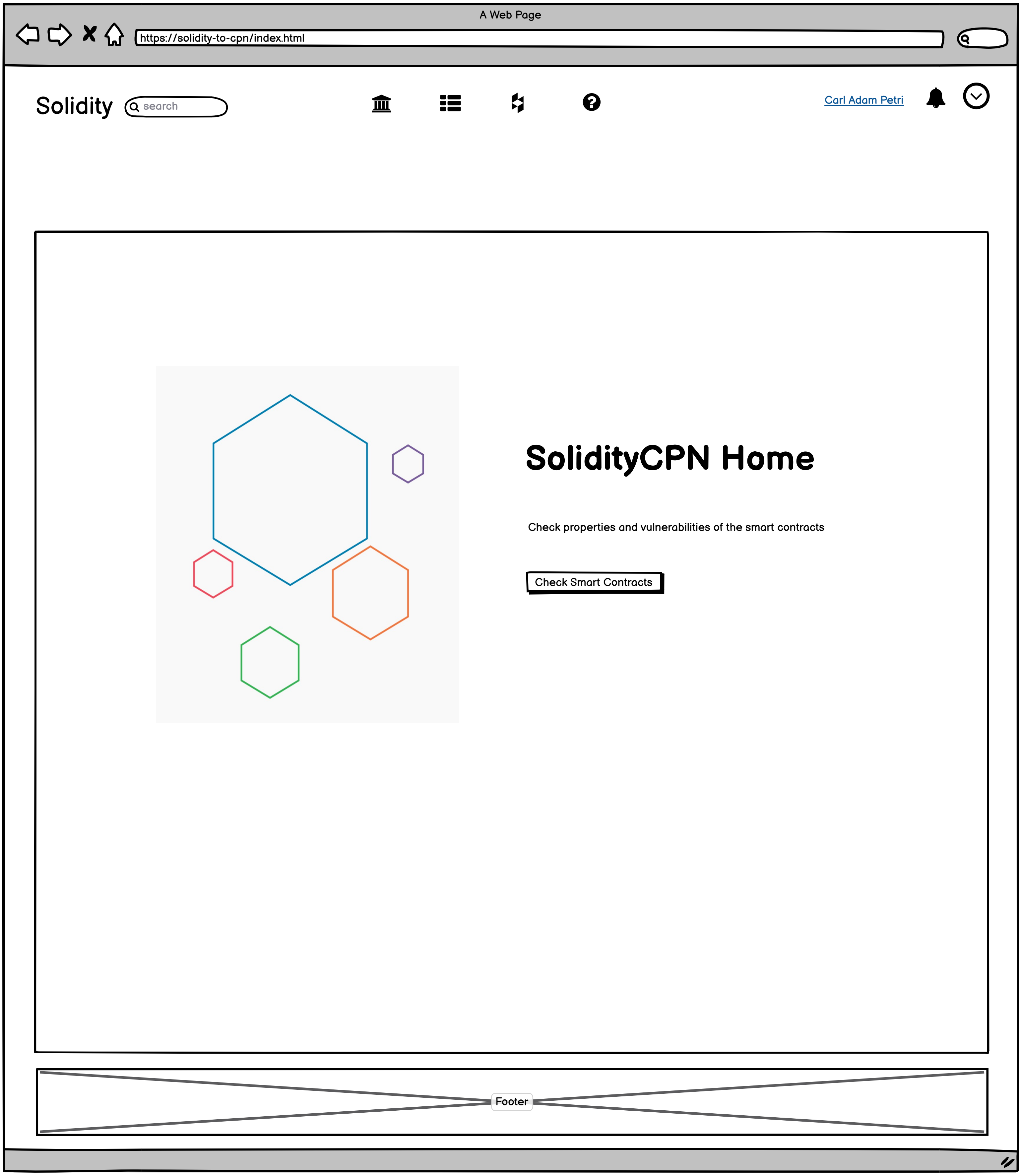
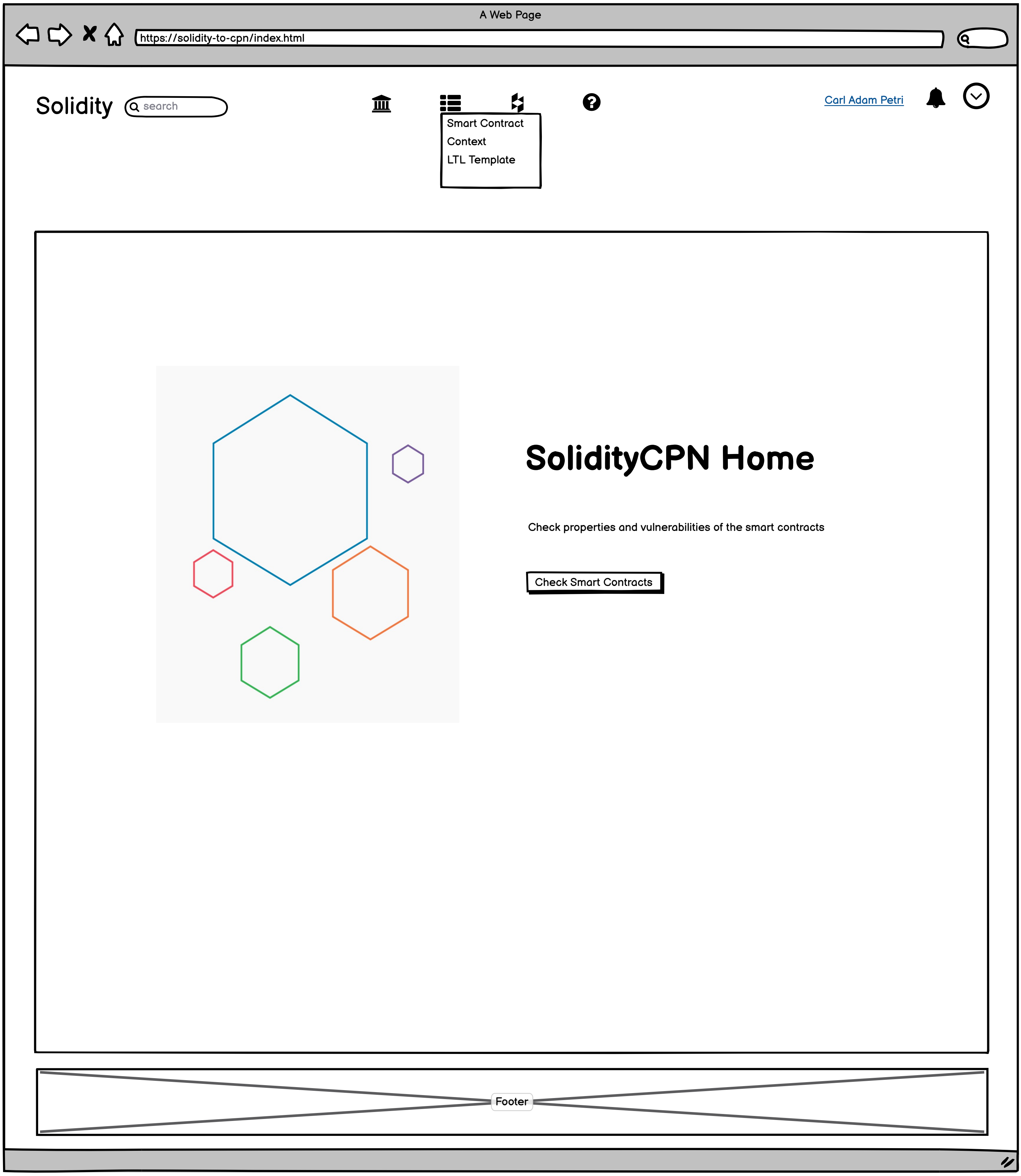


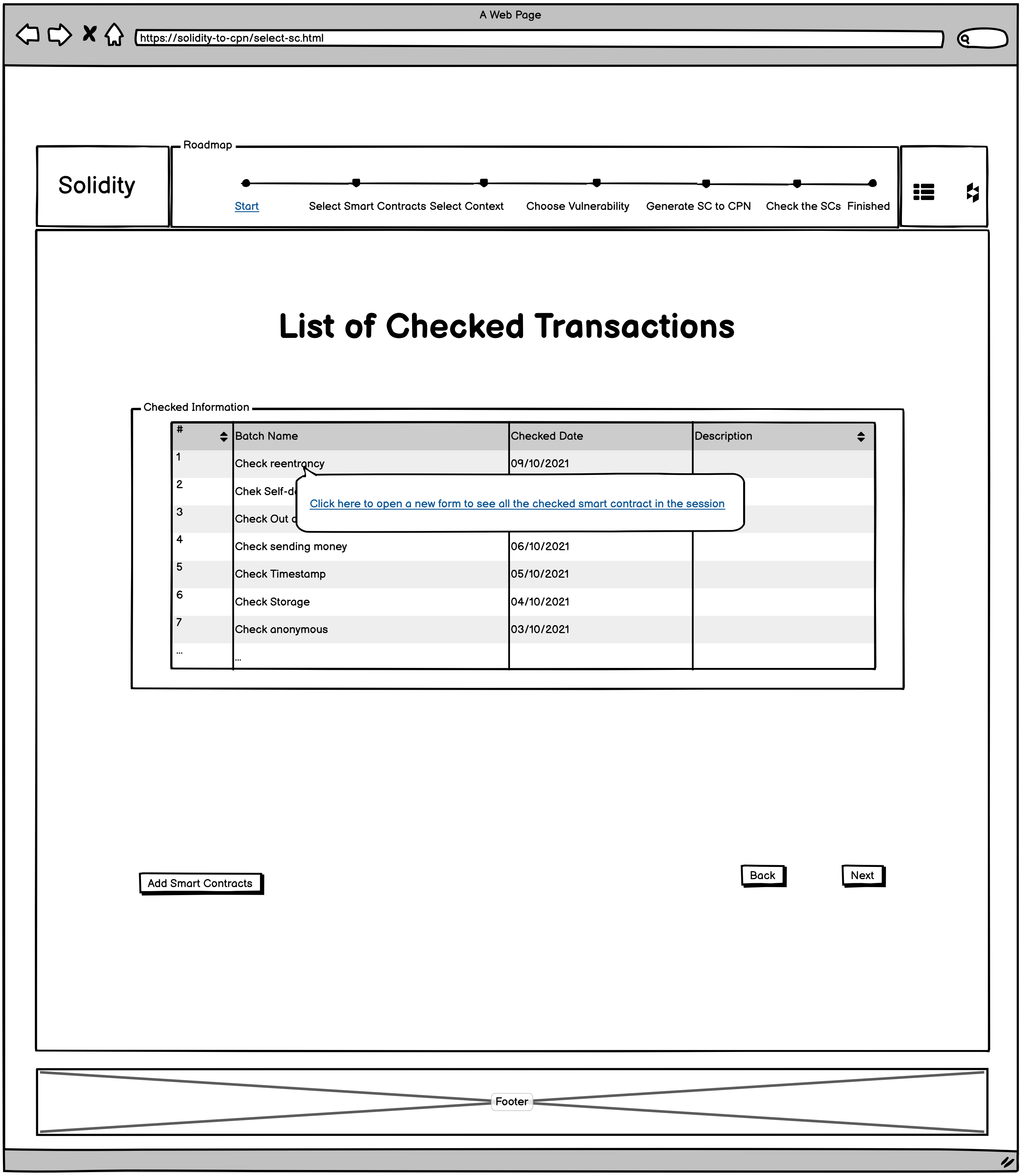
SolidityCPN Home

Check properties and vulnerabilities of the smart contracts



SolidityCPN Home

Check properties and vulnerabilities of the smart contracts

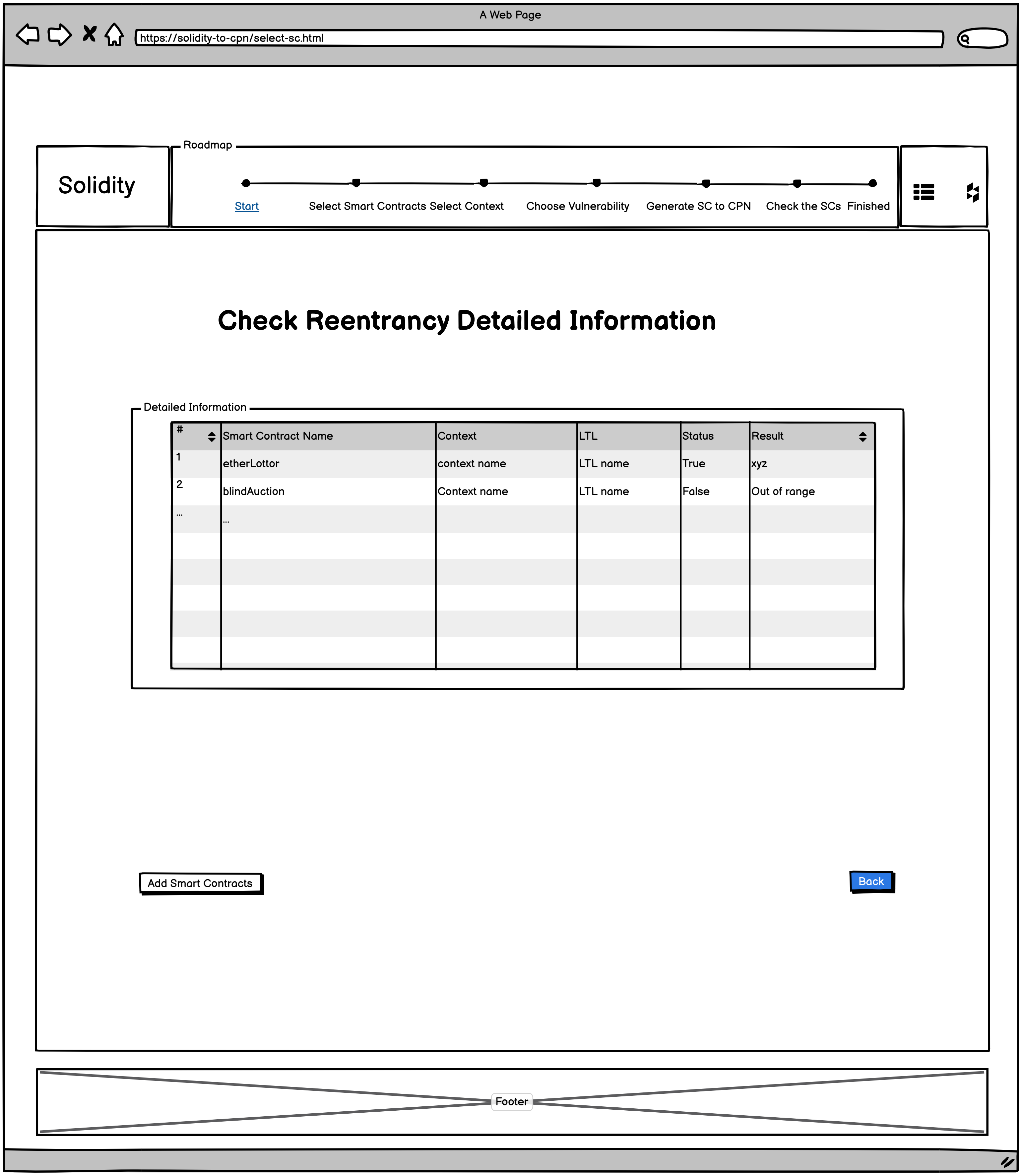


List of Checked Transactions

Checked Information

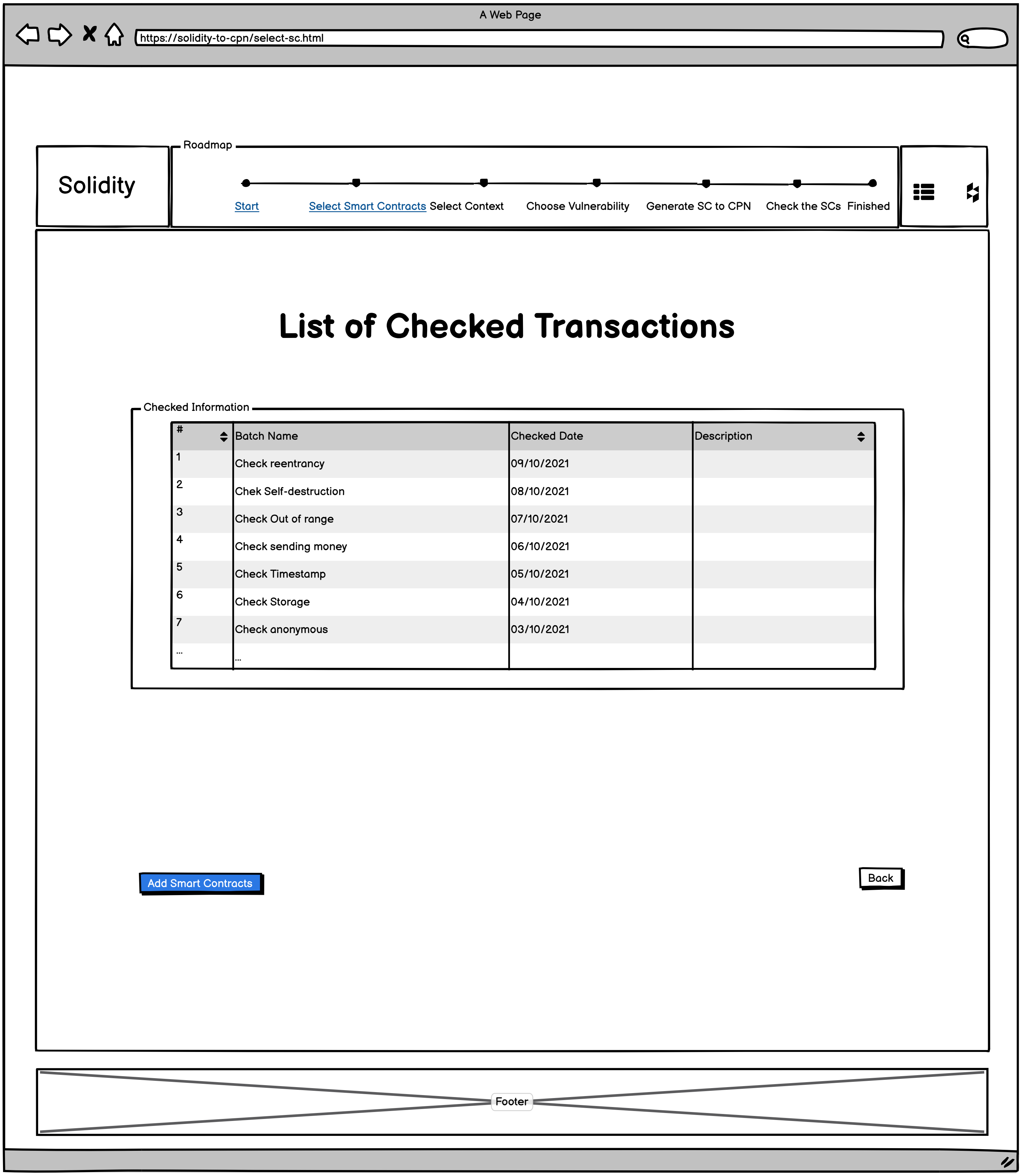
#	Batch Name	Checked Date	Description
1	Check reentrancy	09/10/2021	
2	Chek Self-d		
3	Check Out c		
4	Check sending money	06/10/2021	
5	Check Timestamp	05/10/2021	
6	Check Storage	04/10/2021	
7	Check anonymous	03/10/2021	
...	...		

Click here to open a new form to see all the checked smart contract in the session



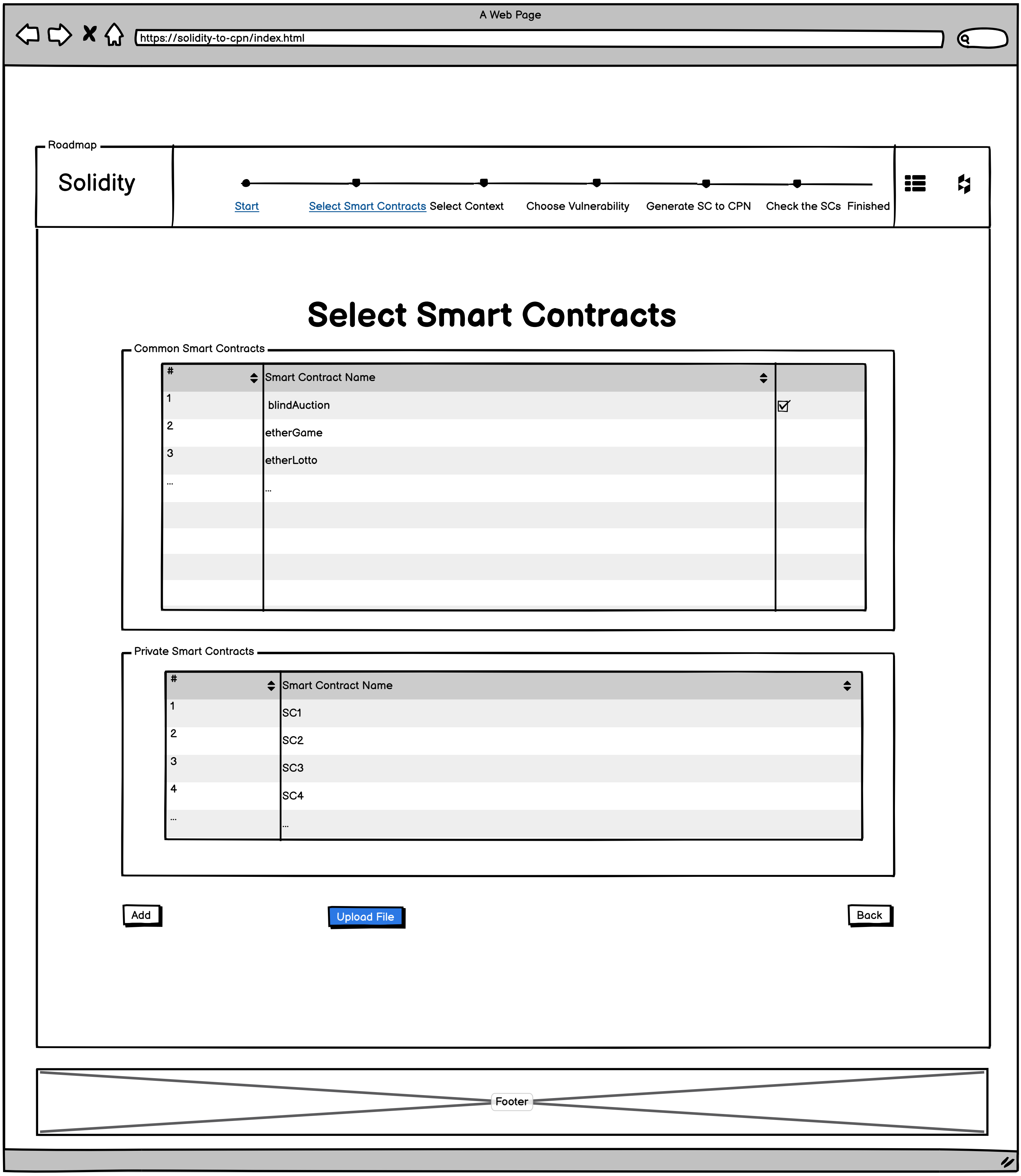
Check Reentrancy Detailed Information

#	Smart Contract Name	Context	LTL	Status	Result
1	etherLottor	context name	LTL name	True	xyz
2	blindAuction	Context name	LTL name	False	Out of range
...	...				



List of Checked Transactions

#	Batch Name	Checked Date	Description
1	Check reentrancy	09/10/2021	
2	Chek Self-destruction	08/10/2021	
3	Check Out of range	07/10/2021	
4	Check sending money	06/10/2021	
5	Check Timestamp	05/10/2021	
6	Check Storage	04/10/2021	
7	Check anonymous	03/10/2021	
...	...		



A Web Page

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

Roadmap

Solidity

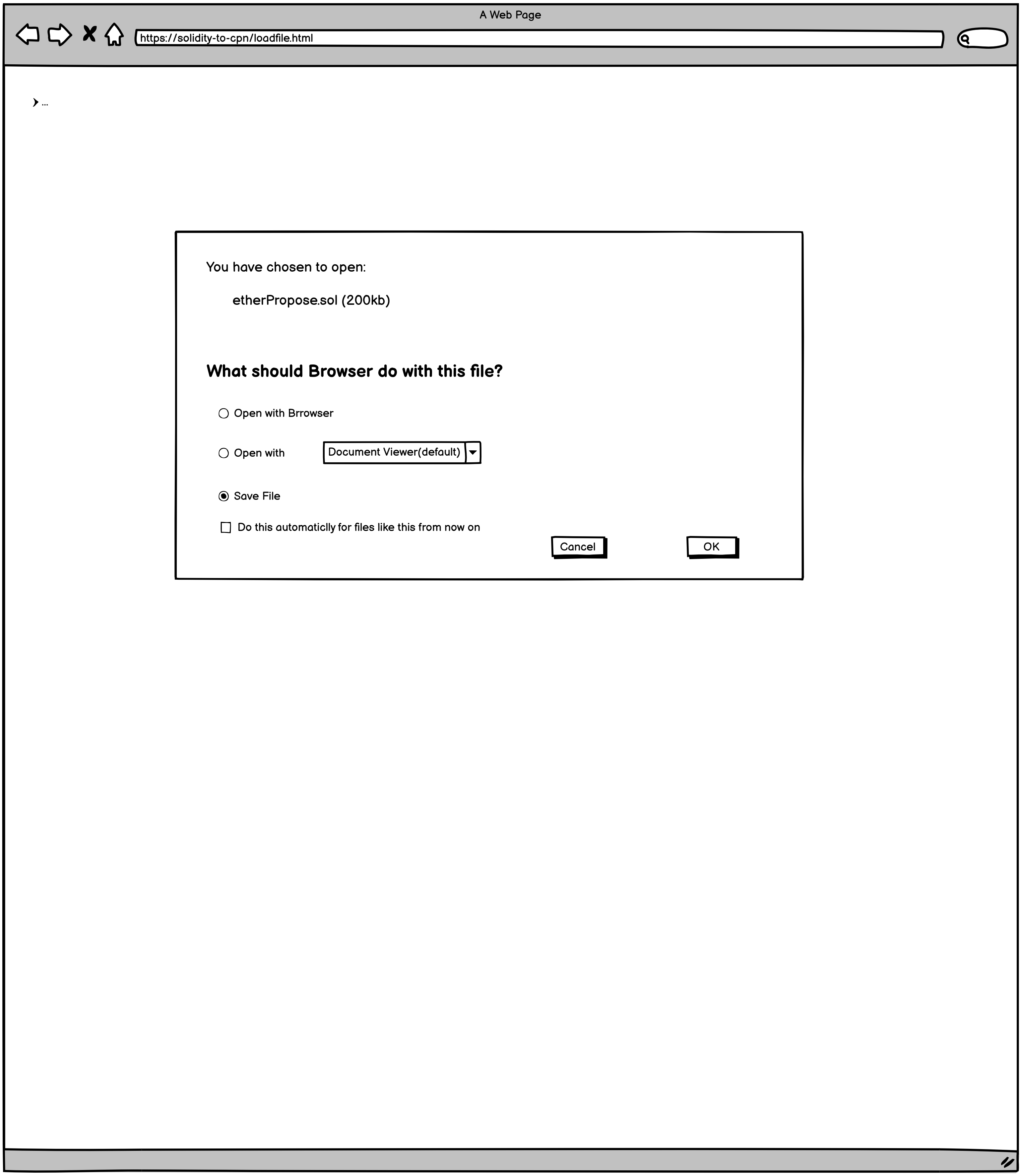
Select Smart Contracts

Common Smart Contracts

#	Smart Contract Name	
1	blindAuction	☑
2	etherGame	
3	etherLotto	
...	...	

Private Smart Contracts

#	Smart Contract Name
1	SC1
2	SC2
3	SC3
4	SC4
...	...



You have chosen to open:

etherPropose.sol (200kb)

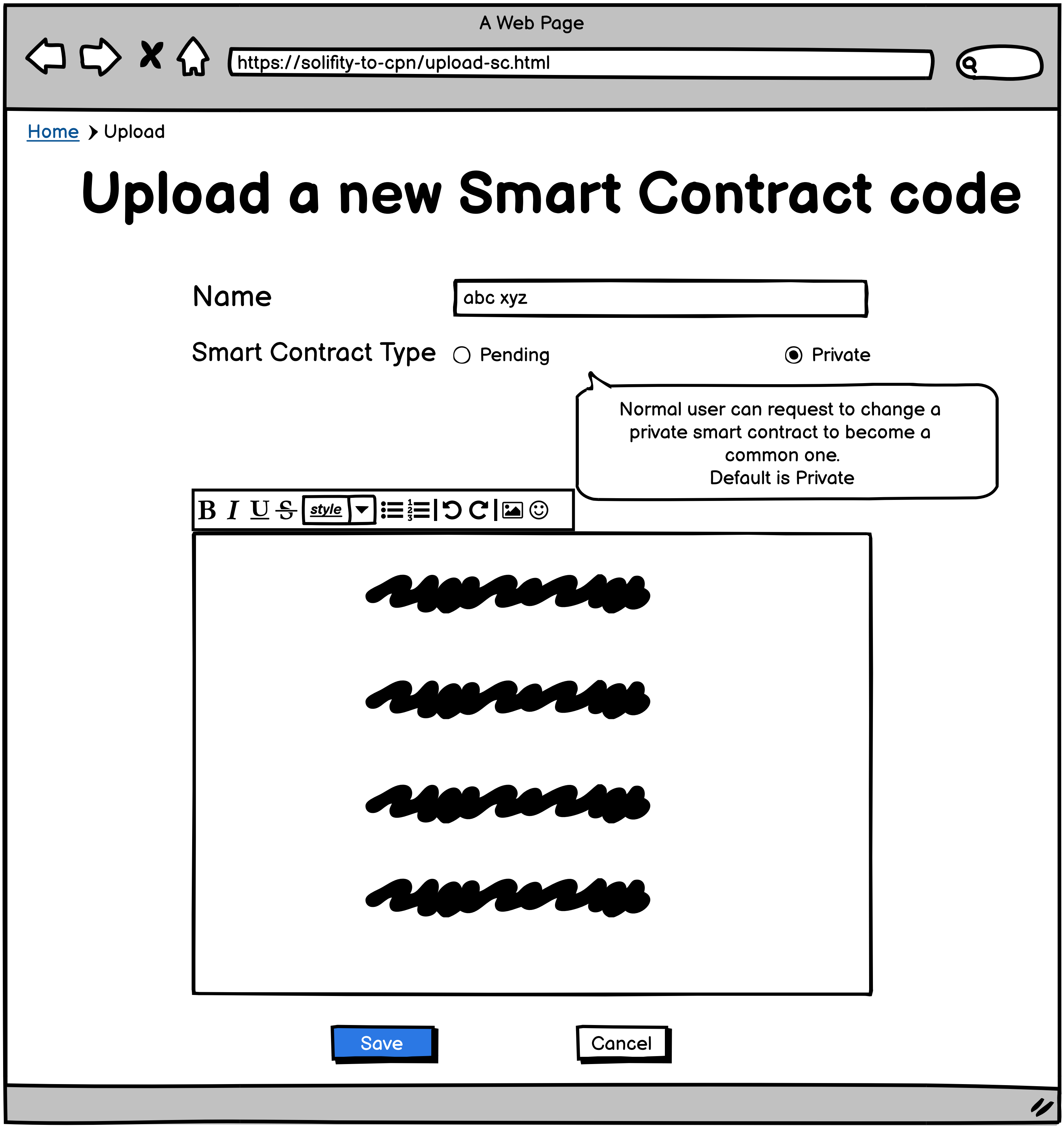
What should Browser do with this file?

○ Open with Brrowser

○ Open with Document Viewer(default)

● Save File

□ Do this automaticlly for files like this from now on



A Web Page

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

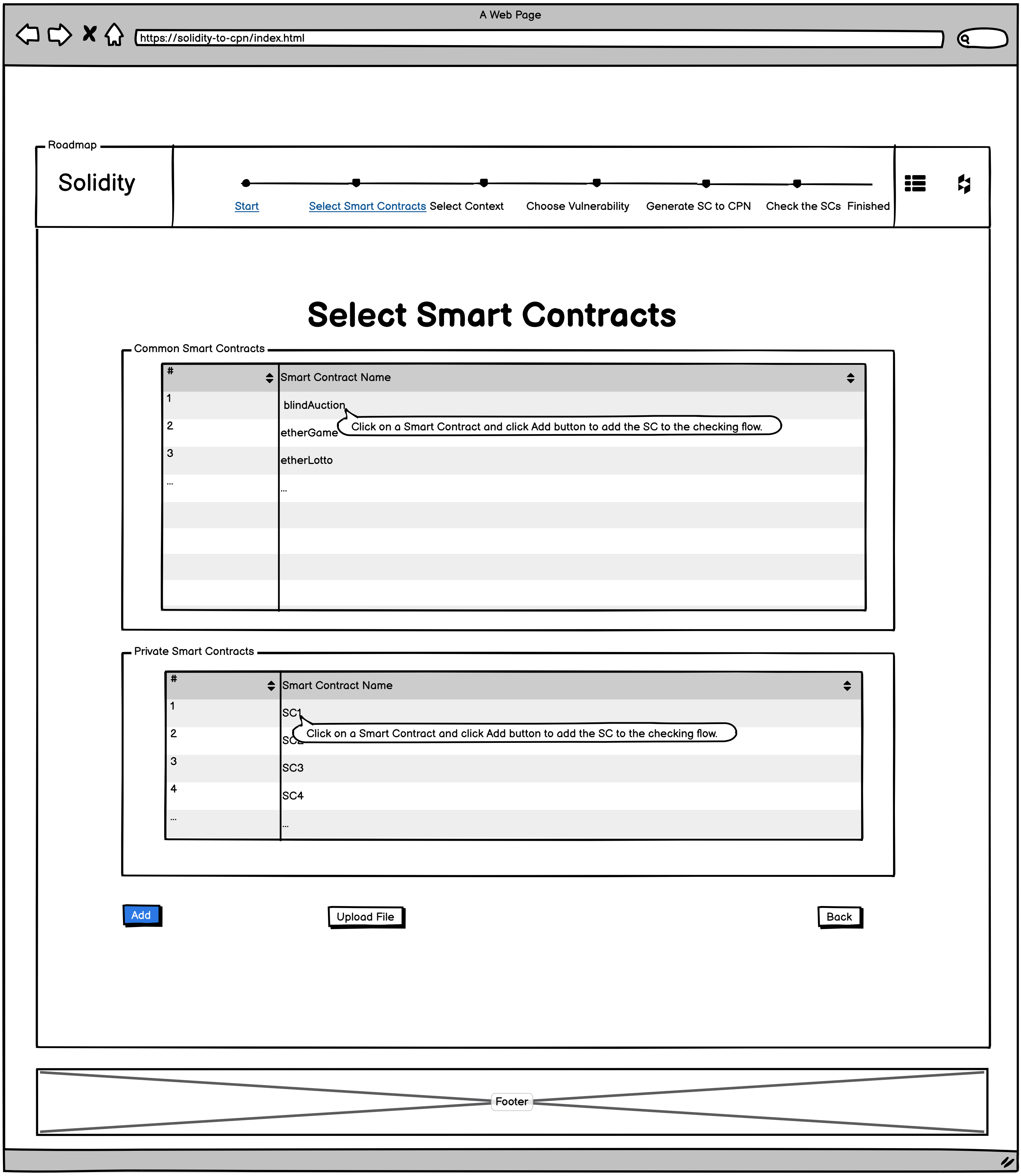
Home › Upload

Upload a new Smart Contract code

Name: abc xyz

Smart Contract Type ○ Pending ● Private

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



Select Smart Contracts

Common Smart Contracts

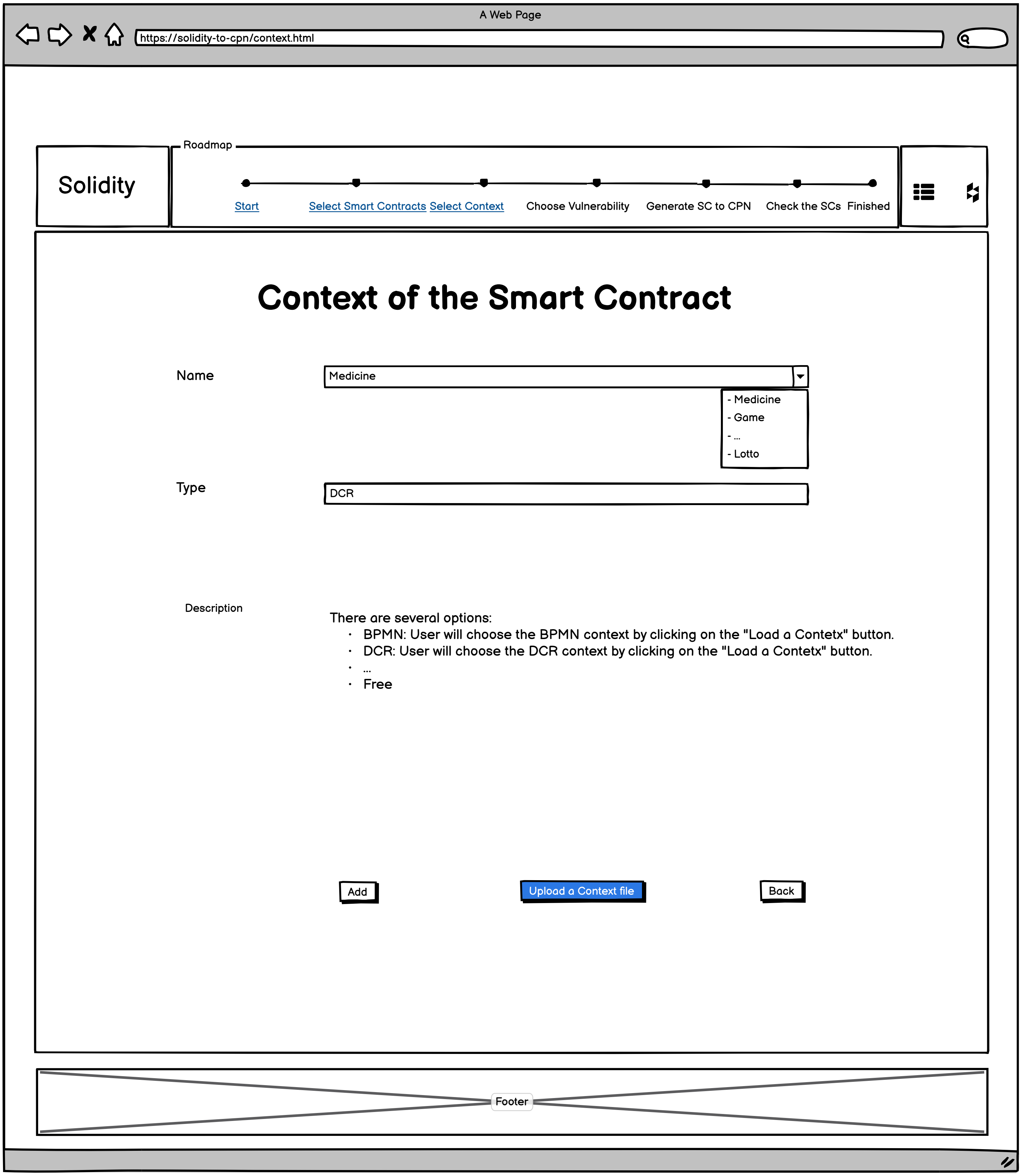
#	Smart Contract Name
1	blindAuction
2	etherGame
3	etherLotto
...	...

Click on a Smart Contract and click Add button to add the SC to the checking flow.

Private Smart Contracts

#	Smart Contract Name
1	SC1
2	SC2
3	SC3
4	SC4
...	...

Click on a Smart Contract and click Add button to add the SC to the checking flow.



Context of the Smart Contract

Name: Medicine

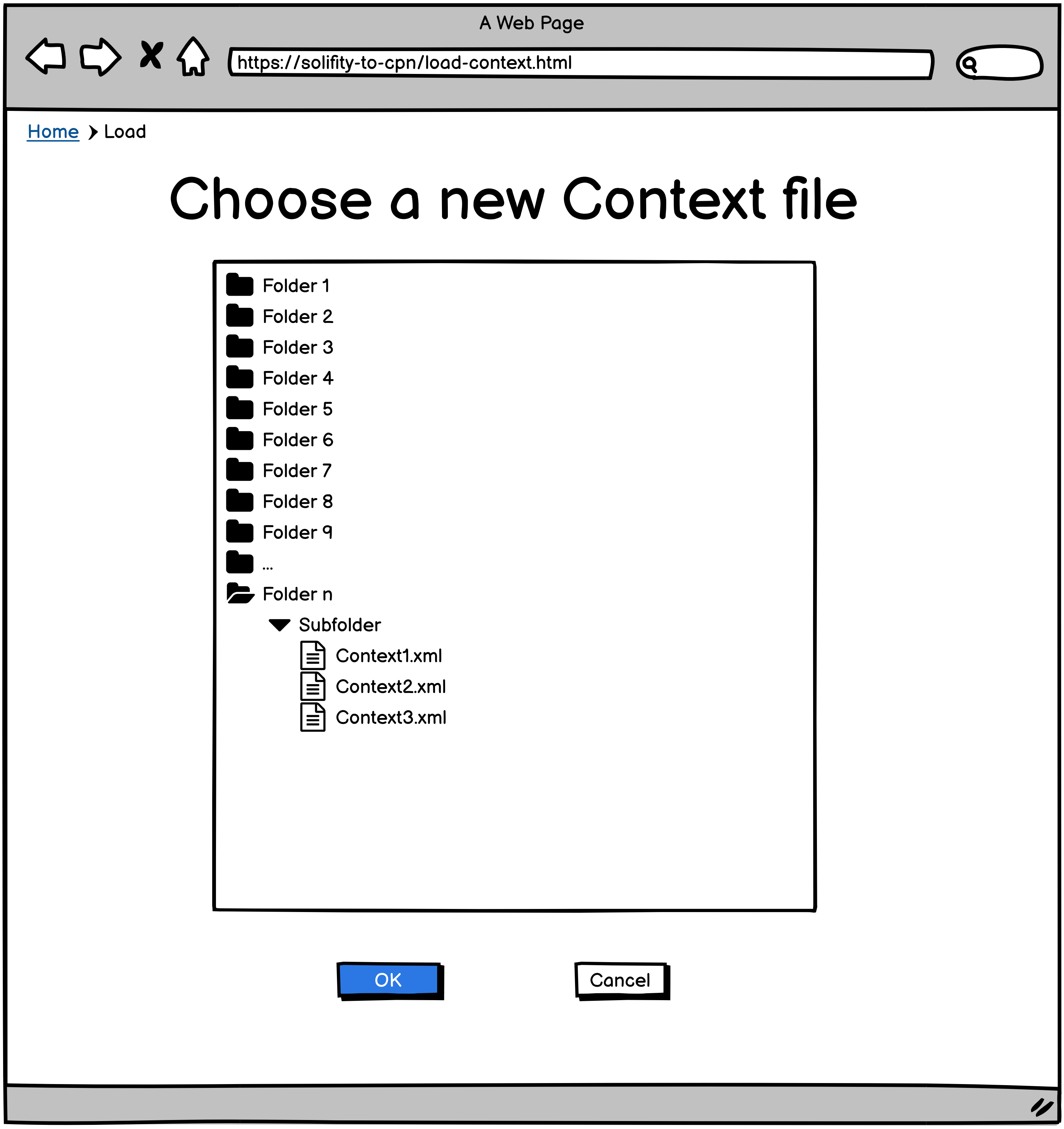
- Medicine
- Game
- ...
- Lotto

Type: DCR

Description

There are several options:

- BPMN: User will choose the BPMN context by clicking on the "Load a Contetx" button.
- DCR: User will choose the DCR context by clicking on the "Load a Contetx" button.
- ...
- Free



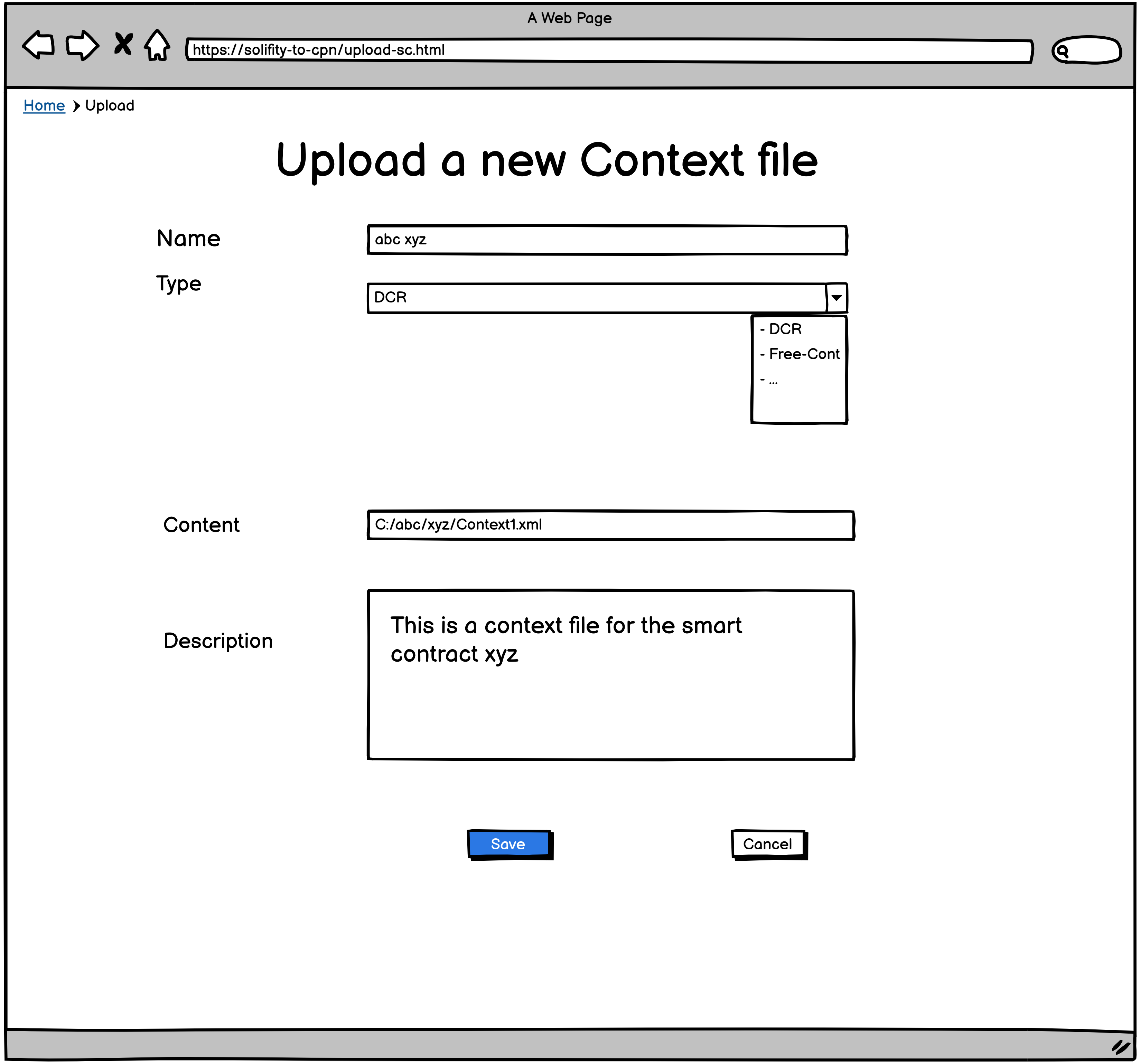
A Web Page

https://solifity-to-cpn/load-context.html

Home ❯ Load

Choose a new Context file

- Folder 1
- Folder 2
- Folder 3
- Folder 4
- Folder 5
- Folder 6
- Folder 7
- Folder 8
- Folder 9
- ...
- Folder n
  - Subfolder
    - Context1.xml
    - Context2.xml
    - Context3.xml



A Web Page

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

Home ❯ Upload

Upload a new Context file

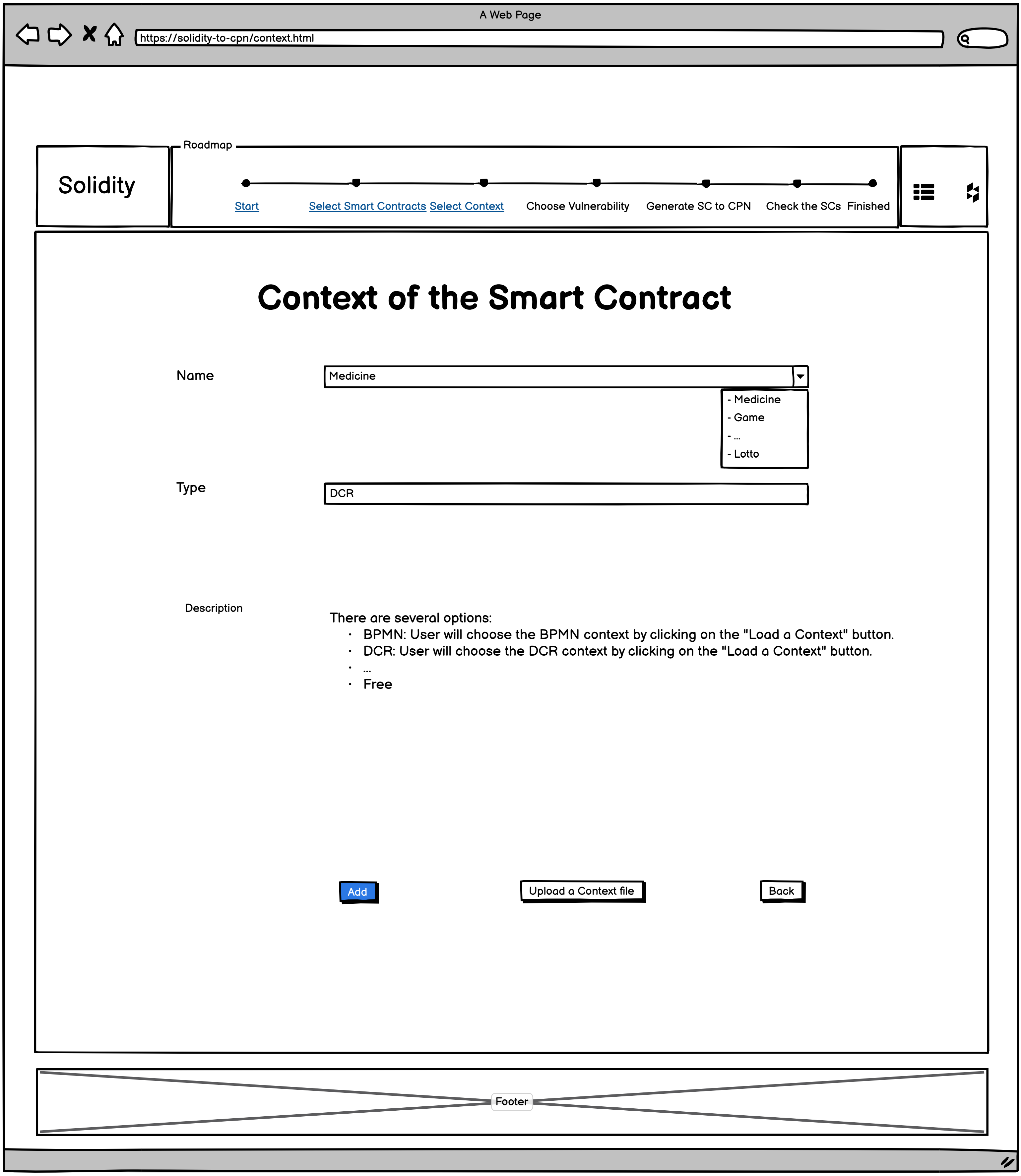
Name: abc xyz

Type: DCR

- DCR
- Free-Cont
- ...

Content: C:/abc/xyz/Context1.xml

Description: This is a context file for the smart contract xyz



Context of the Smart Contract

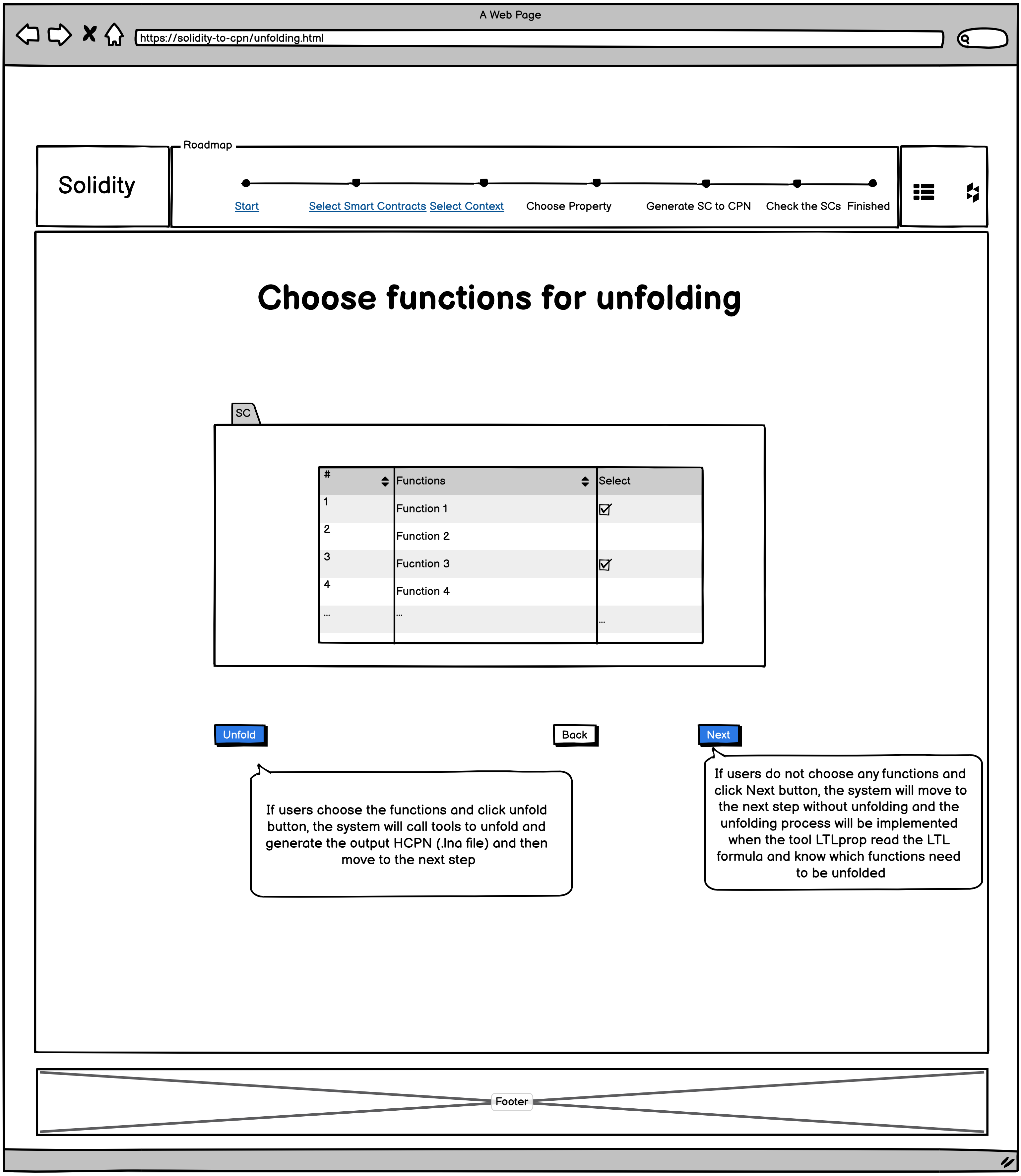
Name: Medicine

Type: DCR

Description

There are several options:

- BPMN: User will choose the BPMN context by clicking on the "Load a Context" button.
- DCR: User will choose the DCR context by clicking on the "Load a Context" button.
- ...
- Free

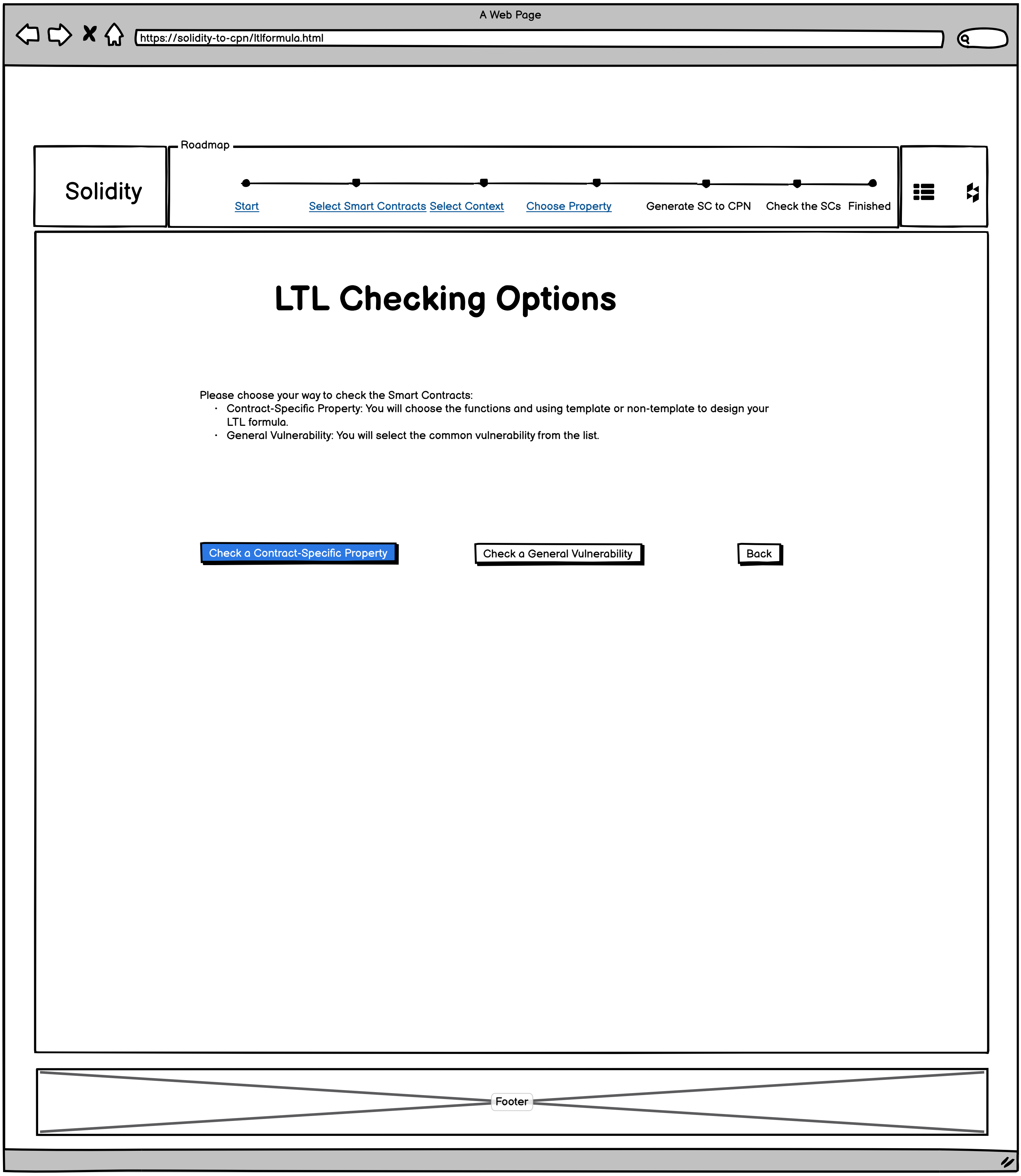


Choose functions for unfolding

#	Functions	Select
1	Function 1	☑
2	Function 2	
3	Fucntion 3	☑
4	Function 4	
...	...	...

If users choose the functions and click unfold button, the system will call tools to unfold and generate the output HCPN (.lna file) and then move to the next step

If users do not choose any functions and click Next button, the system will move to the next step without unfolding and the unfolding process will be implemented when the tool LTLprop read the LTL formula and know which functions need to be unfolded

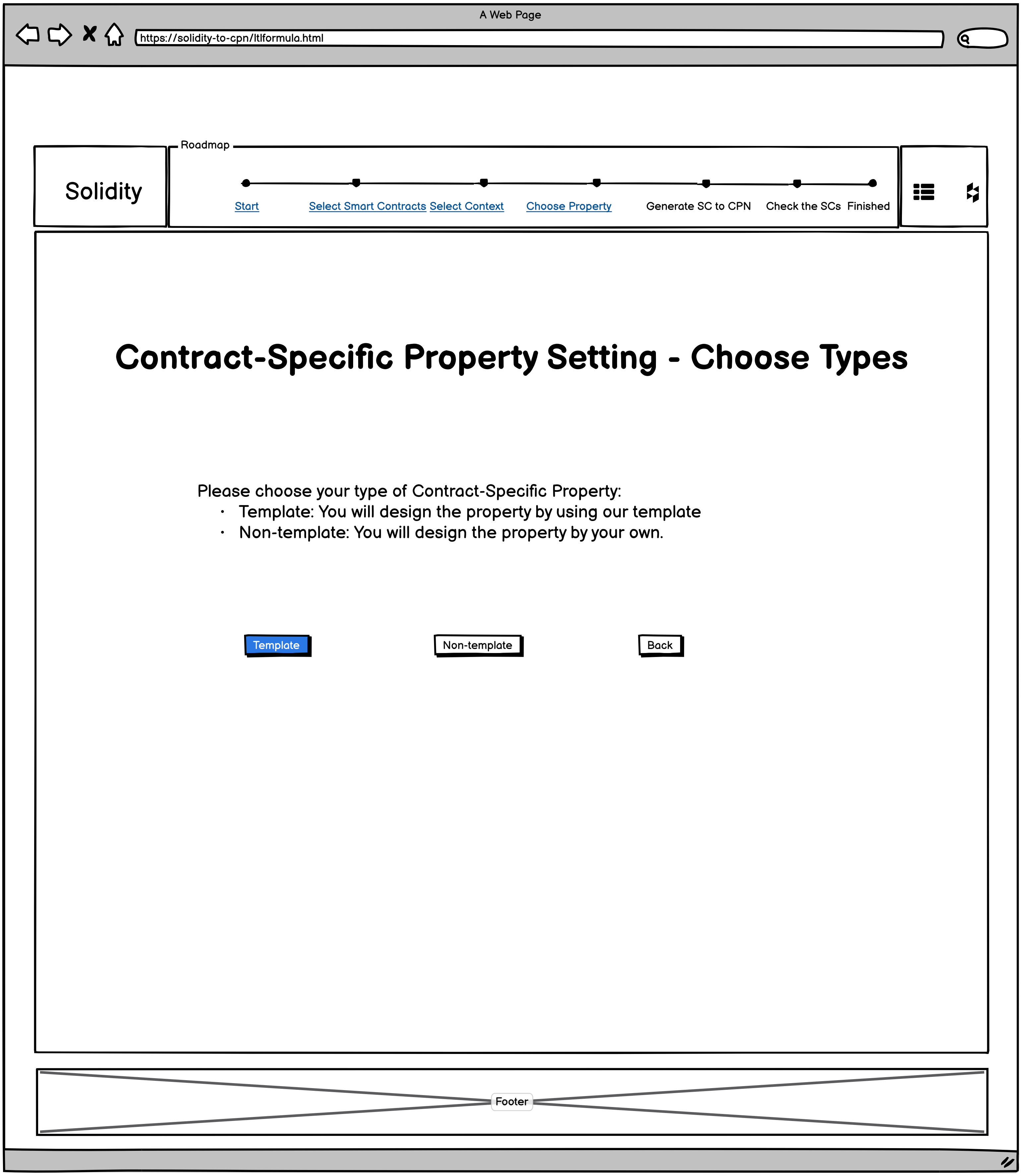


LTL Checking Options

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.

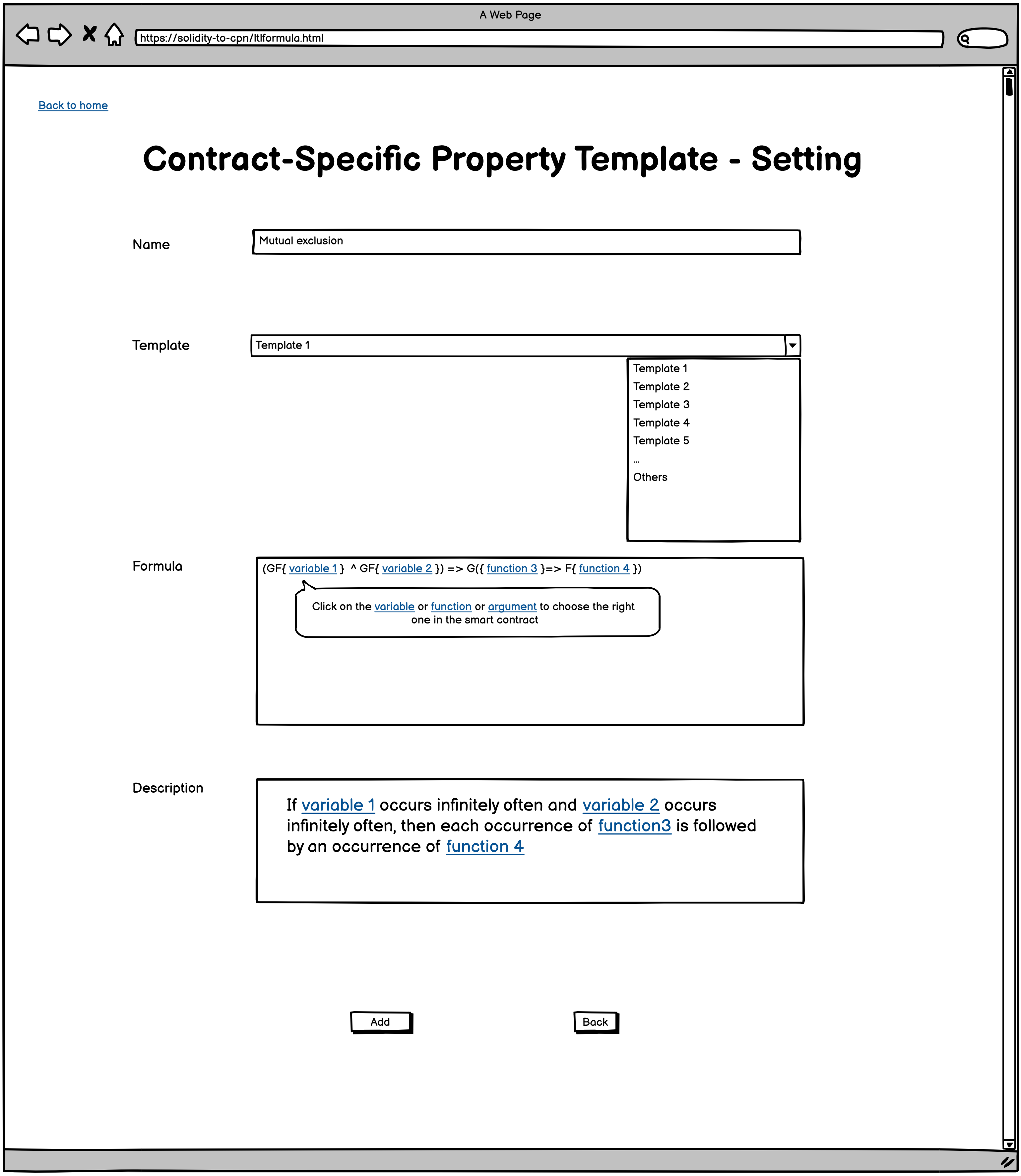
Check a Contract-Specific Property
Check a General Vulnerability
Back
Footer



Contract-Specific Property Setting - Choose Types

Please choose your type of Contract-Specific Property:

- Template: You will design the property by using our template
- Non-template: You will design the property by your own.



A Web Page

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

Back to home

Contract-Specific Property Template - Setting

Name: Mutual exclusion

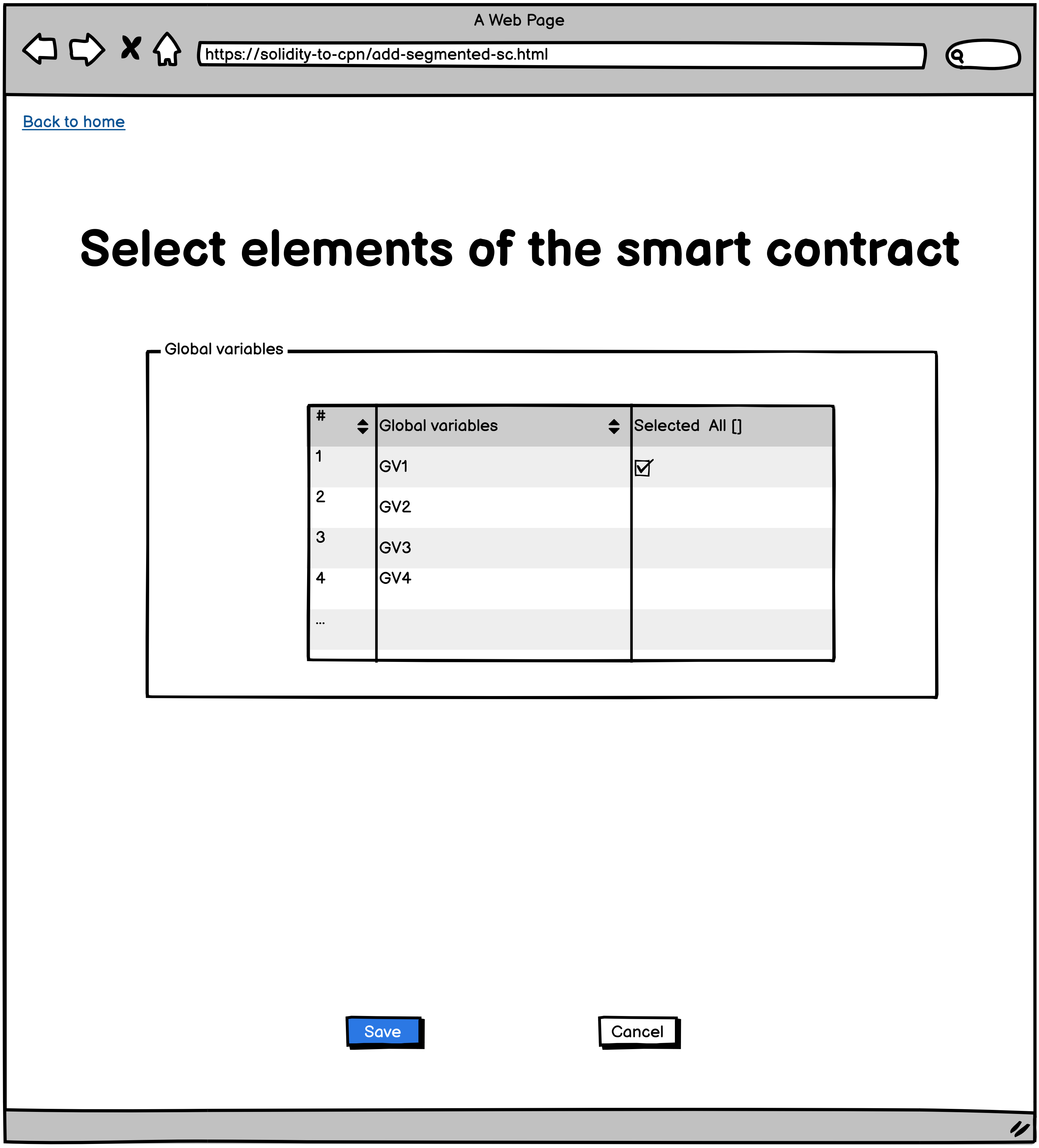
Template: Template 1

- Template 1
- Template 2
- Template 3
- Template 4
- Template 5
- ...
- Others

Formula: (GF{ variable 1 } ^ GF{ variable 2 }) => G({ function 3 }=> F{ function 4 })

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



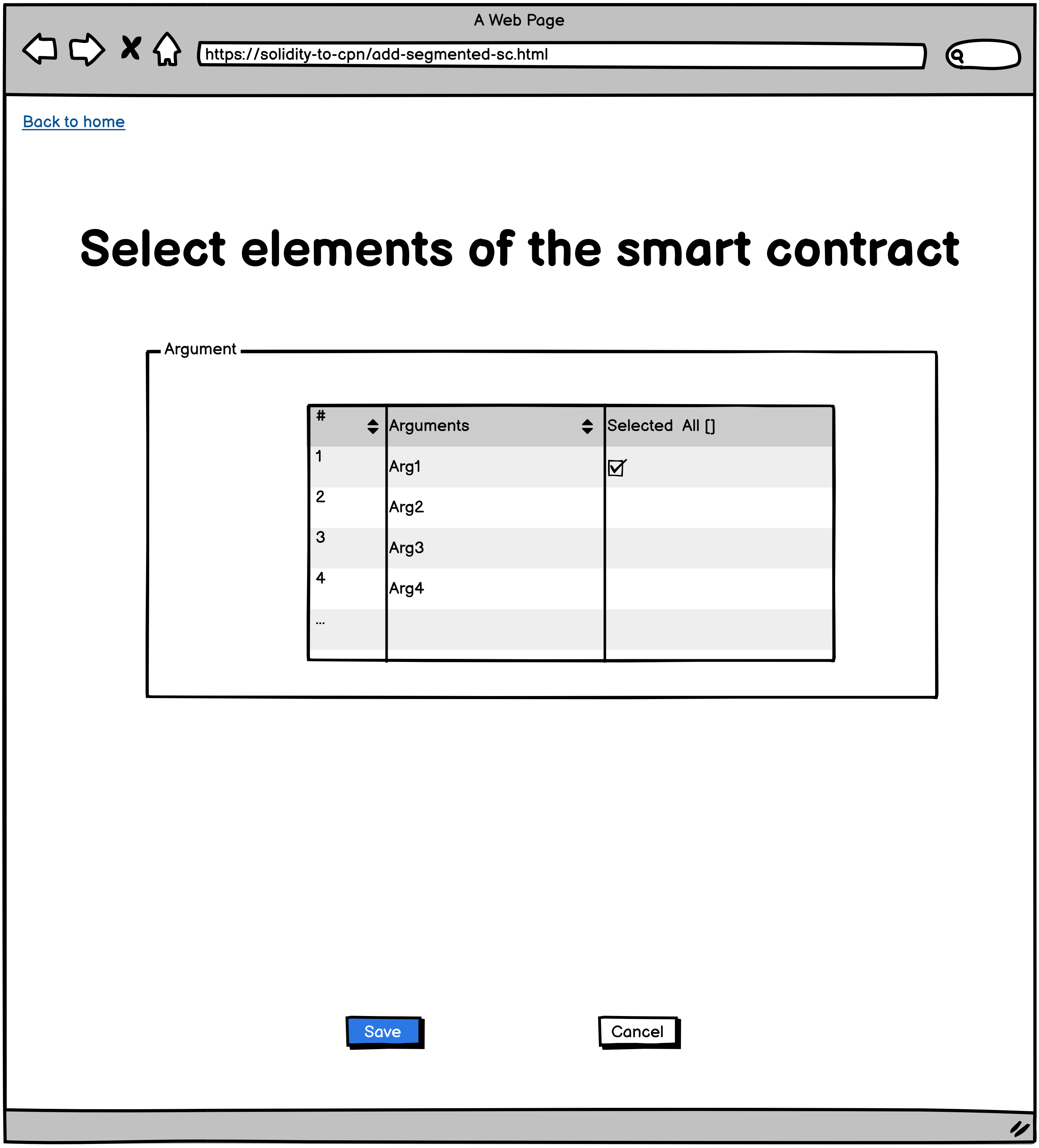
https://solidity-to-cpn/add-segmented-sc.html

Back to home

Select elements of the smart contract

Global variables

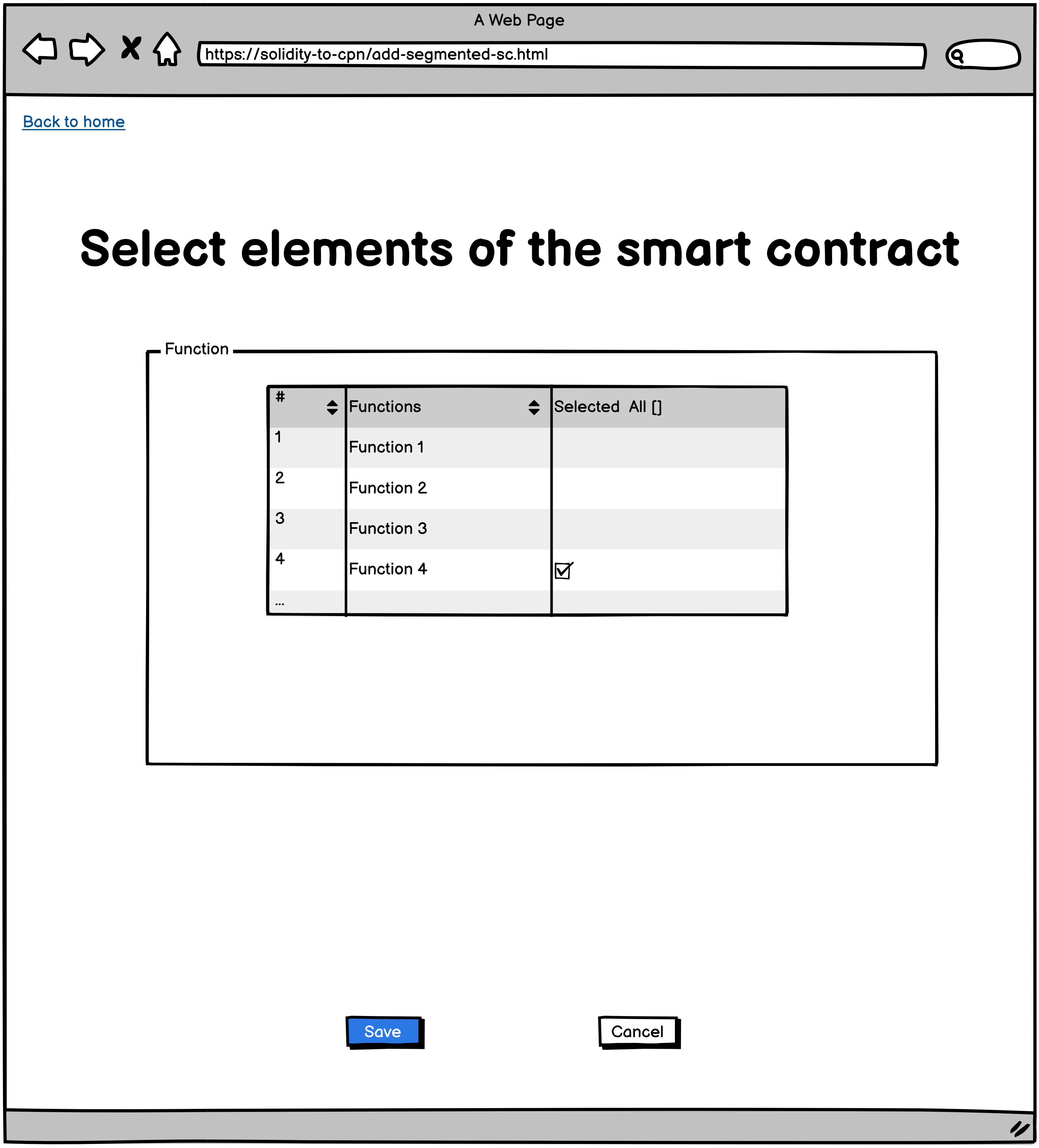
#	Global variables	Selected All []
1	GV1	☑
2	GV2	
3	GV3	
4	GV4	
...		



Select elements of the smart contract

Argument

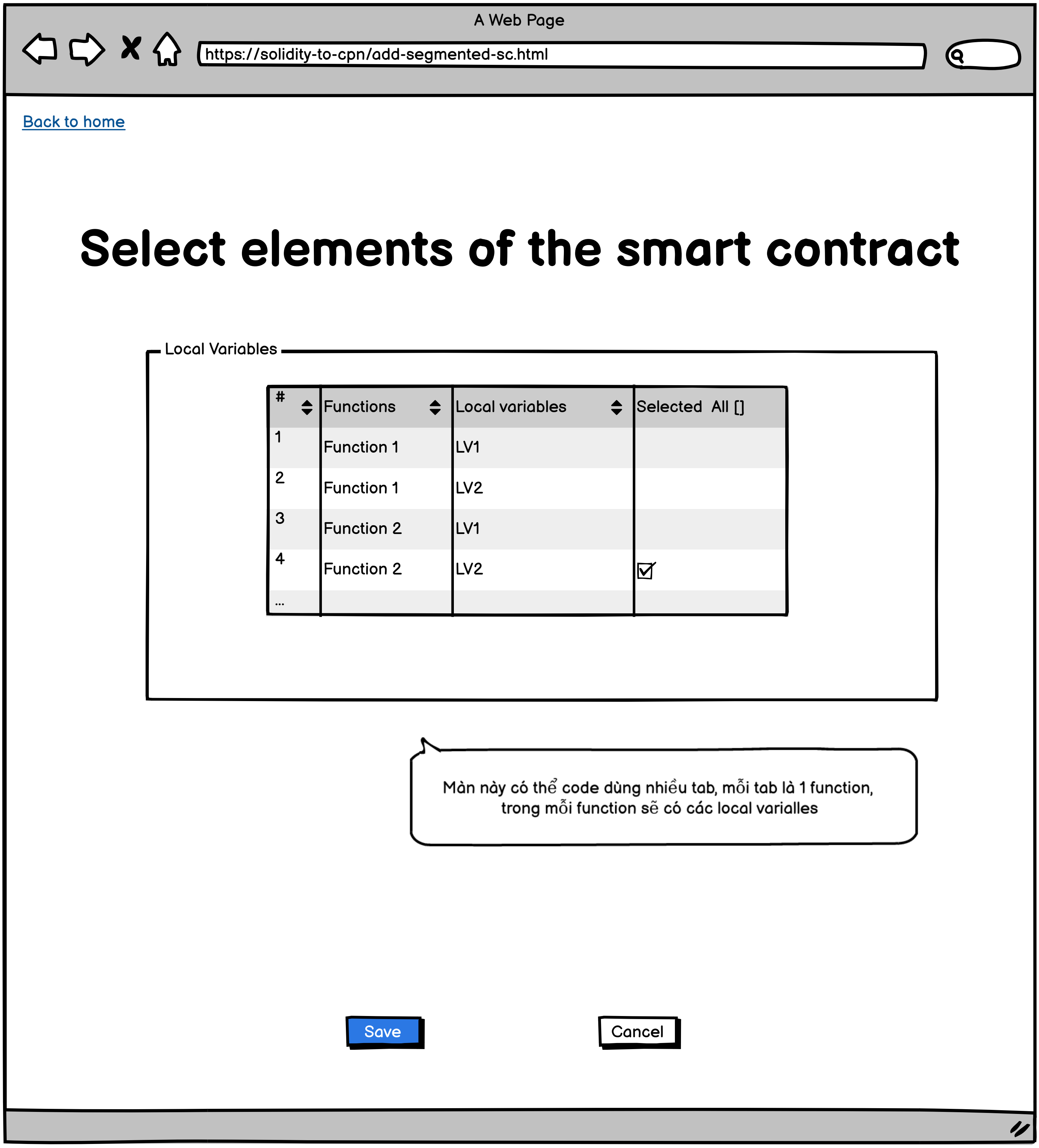
#	Arguments	Selected All []
1	Arg1	☑
2	Arg2	
3	Arg3	
4	Arg4	
...		



Select elements of the smart contract

Function

#	Functions	Selected All []
1	Function 1	
2	Function 2	
3	Function 3	
4	Function 4	☑
...		

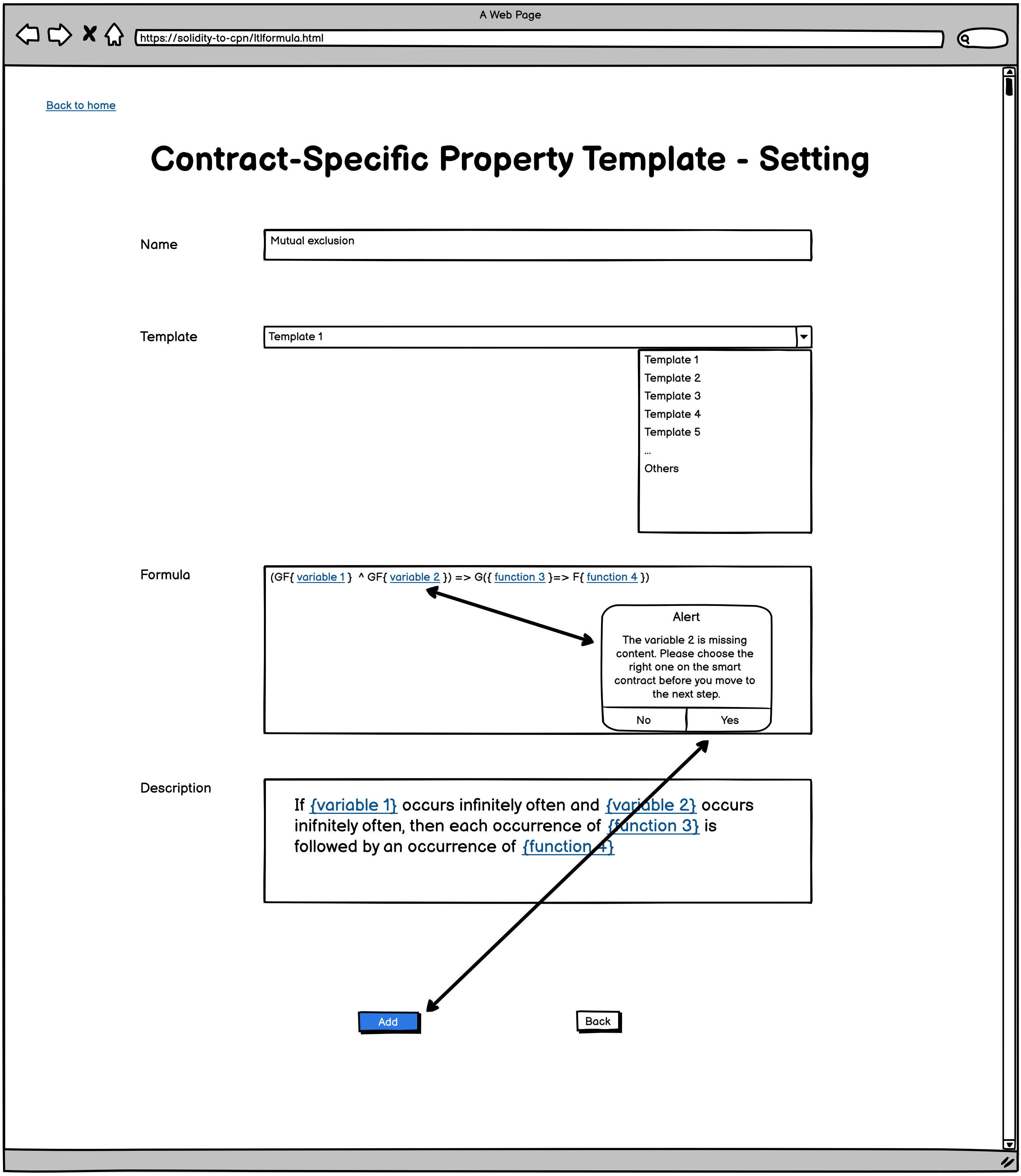


Select elements of the smart contract

Local Variables

#	Functions	Local variables	Selected All []
1	Function 1	LV1	
2	Function 1	LV2	
3	Function 2	LV1	
4	Function 2	LV2	☑
...			

Màn này có thể code dùng nhiều tab, mỗi tab là 1 function, trong mỗi function sẽ có các local varialles



Back to home

Contract-Specific Property Template - Setting

Name: Mutual exclusion

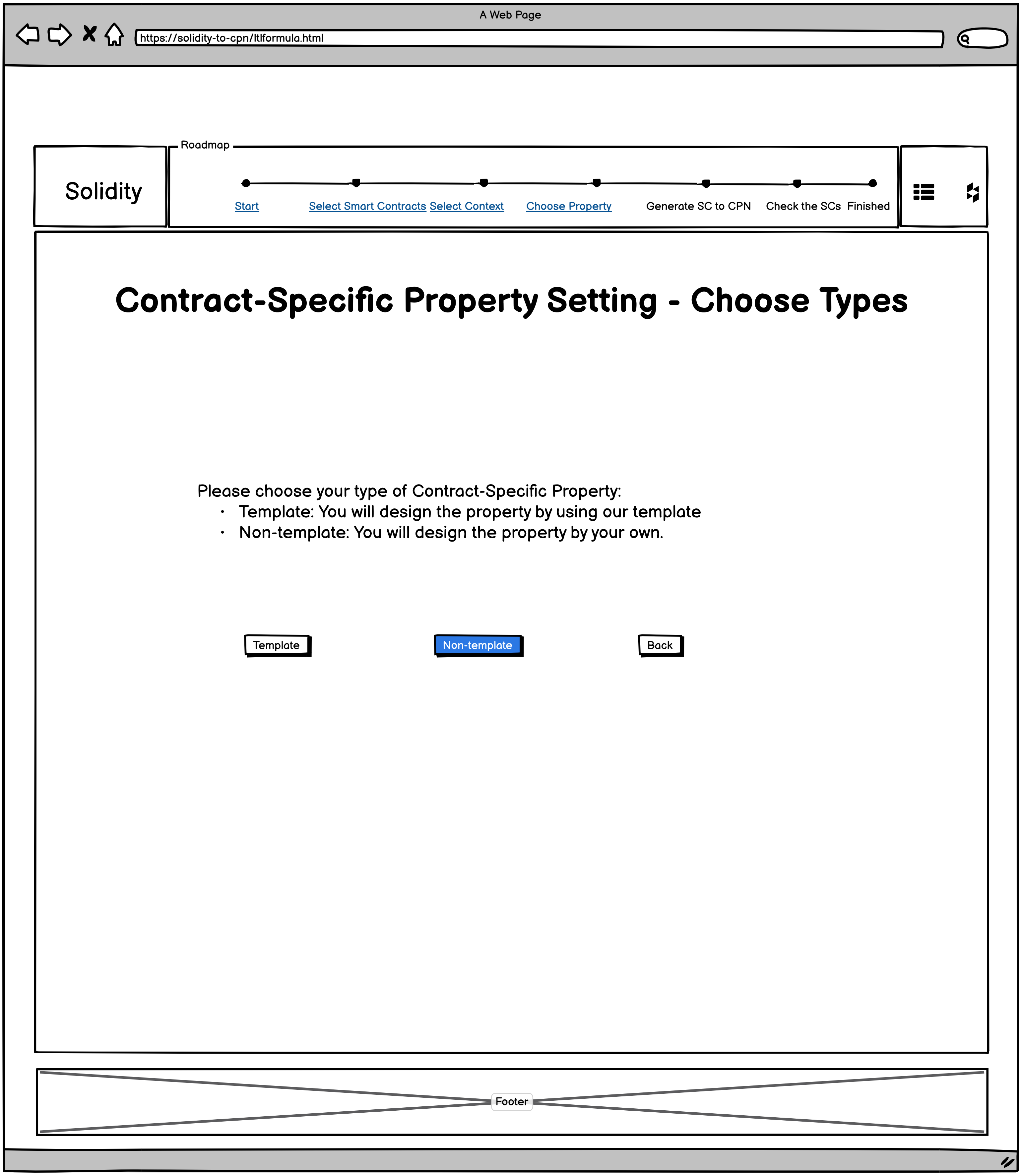
Template: Template 1

Formula: (GF{ variable 1 } ^ GF{ variable 2 }) => G({ function 3 }=> F{ function 4 })

Alert

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

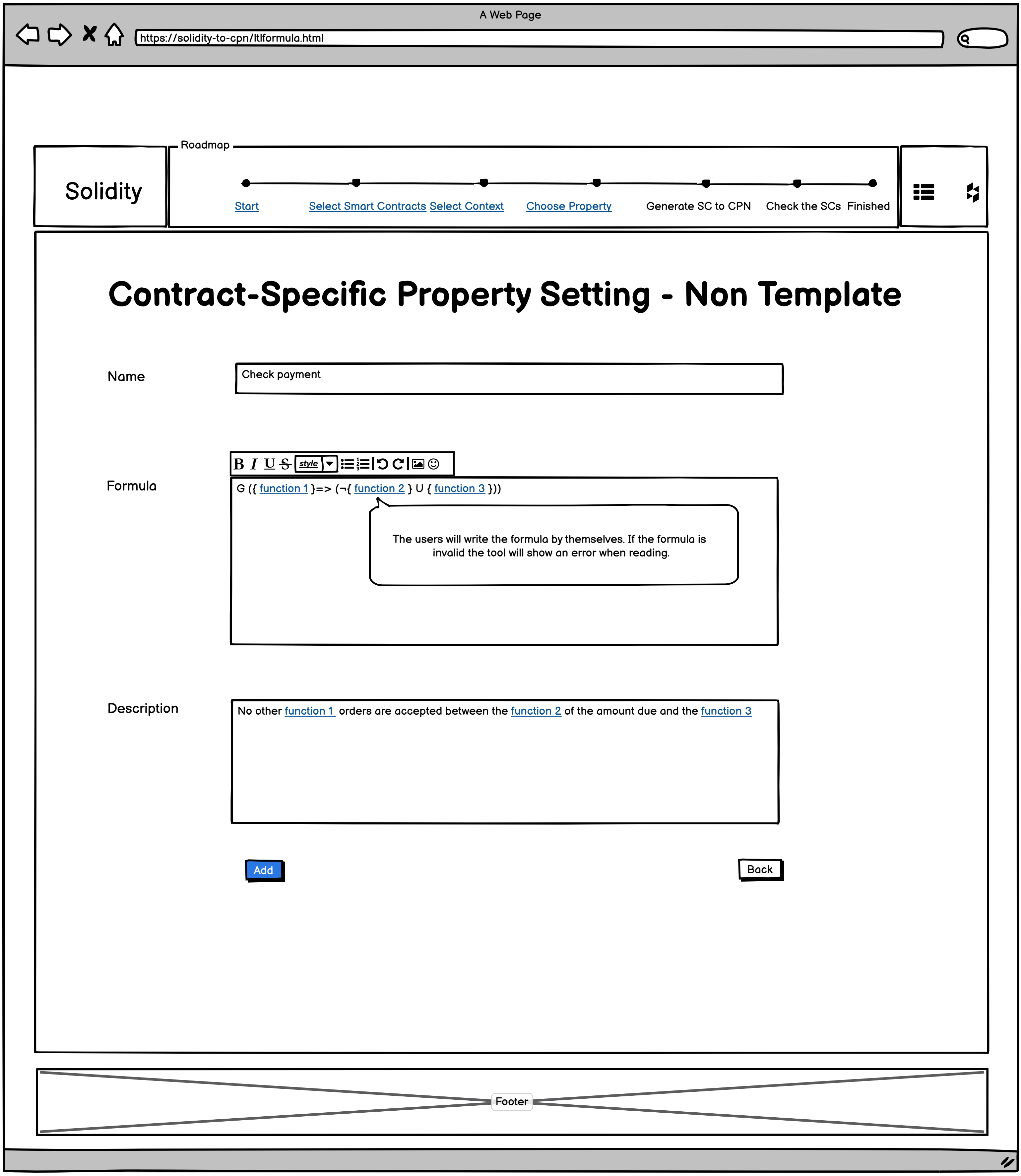
Description: If {variable 1} occurs infinitely often and {variable 2} occurs inifnitely often, then each occurrence of {function 3} is followed by an occurrence of {function 4}



Contract-Specific Property Setting - Choose Types

Please choose your type of Contract-Specific Property:

- Template: You will design the property by using our template
- Non-template: You will design the property by your own.



Contract-Specific Property Setting - Non Template

Name

Check payment

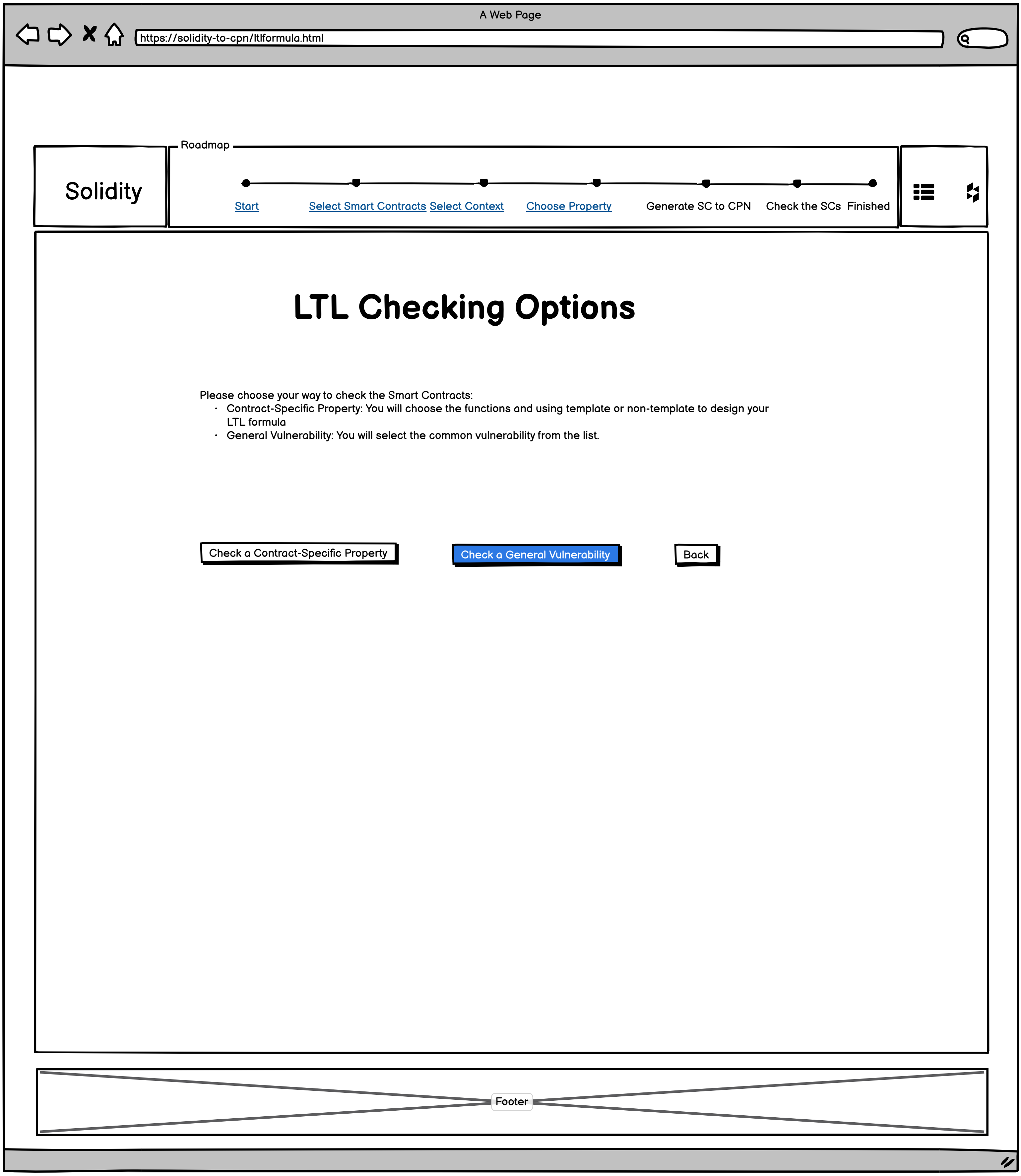
Formula

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

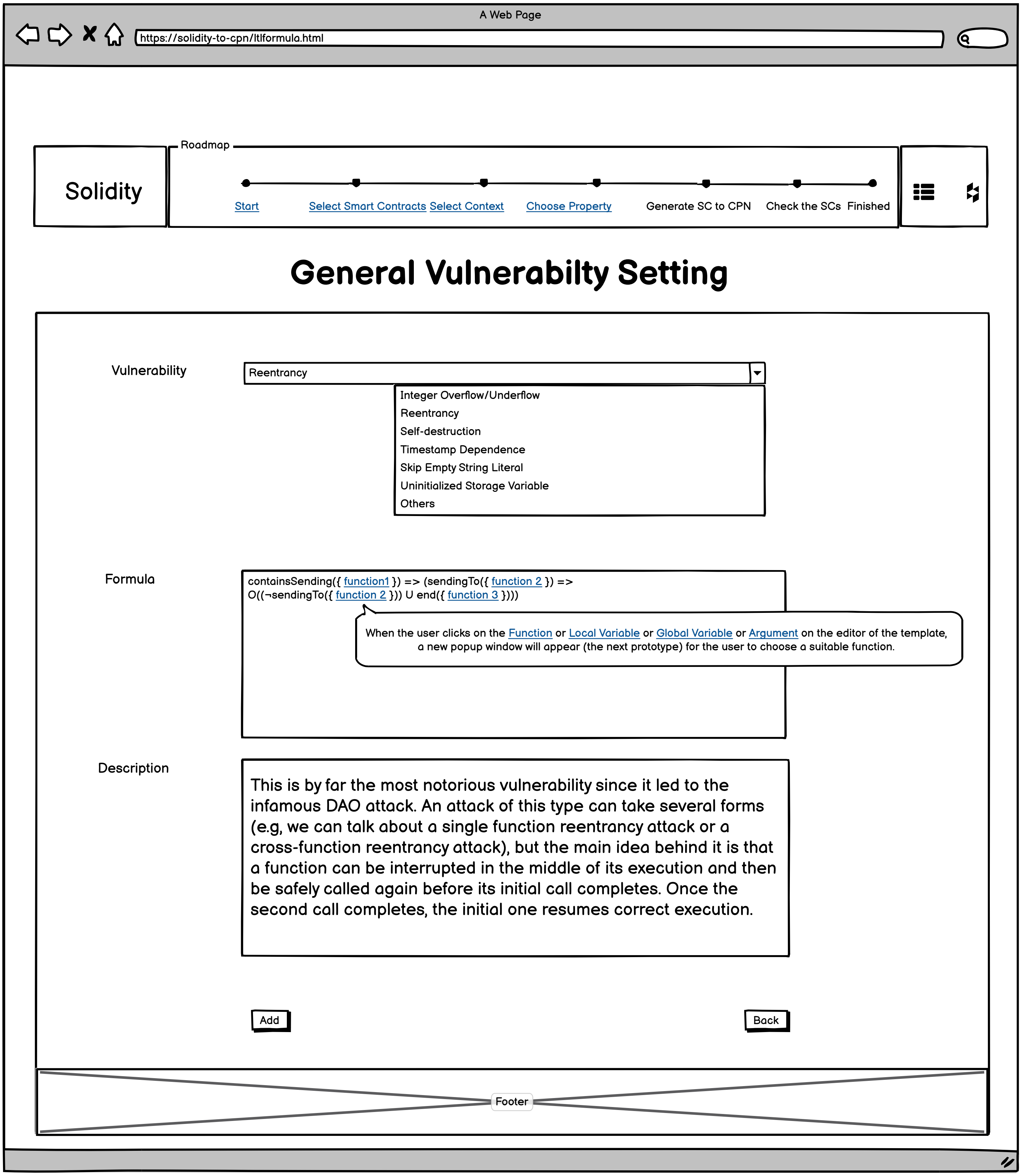


LTL Checking Options

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



General Vulnerabilty Setting

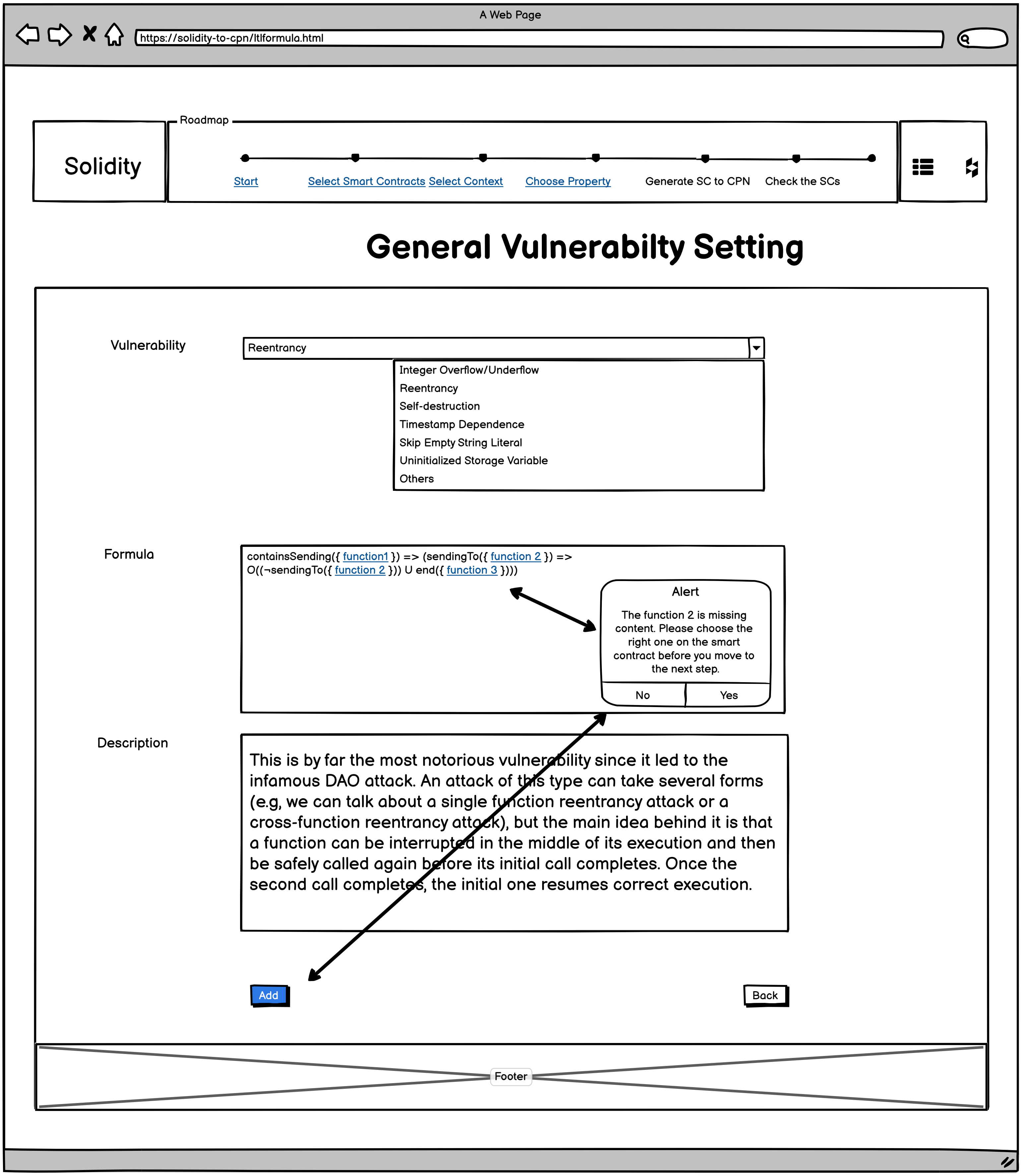
Vulnerability: Reentrancy

Integer Overflow/Underflow
Reentrancy
Self-destruction
Timestamp Dependence
Skip Empty String Literal
Uninitialized Storage Variable
Others

Formula: containsSending({ function1 }) => (sendingTo({ function 2 }) => O((¬sendingTo({ function 2 })) U end({ function 3 })))

When the user clicks on the Function or Local Variable or Global Variable or Argument on the editor of the template, a new popup window will appear (the next prototype) for the user to choose a suitable function.

Description: This is by far the most notorious vulnerability since it led to the infamous DAO attack. An attack of this type can take several forms (e.g, we can talk about a single function reentrancy attack or a cross-function reentrancy attack), but the main idea behind it is that a function can be interrupted in the middle of its execution and then be safely called again before its initial call completes. Once the second call completes, the initial one resumes correct execution.



General Vulnerabilty Setting

Vulnerability: Reentrancy

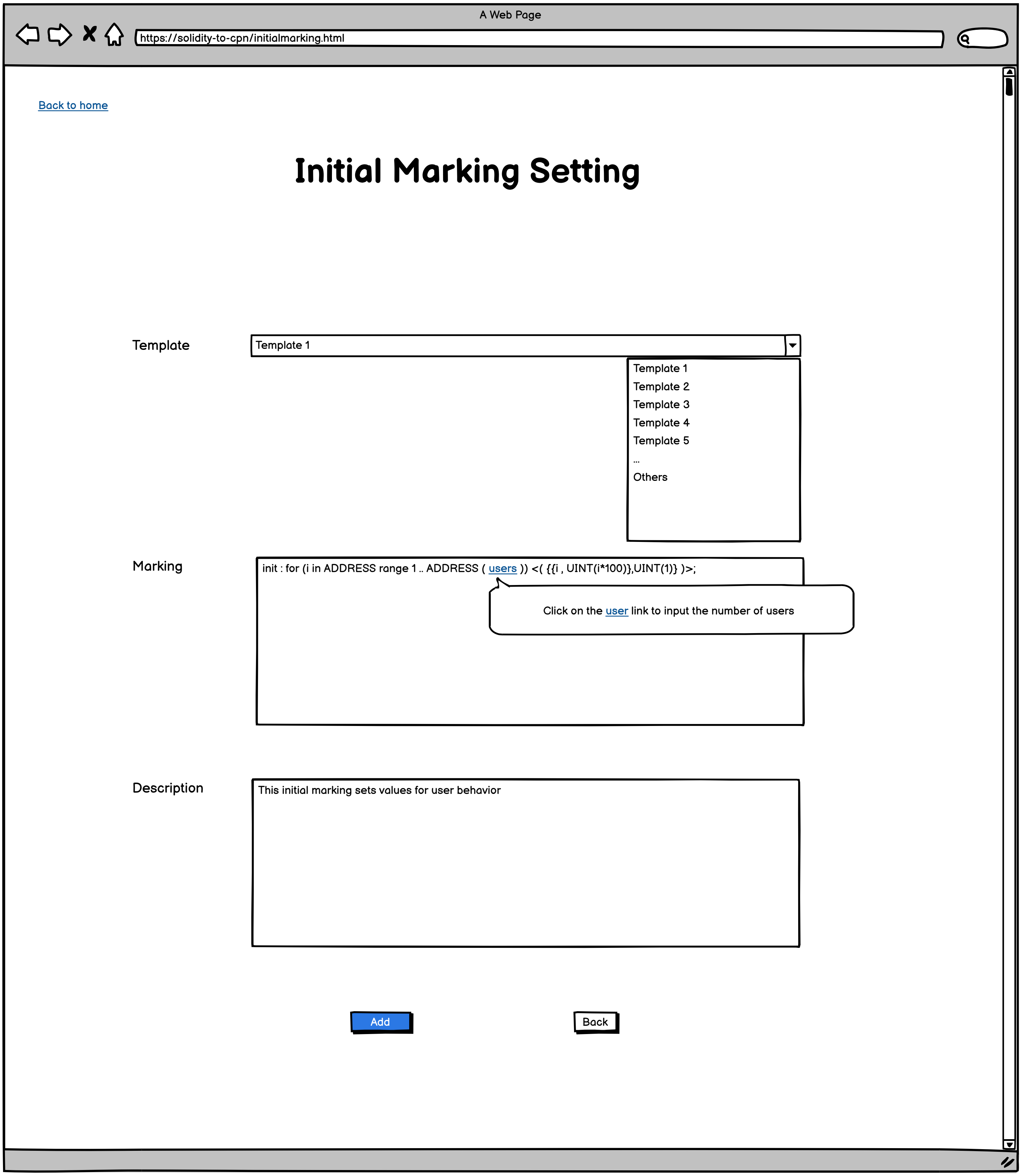
Integer Overflow/Underflow
Reentrancy
Self-destruction
Timestamp Dependence
Skip Empty String Literal
Uninitialized Storage Variable
Others

Formula: containsSending({ function1 }) => (sendingTo({ function 2 }) => O((¬sendingTo({ function 2 })) U end({ function 3 })))

Alert

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

Description: This is by far the most notorious vulnerability since it led to the infamous DAO attack. An attack of this type can take several forms (e.g, we can talk about a single function reentrancy attack or a cross-function reentrancy attack), but the main idea behind it is that a function can be interrupted in the middle of its execution and then be safely called again before its initial call completes. Once the second call completes, the initial one resumes correct execution.



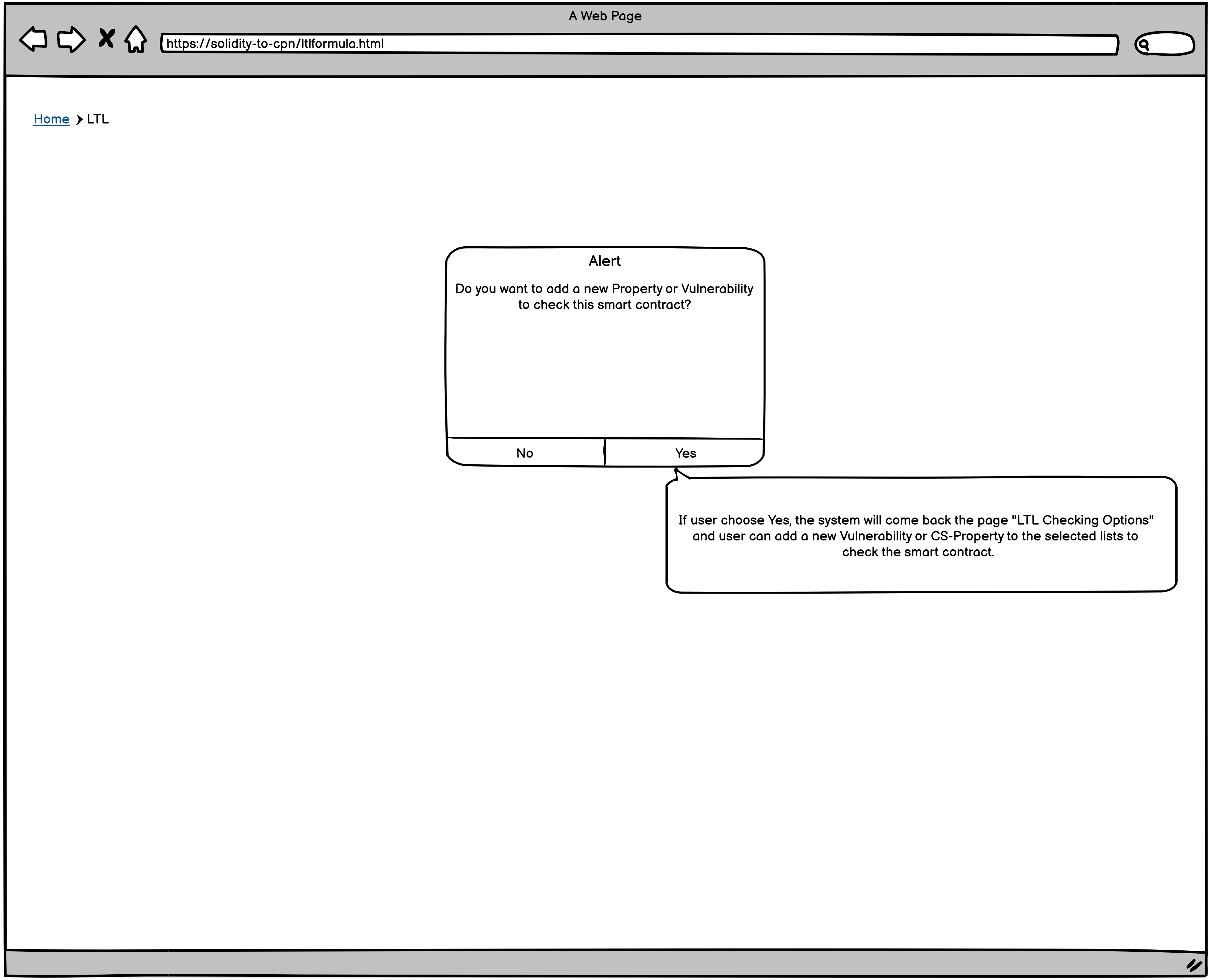
Initial Marking Setting

Template: Template 1

Marking: init : for (i in ADDRESS range 1 .. ADDRESS (users)) <({{i , UINT(i*100)}},UINT(1)})>;

Click on the user link to input the number of users

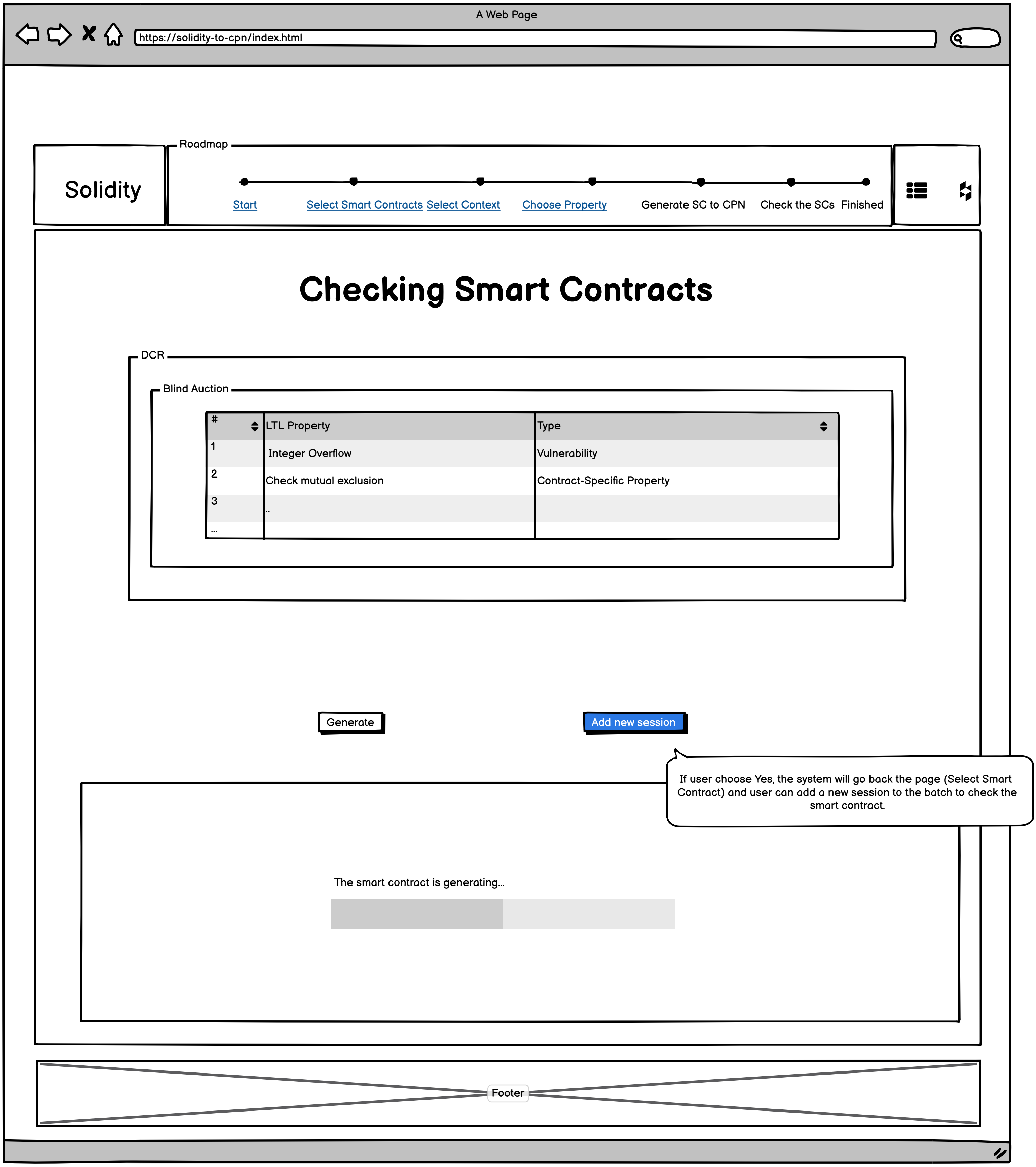
Description: This initial marking sets values for user behavior



Alert

Do you want to add a new Property or Vulnerability to check this smart contract?

If user choose Yes, the system will come back the page "LTL Checking Options" and user can add a new Vulnerability or CS-Property to the selected lists to check the smart contract.



Checking Smart Contracts

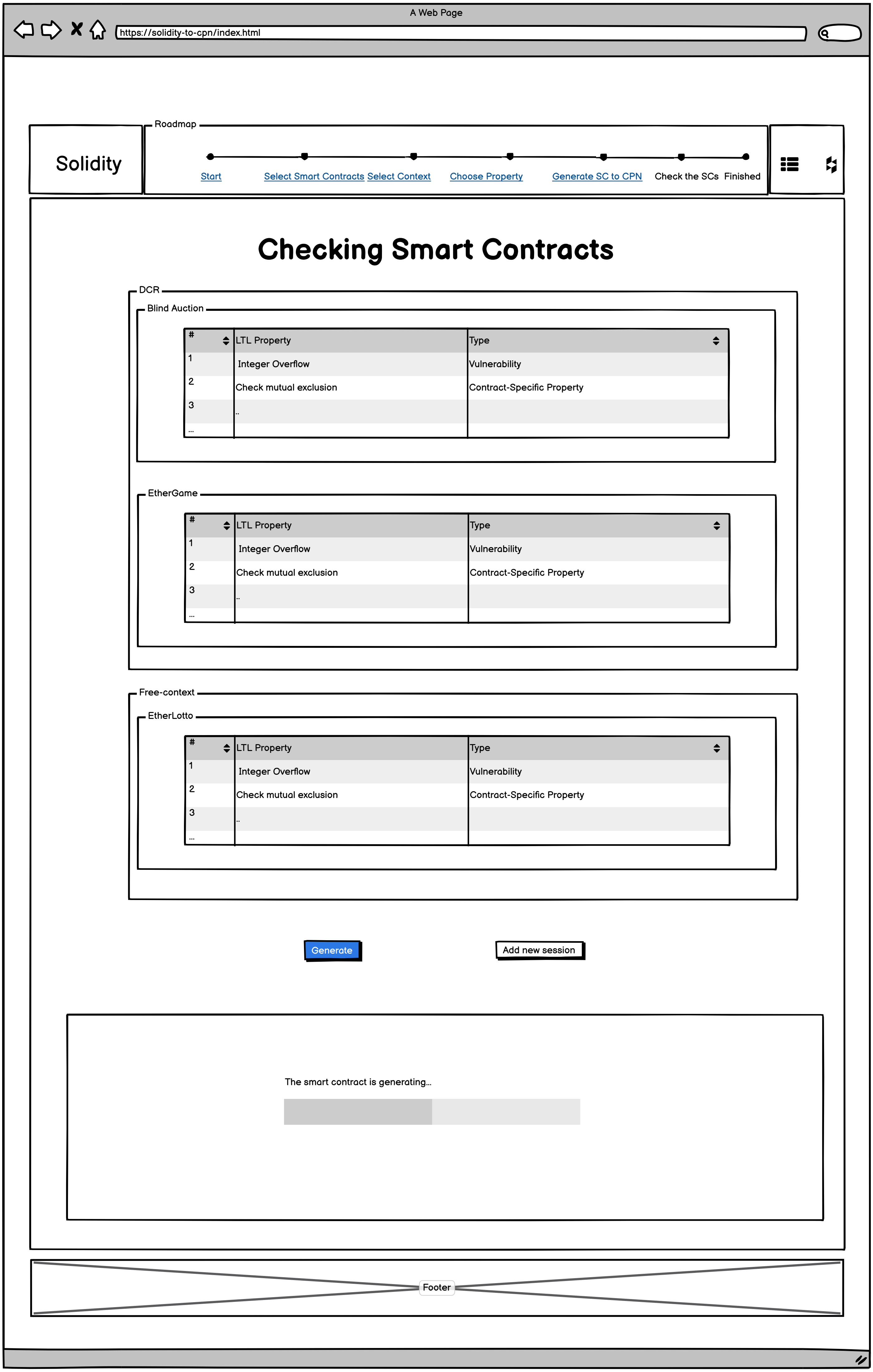
DCR

Blind Auction

#	LTL Property	Type
1	Integer Overflow	Vulnerability
2	Check mutual exclusion	Contract-Specific Property
3	..	
...		

If user choose Yes, the system will go back the page (Select Smart Contract) and user can add a new session to the batch to check the smart contract.

The smart contract is generating...



Checking Smart Contracts

DCR

Blind Auction

#	LTL Property	Type
1	Integer Overflow	Vulnerability
2	Check mutual exclusion	Contract-Specific Property
3	..	
...		

EtherGame

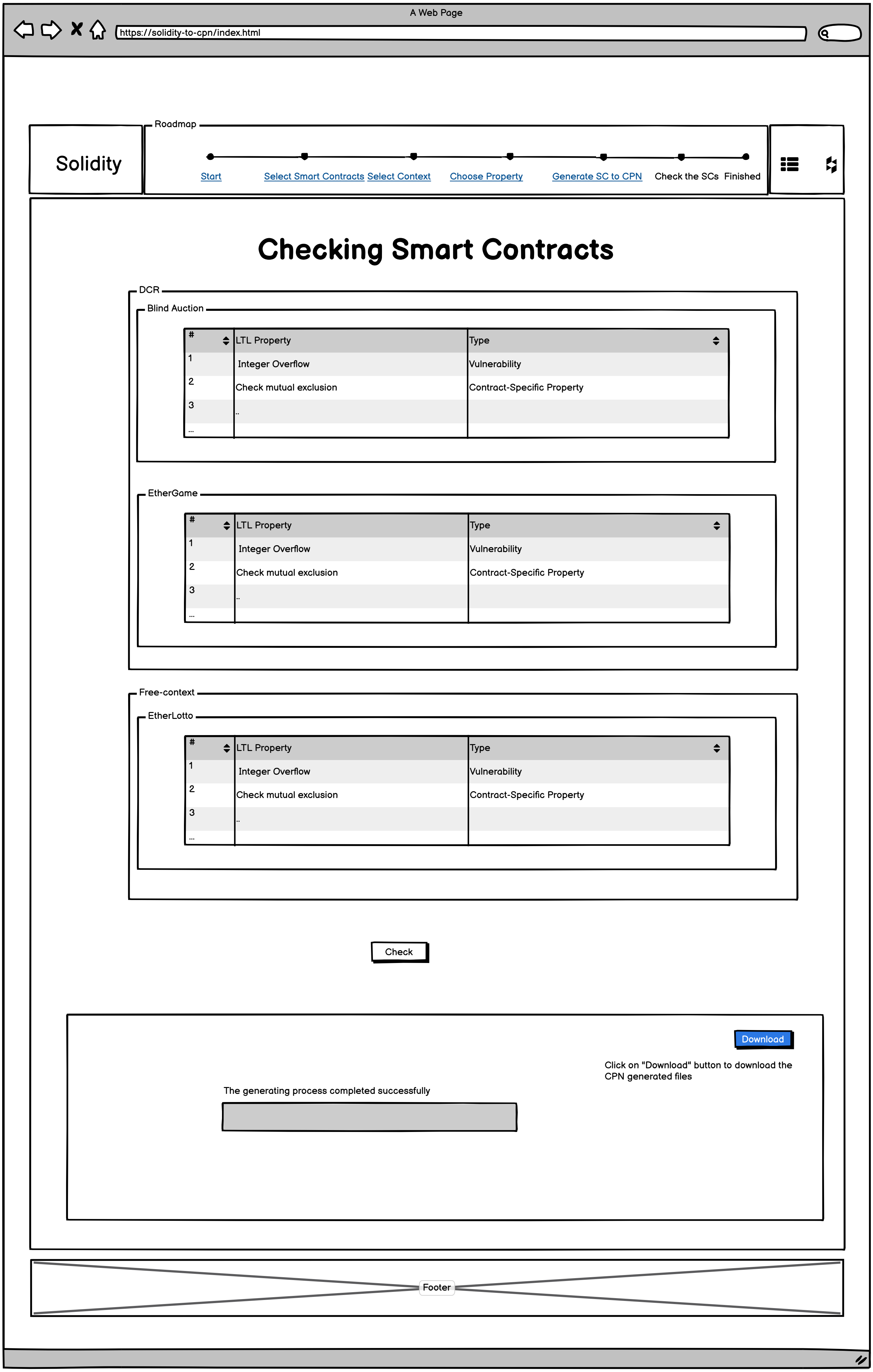
#	LTL Property	Type
1	Integer Overflow	Vulnerability
2	Check mutual exclusion	Contract-Specific Property
3	..	
...		

Free-context

EtherLotto

#	LTL Property	Type
1	Integer Overflow	Vulnerability
2	Check mutual exclusion	Contract-Specific Property
3	..	
...		

The smart contract is generating...



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

DCR

Blind Auction

#	LTL Property	Type
1	Integer Overflow	Vulnerability
2	Check mutual exclusion	Contract-Specific Property
3	..	
...		

EtherGame

#	LTL Property	Type
1	Integer Overflow	Vulnerability
2	Check mutual exclusion	Contract-Specific Property
3	..	
...		

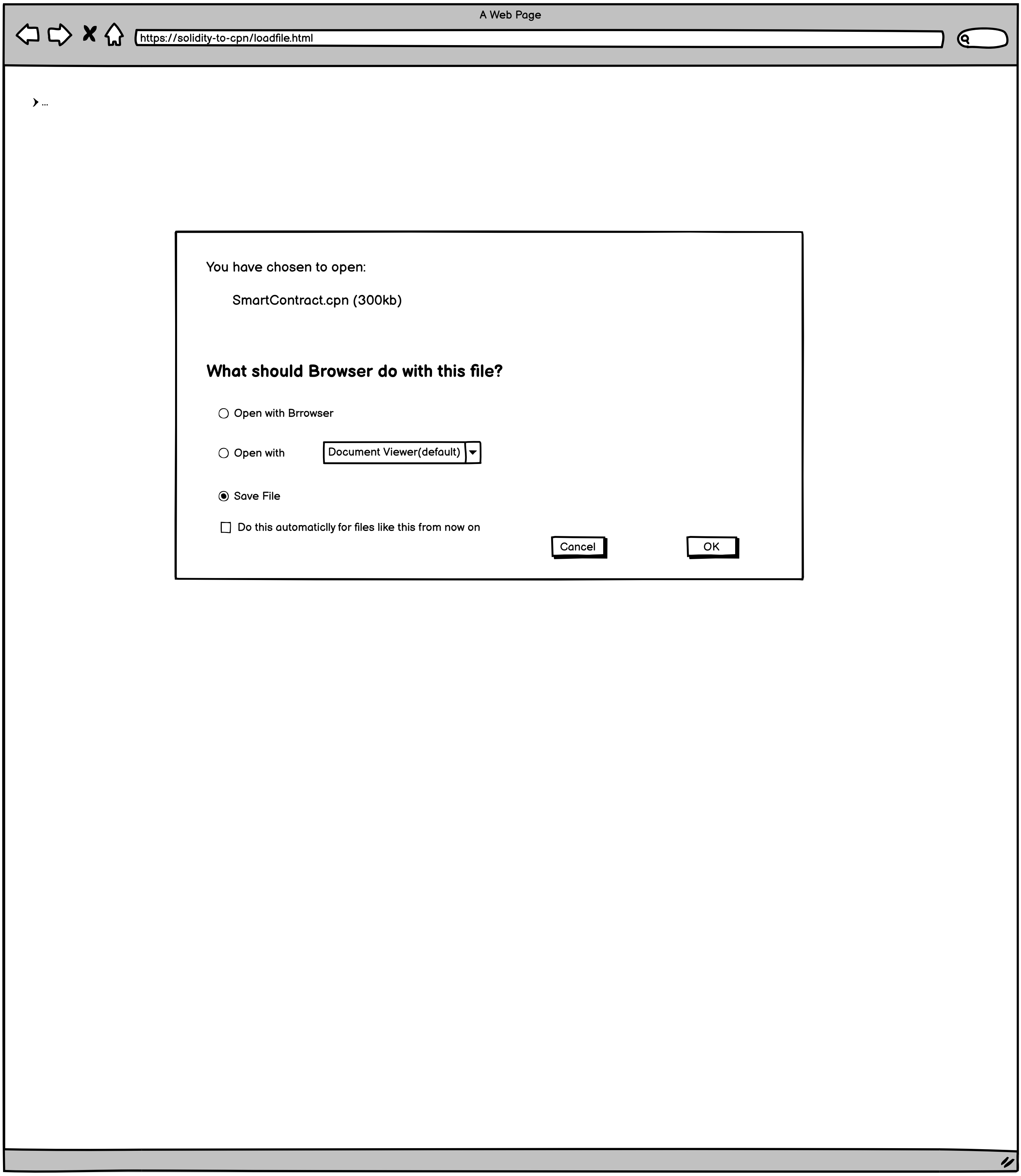
Free-context

EtherLotto

#	LTL Property	Type
1	Integer Overflow	Vulnerability
2	Check mutual exclusion	Contract-Specific Property
3	..	
...		

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

The generating process completed successfully



You have chosen to open:

SmartContract.cpn (300kb)

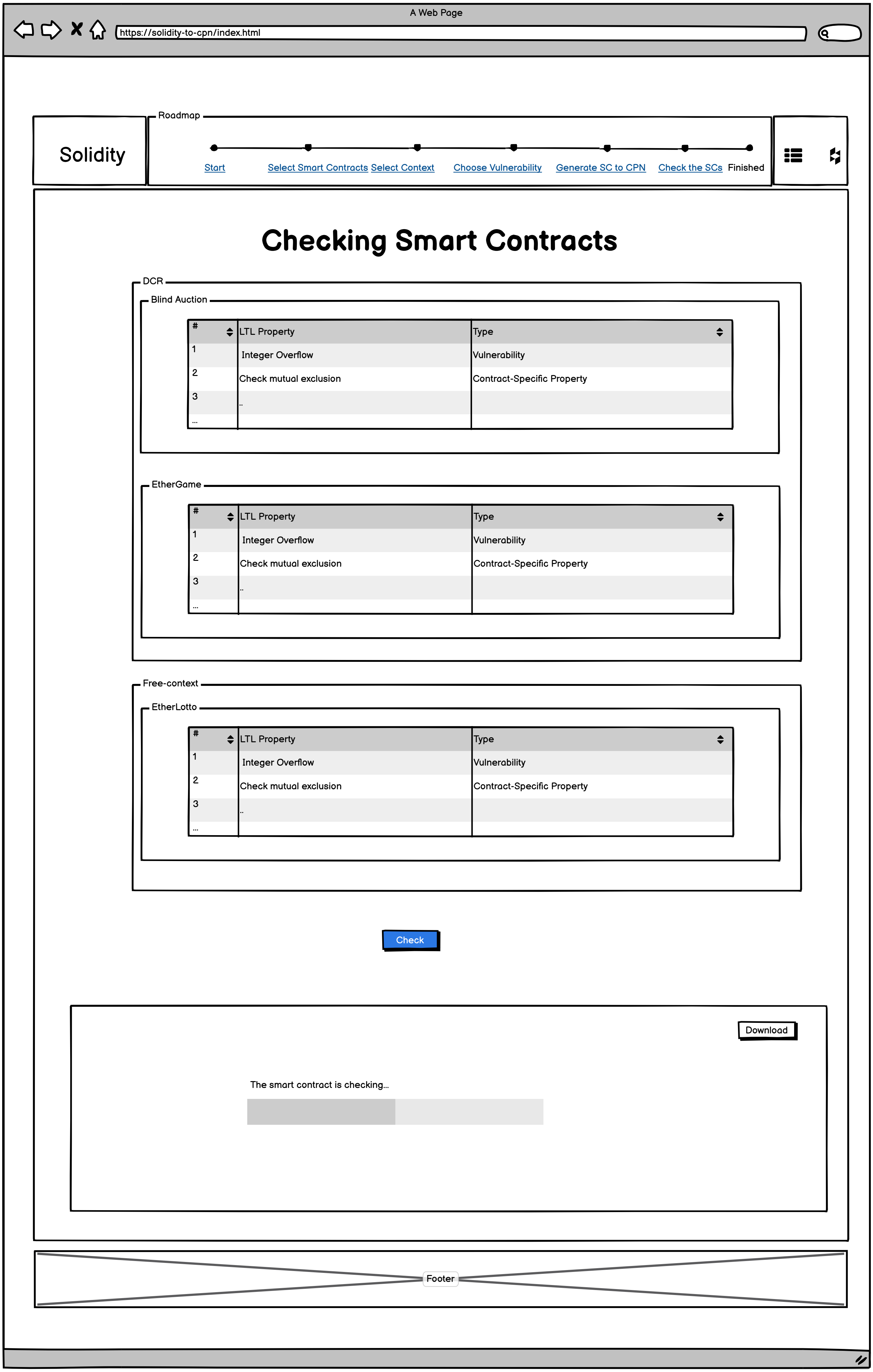
What should Browser do with this file?

○ Open with Brrowser

○ Open with Document Viewer(default) ▾

● Save File

□ Do this automaticlly for files like this from now on



Checking Smart Contracts

DCR

Blind Auction

#	LTL Property	Type
1	Integer Overflow	Vulnerability
2	Check mutual exclusion	Contract-Specific Property
3	..	
...		

EtherGame

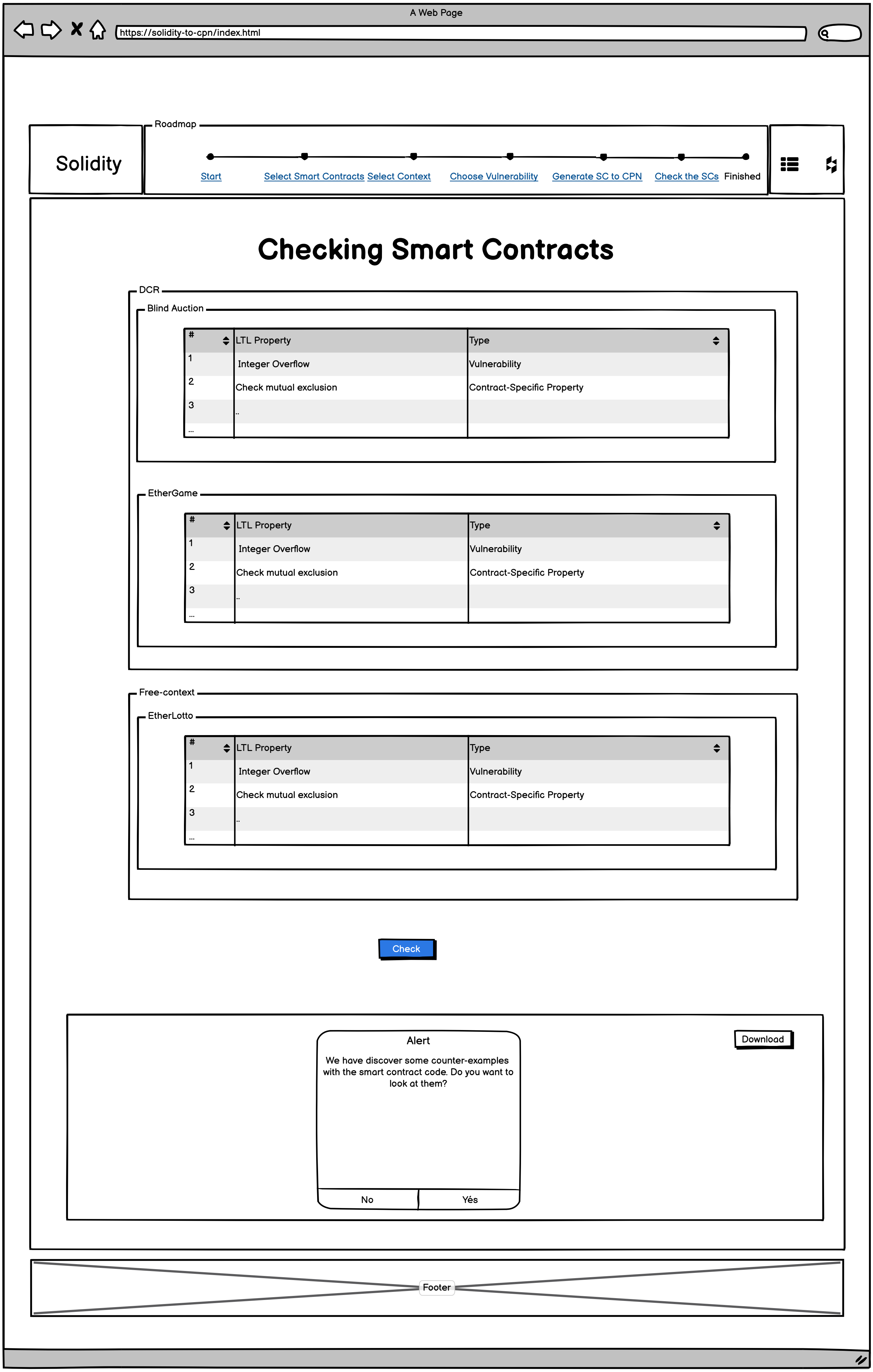
#	LTL Property	Type
1	Integer Overflow	Vulnerability
2	Check mutual exclusion	Contract-Specific Property
3	..	
...		

Free-context

EtherLotto

#	LTL Property	Type
1	Integer Overflow	Vulnerability
2	Check mutual exclusion	Contract-Specific Property
3	..	
...		

The smart contract is checking...



Checking Smart Contracts

DCR

Blind Auction

#	LTL Property	Type
1	Integer Overflow	Vulnerability
2	Check mutual exclusion	Contract-Specific Property
3	..	
...		

EtherGame

#	LTL Property	Type
1	Integer Overflow	Vulnerability
2	Check mutual exclusion	Contract-Specific Property
3	..	
...		

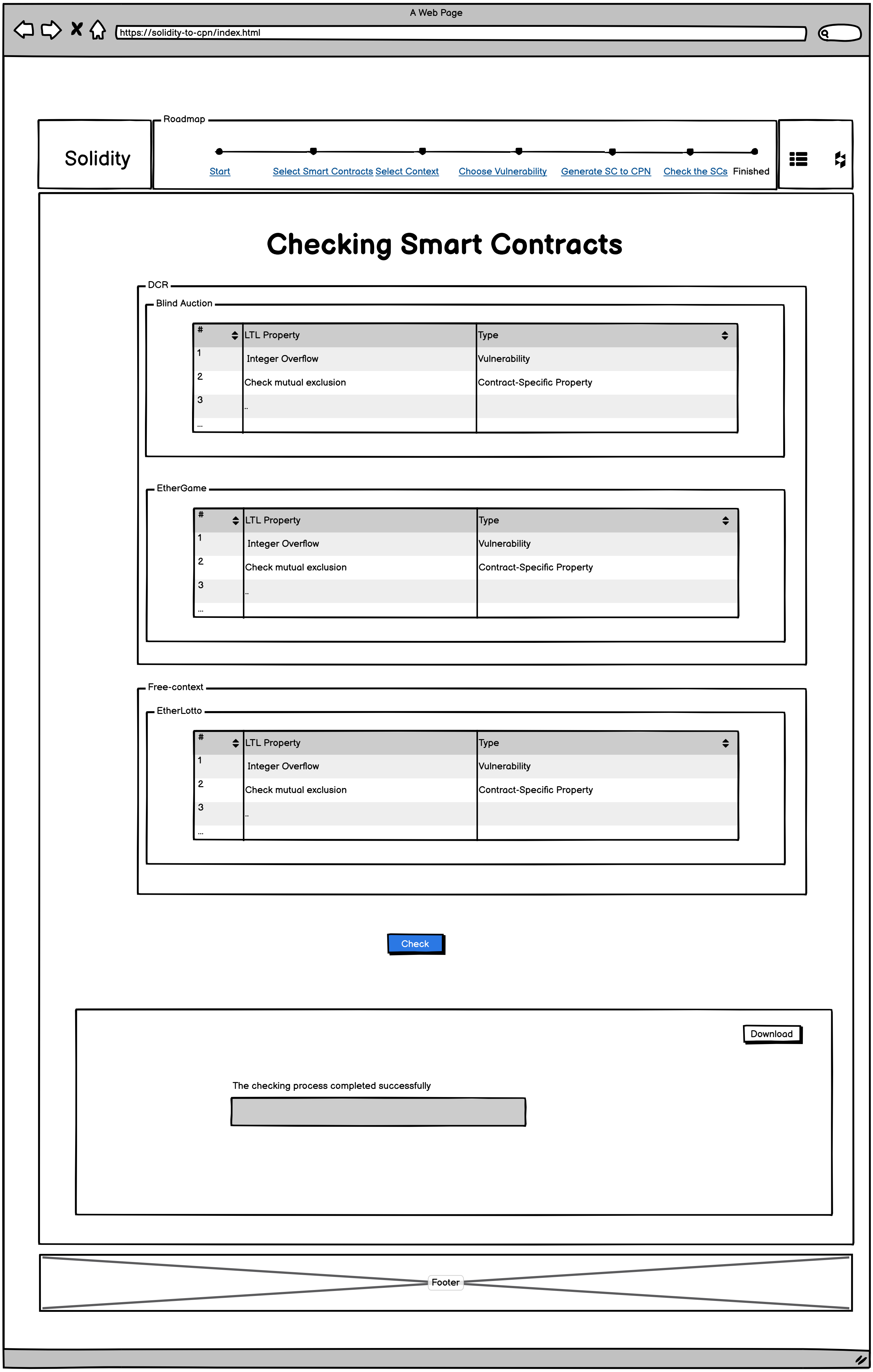
Free-context

EtherLotto

#	LTL Property	Type
1	Integer Overflow	Vulnerability
2	Check mutual exclusion	Contract-Specific Property
3	..	
...		

Alert

We have discover some counter-examples with the smart contract code. Do you want to look at them?



Checking Smart Contracts

DCR

Blind Auction

#	LTL Property	Type
1	Integer Overflow	Vulnerability
2	Check mutual exclusion	Contract-Specific Property
3	..	
...		

EtherGame

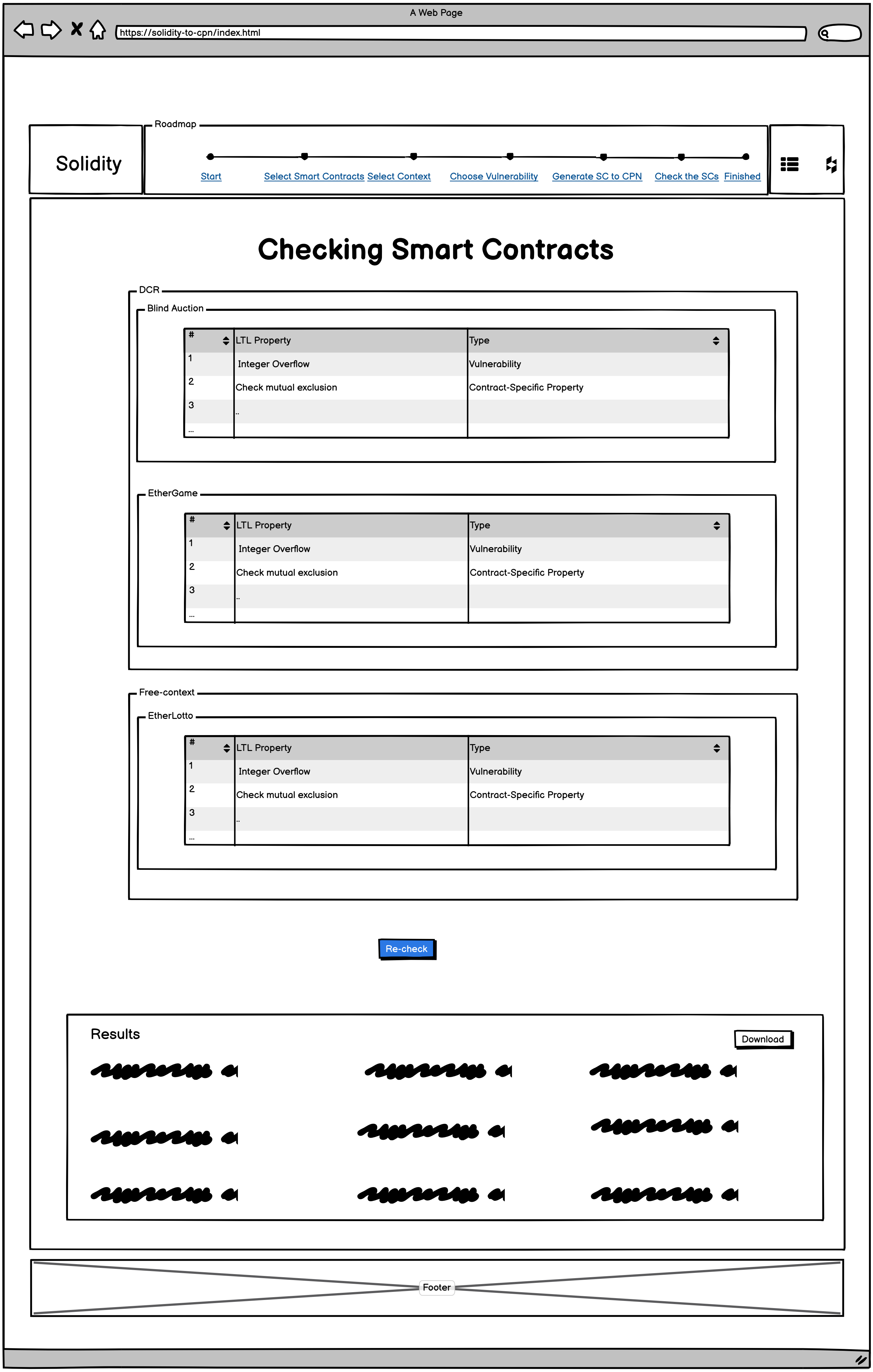
#	LTL Property	Type
1	Integer Overflow	Vulnerability
2	Check mutual exclusion	Contract-Specific Property
3	..	
...		

Free-context

EtherLotto

#	LTL Property	Type
1	Integer Overflow	Vulnerability
2	Check mutual exclusion	Contract-Specific Property
3	..	
...		

The checking process completed successfully



Solidity

Roadmap

Checking Smart Contracts

DCR

Blind Auction

#	LTL Property	Type
1	Integer Overflow	Vulnerability
2	Check mutual exclusion	Contract-Specific Property
3	..	
...		

EtherGame

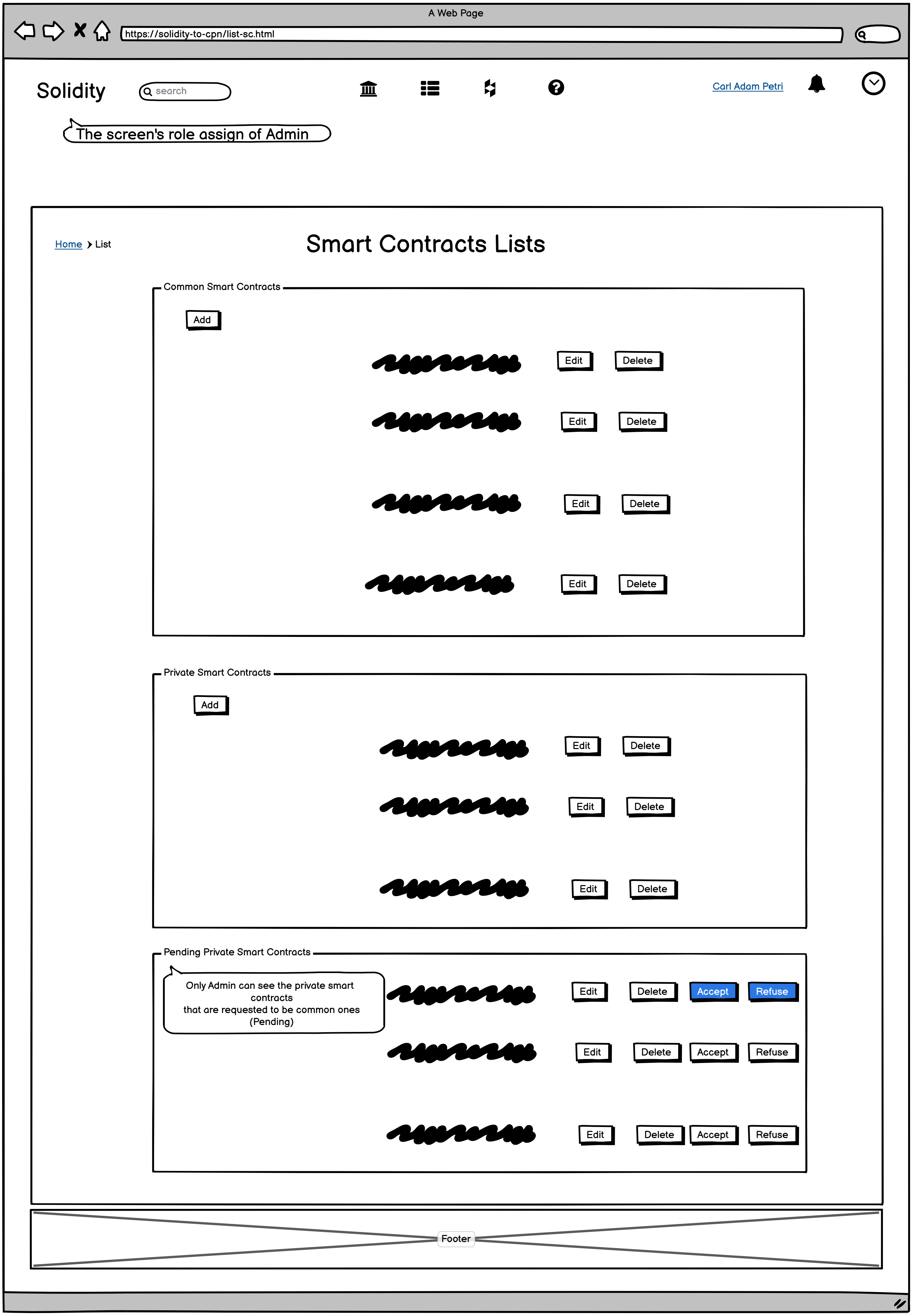
#	LTL Property	Type
1	Integer Overflow	Vulnerability
2	Check mutual exclusion	Contract-Specific Property
3	..	
...		

Free-context

EtherLotto

#	LTL Property	Type
1	Integer Overflow	Vulnerability
2	Check mutual exclusion	Contract-Specific Property
3	..	
...		

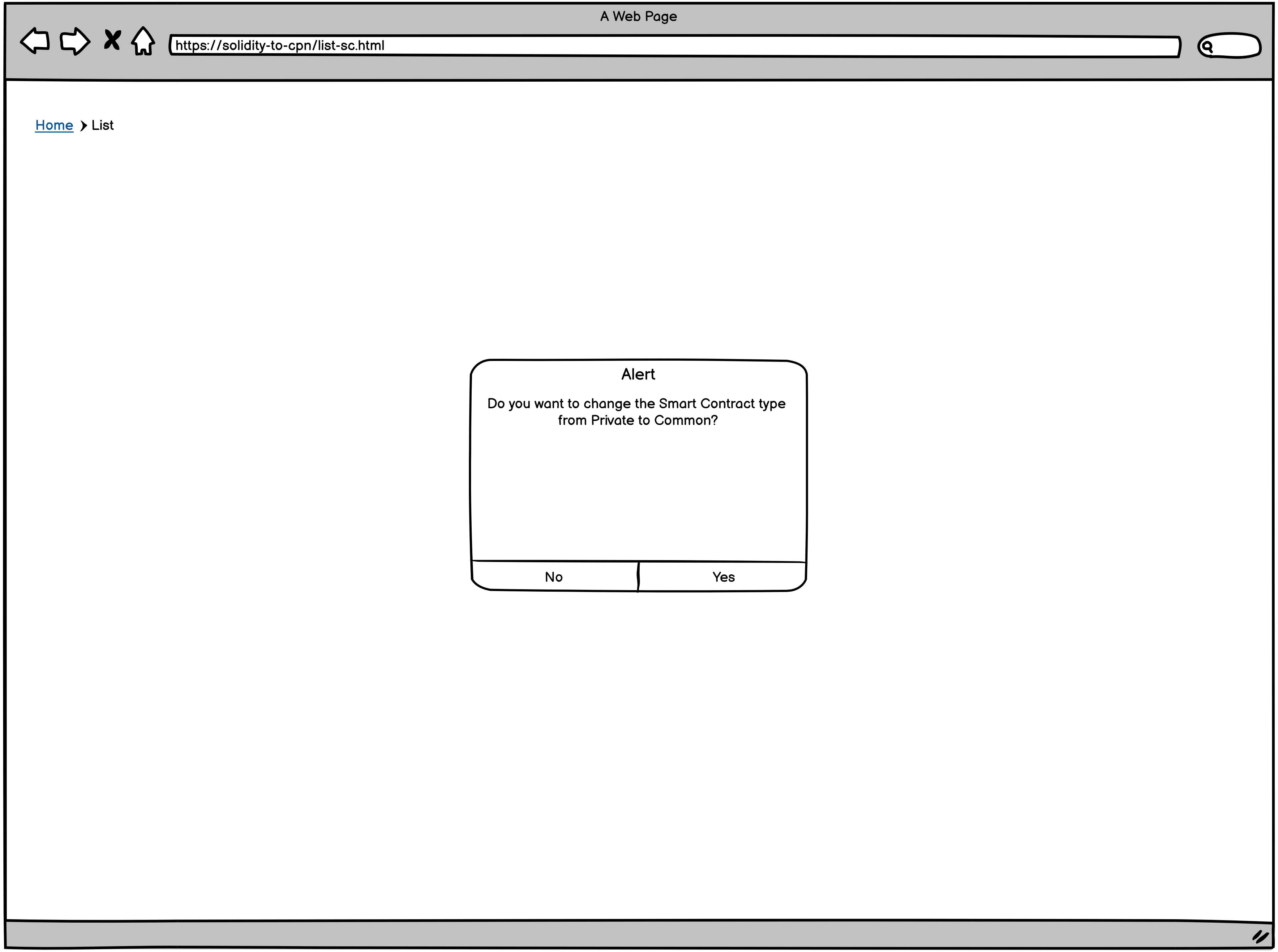
Results



The screen's role assign of Admin

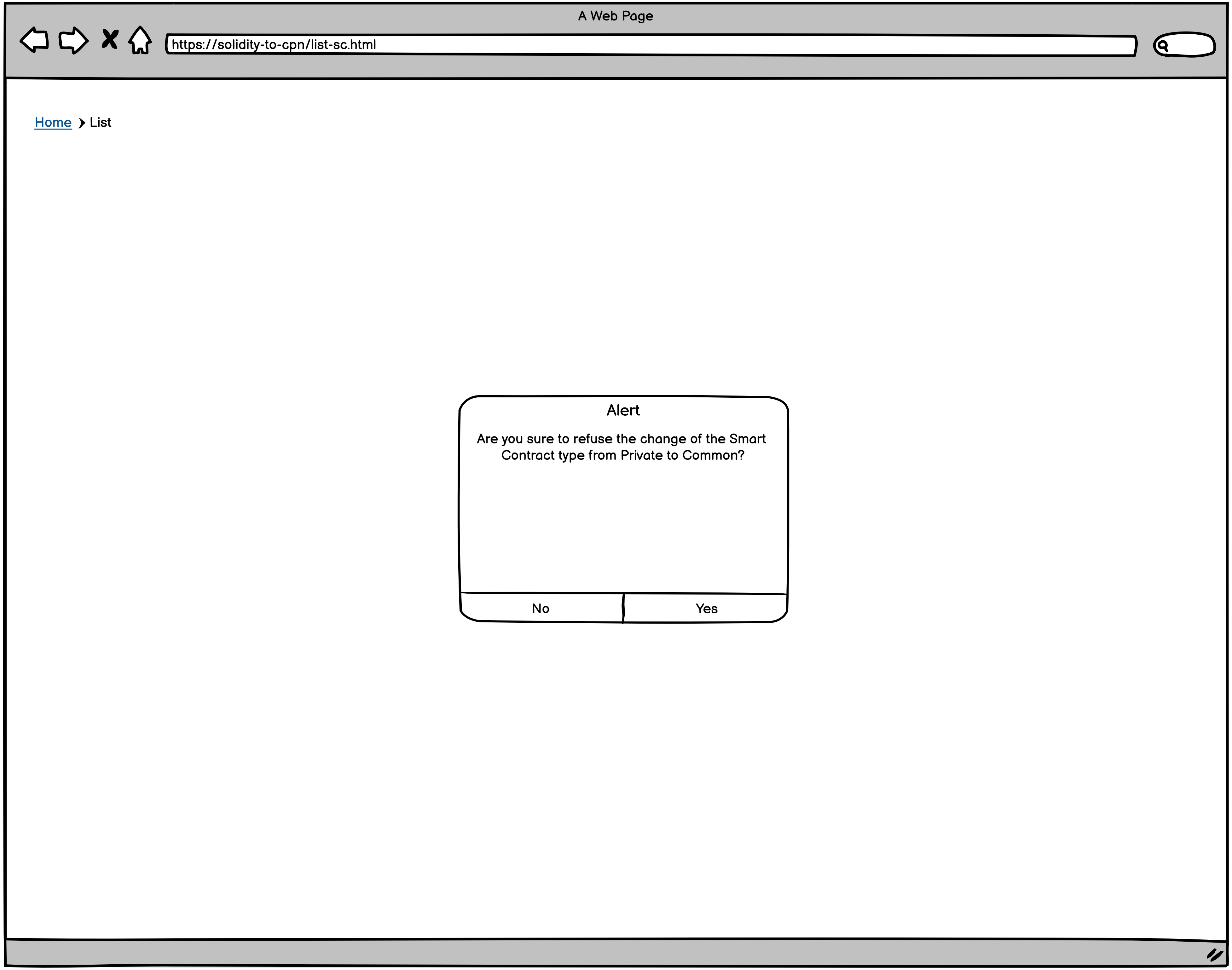
Smart Contracts Lists

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

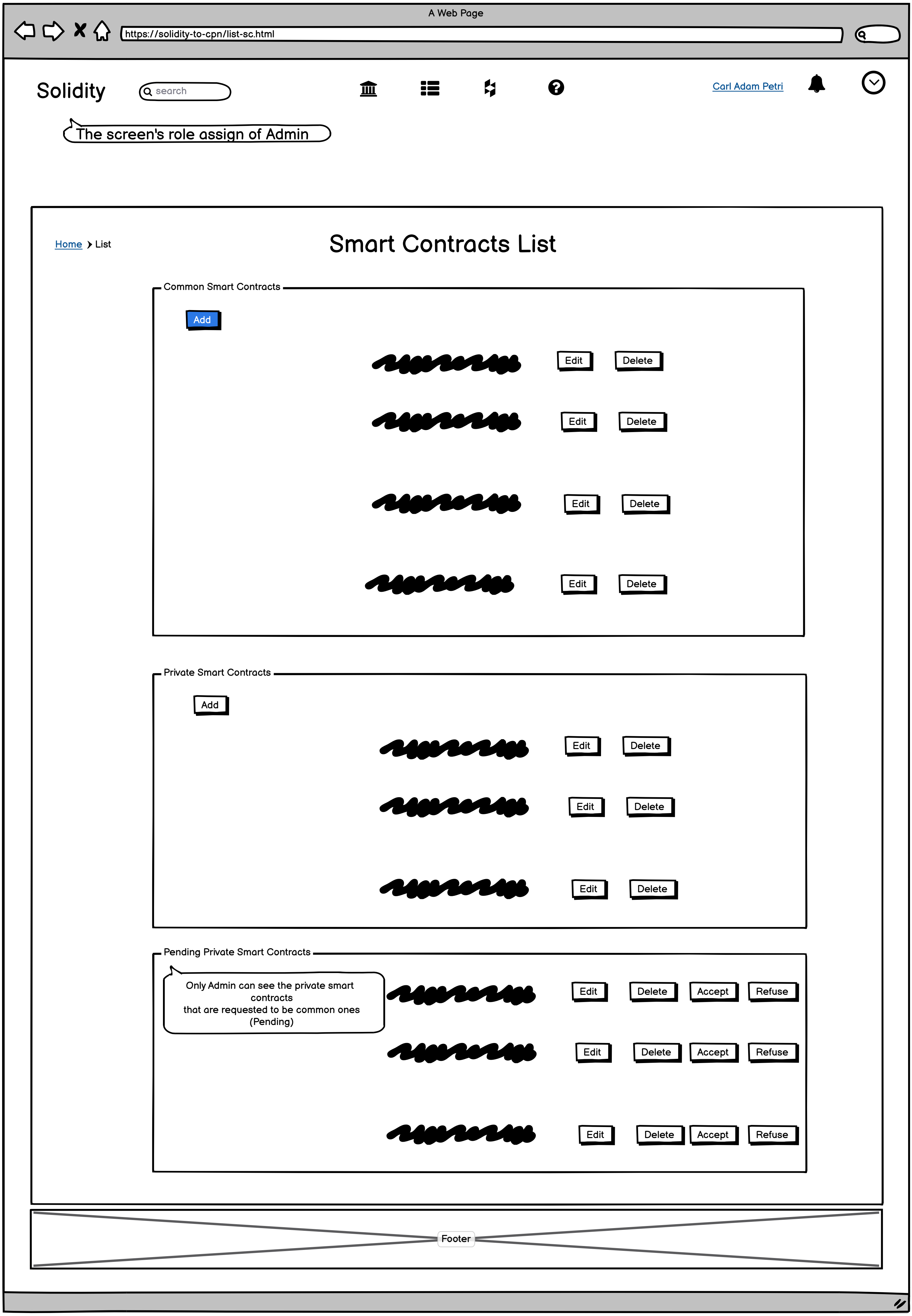


Alert

Do you want to change the Smart Contract type from Private to Common?



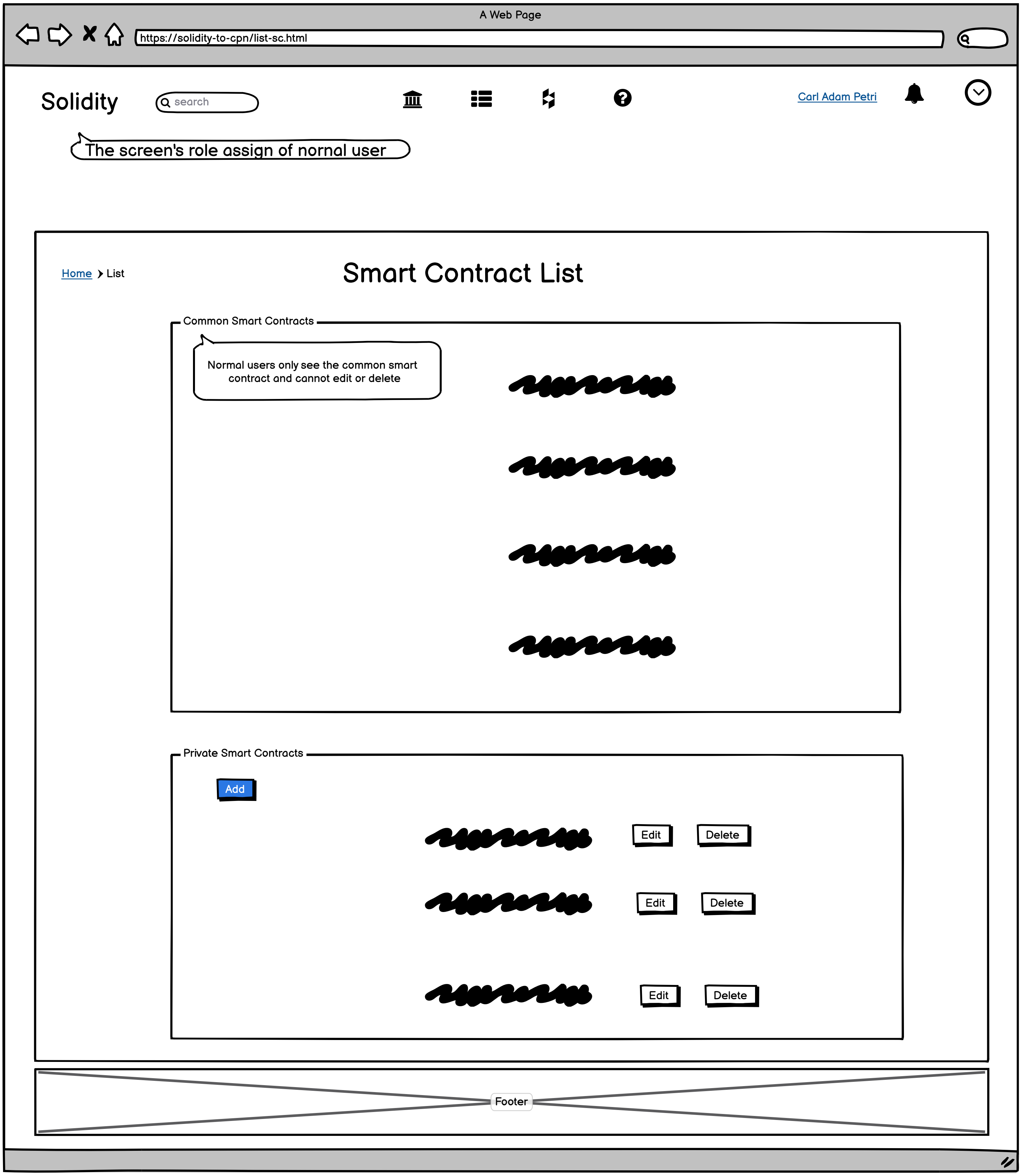
Are you sure to refuse the change of the Smart Contract type from Private to Common?



The screen's role assign of Admin

Smart Contracts List

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



A Web Page

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

Solidity

Carl Adam Petri

The screen's role assign of nornal user

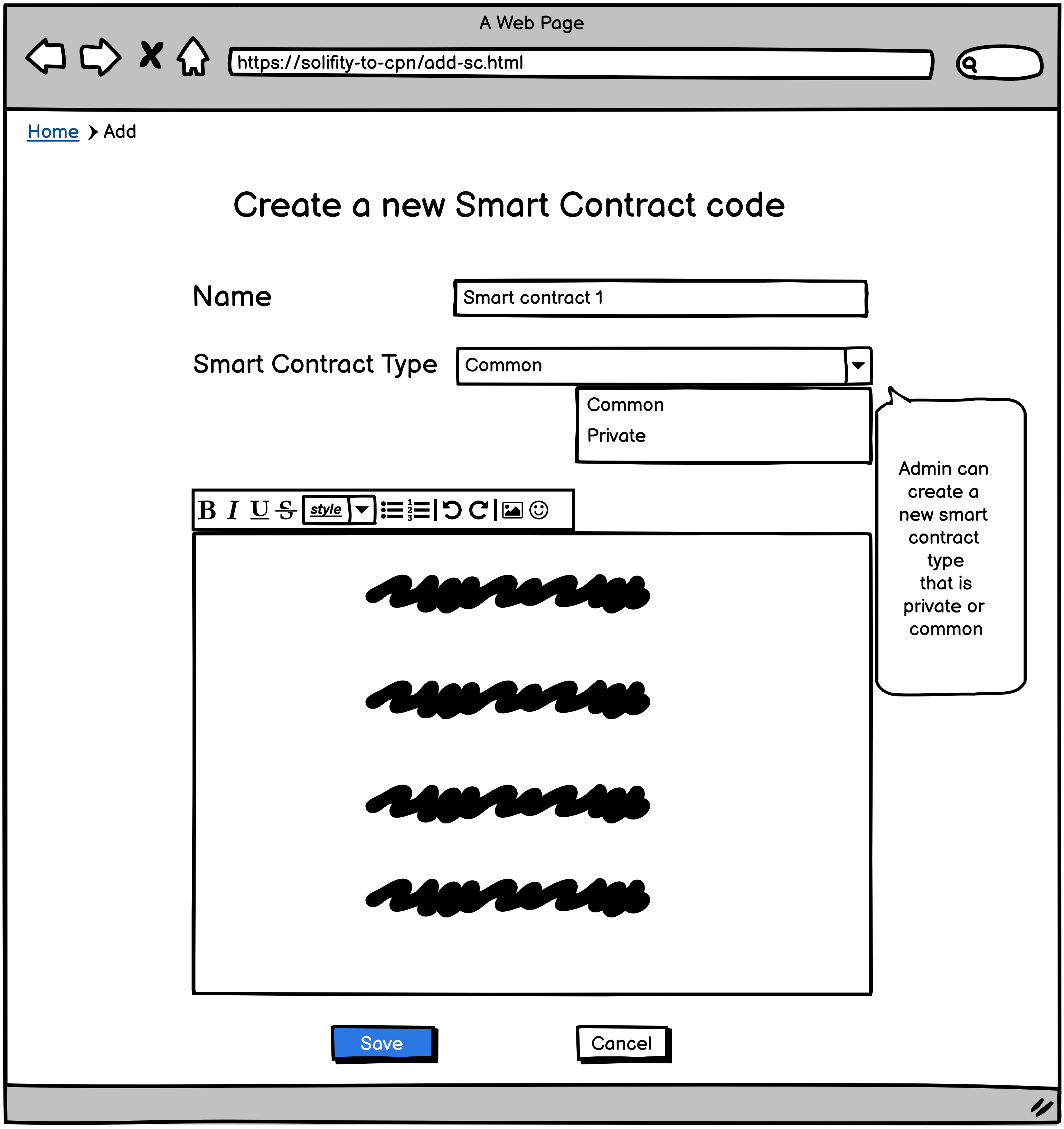
Home > List

Smart Contract List

Common Smart Contracts

Normal users only see the common smart contract and cannot edit or delete

Private Smart Contracts



A Web Page

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

Home > Add

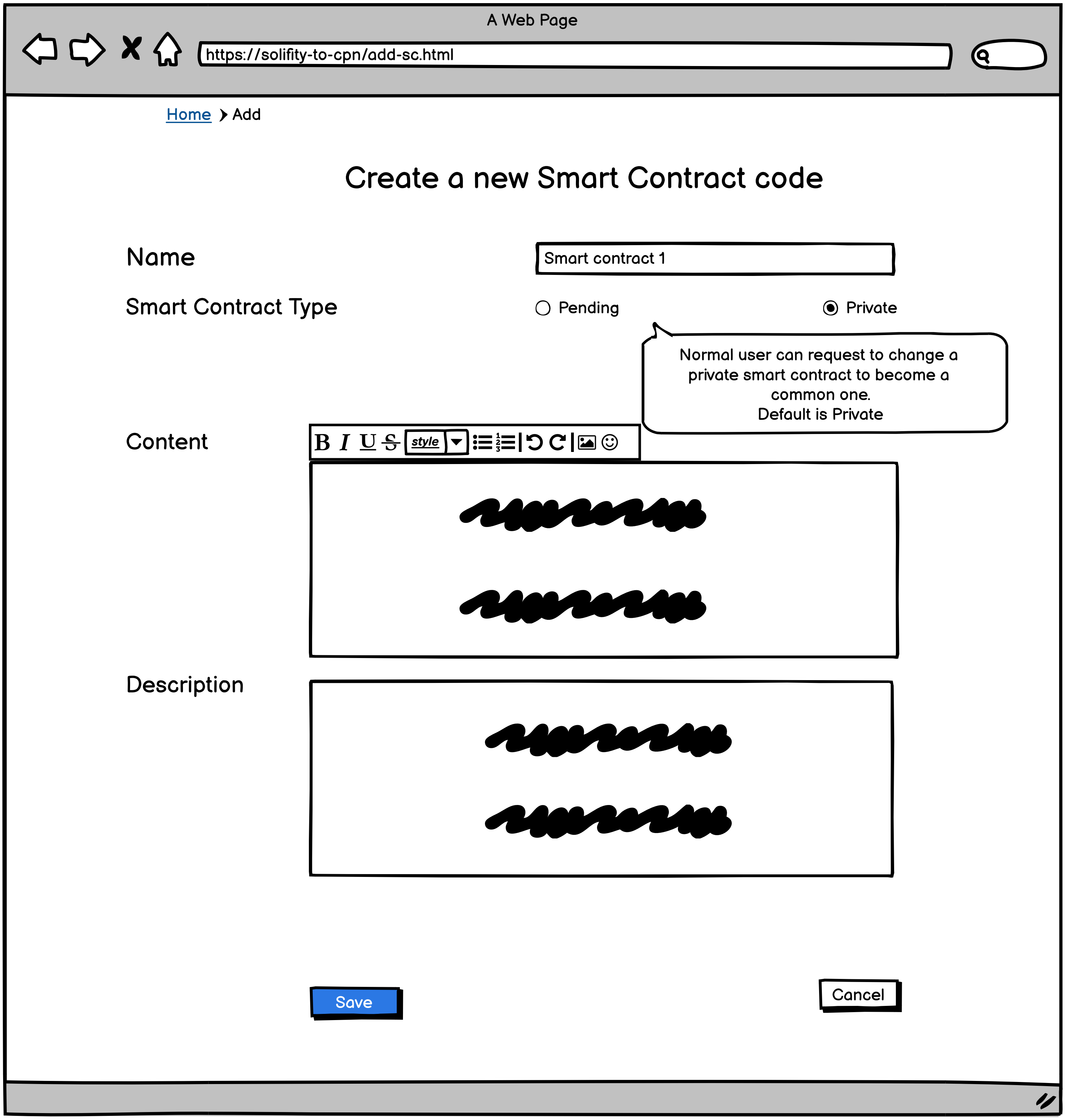
Create a new Smart Contract code

Name: Smart contract 1

Smart Contract Type: Common

Common
Private

Admin can create a new smart contract type that is private or common



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

Home ❯ Add

Create a new Smart Contract code

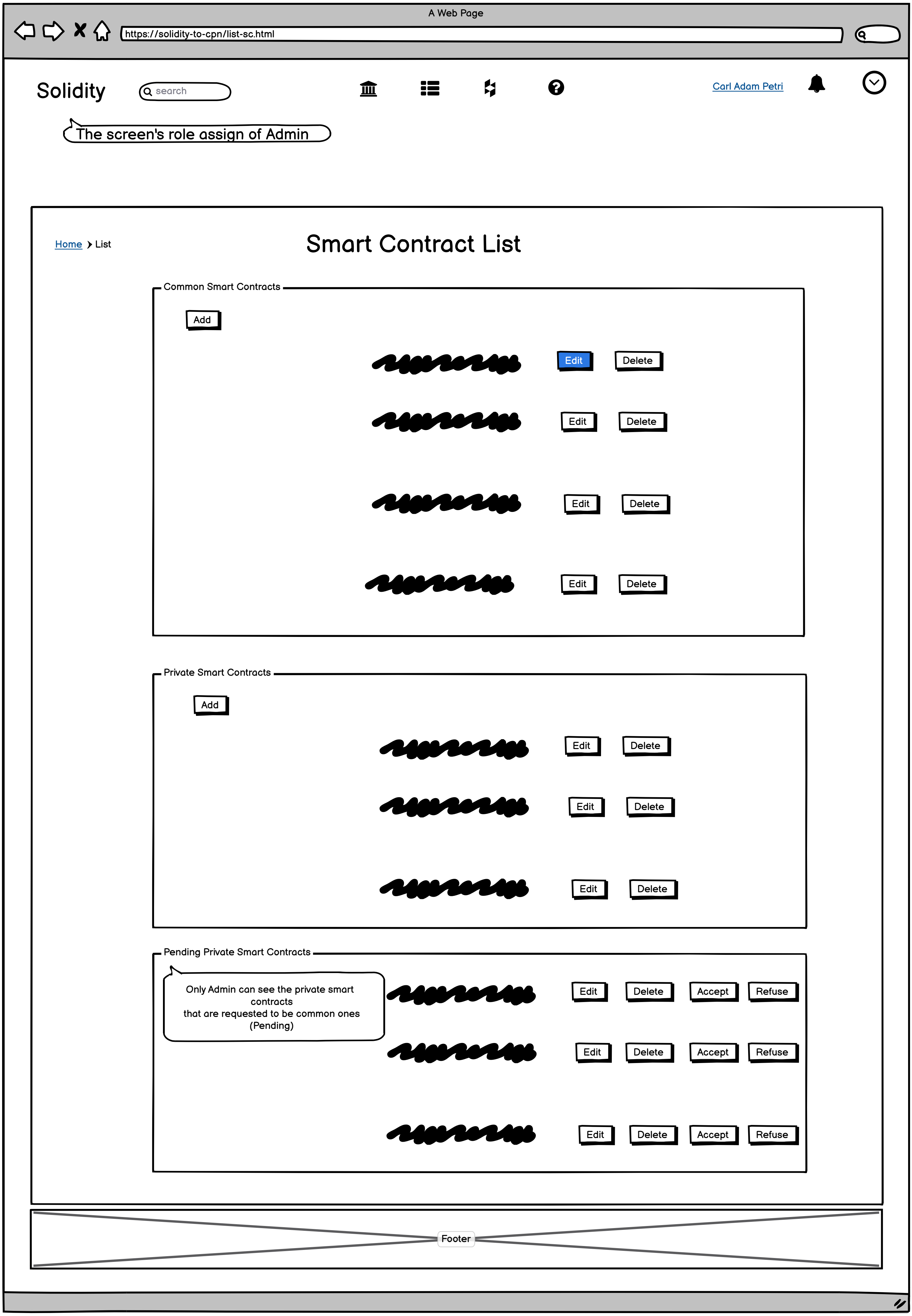
Name: Smart contract 1

Smart Contract Type: ○ Pending ● Private

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

Content

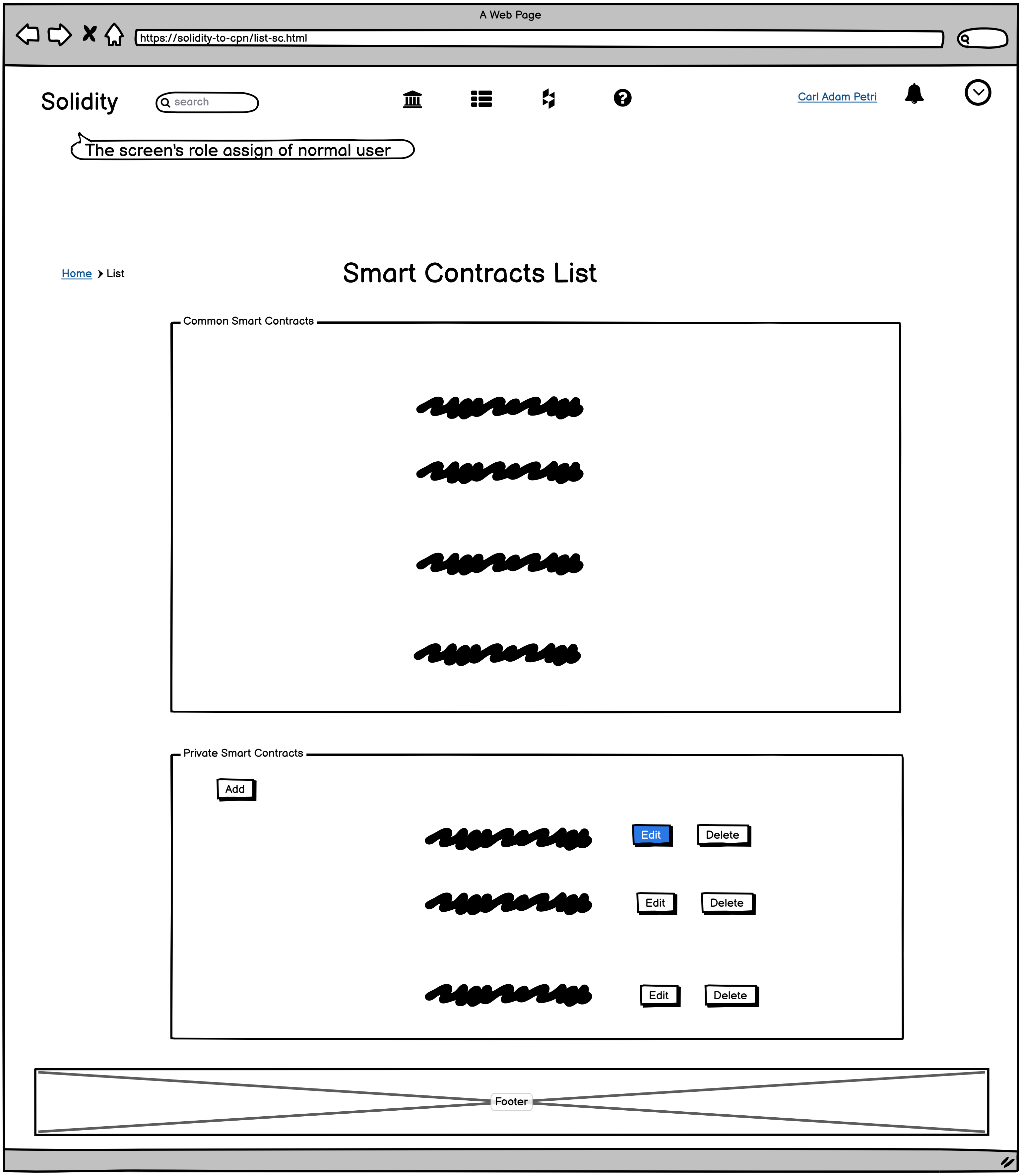
Description

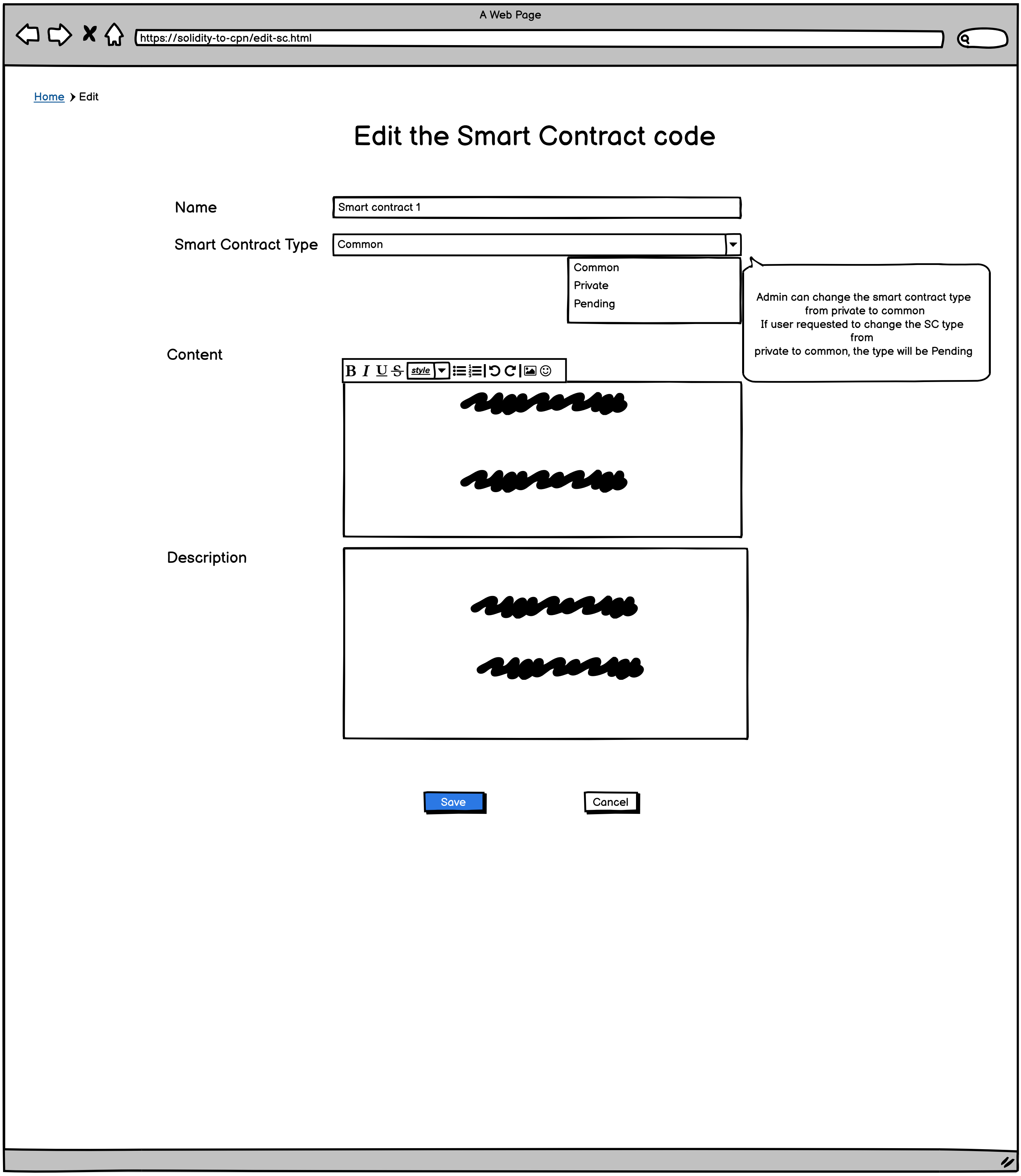


The screen's role assign of Admin

Smart Contract List

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


A Web Page
https://solidity-to-cpn/list-sc.html
Solidity
search
Carl Adam Petri
The screen's role assign of normal user
Home
List
Smart Contracts List
Common Smart Contracts
Private Smart Contracts
Add
Edit
Delete
Edit
Delete
Edit
Delete
Footer



Edit the Smart Contract code

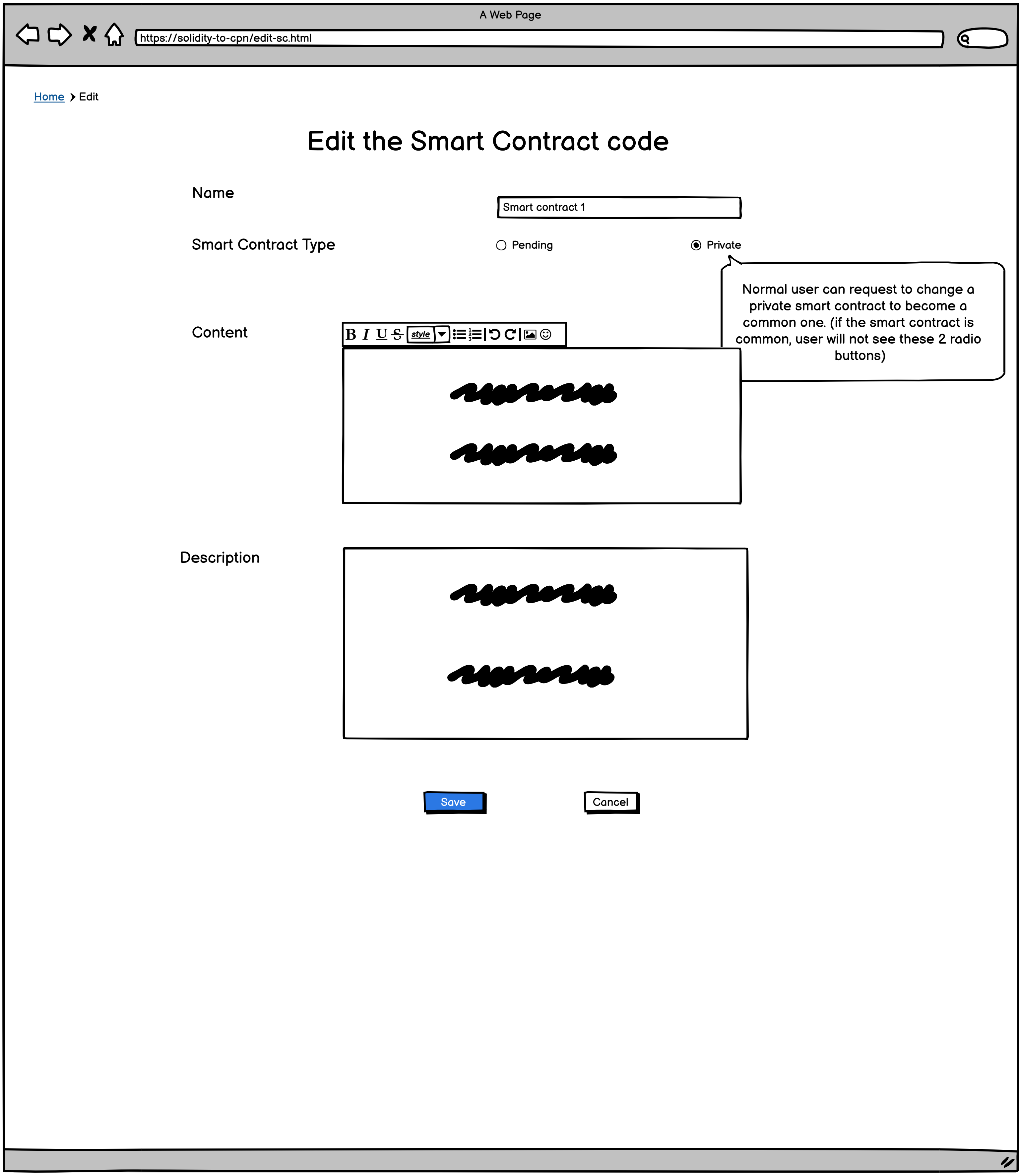
Name: Smart contract 1

Smart Contract Type: Common

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

Content

Description



A Web Page

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

Home > Edit

Edit the Smart Contract code

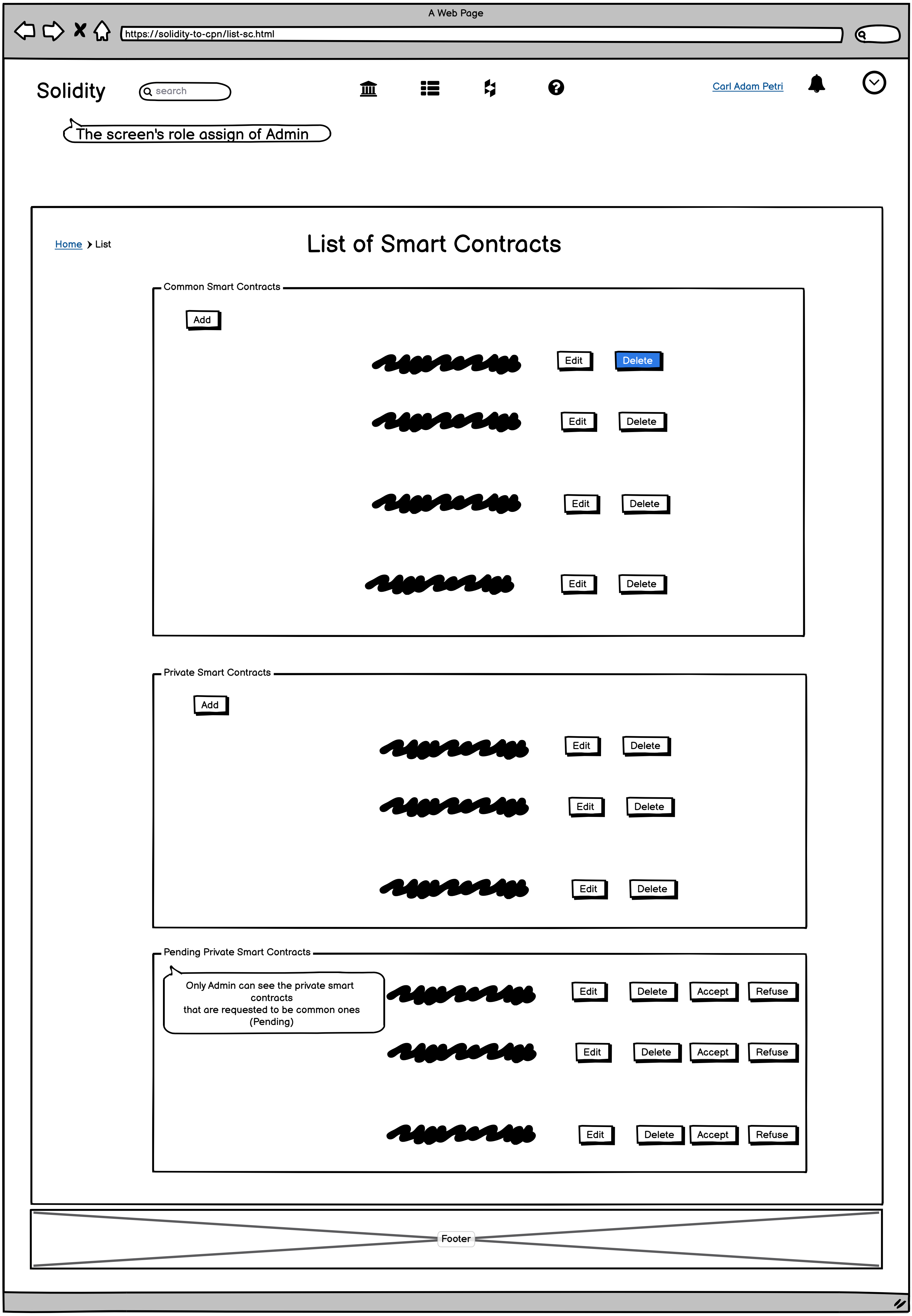
Name: Smart contract 1

Smart Contract Type: ○ Pending ● Private

Normal user can request to change a private smart contract to become a common one. (if the smart contract is common, user will not see these 2 radio buttons)

Content

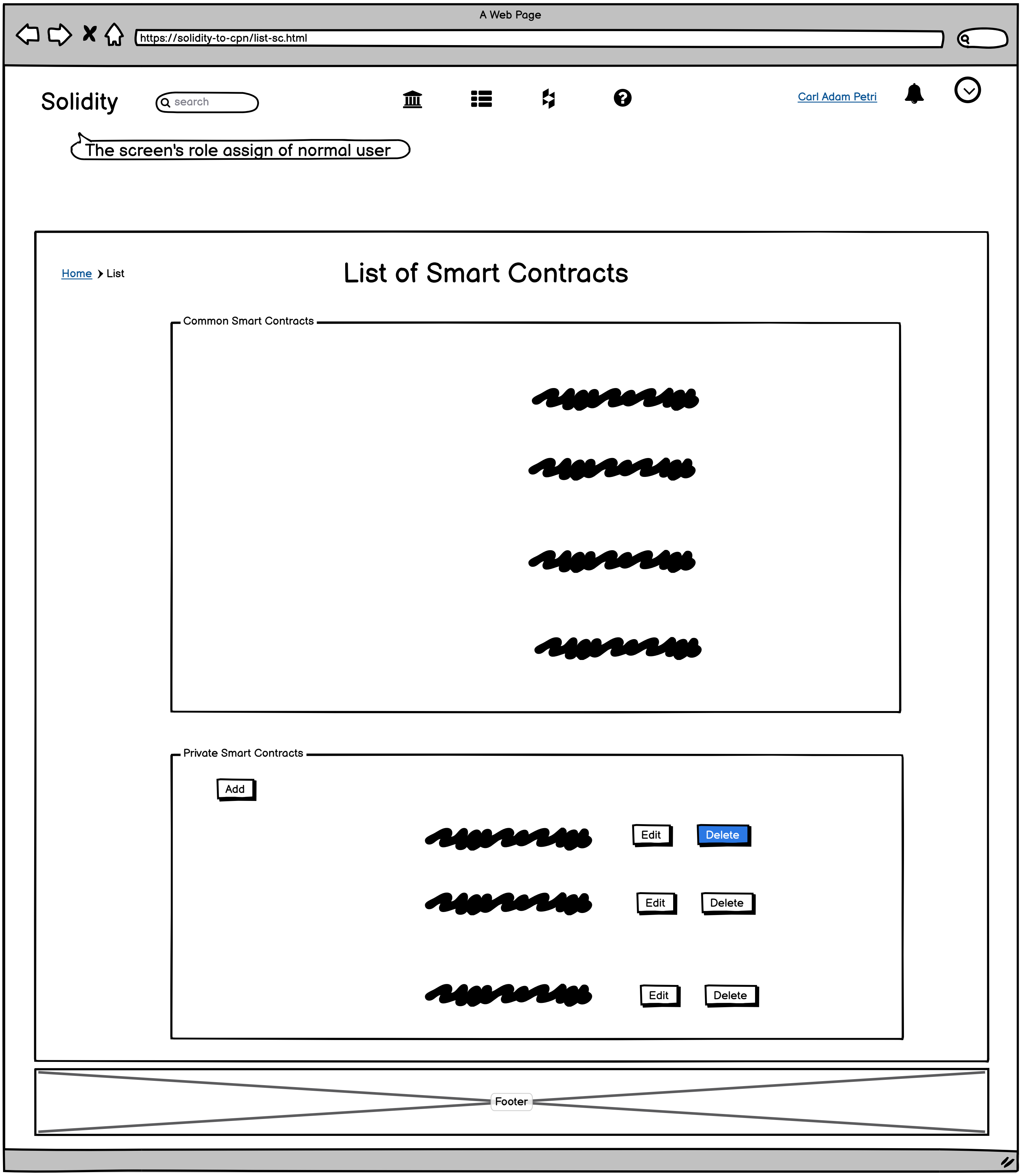
Description

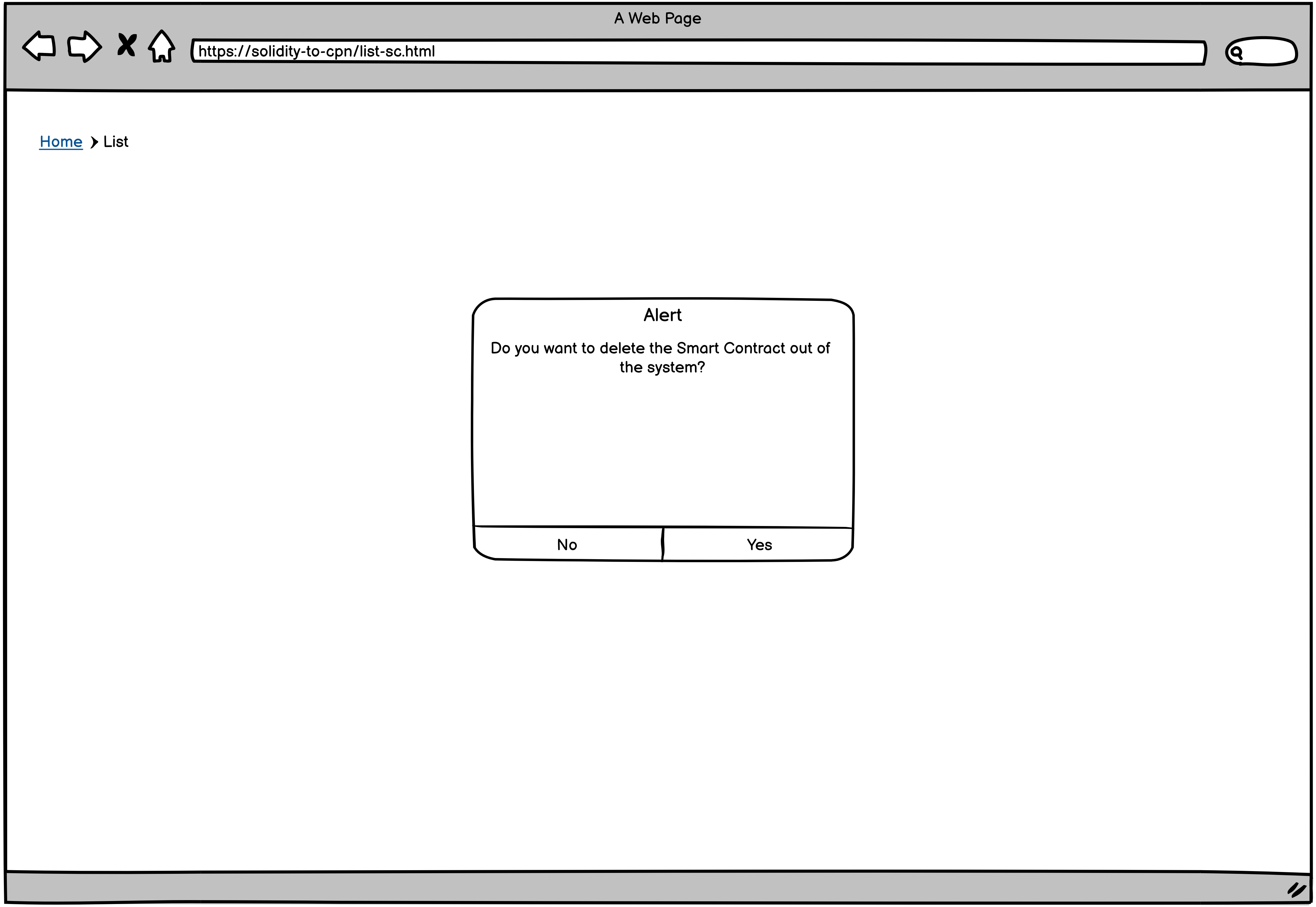


The screen's role assign of Admin

List of Smart Contracts

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

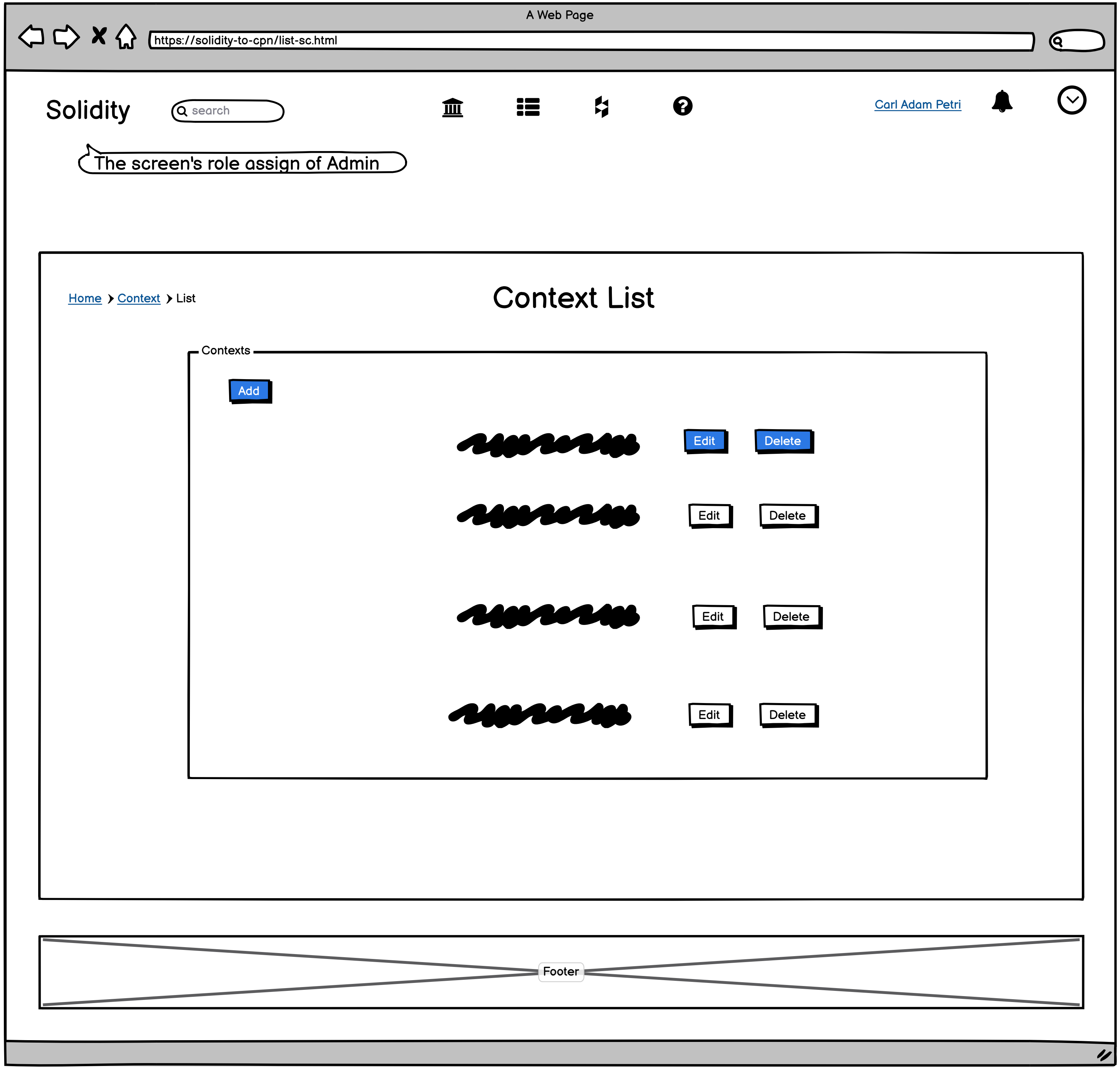

A Web Page
https://solidity-to-cpn/list-sc.html
Solidity
search
Carl Adam Petri
The screen's role assign of normal user
Home
List
List of Smart Contracts
Common Smart Contracts
Private Smart Contracts
Add
Edit
Delete
Edit
Delete
Edit
Delete
Footer



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

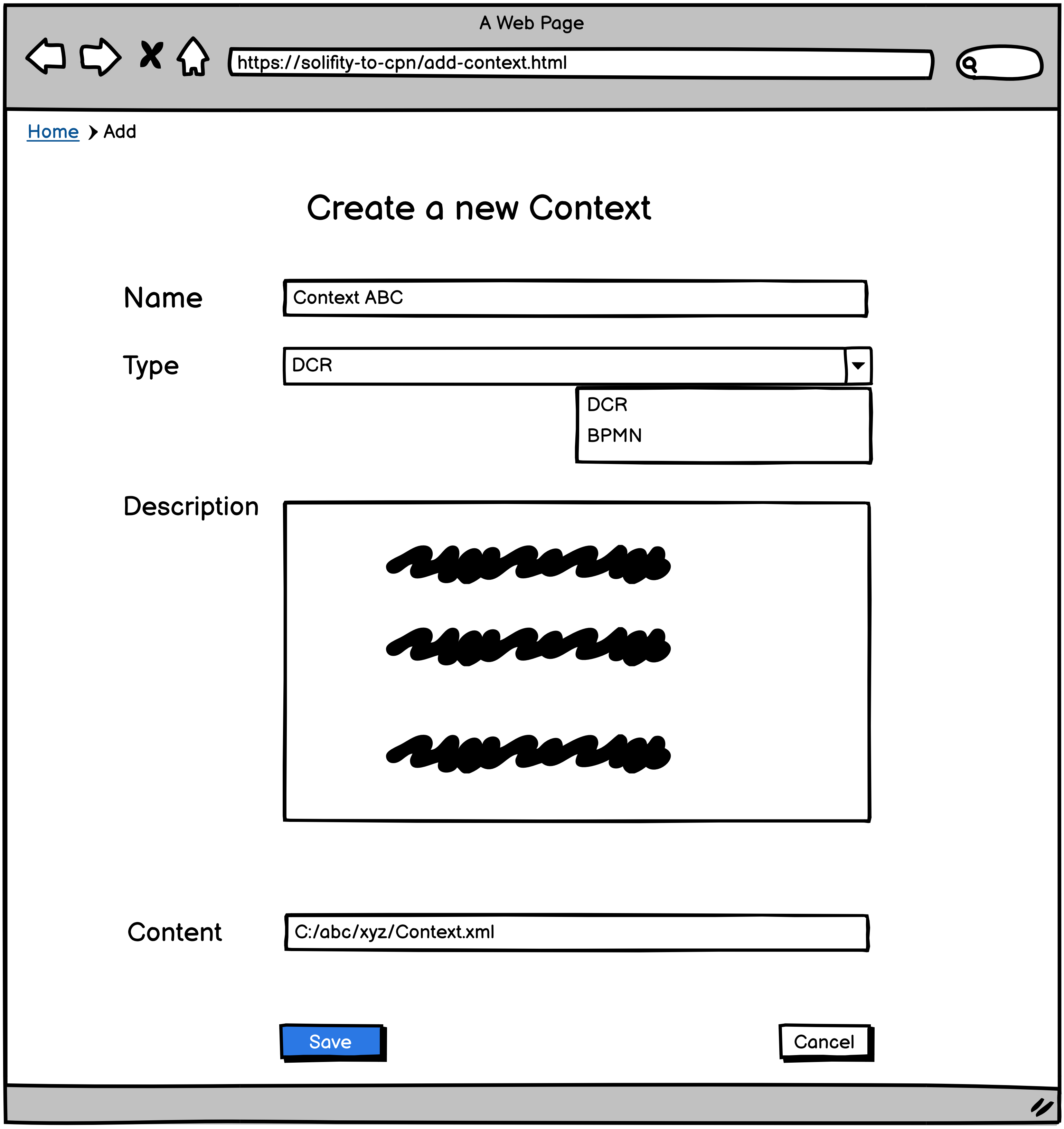
Alert

Do you want to delete the Smart Contract out of the system?



The screen's role assign of Admin

Context List



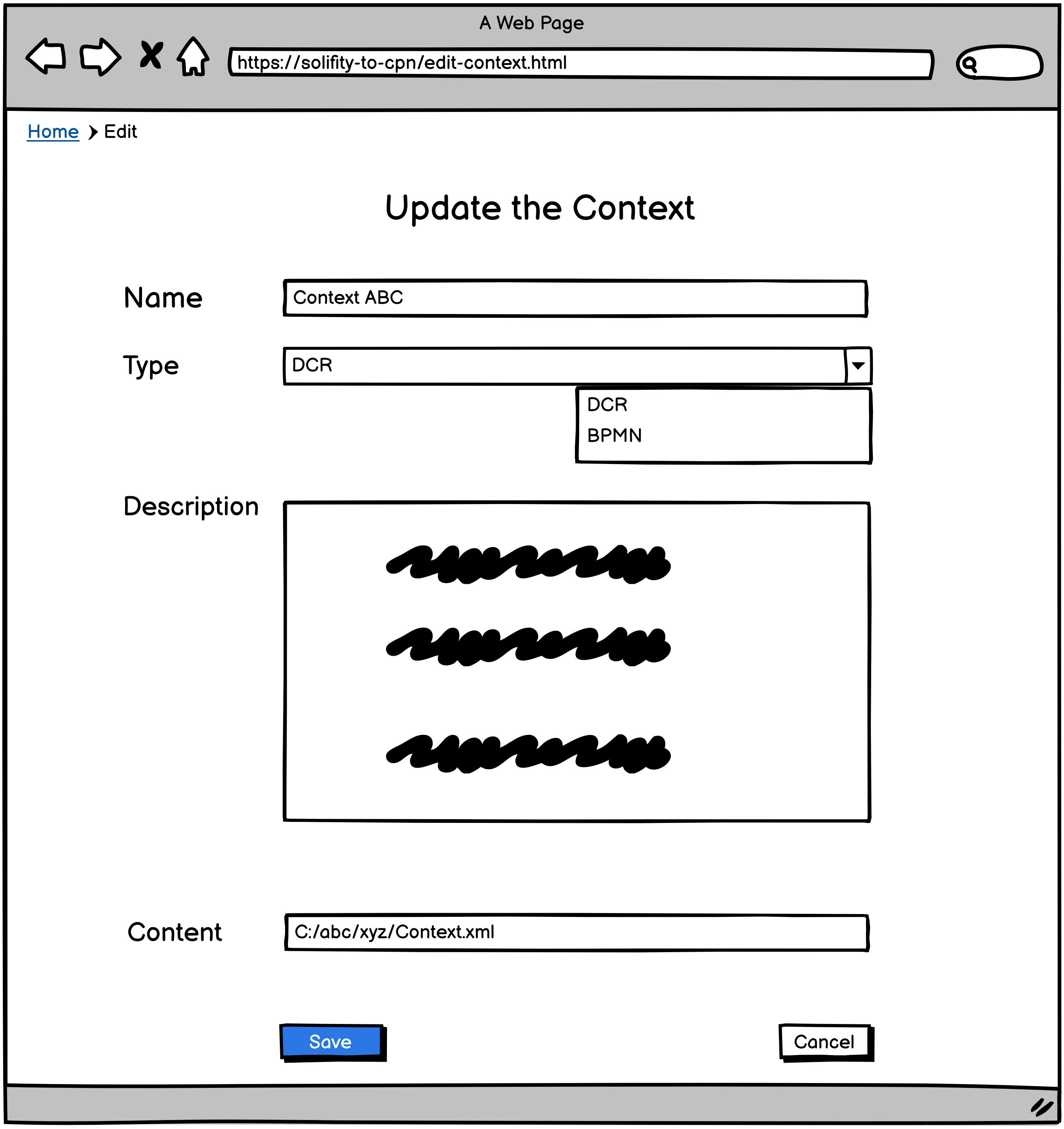
Create a new Context

Name: Context ABC

Type: DCR

Description

Content: C:/abc/xyz/Context.xml



A Web Page

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

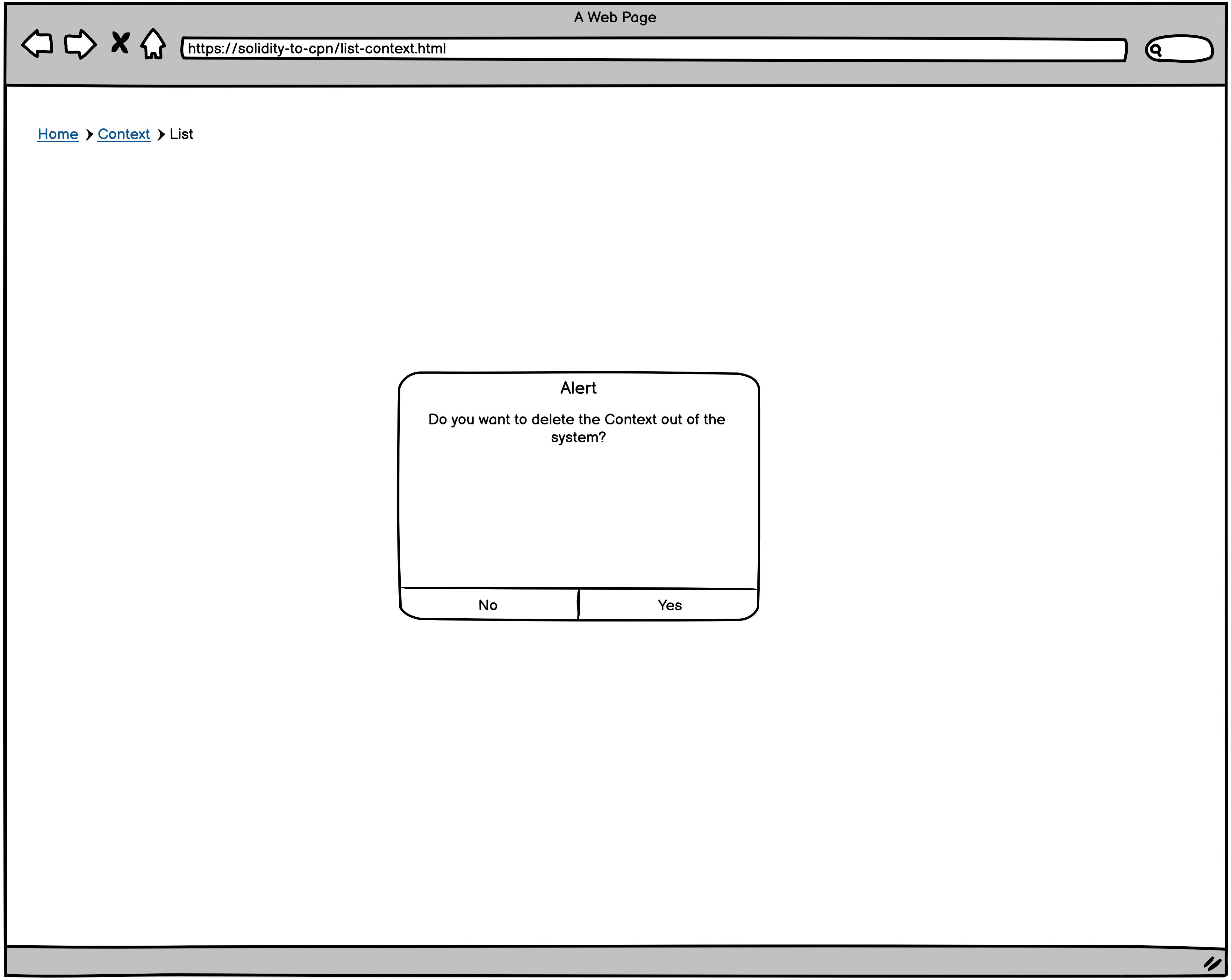
Home › Edit

Update the Context

Name: Context ABC

Type: DCR

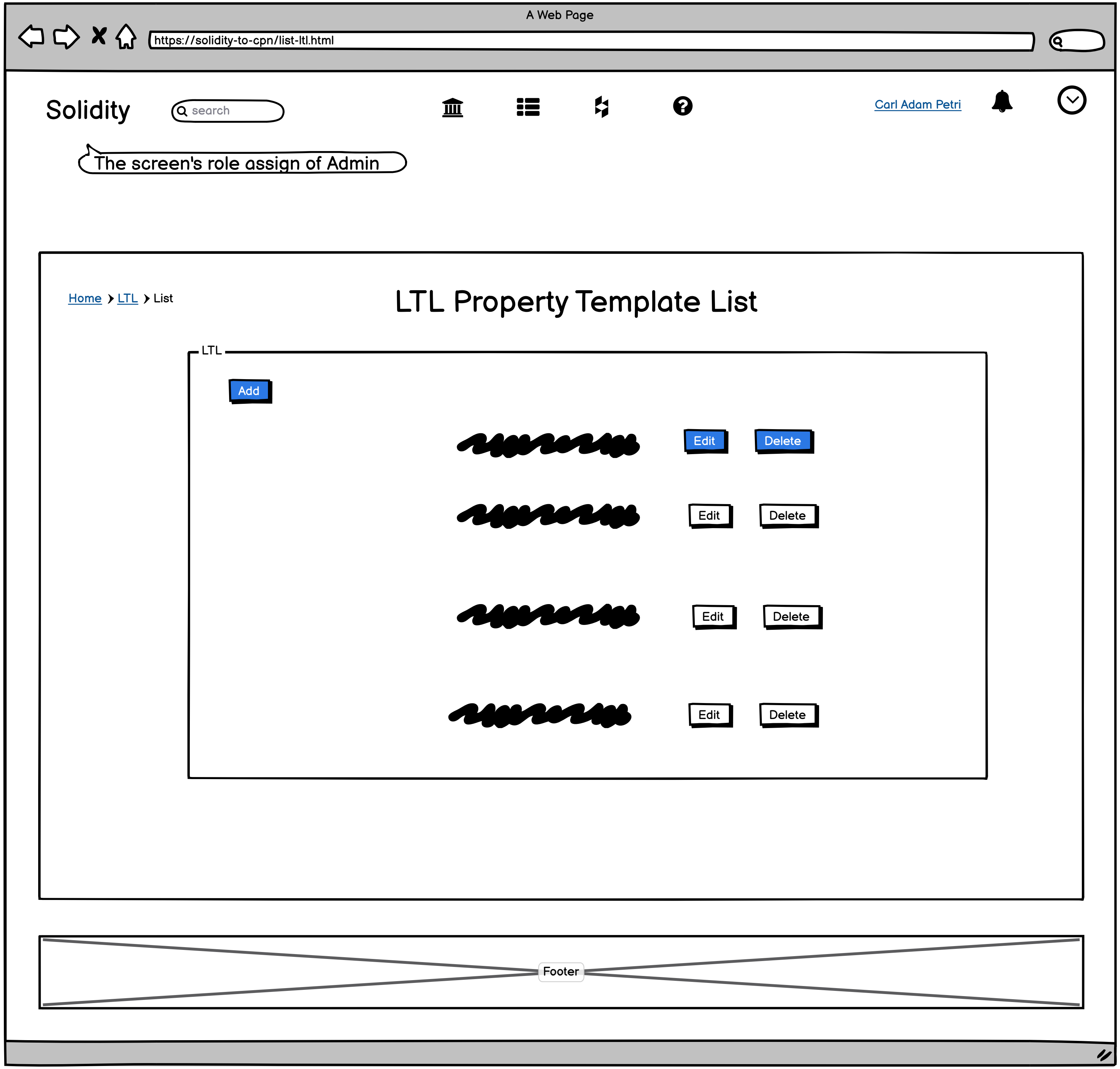
Content: C:/abc/xyz/Context.xml



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

Alert

Do you want to delete the Context out of the system?



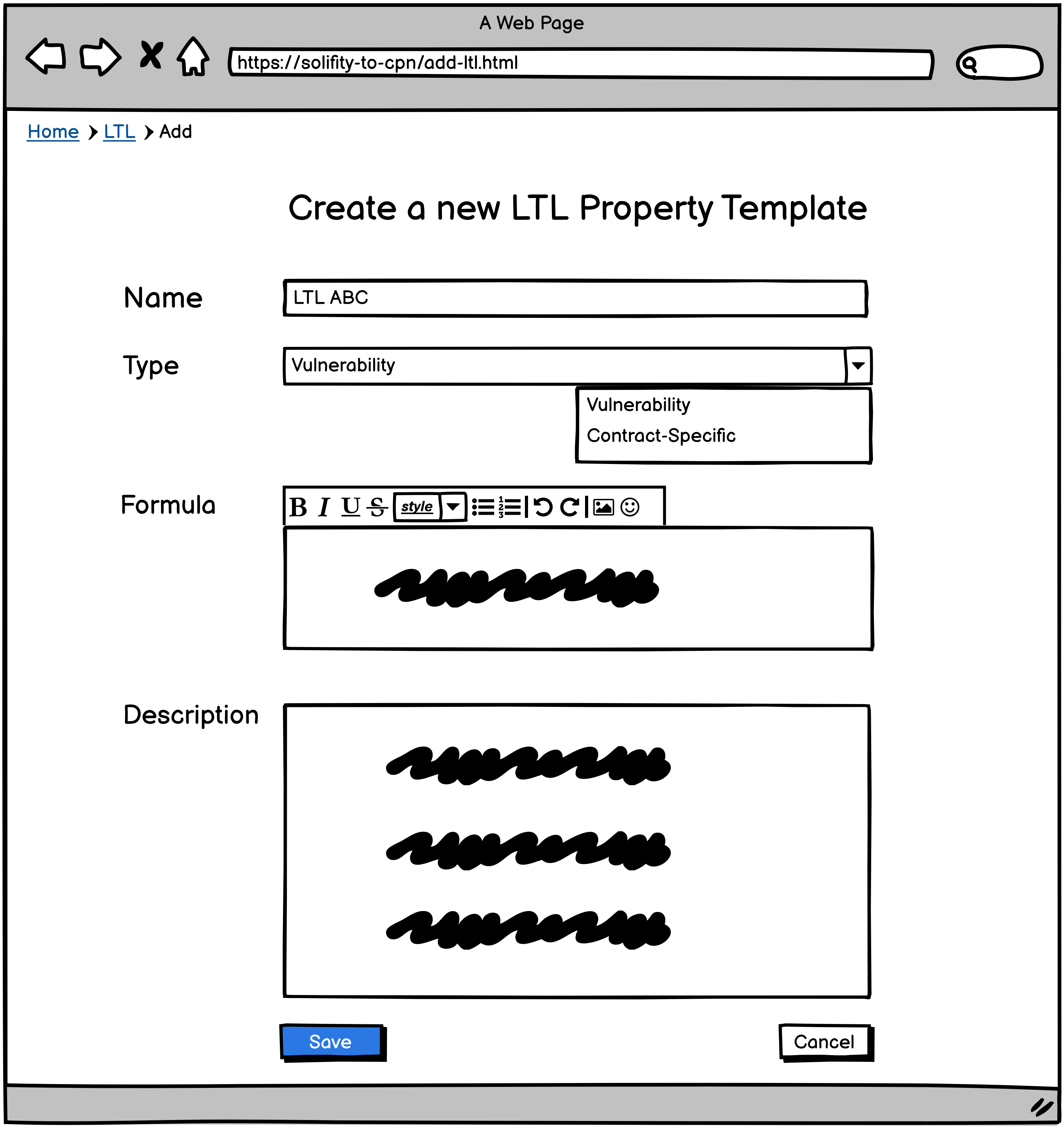
A Web Page

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

The screen's role assign of Admin

Home > LTL > List

LTL Property Template List



A Web Page

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

Home › LTL › Add

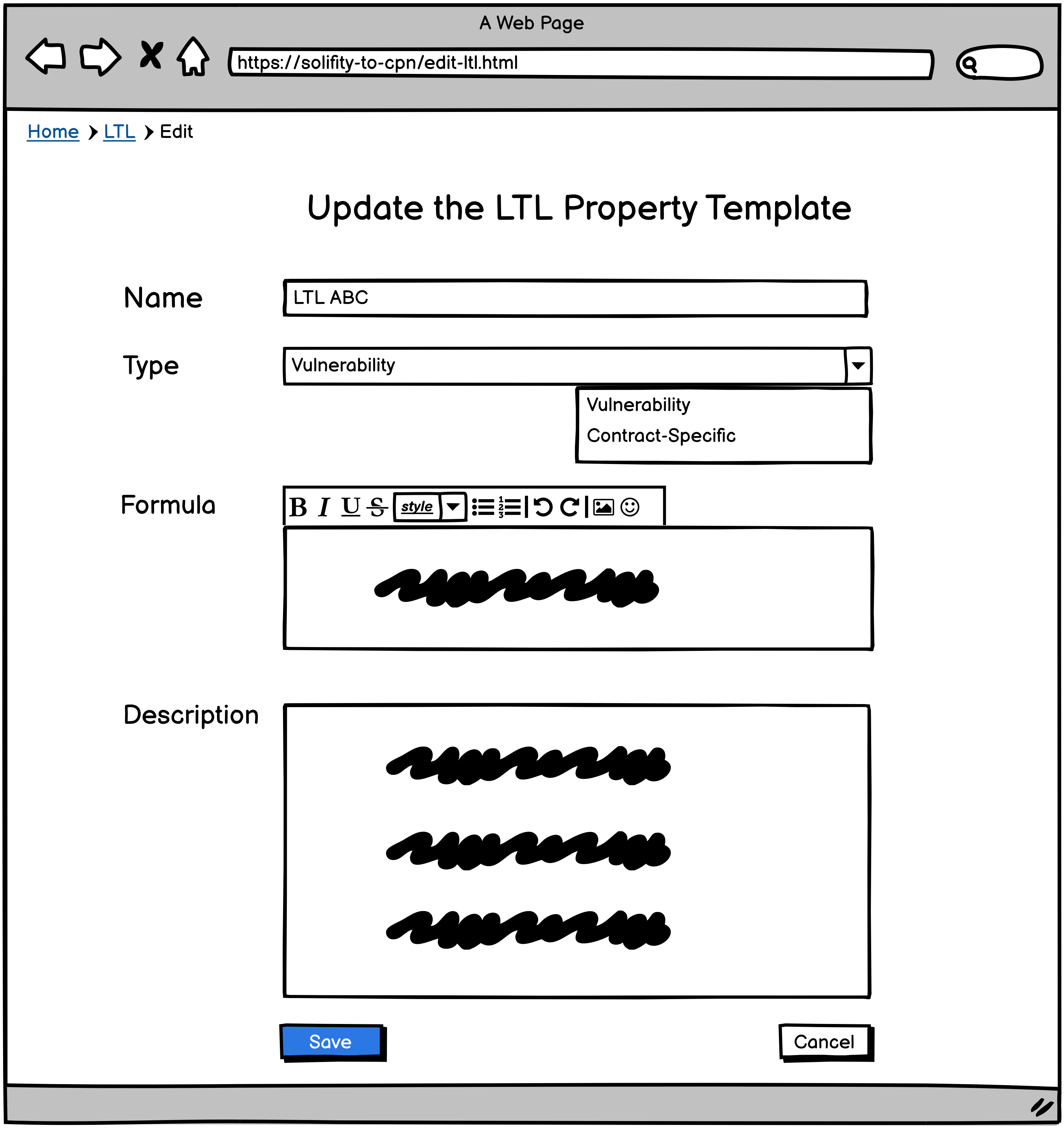
Create a new LTL Property Template

Name: LTL ABC

Type: Vulnerability

Formula

Description



A Web Page

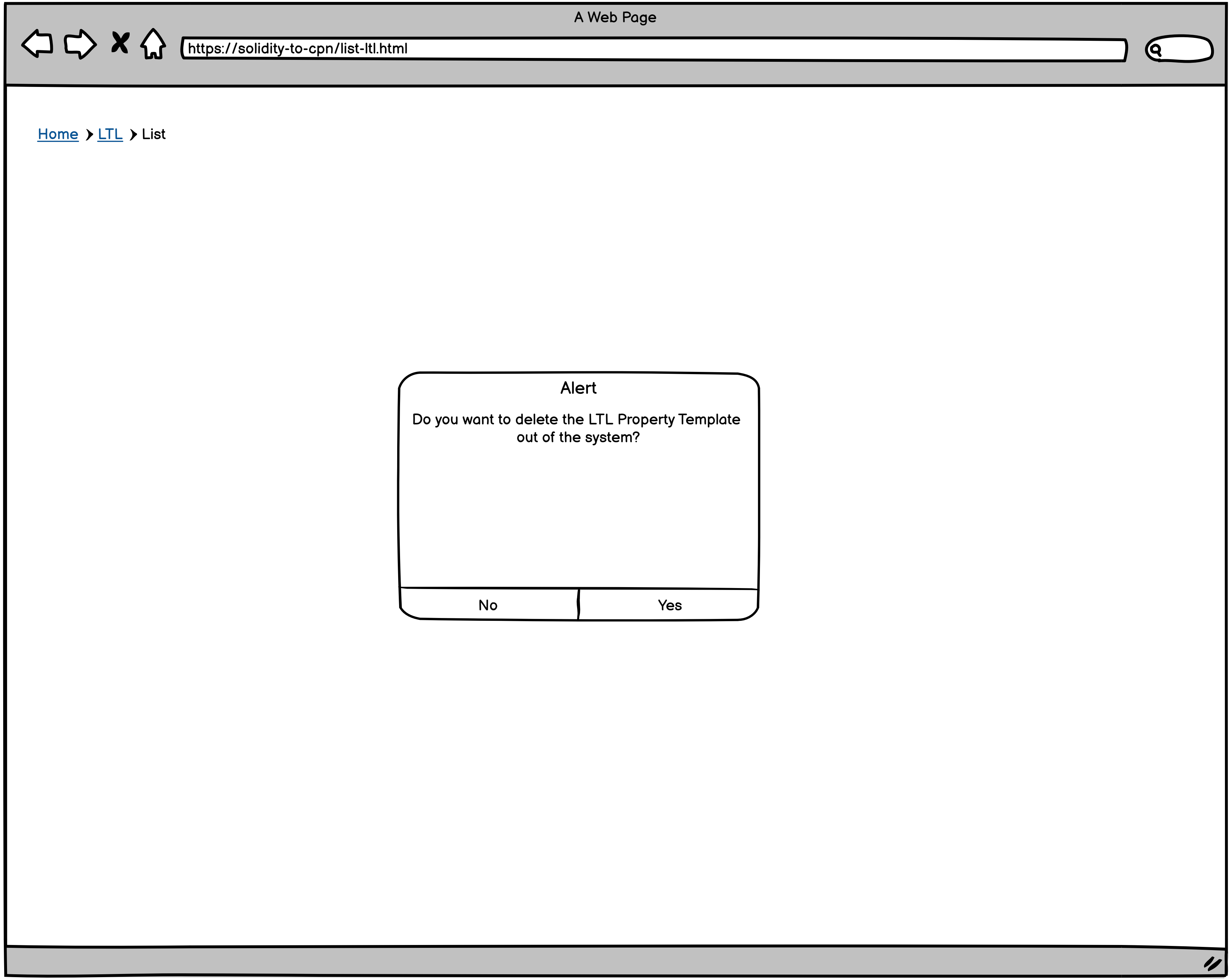
https://solifity-to-cpn/edit-ltl.html

Home › LTL › Edit

Update the LTL Property Template

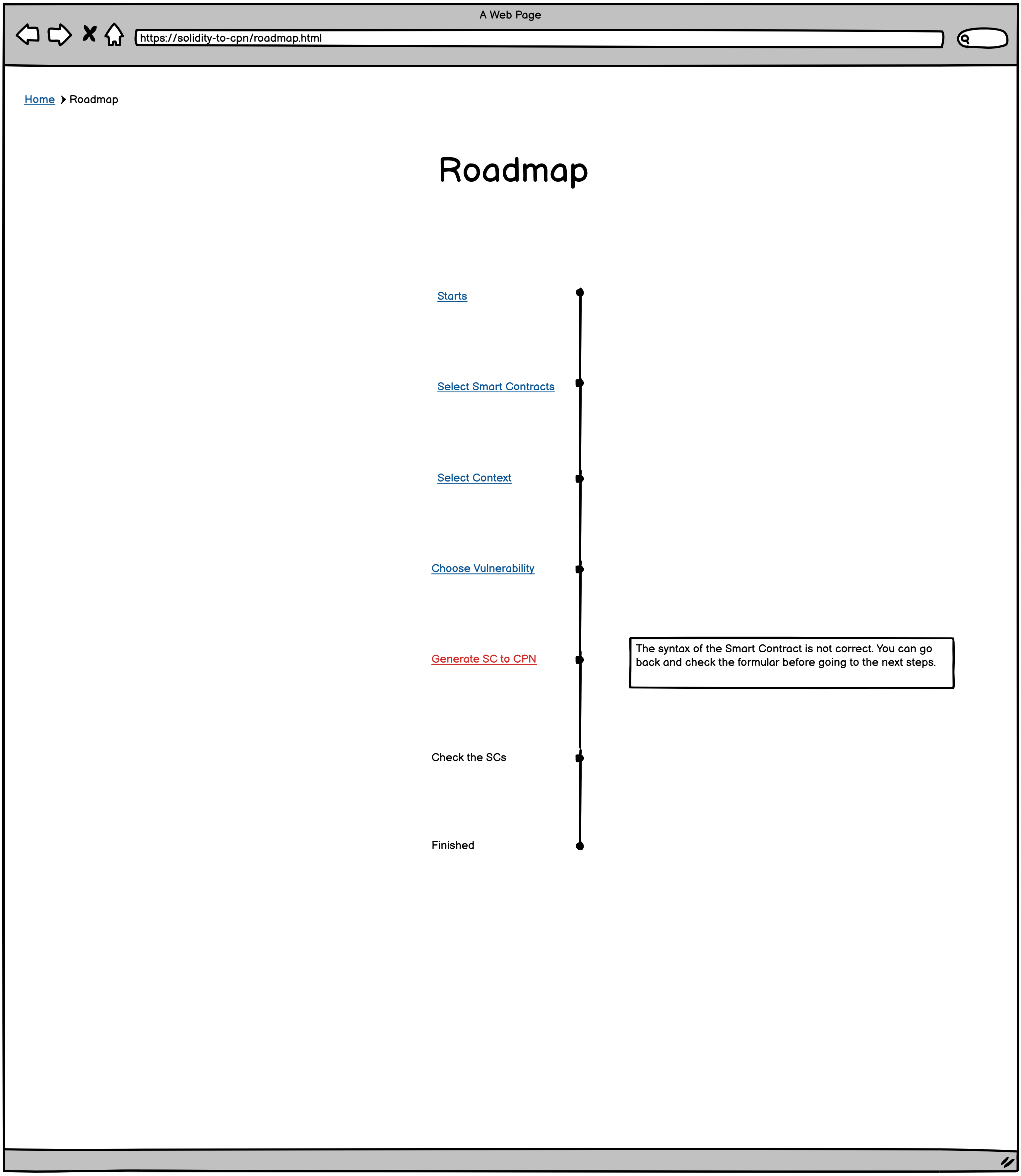
Name: LTL ABC

Type: Vulnerability



Alert

Do you want to delete the LTL Property Template out of the system?



Roadmap

The syntax of the Smart Contract is not correct. You can go back and check the formular before going to the next steps.