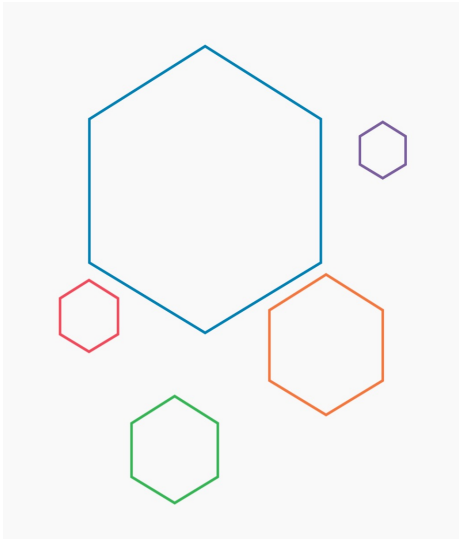




1



# SolidityCPN Home

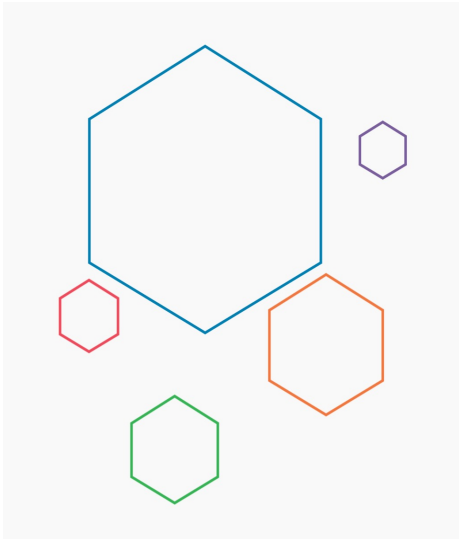
Check properties and vulnerabilities of the smart contracts

Check Smart Contracts



- Smart Contract
- Context
- LTL Template

1



# SolidityCPN Home

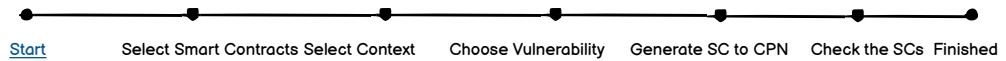
Check properties and vulnerabilities of the smart contracts

Check Smart Contracts



## Solidity

Roadmap



## 2

## List of Checked Transactions

Checked Information

#	Batch Name	Checked Date	Description
1	Check reentrancy	09/10/2021	
2	Chek Self-d		
3	Check Out d		
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](#)

Add Smart Contracts

Back

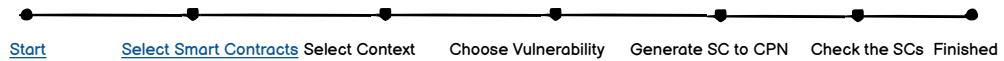
Next





## Solidity

Roadmap



## 2

## List of Checked Transactions

Checked Information

#	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	
...	...		

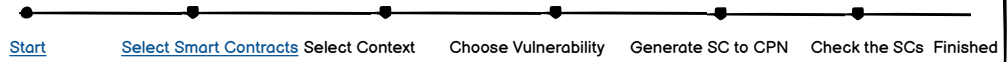
Add Smart Contracts

Back



Roadmap

Solidity



4

## Select Smart Contracts

Common Smart Contracts

#	Smart Contract Name	
1	blindAuction	<input checked="" type="checkbox"/>
2	etherGame	
3	etherLotto	
...	...	

Private Smart Contracts

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

Add

Upload File

Back



> ...

5

You have chosen to open:

etherPropose.sol (200kb)

**What should Browser do with this file?**

☐ Open with Browser

☐ Open with Document Viewer(default) ▼

☒ Save File

☐ Do this automaticly for files like this from now on

Cancel

OK

6

A Web Page

X

https://solify-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

B

I

U

style

Save

Cancel



Roadmap

Solidity

Progress bar with steps: Start, Select Smart Contracts, Select Context, Choose Vulnerability, Generate SC to CPN, Check the SCs, Finished



# 4

## 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.

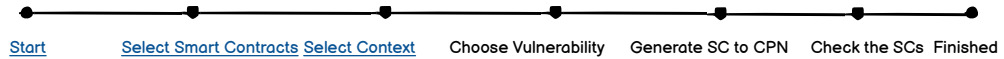
Add

Upload File

Back

## Solidity

Roadmap



7

## Context of the Smart Contract

Name

- Medicine
- Game
- ...
- Lotto

Type

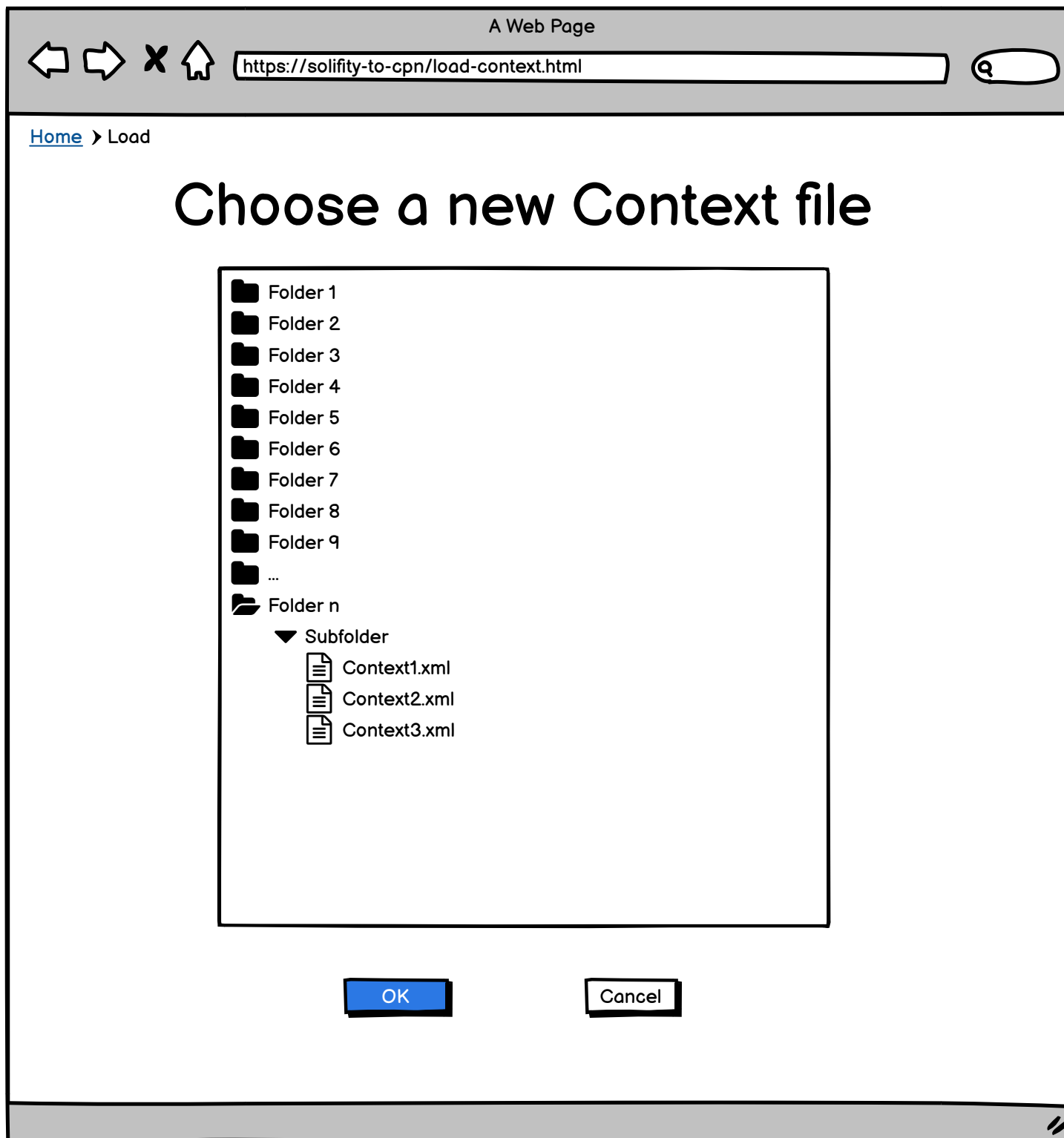
Description

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

Footer

8





[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

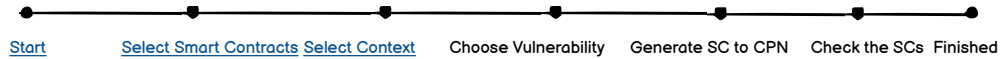
Save

Cancel



## Solidity

Roadmap



## Context of the Smart Contract

7

Name

- Medicine

- Game

- ...

- Lotto

Type

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

Add

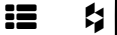
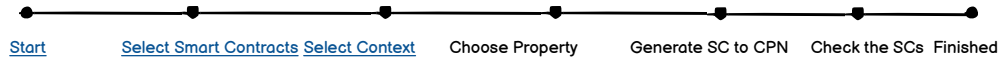
Upload a Context file

Back

Footer

## Solidity

Roadmap



# Choose functions for unfolding

10

SC

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

Unfold

Back

Next

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

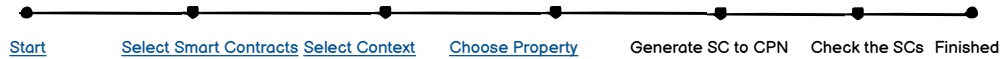
If users do not choose any functions and click Next button, the system will move to the next step without unfolding and the unfolding process will be implemented when the tool LTLprop read the LTL formula and know which functions need to be unfolded

Footer



Solidity

Roadmap



11

## 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

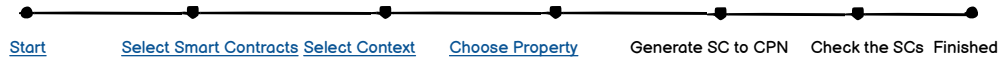
Check a General Vulnerability

Back



Solidity

Roadmap



## Contract-Specific Property Setting - Choose Types

# 12

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.

Template

Non-template

Back

Footer



[Back to home](#)

13

## Contract-Specific Property Template - Setting

Name

Mutual exclusion

Template

Template 1

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

Formula

$(GF\{ \text{variable 1} \} \wedge GF\{ \text{variable 2} \}) \Rightarrow G(\{ \text{function 3} \} \Rightarrow F\{ \text{function 4} \})$

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](#)

Add

Back

14

A Web Page

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	<input checked="" type="checkbox"/>
2	GV2	<input type="checkbox"/>
3	GV3	<input type="checkbox"/>
4	GV4	<input type="checkbox"/>
...		

Save

Cancel

15

A Web Page

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

Q

[Back to home](#)

Select elements of the smart contract

Argument

#	Arguments	Selected	All []
1	Arg1	<input checked="" type="checkbox"/>	
2	Arg2	<input type="checkbox"/>	
3	Arg3	<input type="checkbox"/>	
4	Arg4	<input type="checkbox"/>	
...			

Save

Cancel

16

A Web Page

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

[Back to home](#)

Select elements of the smart contract

Function

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

Save

Cancel

17

A Web Page

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

[Back to home](#)

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	<input checked="" type="checkbox"/>	
...				

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

Save

Cancel

[Back to home](#)

# 13 Contract-Specific Property Template - Setting

Name

Mutual exclusion

Template

Template 1

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

Formula

$$(GF\{ \text{variable 1} \} \wedge GF\{ \text{variable 2} \}) \Rightarrow G(\{ \text{function 3} \} \Rightarrow F\{ \text{function 4} \})$$

Alert

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

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}](#)

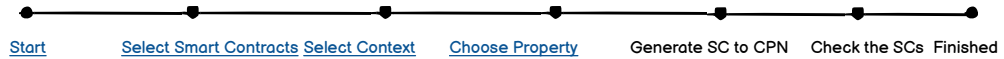
Add

Back



Solidity

Roadmap



## Contract-Specific Property Setting - Choose Types

12

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.

Footer



## Solidity

Roadmap



# Contract-Specific Property Setting - Non Template

18

Name

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

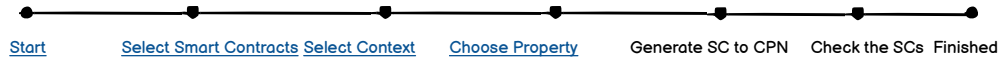
No other [function 1](#) orders are accepted between the [function 2](#) of the amount due and the [function 3](#)





Solidity

Roadmap



# 11

## 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

Solidity

Roadmap

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



## General Vulnerability Setting

19

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.

Add

Back

Footer

Solidity

Roadmap

[Start](#)

[Select Smart Contracts](#)

[Select Context](#)

[Choose Property](#)

Generate SC to CPN

Check the SCs



## General Vulnerability Setting

19

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.

No

Yes

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.

Add

Back

Footer



[Back to home](#)

## Initial Marking Setting

20

Number of users

5

Users balance

10

Sender value

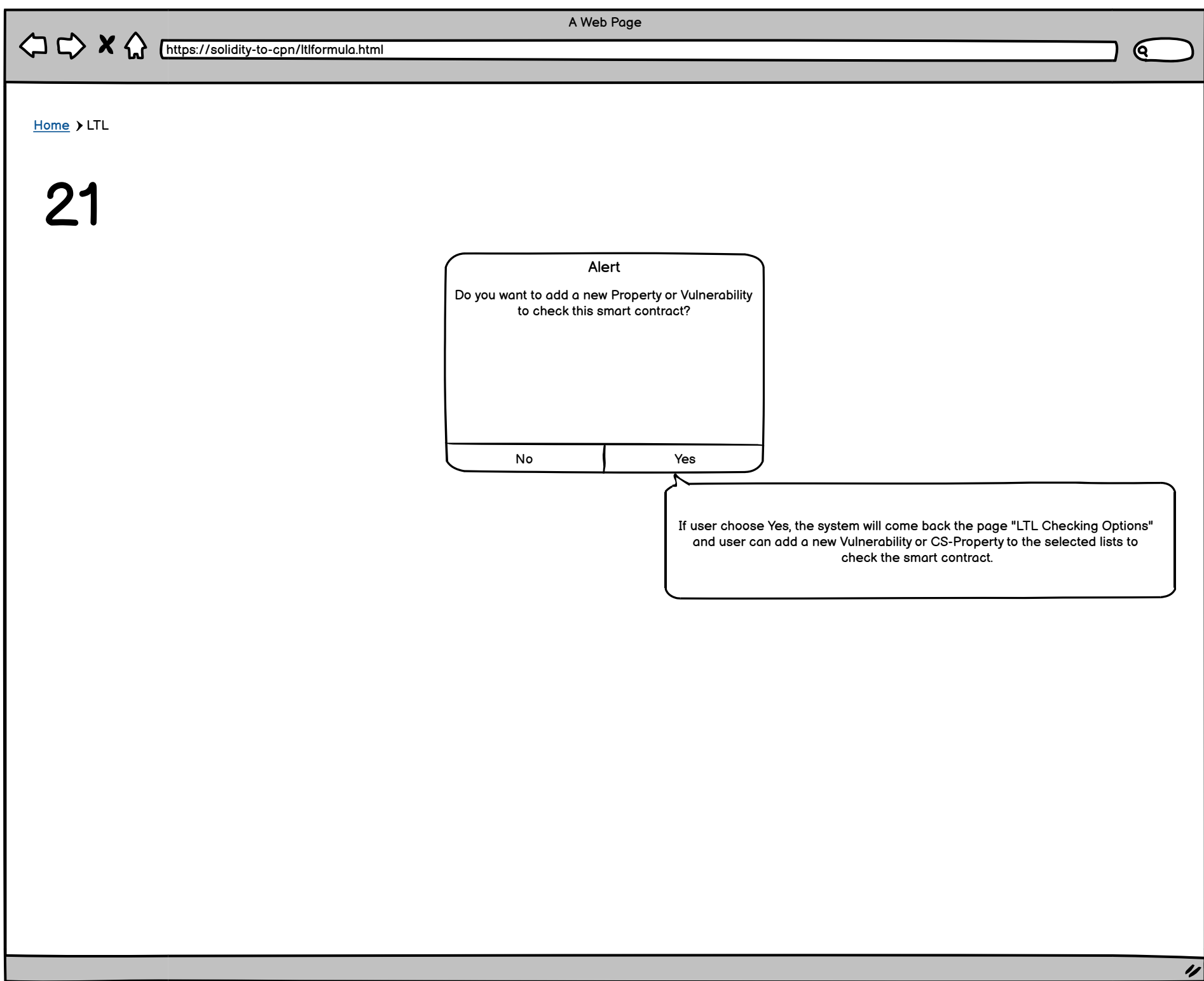
2

Other parameters

Sau này có thể user sẽ đẩy nội dung như XML, JSON vào đây và tool sẽ đọc ra để lấy thông tin

Add

Back





Solidity

Roadmap

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

22

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	..	
...		

Generate

Add new session

The smart contract is generating...

Solidity

Roadmap

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

23

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	..	
...		

Check

The generating process completed successfully

Download

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





> ...

24

You have chosen to open:

SmartContract.cpn (300kb)

What should Browser do with this file?

☐ Open with Browser

☐ Open with 

Document Viewer(default) ▾

☒ Save File

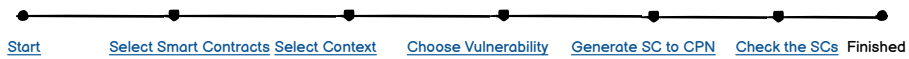
☐ Do this automaticly for files like this from now on

Cancel

OK

Solidity

Roadmap



23

## 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	..	
...		

Check

Download

The smart contract is checking...



Footer

Solidity

Roadmap



# 23

## 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	..	
...		

Check

Alert

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

Download

No

Yes

Footer

Solidity

Roadmap

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

23

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	..	
...		

Check

Download

The checking process completed successfully

Solidity

Roadmap

Start    Select Smart Contracts    Select Context    Choose Vulnerability    Generate SC to CPN    Check the SCs    Finished



## Checking Smart Contracts

23

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	..	
...		

Re-check

Results

Download



The screen's role assign of Admin

24

[Home](#) > List

Smart Contracts Lists

Common Smart Contracts

Add



Edit

Delete



Edit

Delete



Edit

Delete



Edit

Delete

Private Smart Contracts

Add



Edit

Delete



Edit

Delete



Edit

Delete

Pending Private Smart Contracts

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



Edit

Delete

Accept

Refuse



Edit

Delete

Accept

Refuse



Edit

Delete

Accept

Refuse



[Home](#) › List

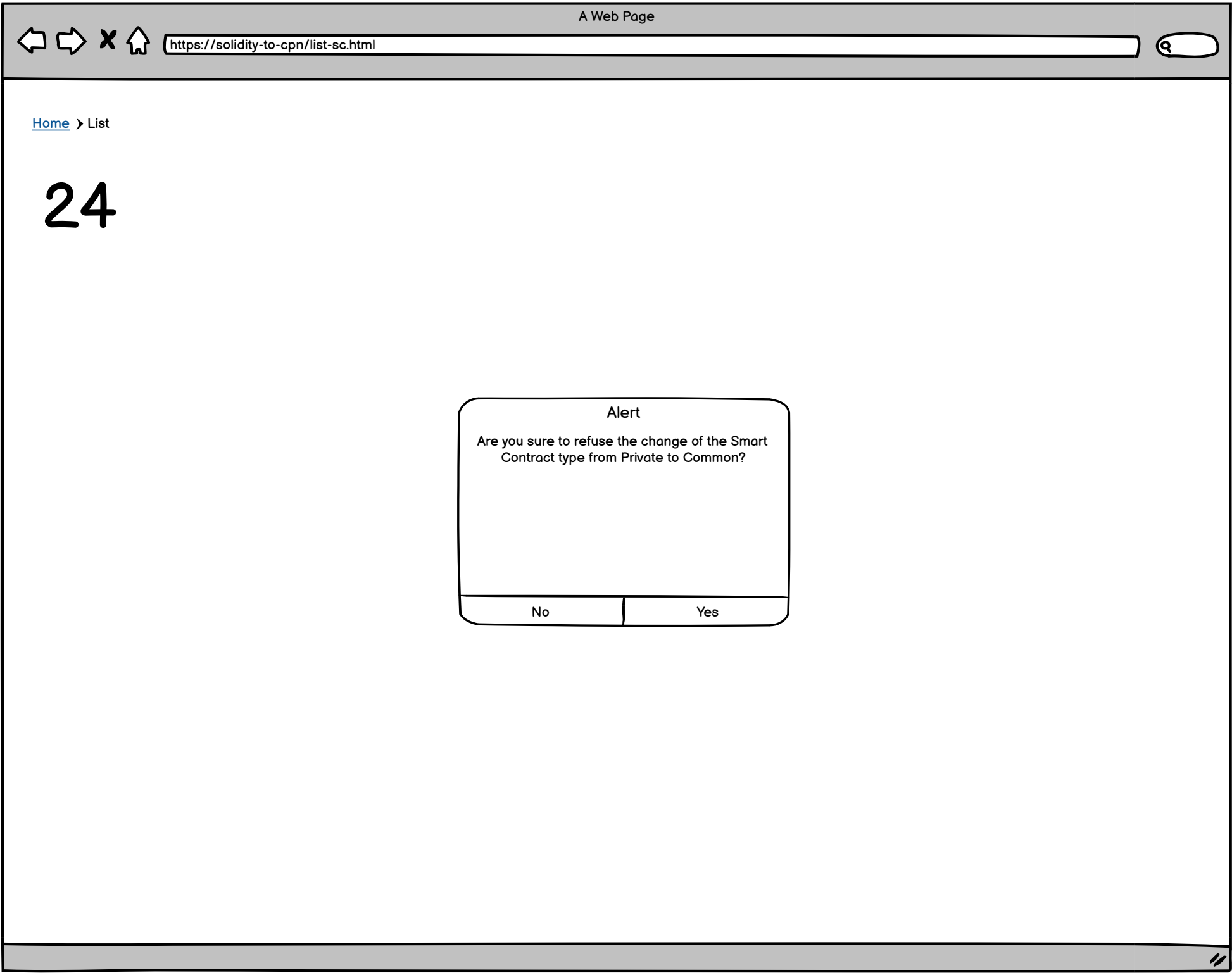
24

Alert

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

No

Yes





The screen's role assign of Admin

[Home](#) > List

24

# Smart Contracts List

## Common Smart Contracts

Add



Edit

Delete



Edit

Delete



Edit

Delete



Edit

Delete

## Private Smart Contracts

Add



Edit

Delete



Edit

Delete



Edit

Delete

## Pending Private Smart Contracts

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



Edit

Delete

Accept

Refuse



Edit

Delete

Accept

Refuse



Edit

Delete

Accept

Refuse

The screen's role assign of normal user

[Home](#) > List

24

# Smart Contract List

## Common Smart Contracts

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



## Private Smart Contracts

Add



Edit

Delete



Edit

Delete



Edit

Delete

25

A Web Page

X

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

Q

[Home](#) > Add

Create a new Smart Contract code

Name


Smart contract 1



Smart Contract Type

Common

Common

Private

B I U  style

Save

Cancel

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

## Create a new Smart Contract code

### Smart contract 1

☐ Pending

Private

## Content

**B** *I* U  $\frac{S}{\text{ }}$  style ▼  $\frac{1}{2}$   $\frac{2}{3}$  | ↺ ↻ |  

~~XXXXXXXXXXXX~~

~~XXXXXXXXXXXX~~

~~XXXXXXXXXXXXXXXXXXXX~~

~~XXXXXXXXXXXXXXXXXXXX~~

Save

Cancel

The screen's role assign of Admin

[Home](#) > List

# Smart Contract List

24

## Common Smart Contracts

Add



Edit

Delete



Edit

Delete



Edit

Delete



Edit

Delete

## Private Smart Contracts

Add



Edit

Delete



Edit

Delete



Edit

Delete

## Pending Private Smart Contracts

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



Edit

Delete

Accept

Refuse



Edit

Delete

Accept

Refuse



Edit

Delete

Accept

Refuse

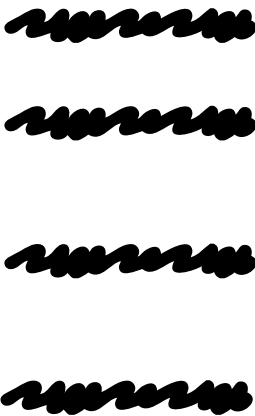
The screen's role assign of normal user

[Home](#) > List

# Smart Contracts List

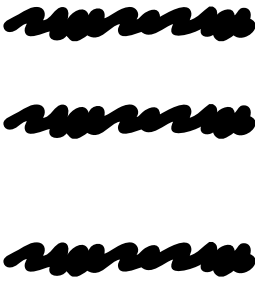
24

Common Smart Contracts



Private Smart Contracts

Add



Edit

Delete

Edit

Delete

Edit

Delete

Footer

[Home](#) > Edit

26

## Edit the Smart Contract code

Name

Smart Contract Type

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

Content

**B I U**

*[Redacted content]*

Description

*[Redacted content]*

Save

Cancel

[Home](#) > Edit

26

# Edit the Smart Contract code

Name

Smart Contract Type

☐ Pending ☒ Private

Content

Rich text editor toolbar: Bold, Italic, Underline, Style dropdown, Bulleted list, Numbered list, Indent, Outdent, Link, Unlink, Image, Smileys

Content area with two lines of placeholder text (scribbles)

Description

Description area with two lines of placeholder text (scribbles)

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)



The screen's role assign of Admin

[Home](#) > List

# List of Smart Contracts

24

## Common Smart Contracts

Add



Edit

Delete



Edit

Delete



Edit

Delete



Edit

Delete

## Private Smart Contracts

Add



Edit

Delete



Edit

Delete



Edit

Delete

## Pending Private Smart Contracts

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



Edit

Delete

Accept

Refuse



Edit

Delete

Accept

Refuse



Edit

Delete

Accept

Refuse



The screen's role assign of normal user

[Home](#) > List

## List of Smart Contracts

24

Common Smart Contracts

████████████████████

████████████████████

████████████████████

████████████████████

Private Smart Contracts

Add

████████████████████

Edit

Delete

████████████████████

Edit

Delete

████████████████████

Edit

Delete



[Home](#) › List

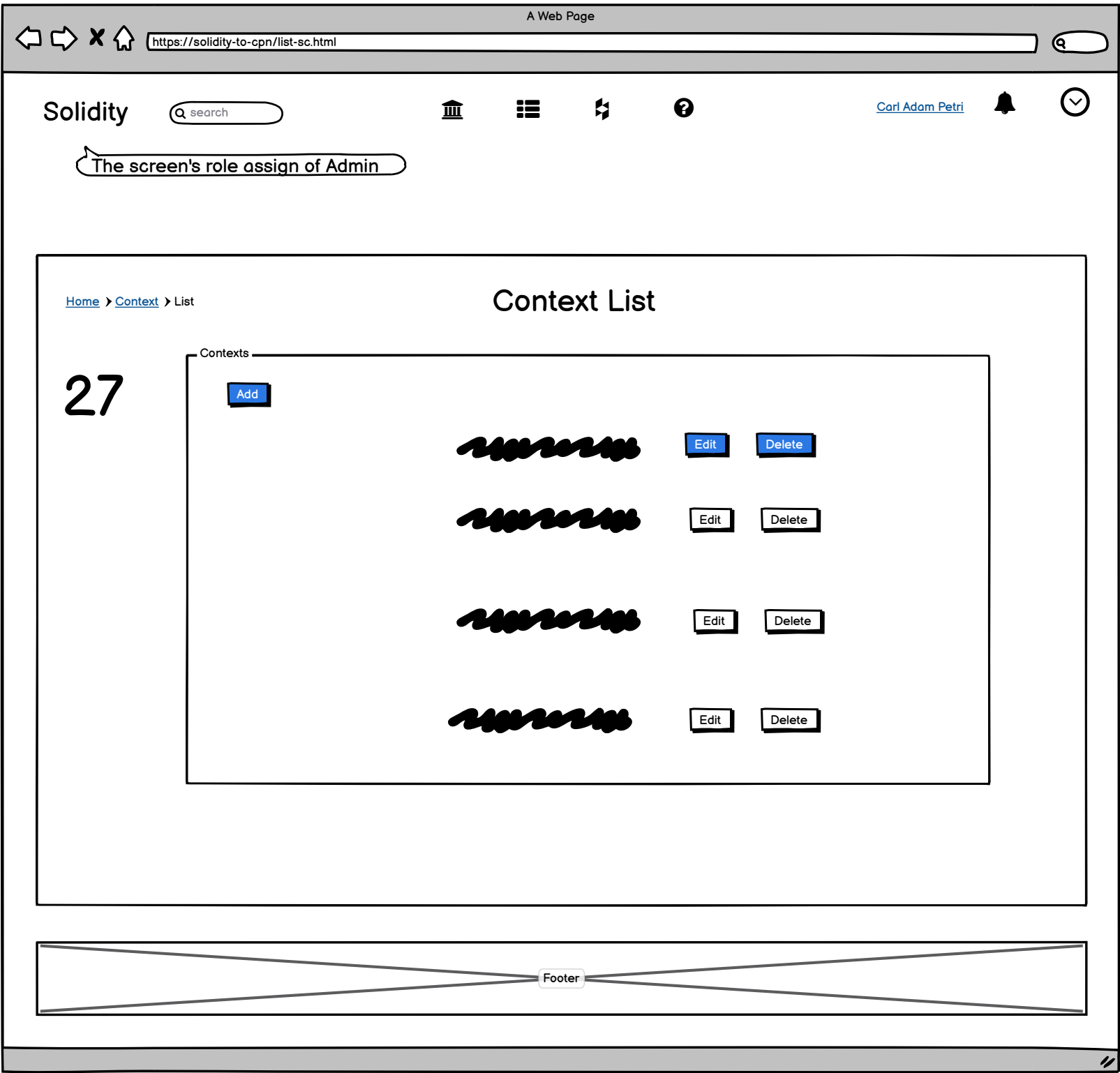
# 24

### Alert

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

No

Yes



28

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

29

A Web Page

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

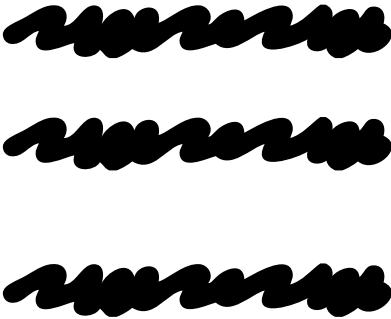
[Home](#) > Edit

## Update the Context

Name

Type

Description 



Content



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



[Home](#) > [Context](#) > List

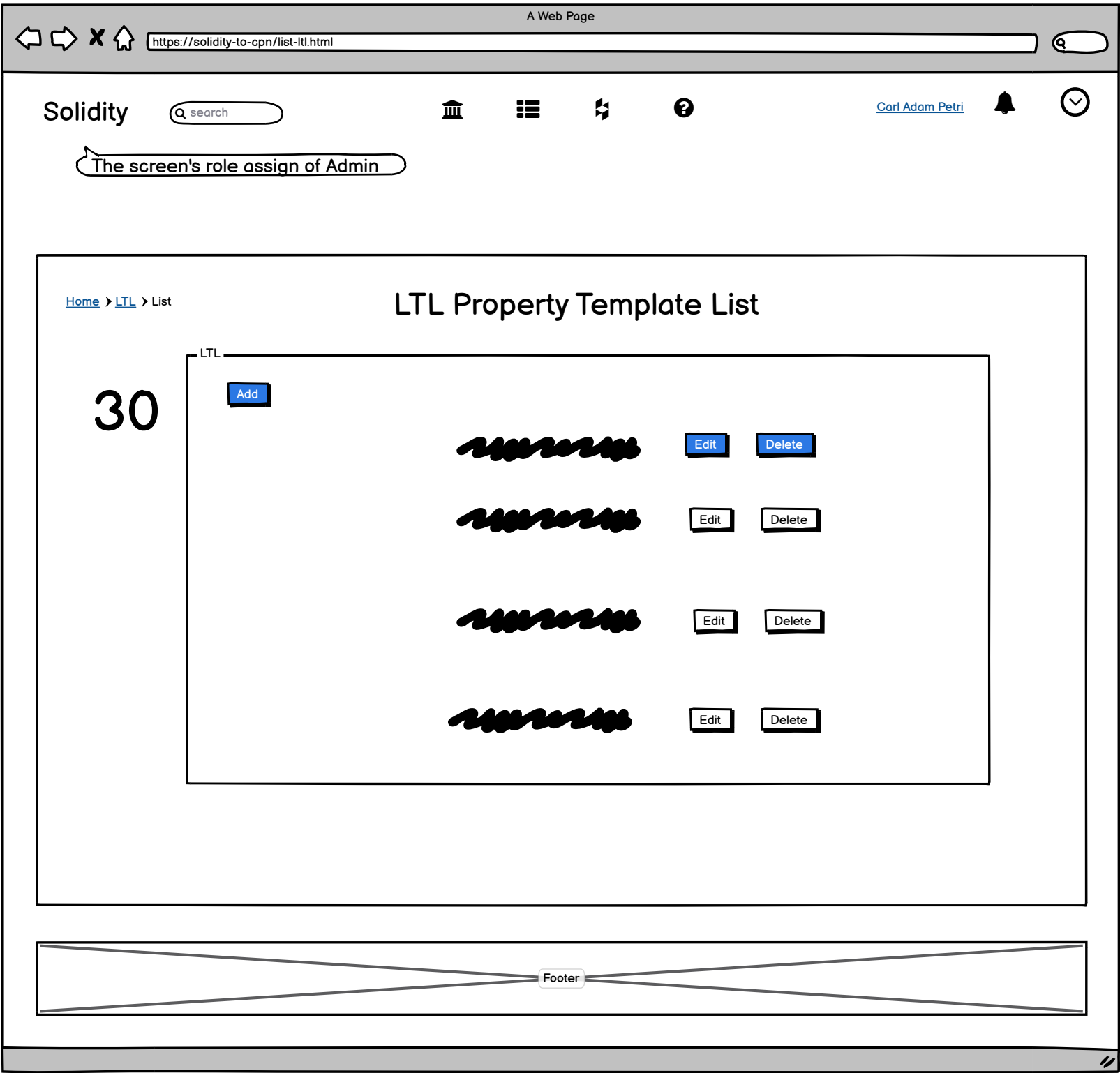
27

Alert

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

No

Yes





31

A Web Page

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

Home > LTL > Add


## Create a new LTL Property Template


Name

Type




Vulnerability  
Contract-Specific

Formula

**B I U** 



Description

32

A Web Page

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

Home > LTL > Edit

## Update the LTL Property Template

Name

Type

Formula

**B I U**

Description



[Home](#) > [LTL](#) > List

30

Alert

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

No

Yes



[Home](#) > Roadmap

33

# Roadmap

[Starts](#)

[Select Smart Contracts](#)

[Select Context](#)

[Choose Vulnerability](#)

[Generate SC to CPN](#)

Check the SCs

Finished

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