



# TORNADO.CASH


By Simon CHEREL & Enguerrand DECLERCQ





# Contents

## Topics to tackle

- 
1. Tornado's interface
  2. Tornado's contracts explanation
  3. Tornado's ZKP implementation
  4. Questions





# Deposit UI

 [Airdrop](#) [Minage ▼](#) [Voter](#) [Conformité](#) [Docs](#) [Gö](#) [Goerli](#)   [Réglages](#)

 Tornado.cash a été audité. Cependant, il s'agit d'un logiciel en phase d'expérimentation. Veuillez l'utiliser à vos propres risques. 

DéposerRetirer

Token

ETH

Montant ⓘ

0,1 ETH1 ETH10 ETH100 ETH

Déposer

eth-01.tornadocash.eth

Statistiques0.1 ETH

Niveau d'anonymat ⓘ

13107 dépôts équivalents

Dernier dépôt

13107. il y a une heure

13102. il y a 2 jours

13106. il y a 2 jours

13101. il y a 2 jours

13105. il y a 2 jours

13100. il y a 2 jours

13104. il y a 2 jours

13099. il y a 2 jours

13103. il y a 2 jours

13098. il y a 3 jours

Votre IP 192.40.57.234, Amsterdam, NL

Filtrer par

ETH

DAI

eDAI

USDC

USDT

WBTC

Dépensée

Non dépensée

Régulier

Encryptée

Temps passé ▼

Montant

Dépôts postérieurs

Hash de transaction

Statut

Récompenses ⓘ

1

# The deposit note

The screenshot shows the Tornado.cash web interface. A modal window titled "Votre note d'enregistrement privée" is open, displaying a long hexadecimal string: `tornado-eth-1-5-0x4599c0445e35d33315d34696716666c3037e424d34565941e29fd65d84047c7736b67d368d7d6dfe97593e022d870f9bc88313c99819e91fc4072b66f43e`. The modal also contains instructions to save the note as a text file and a checkbox for "J'ai sauvegardé ma note d'enregistrement". In the background, the "Déposer" (Deposit) form is visible, showing "Token: ETH" and a "Montant" (Amount) slider set to 1 ETH. A list of previous transactions is partially visible on the right side of the interface.

**Votre note d'enregistrement privée**

Veuillez sauvegarder votre note d'enregistrement. Vous allez en avoir besoin plus tard pour retirer votre dépôt. Traitez votre note d'enregistrement comme une clé privée - ne la partagez jamais avec quiconque, y compris les développeurs de tornado.cash.

tornado-eth-1-5-0x4599c0445e35d33315d34696716666c3037e424d34565941e29fd65d84047c7736b67d368d7d6dfe97593e022d870f9bc88313c99819e91fc4072b66f43e

Le navigateur va vous demander de sauvegarder votre note d'enregistrement sous forme de fichier: backup-tornado-eth-1-5-0x4599c044.txt

Vous pouvez aussi encrypter vos notes d'enregistrement dans la Blockchain en créant un Compte de Notes, créez-en un dans la page [compte](#).

☐ J'ai sauvegardé ma note d'enregistrement

Envoyer le dépôt

Token: ETH

Montant: 0,1 ETH 1 ETH 10 ETH

Déposer

eth-1 tornadocash.eth

Filtrer par: ETH BAI eDAI US

Temps passé: Montant

postérieurs transaction Statut Récompenses

3858. il y a 4 heures

3857. il y a 5 heures

3856. il y a 21 heures


3855. il y a 2 jours

3854. il y a 2 jours

Votre IP 192.40.57.234, Amsterdam, NL

Encryptée


# Withdrawal UI


 tornado

[Airdrop](#) [Minage ▼](#) [Voter](#) [Conformité](#) [Docs](#)

Gö

Goerli





Réglages

!

Tornado.cash a été audité. Cependant, il s'agit d'un logiciel en phase d'expérimentation. Veuillez l'utiliser à vos propres risques.

×

DéposerRetirer

Note ⓘ

7593e022d870f9bc88313c99819e91fc4072b66f43e

Montant1 ETH

Temps passéune minute

Dépôts postérieursaucun dépôt

Adresse de réceptionFaire un don

Veuillez coller l'adresse ici

Retirer

eth-1.tornadocash.eth

Statistiques1 ETH

Niveau d'anonymat ⓘ

3864 dépôts équivalents

Dernier dépôt

3864. il y a une minute

3859. il y a 4 heures

3863. il y a 8 minutes

3858. il y a 4 heures

3862. il y a 29 minutes

3857. il y a 5 heures

3861. il y a 41 minutes

3856. il y a 21 heures

3860. il y a une heure

3855. il y a 2 jours

Votre IP 192.40.57.234, Amsterdam, NL

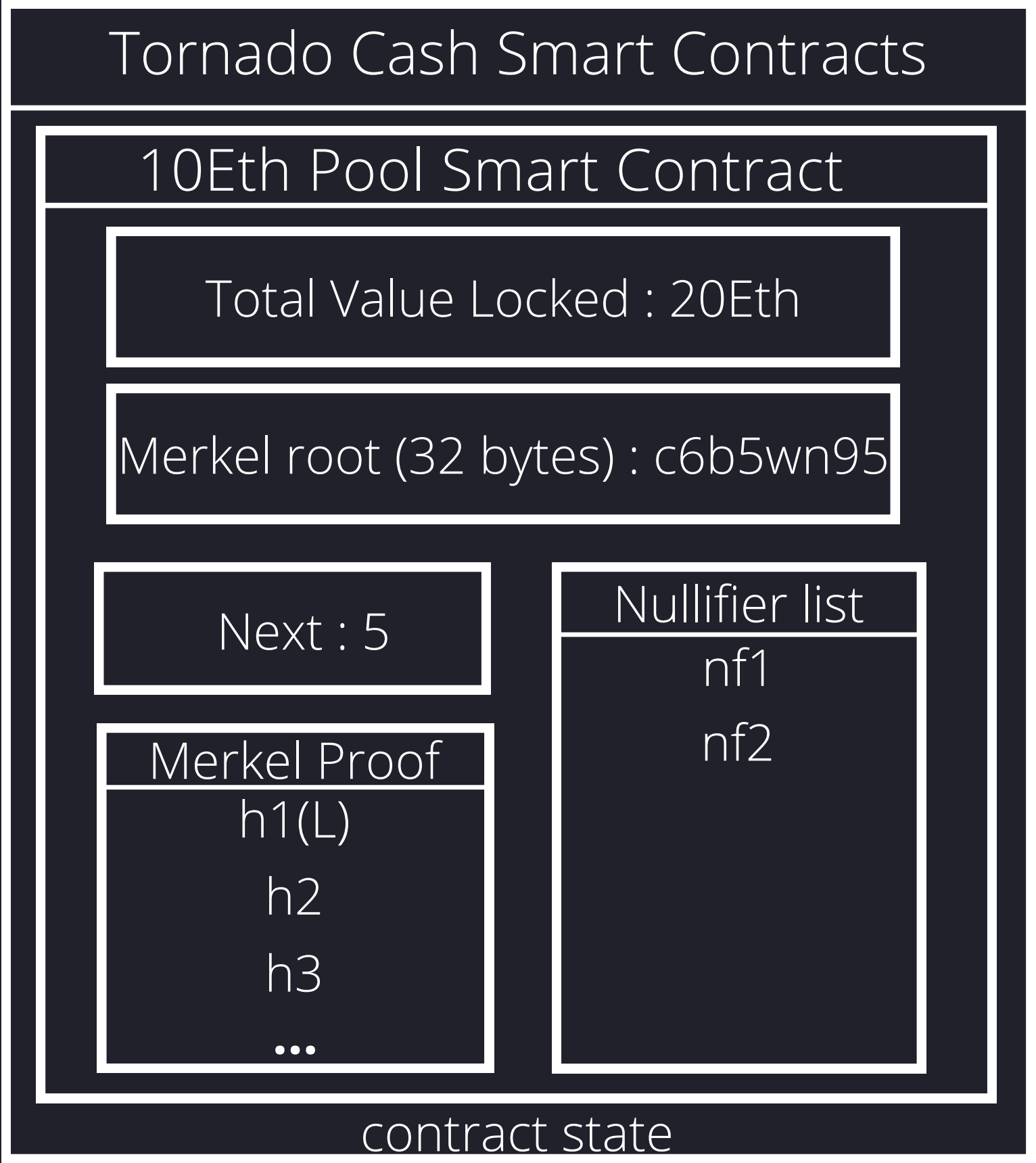
Filtrer par

ETHDAIeDAIUSDCUSDTWBTC

DépenséeNon dépensée

RégulierEncryptée

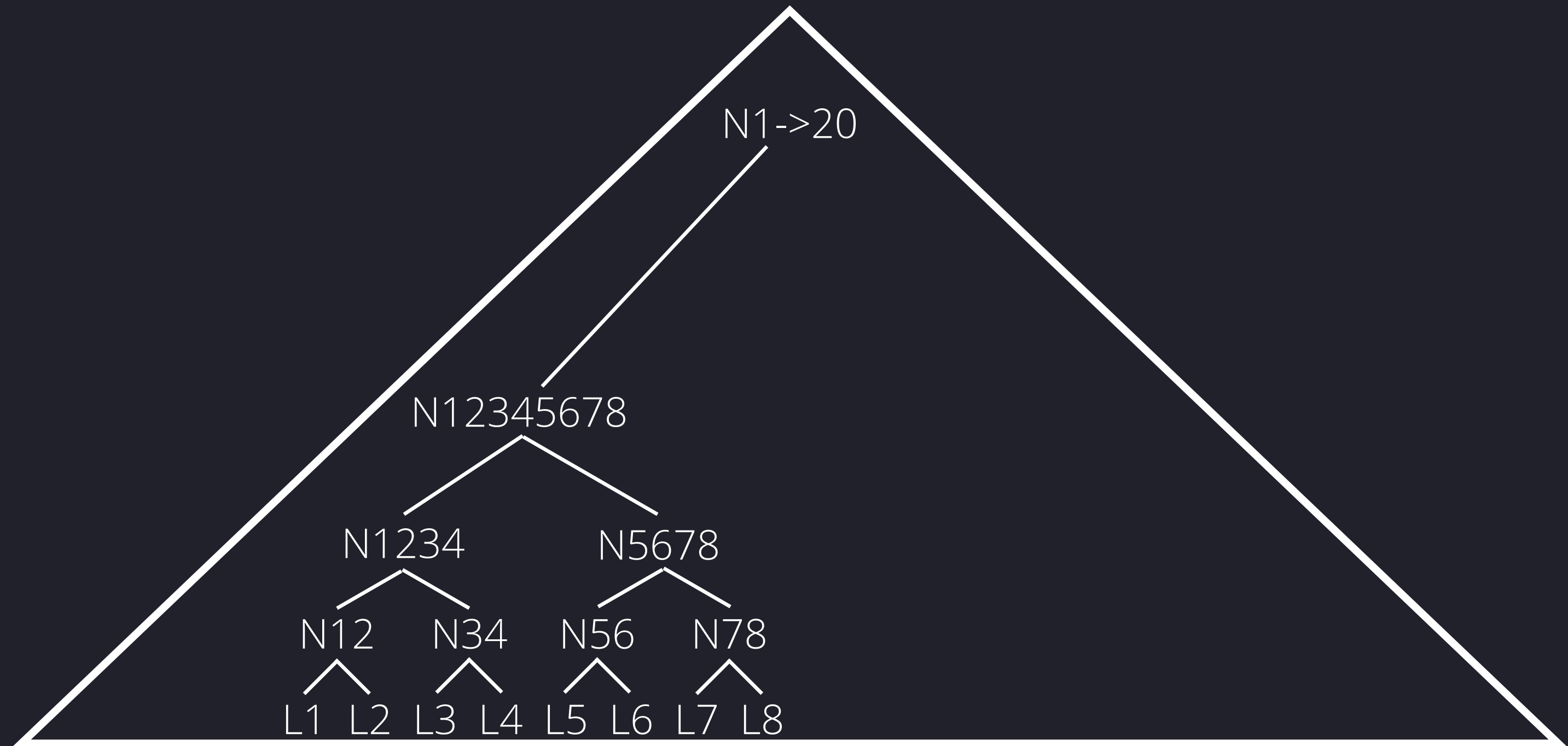
Temps passé ▼MontantDépôtsHash deStatutRécompense ⓘ



Smart contract state

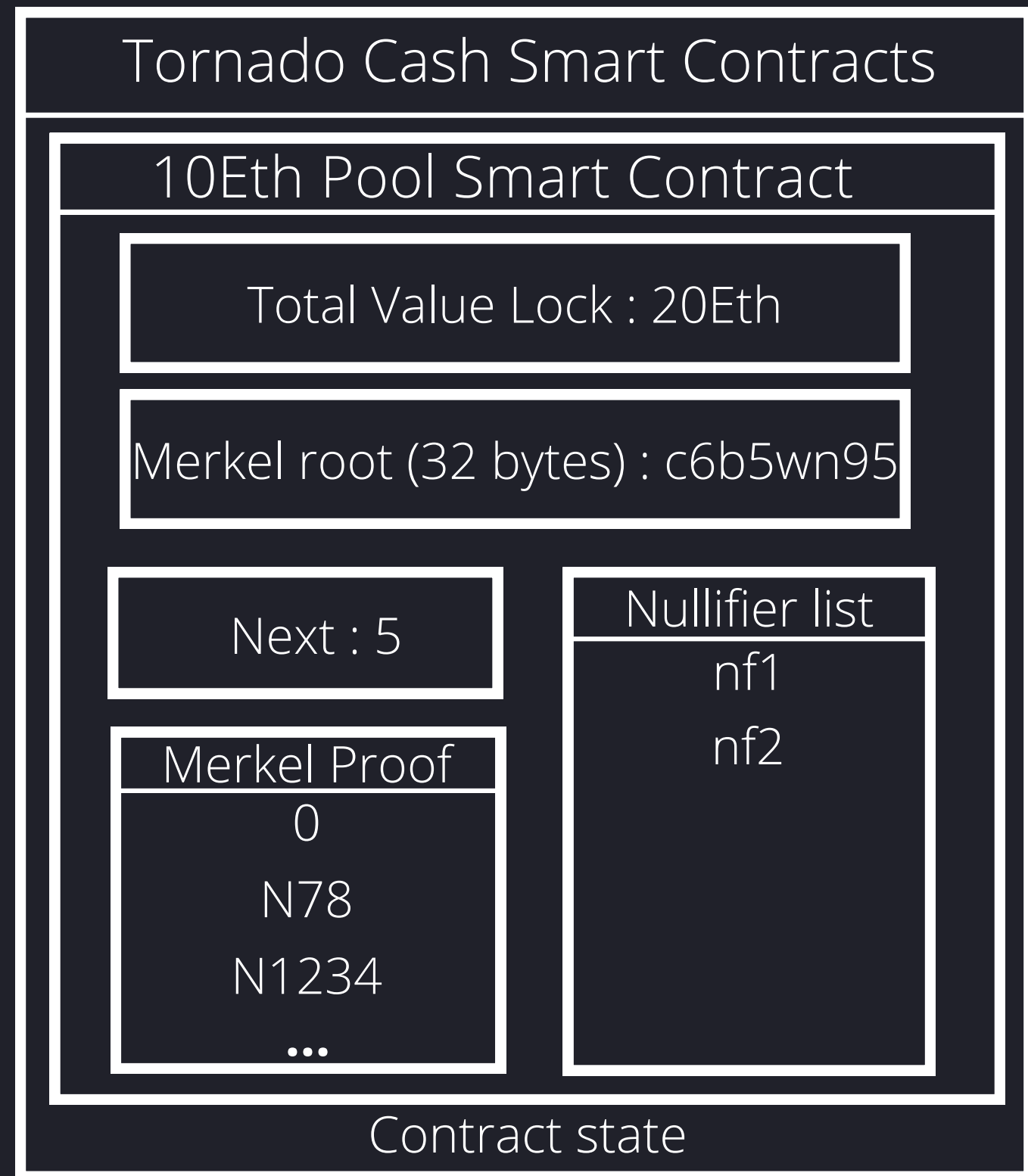


Merkel root : c6b5wn95

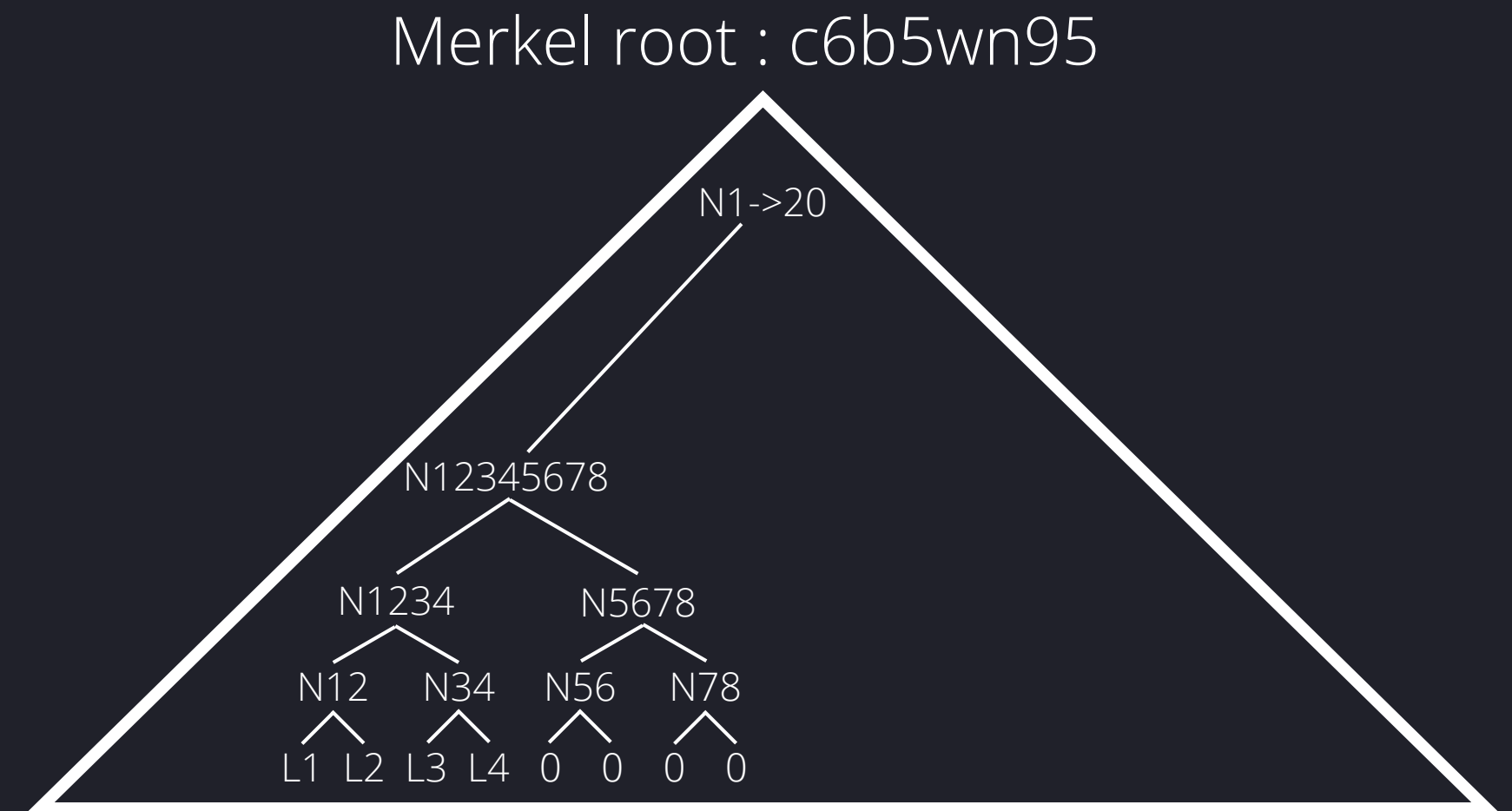


Merkel tree





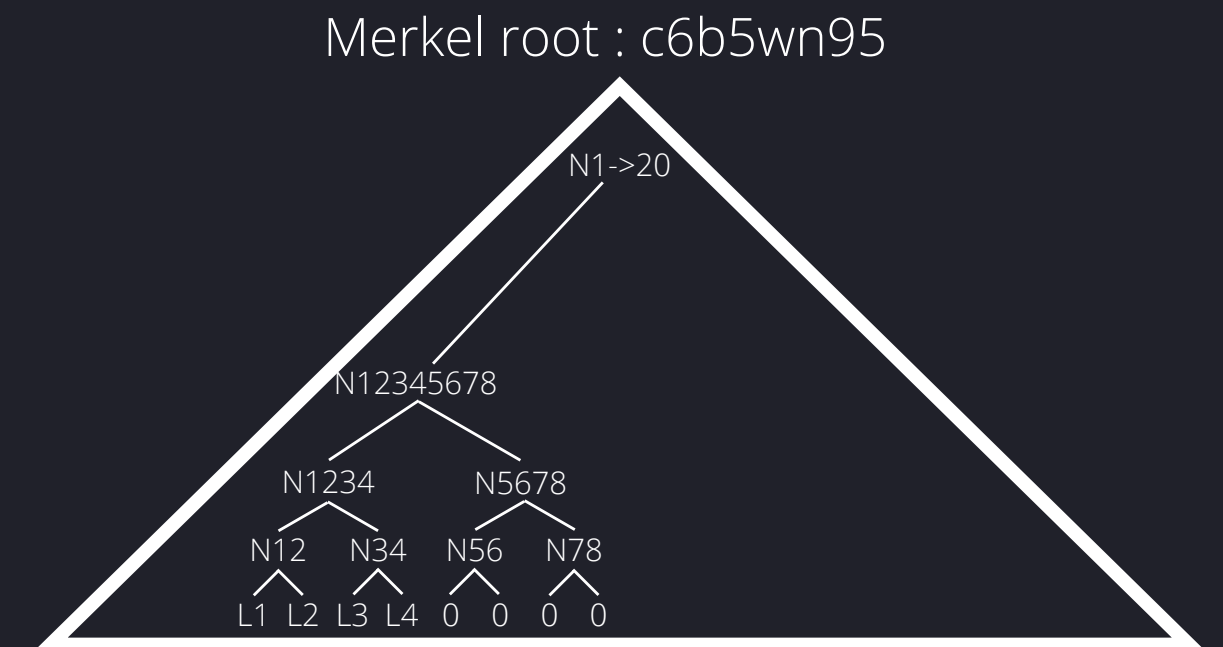
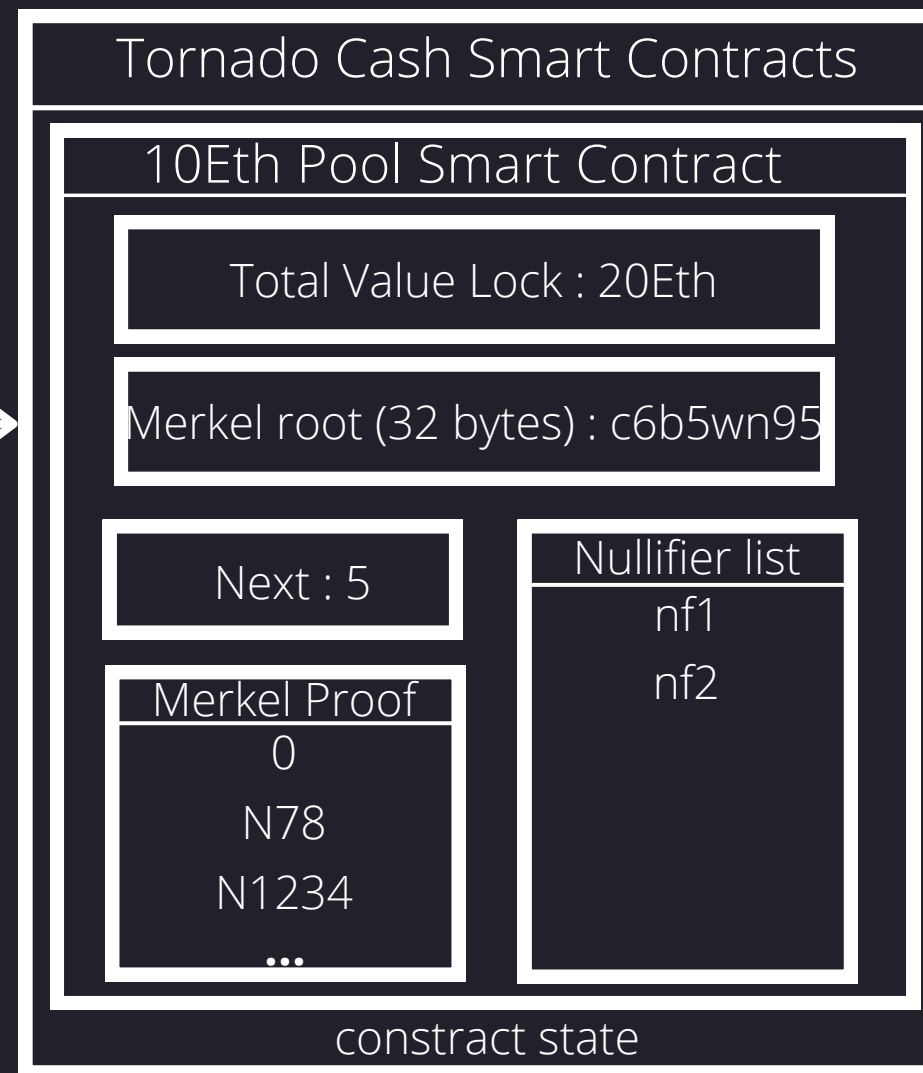
Initial state



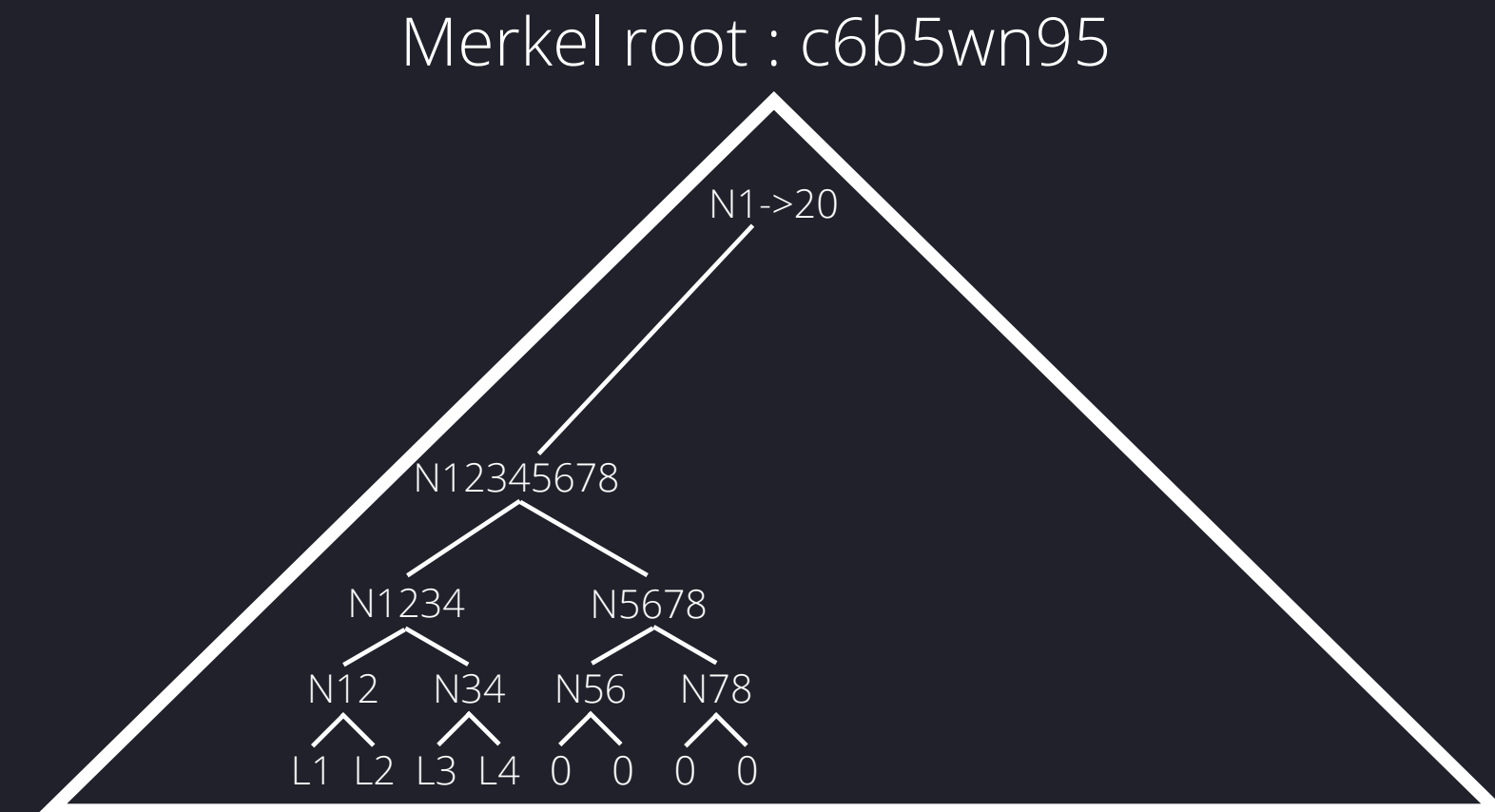
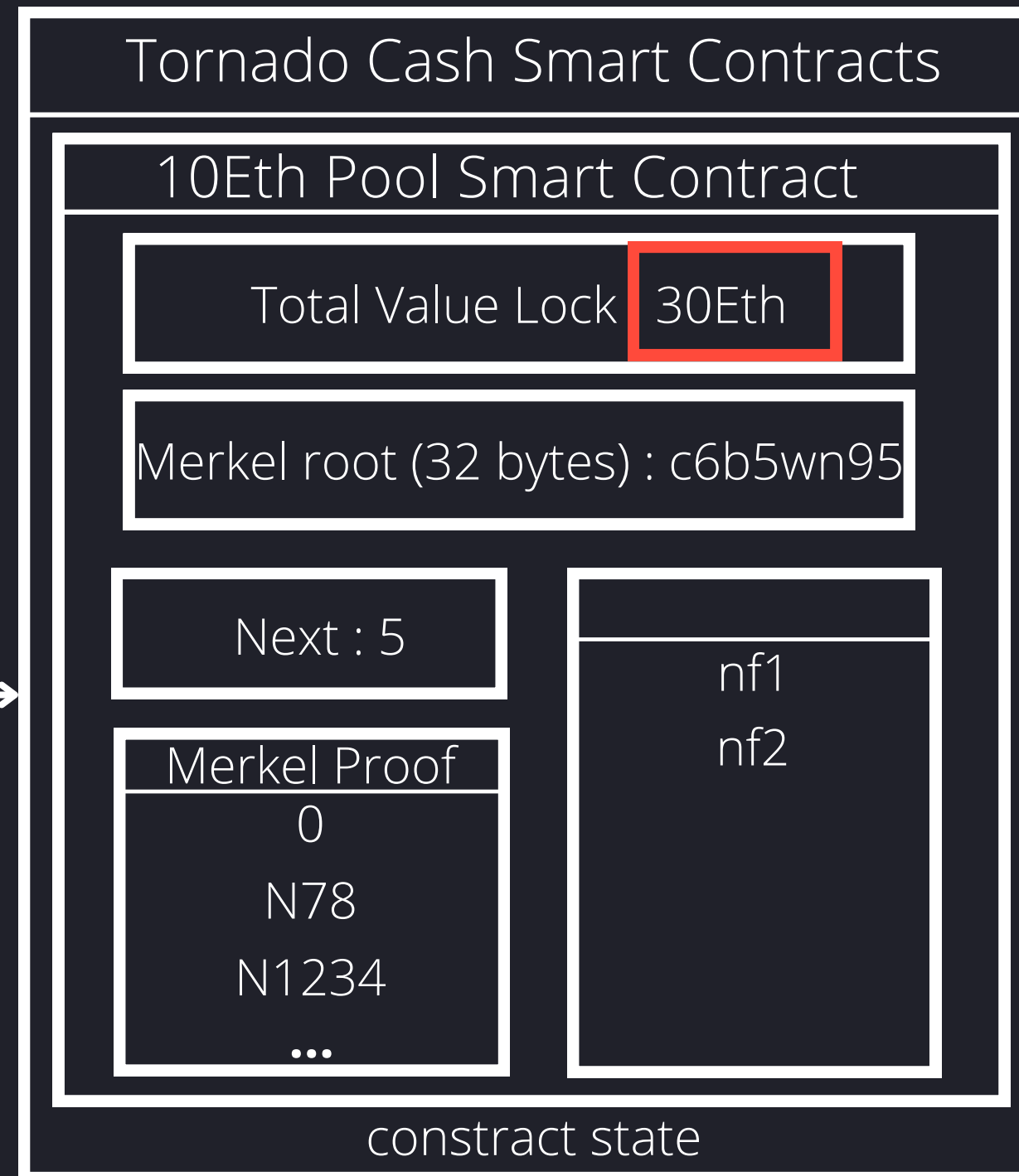




$L5 = \text{hash}(k || r) \quad 10\text{Eth}$



Deposit session



Deposit state



S

L5= hash( k | | r) 10Eth

Tornado Cash Smart Contracts

10Eth Pool Smart Contract

Total Value Lock : 30Eth

Merkel root (32 bytes) : c6b5wn95

Next : 5

Merkel Proof

0

N78

N1234

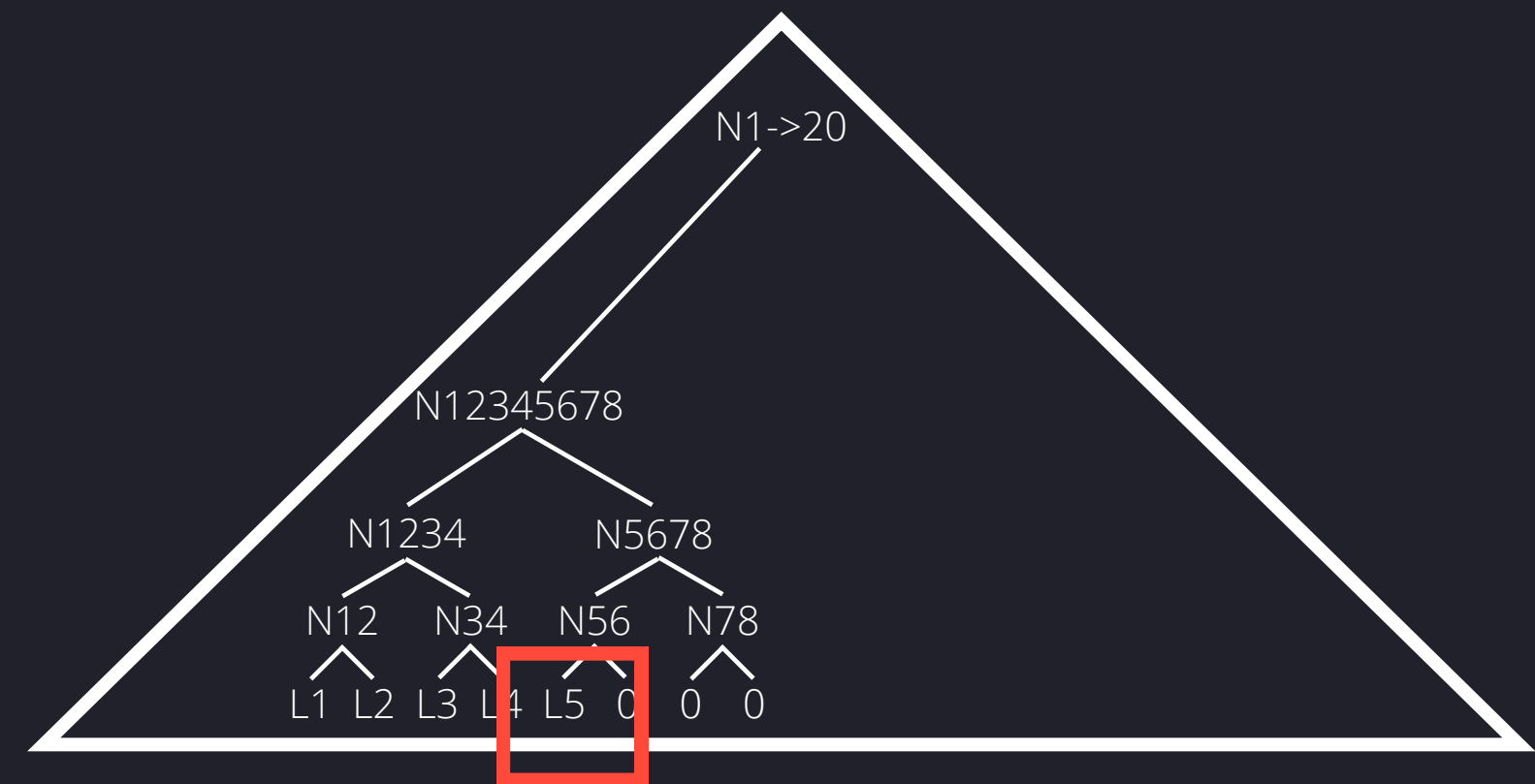
...

nf1

nf2

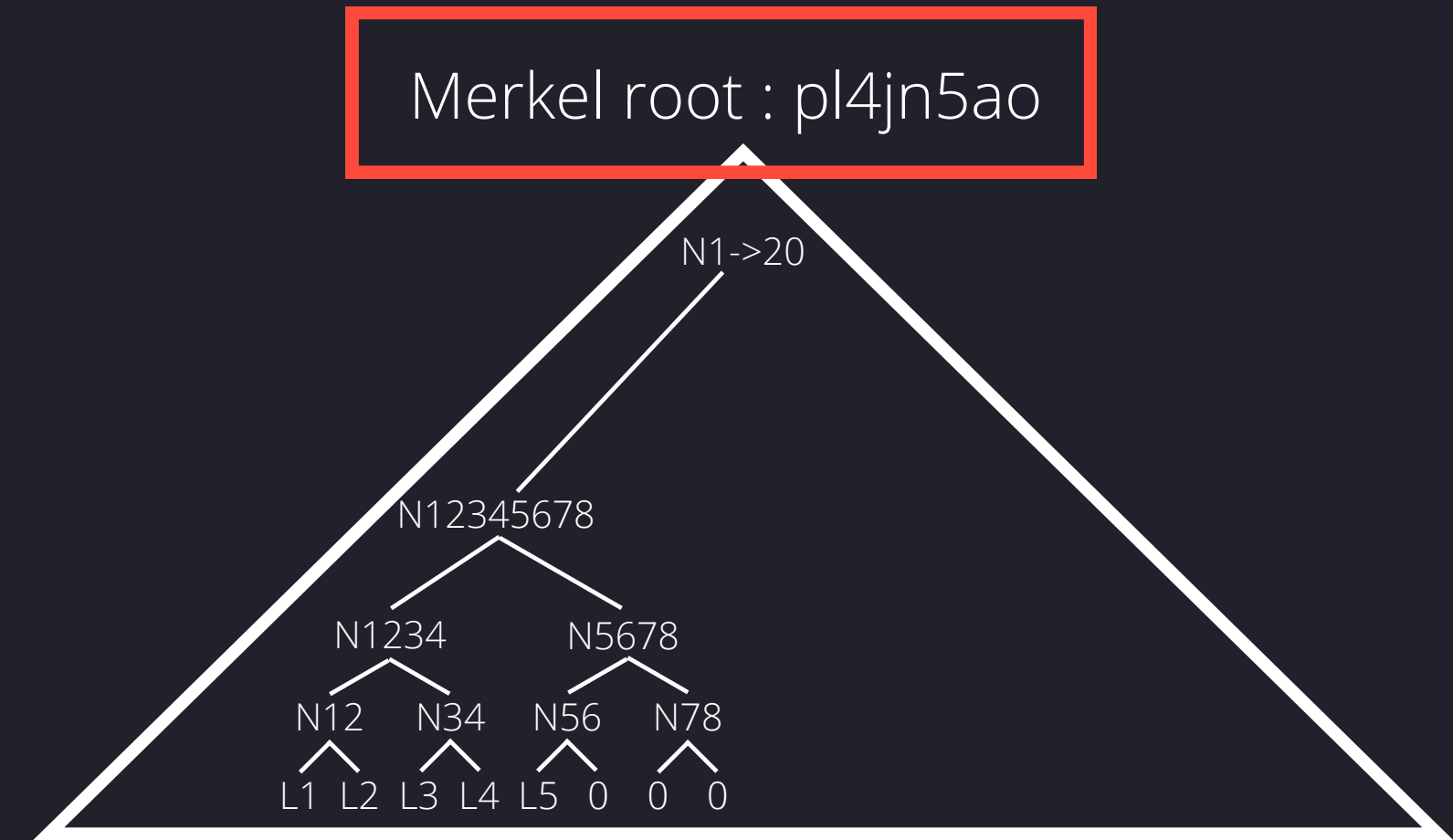
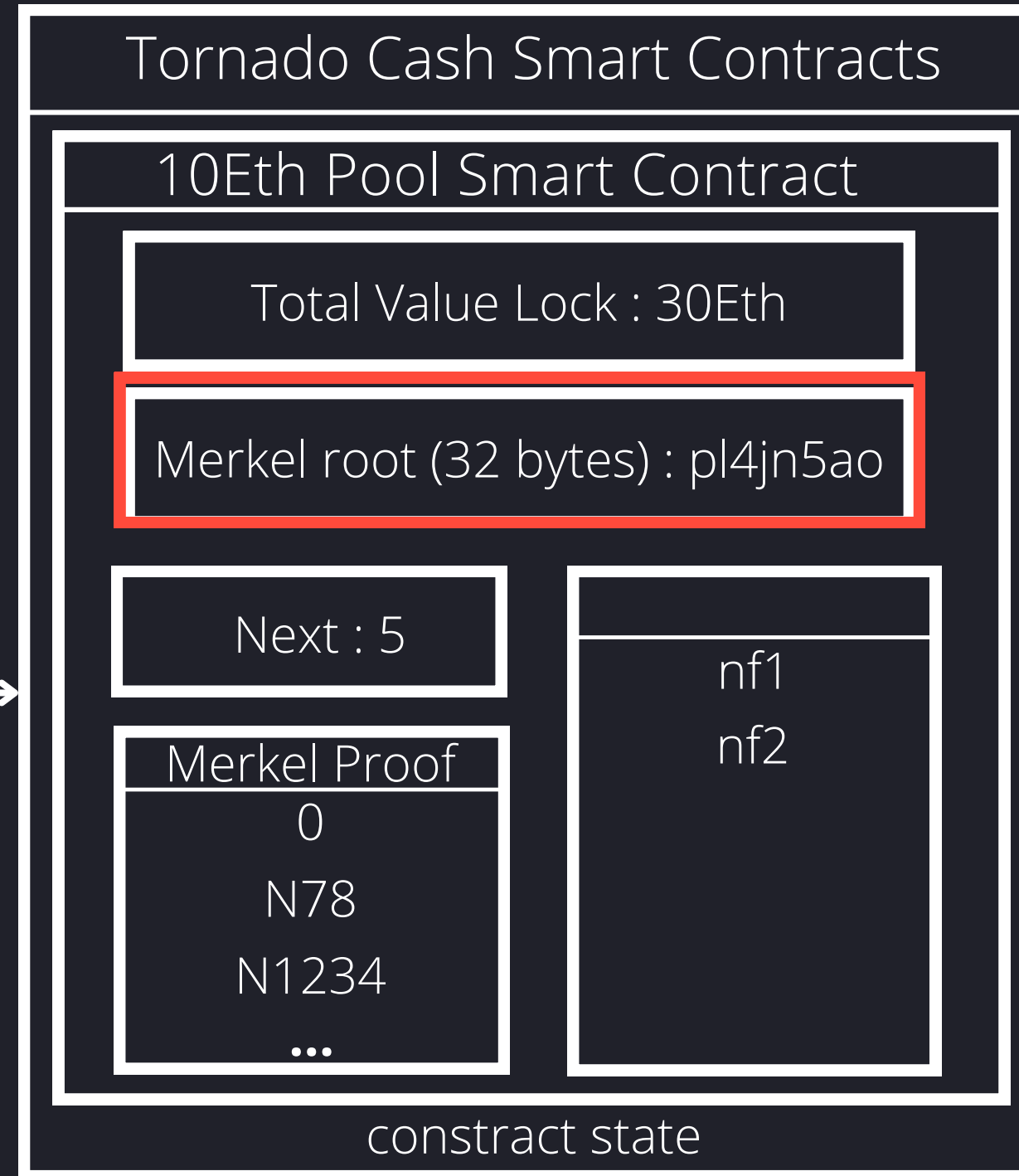
contract state

Merkel root : c6b5wn95



Deposit state





Deposit state







L5= hash( k || r ) 10Eth

## Tornado Cash Smart Contracts

### 10Eth Pool Smart Contract

Total Value Lock : 30Eth

Merkel root (32 bytes) : pl4jn5ao

Next : 6

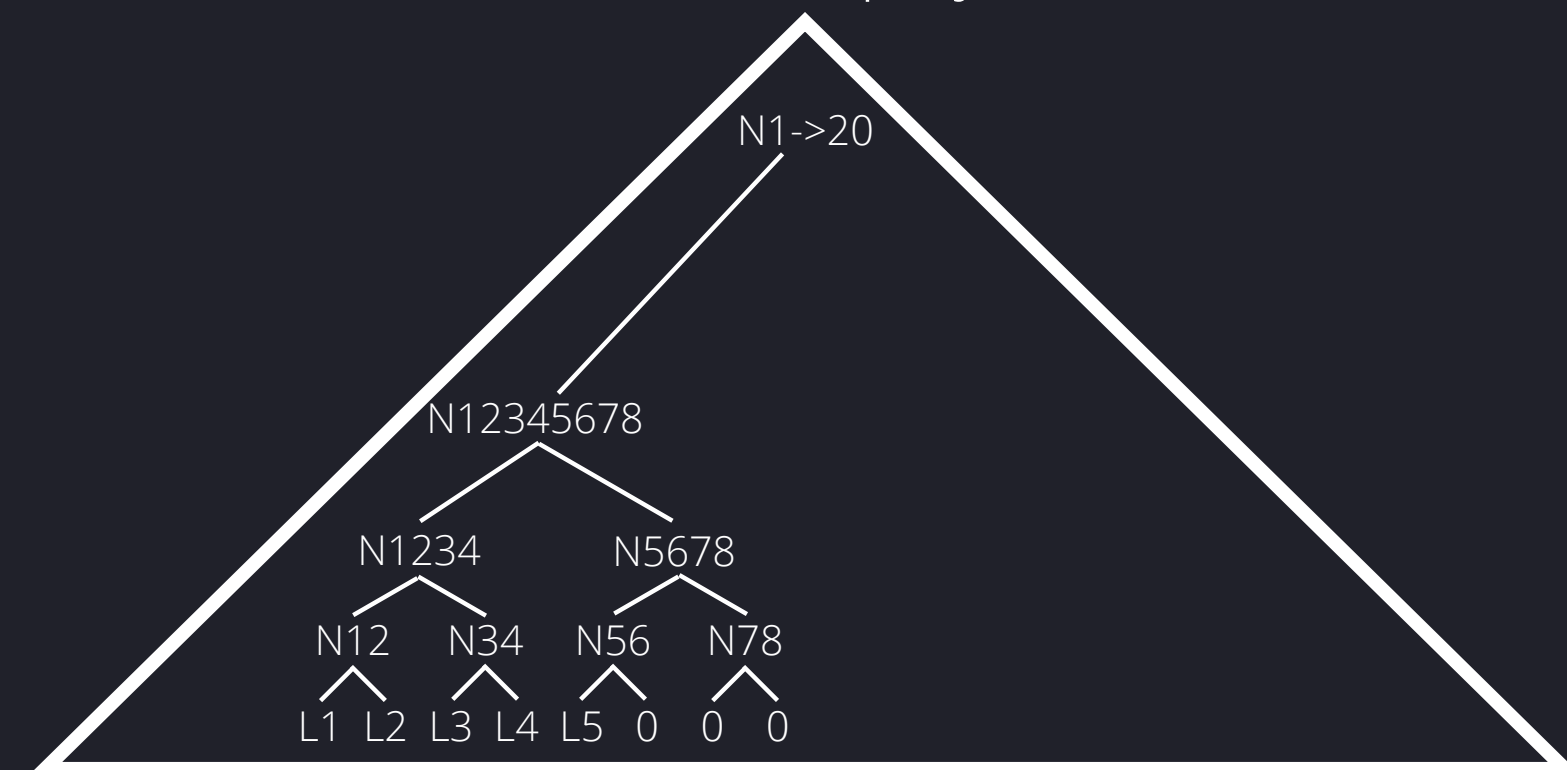
#### Merkel Proof

L5  
N78  
N1234  
...

nf1  
nf2

contract state

Merkel root : pl4jn5ao

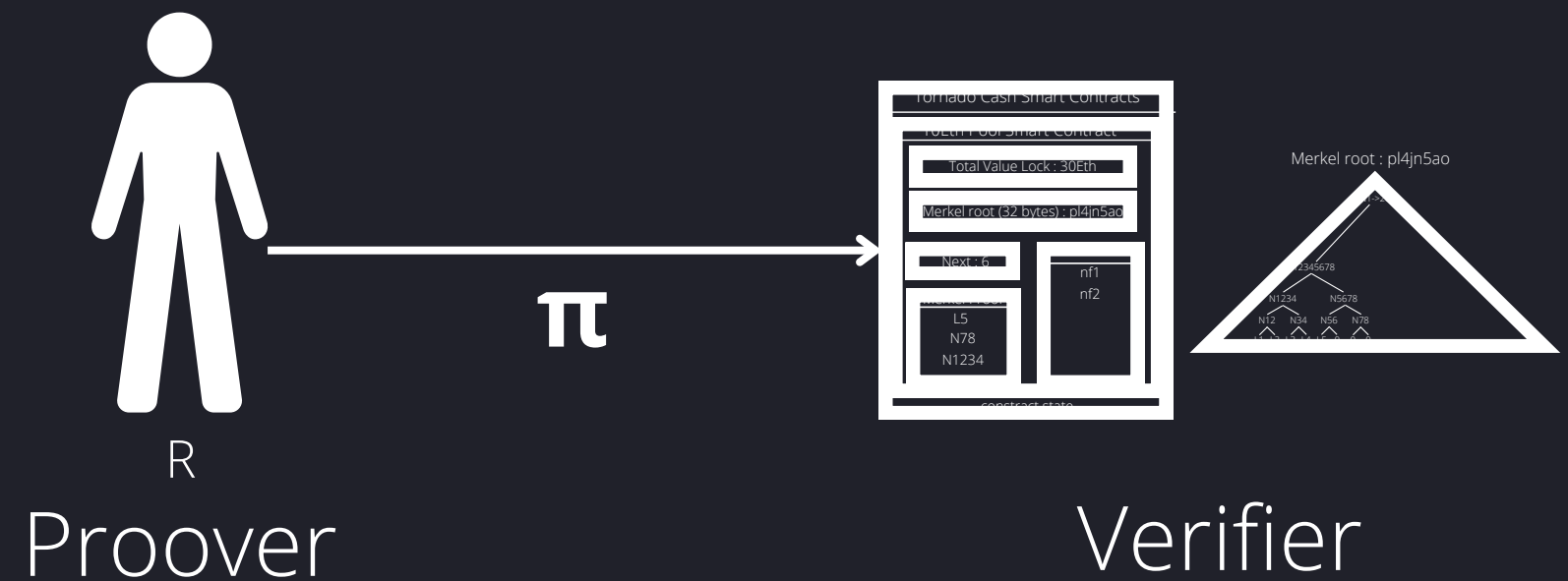


# Deposit state



# ZKP

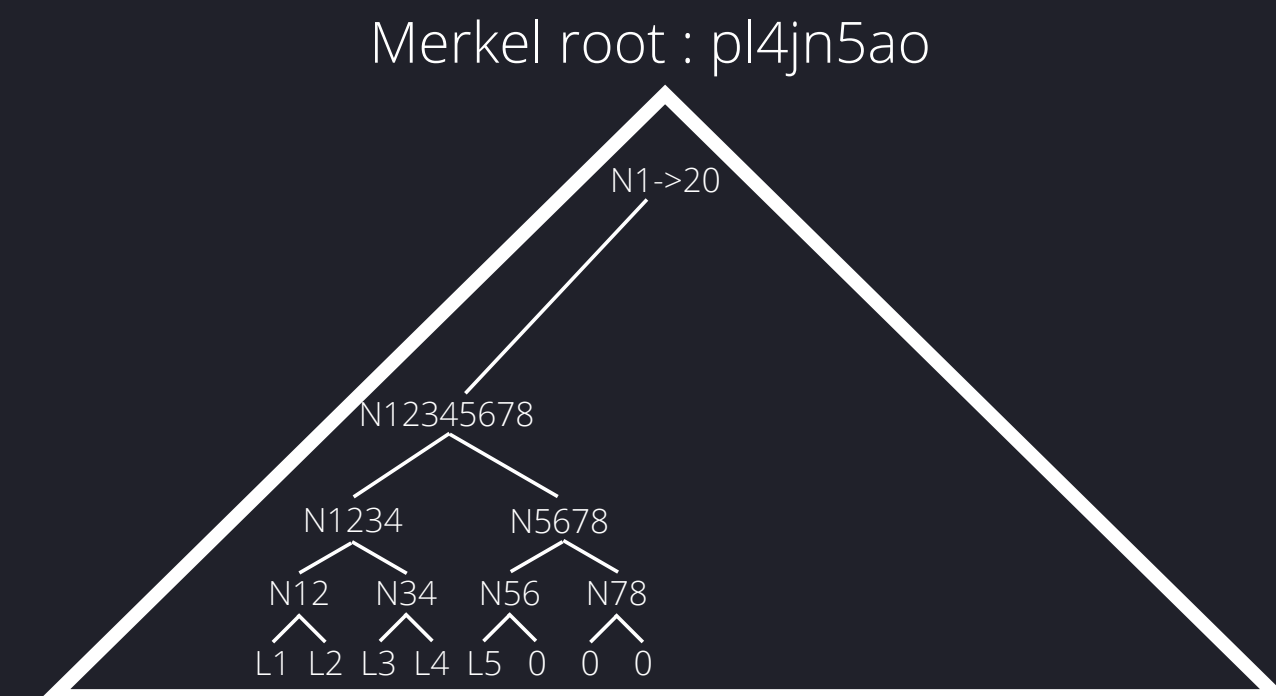
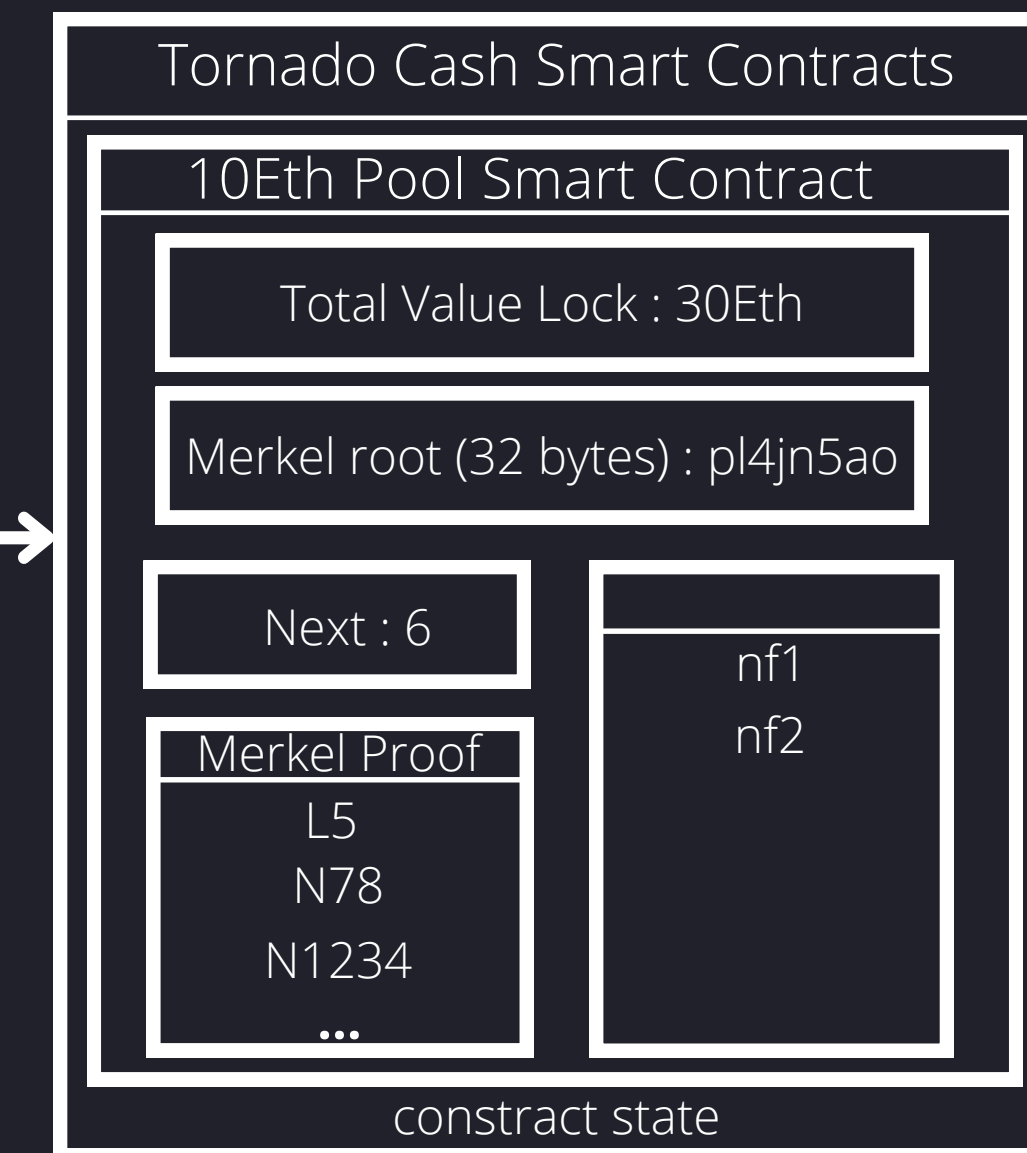
## A cryptosystem



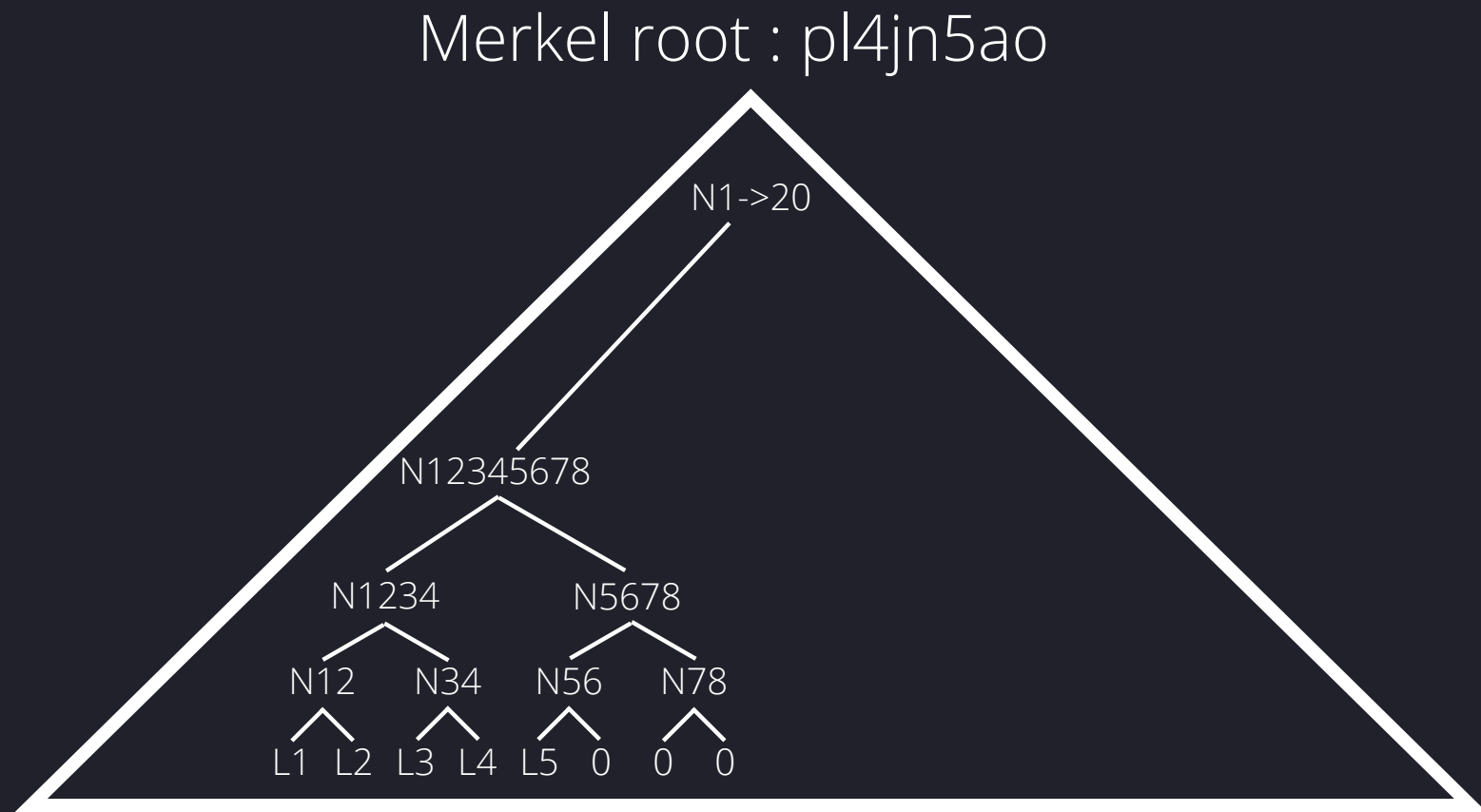
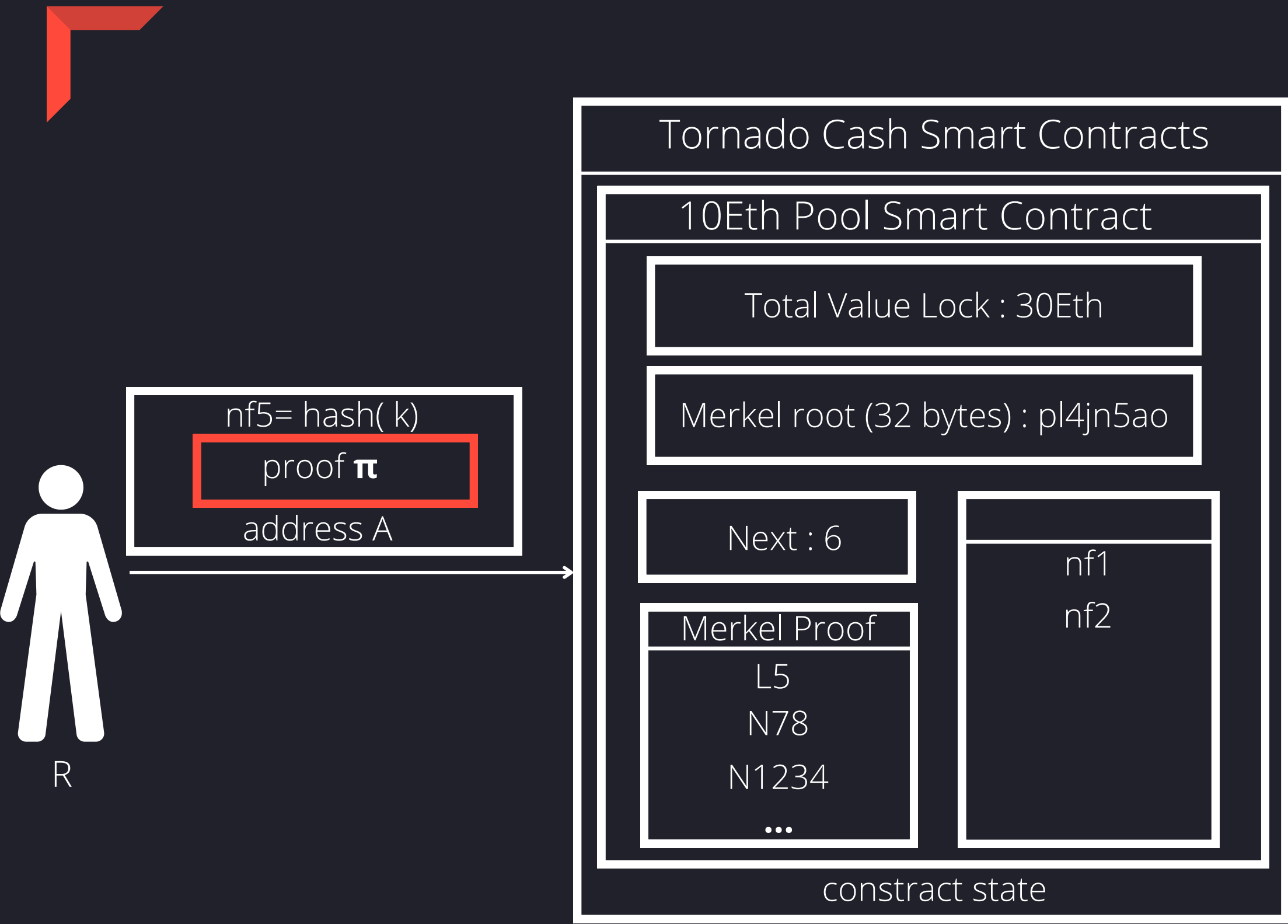
- R and smart contract want to prove  $\exists w, \exists x \mid w$  belongs Merkel Tree
- $w=(k,r,C,\text{MerkelProof}(C))$
- $x=(R,nf,\text{WithdrawalAdress})$  where  $nf=H1(k)$
- Build  $\pi$



nf5= hash( k)  
proof  $\pi$   
address A

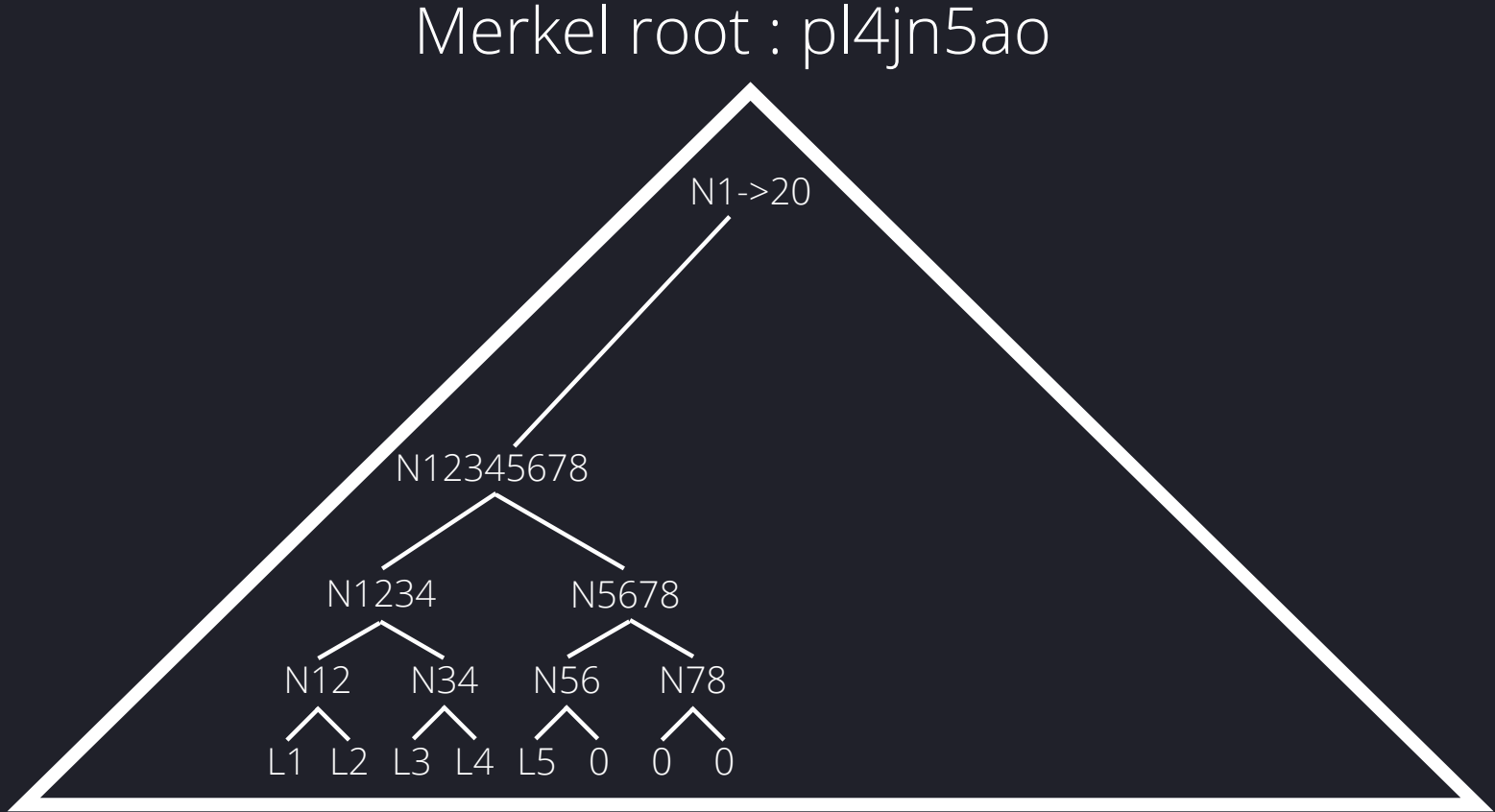
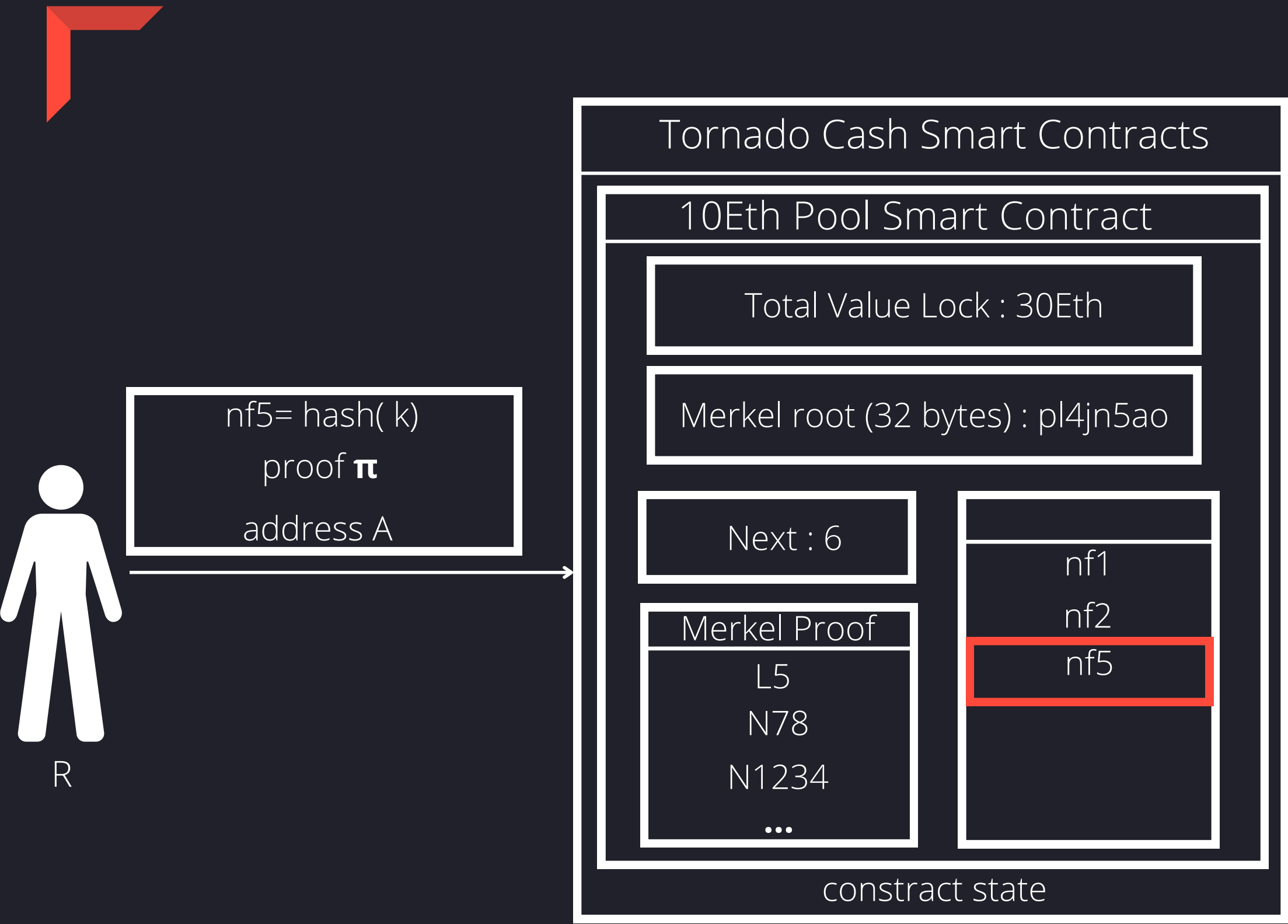


Withdrawal session

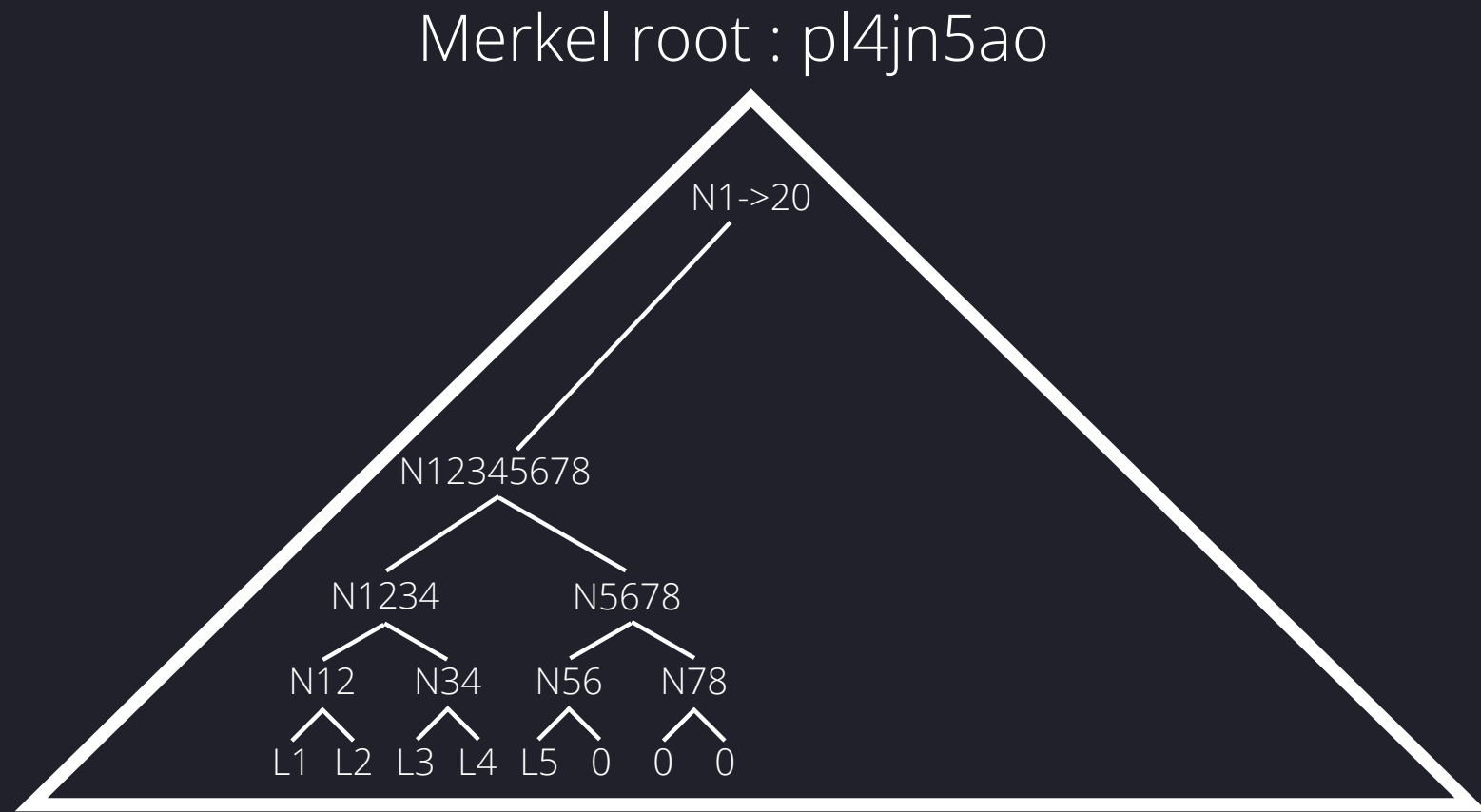
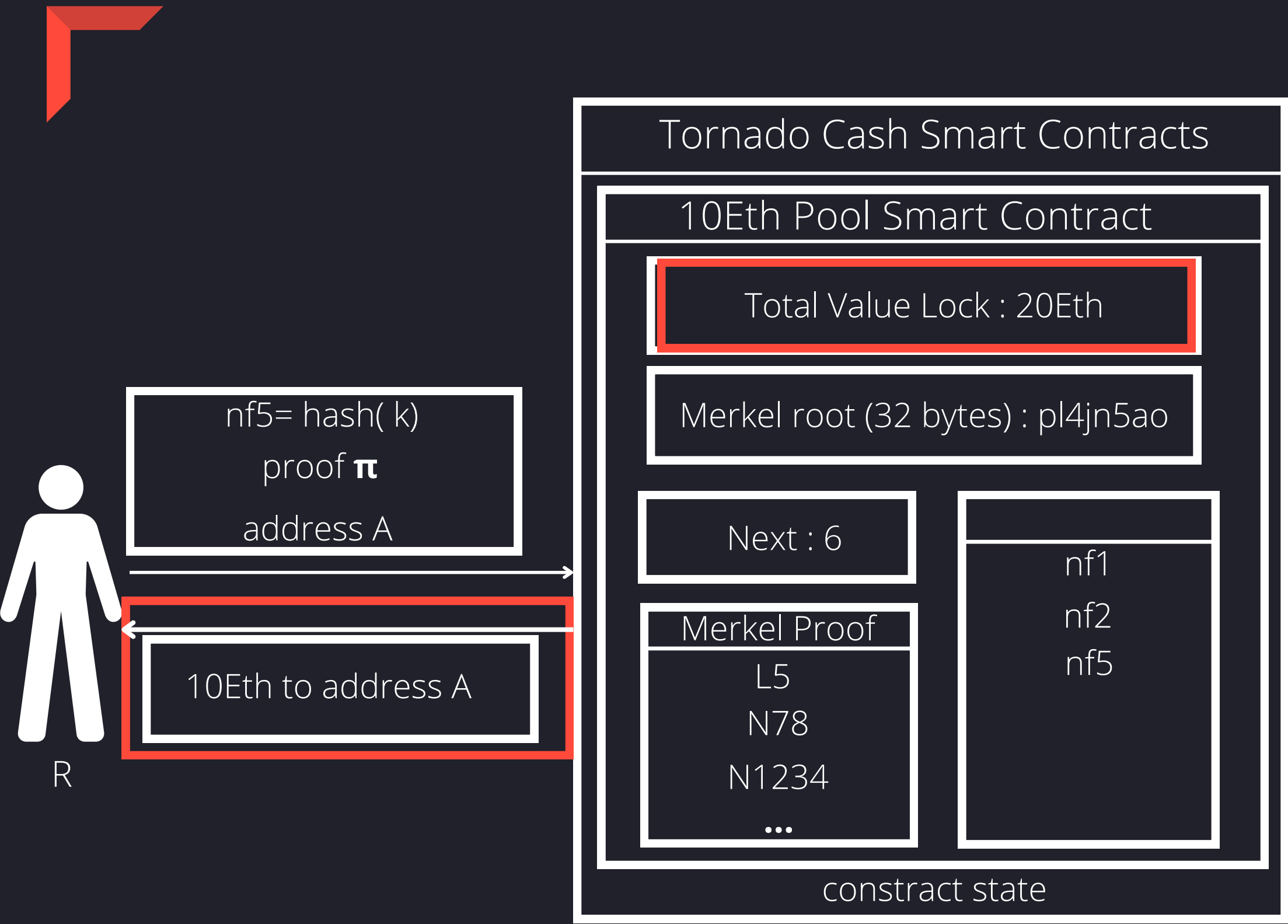


Withdrawal state





Withdrawal state

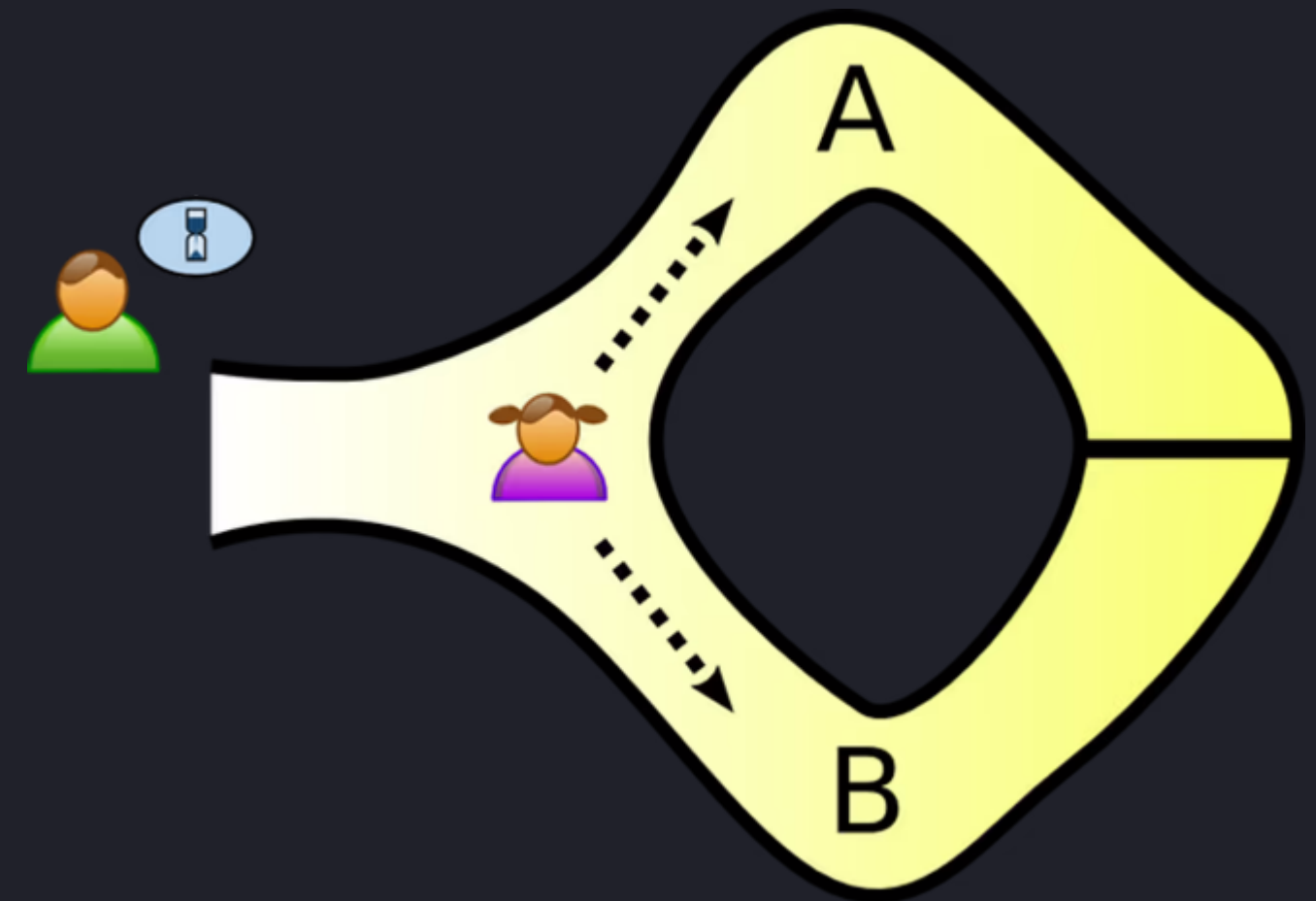


Withdrawal state

# ZKP

## A cryptosystem

- Prover and Verifier want to prove  $\exists w \mid Q(x,w)=0$
- Anyone has access to the context  $x$
- Prover has a secret  $w$
- Verifier wants to verify  $Q(x,w)=0$
- Prover and verifier cannot share  $w$
- Prover sends proof  $\pi$  which does not reveal  $w$  but verifies  $Q(x,w)=0$



An exemple of zkp



# zk-SNARK

Succinct non-interactive argument of knowledge



- **Argument of knowledge:**  $V$  accepts  $\pi \Rightarrow P$  knows  $w \mid Q(x,w)=0$ ;
- **Succint:**  $\pi$  is easy to compute and easy to verify (vital to minimize gas fees);
- **Non-interactive:** a single exchange between  $P$  and  $V$  is sufficient to transmit  $\pi$ .





# Questions

Tornado.cash est-il basé sur un seul Smart Contract ? Le SC étant géré par la même entité intermédiaire (représentant Tornado.cash?).




- Tornado Cash possède plusieurs contrats :  
Tornado.sol, Verifier.sol, MerkleTreeWithHistory.sol



# Questions


Comment sont créés les pools ? Comment faire entrer des users (pré-authentification/validation des credentials ?).

- 
- Envoie de transaction sur Ethereum se fait par une adresse publique et sa signature faite à partir de sa clé privée
  - Entrée dans la pool se fait après avoir généré la note (concaténation de k et de r)
  - Pool est un smart contract déployé par Tornado Cash, chaque pool possède son arbre de Merkel et son propre smart contract



# Questions

Comment sont-ils élus ? les validateurs (ouvert ou c'est géré par Tornado.cash?).

- 
- Valideurs d'Ethereum
  - Indépendants à Tornado Cash