

Prototype d'un outil d'anonymisation des transactions financières sur la blockchain Ethereum.

Master : Sécurité Informatique

Farold Hufranc **ADOUKONOU**

Encadreur: Prof Eugène **EZIN**

4 avril 2025

► **Introduction**

► État de l'Art

► Méthodologie et conception du prototype

► Résultats

► Perspectives et Conclusion

- L'essor de la technologie Blockchain et des cryptomonnaies a révolutionné le secteur de la finance décentralisée.
- Les blockchains publiques permettent des transactions transparentes mais pose un problème de confidentialité.

Problématique

Comment anonymiser les transactions sur la blockchain Ethereum tout en respectant les réglementations KYC/AML ?

- Développer un outil d'anonymisation de transactions (mixeur de cryptomonnaies) basé sur Zero-Knowledge Proofs.
- Intégrer un mécanisme de vérification d'identité basé sur Zero-Knowledge Proofs (zk-KYC) pour assurer la conformité réglementaire.

► Introduction

► État de l'Art

► Méthodologie et conception du prototype

► Résultats

► Perspectives et Conclusion

- Registre distribué qui enregistre les transactions de manière transparente et immuable.
- Contrairement aux systèmes traditionnelles, elle fonctionne sans autorité centrale et repose sur un réseau de nœuds interconnectés.
- Mécanisme de Consensus : Les nœuds doivent s'accorder sur l'ajout d'un nouveau bloc via un protocole (ex. : Proof of Work, Proof of Stake).

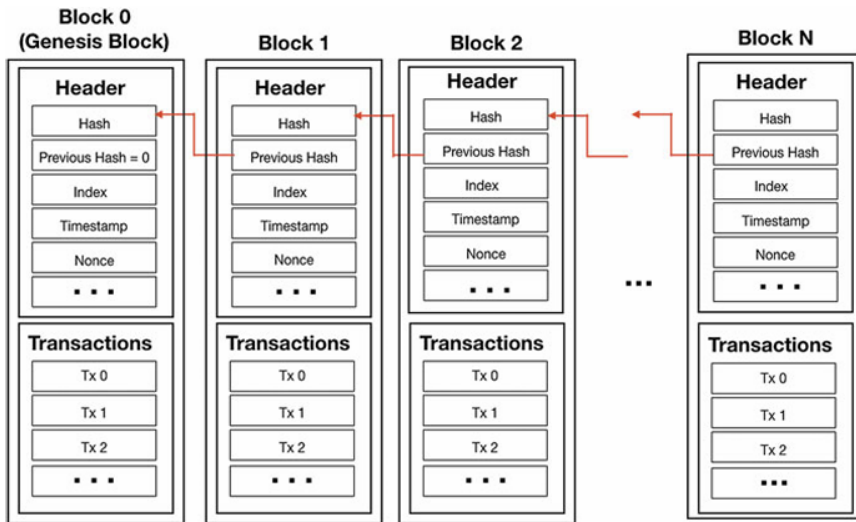


Figure – Structure de la blockchain

- **Blockchain Publique** : Accessible à tous, totalement transparente (ex. : Bitcoin, Ethereum).
- **Blockchain Privée** : Restreinte à un groupe d'utilisateurs (ex. : entreprises, consortiums).
- **Blockchain de Consortium** : Gérée par plusieurs entités avec des droits de validation limités.

- **Ethereum** est une blockchain publique
- Créée en 2015 par **Vitalik Buterin**



Spécificité

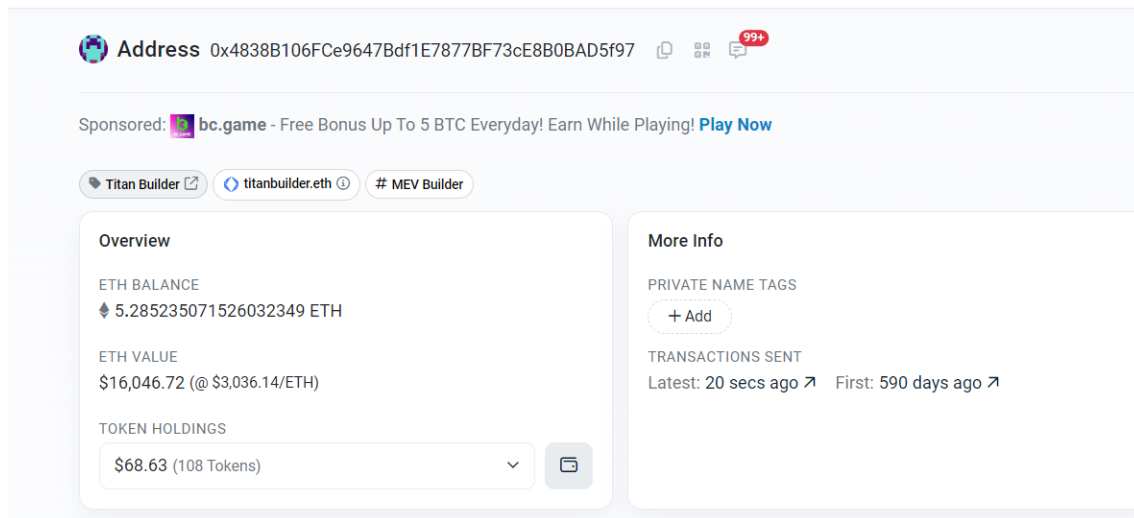
Ethereum permet l'exécution de smart contracts et la création d'applications décentralisées (dApps).

- **Smart Contracts** : Programmes autonomes qui s'exécutent automatiquement lorsqu'une condition est remplie.
- **Ethereum Virtual Machine (EVM)** : Une machine virtuelle qui exécute les smart contracts de manière décentralisée.
- **dApps (Applications Décentralisées)** : Applications fonctionnant sans intermédiaire, construites sur des smart contracts.

Transparence vs Confidentialité


Ethereum est une blockchain publique où toutes les transactions sont enregistrées et visibles par n'importe qui via des explorateurs comme Etherscan.

- Les transactions sur les blockchains publiques sont pseudonymes, pas anonyme.
- La dé-anonymisation des transactions.



The screenshot shows the Etherscan interface for an Ethereum address. At the top, the address is displayed as 0x4838B106FCe9647Bdf1E7877BF73cE8B0BAD5f97. Below the address, there is a sponsored banner for 'bc.game' offering a free bonus up to 5 BTC everyday. Underneath the banner, there are three buttons: 'Titan Builder' with an external link icon, 'titanbuilder.eth' with a verified domain icon, and '# MEV Builder'. The main content is divided into two columns. The left column, titled 'Overview', shows the 'ETH BALANCE' as 5.285235071526032349 ETH, the 'ETH VALUE' as \$16,046.72 (@ \$3,036.14/ETH), and 'TOKEN HOLDINGS' as \$68.63 (108 Tokens). The right column, titled 'More Info', shows 'PRIVATE NAME TAGS' with a '+ Add' button, and 'TRANSACTIONS SENT' with the latest transaction 20 seconds ago and the first transaction 590 days ago.

Address 0x4838B106FCe9647Bdf1E7877BF73cE8B0BAD5f97

Sponsored:  **bc.game** - Free Bonus Up To 5 BTC Everyday! Earn While Playing! [Play Now](#)

[Titan Builder](#) [titanbuilder.eth](#) [# MEV Builder](#)

Overview

ETH BALANCE
5.285235071526032349 ETH

ETH VALUE
\$16,046.72 (@ \$3,036.14/ETH)

TOKEN HOLDINGS
\$68.63 (108 Tokens)

More Info

PRIVATE NAME TAGS
[+ Add](#)

TRANSACTIONS SENT
Latest: 20 secs ago [↗](#) First: 590 days ago [↗](#)

Figure – Etherscan, l'explorateur de Blockchain Ethereum

Différence entre pseudonymat et anonymat

- **Pseudonymat** : Les utilisateurs sont identifiés par une adresse publique qui ne contient aucune information personnelle.
- **Anonymat** : Empêche d'associer une transaction à un utilisateur spécifique.

Risques liés au manque de confidentialité

- Les régulateurs imposent des contrôles Know Your Customer (KYC) et Anti-Money Laundering (AML) pour limiter les usages criminels.
- Défi : Comment concilier anonymat et respect des réglementations avec une solution comme le zk-KYC

- Les mixeurs (mixers/tumblers)
- Les privacy coins (ex. : Monero, Zcash)

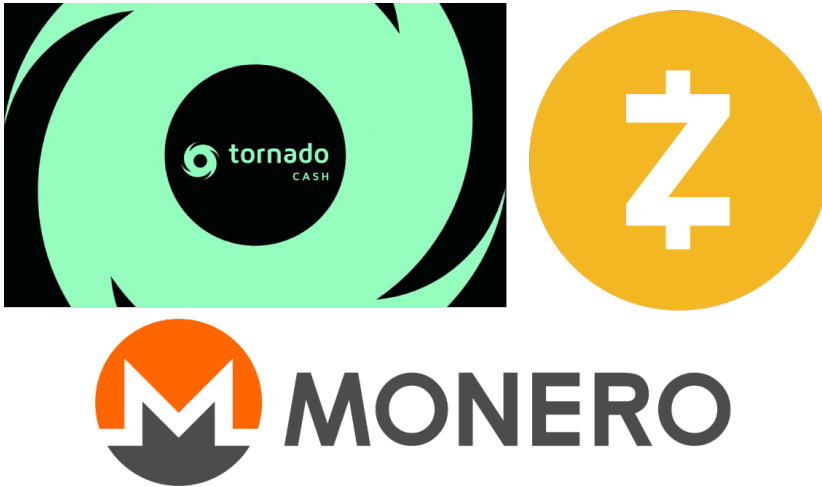


Figure – Solutions existantes

Zero-Knowledge Proofs (ZKP) : Preuves à Divulgaration Nulle de Connaissance

- Permettent à une partie (le prouveur) de prouver à une autre (le vérificateur) qu'une déclaration est vraie sans révéler d'informations sensibles.
- Deux types de ZKP : Les **Interactive ZKP** et les **Non Interactive ZKP**

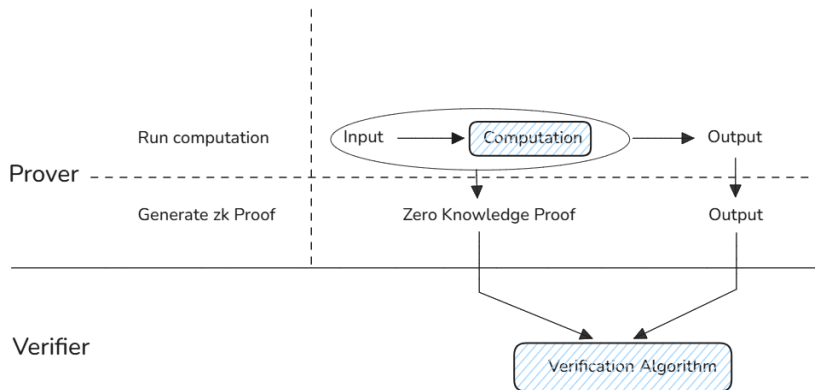


Figure – Fonctionnement du ZKP

zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge)

- Variante avancée des ZKP utilisée sur les blockchains.
- Permet de garantir la confidentialité des transactions.
- Vérification rapide et efficace, optimisé pour les blockchains

- Développée par Ralph Merkle dans les années 1980.
- Présente une structure arborescente dans laquelle chaque feuille est un bloc de données, et chaque nœud interne est le hash de ses nœuds enfants.
- Cas d'utilisation : Git, Bitcoin, Déduplication de données

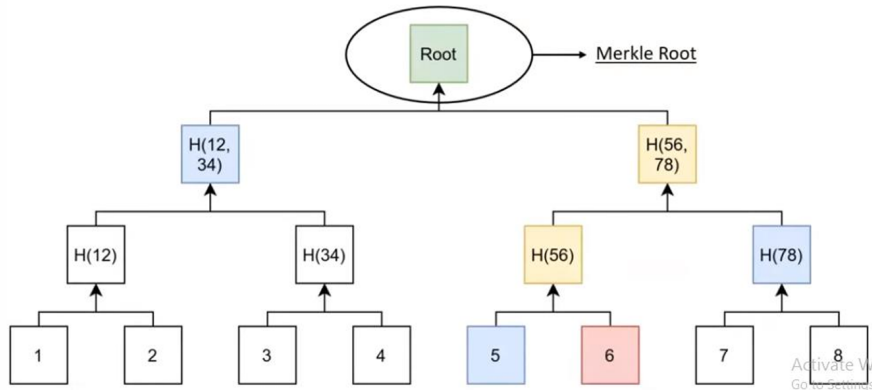
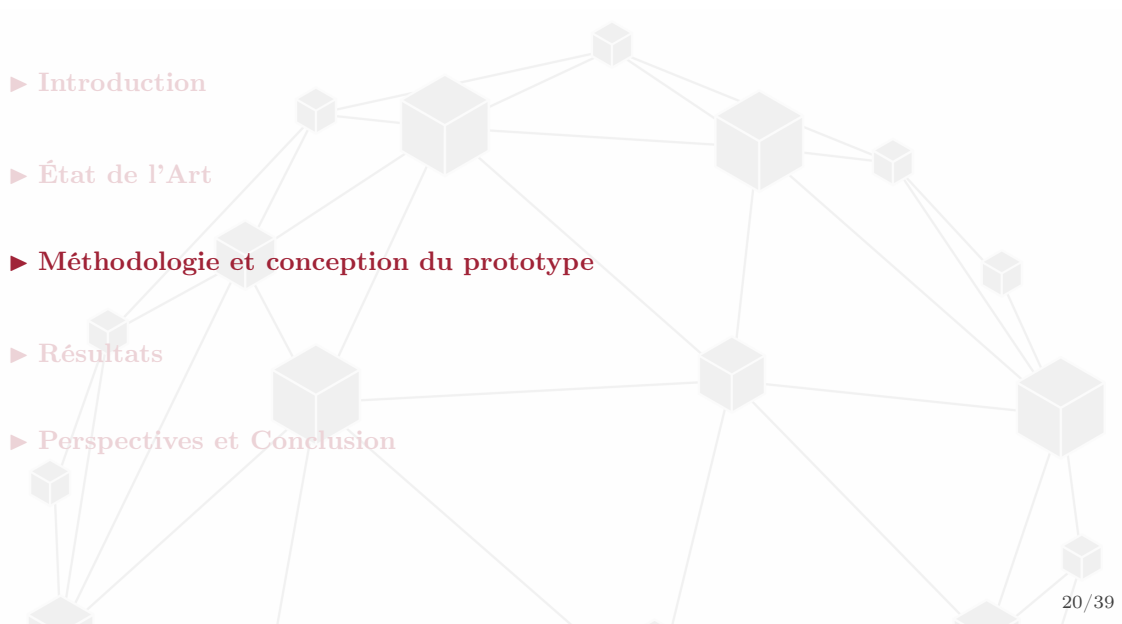


Figure – Schéma d'un arbre de Merkle

Solution

- Permet de prouver qu'un utilisateur a fait une procédure KYC sans révéler son identité.
- Aucune information personnelle de l'utilisateur n'est exposée.
- Equilibre entre anonymat et conformité réglementaire (KYC/AML)

- 
- A network diagram is overlaid on the slide, consisting of several gray 3D cubes connected by thin gray lines. The cubes are arranged in a complex, interconnected pattern, with some cubes acting as central hubs and others as peripheral nodes. The diagram is rendered in a light gray, semi-transparent style.
- ▶ Introduction
 - ▶ État de l'Art
 - ▶ **Méthodologie et conception du prototype**
 - ▶ Résultats
 - ▶ Perspectives et Conclusion

Pour atteindre les objectifs du projet, la méthodologie suivante a été adoptée :

Méthodologie

- Étude des solutions existantes
- Définition de l'architecture du système
- Implémentation et développement du prototype



Le système repose sur les composants suivants :

Implémentation et développement du prototype

- Module KYC (zk-KYC).
- Smart Contract du Mixer
- Interface Utilisateur (Frontend)
- Le relayeur de transaction

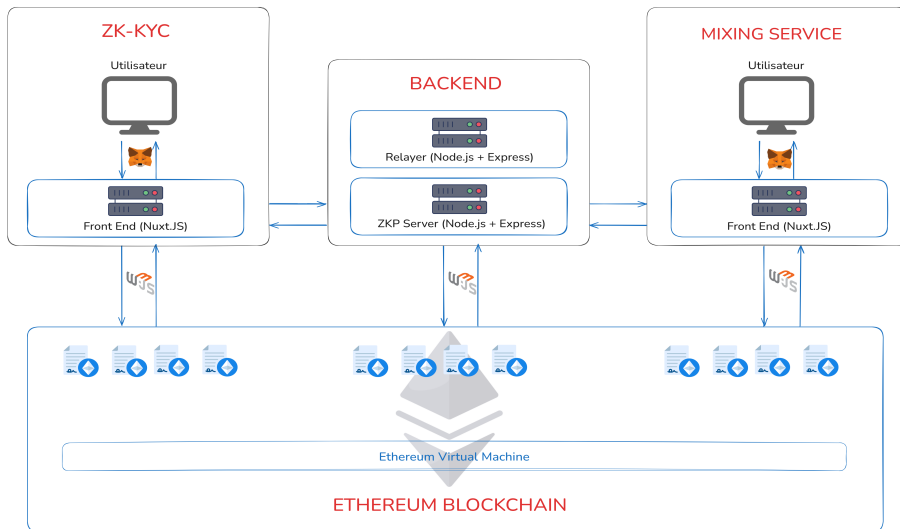


Figure – Architecture du système

Flux de fonctionnement du système

- Vérification KYC
- Dépôt des fonds
- Génération des preuves et initiation du retrait
- Exécution du retrait par le relayeur et transfert des fonds

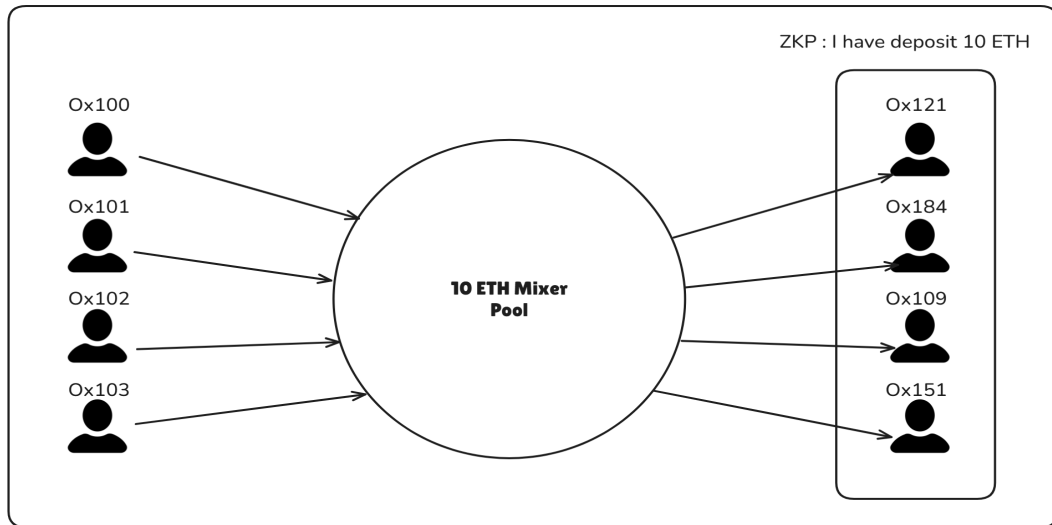


Figure – Protocole de mixage des fonds

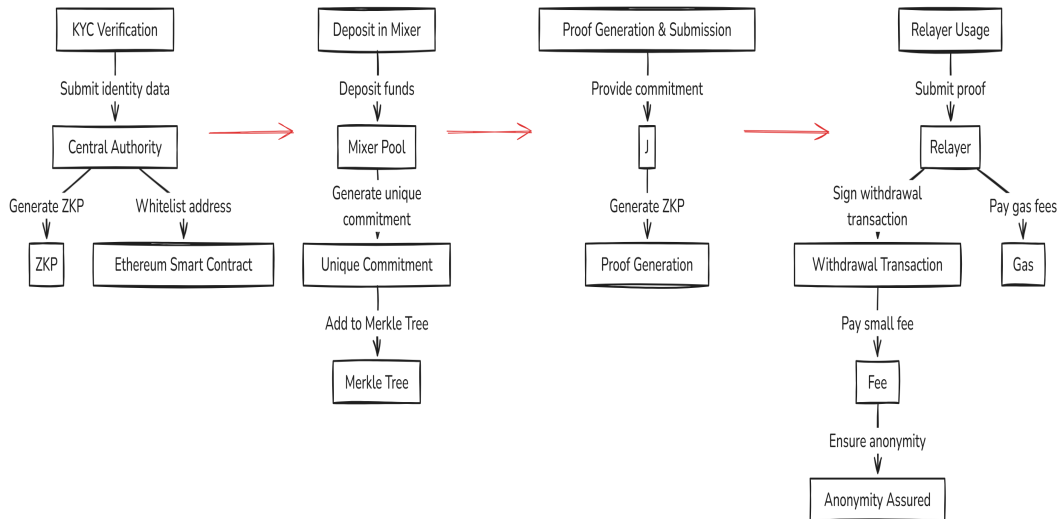


Figure – Flux de fonctionnement du système

Circom

- Langage de description matérielle (HDL) spécialement utilisé pour créer des circuits arithmétiques qui sont ensuite utilisés pour générer des preuves à divulgation nulle de connaissance.

Développement des circuits ZK

- Développement du circuit `kyc_verifier.circom`
- Développement du circuit `merkle_tree.circom`
- Développement du circuit `withdraw.circom`

```
// Verifies that merkle proof is correct for given merkle root and a leaf
// pathIndices input is an array of 0/1 selectors telling whether given pathElement is on the left or right side of merkle path
template MerkleTreeChecker(levels) {
    signal input leaf;
    signal input root;
    signal input pathElements[levels];
    signal input pathIndices[levels];

    component selectors[levels];
    component hashers[levels];

    for (var i = 0; i < levels; i++) {
        selectors[i] = DualMux();
        selectors[i].in[0] <== i == 0 ? leaf : hashers[i - 1].hash;
        selectors[i].in[1] <== pathElements[i];
        selectors[i].s <== pathIndices[i];

        hashers[i] = HashLeftRight();
        hashers[i].left <== selectors[i].out[0];
        hashers[i].right <== selectors[i].out[1];
    }

    root == hashers[levels - 1].hash;
}
```

Figure – Exemple de circuit circom

Développement et déploiement des smart contracts

- Développement du contrat de vérification KYC `KYCRegistry.sol`
- Développement du contrat `MerkleTreeWithHistory.sol`
- Développement du contrat du mixeur `Mixer.sol`

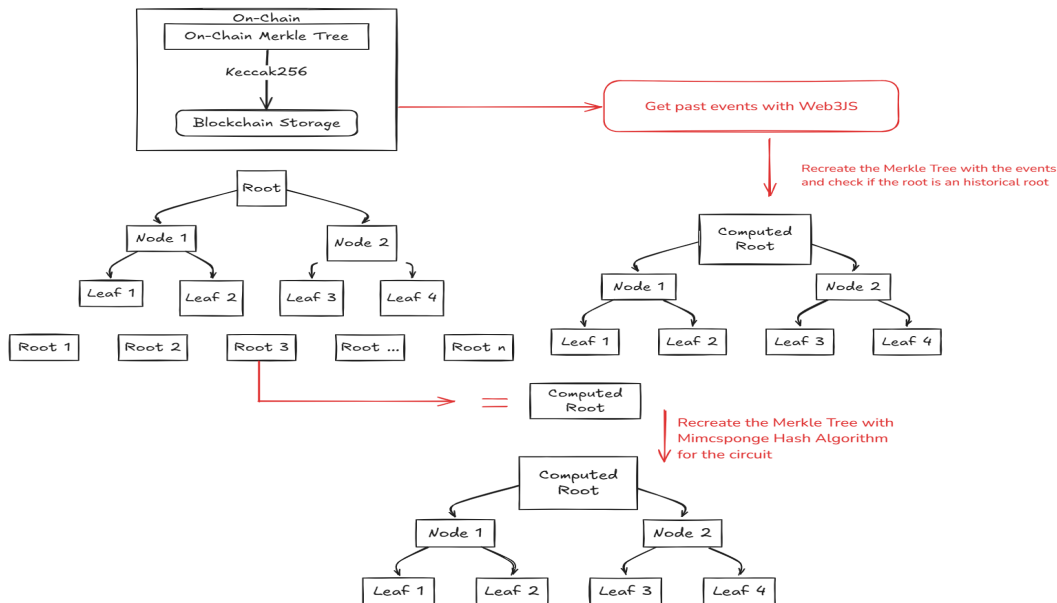


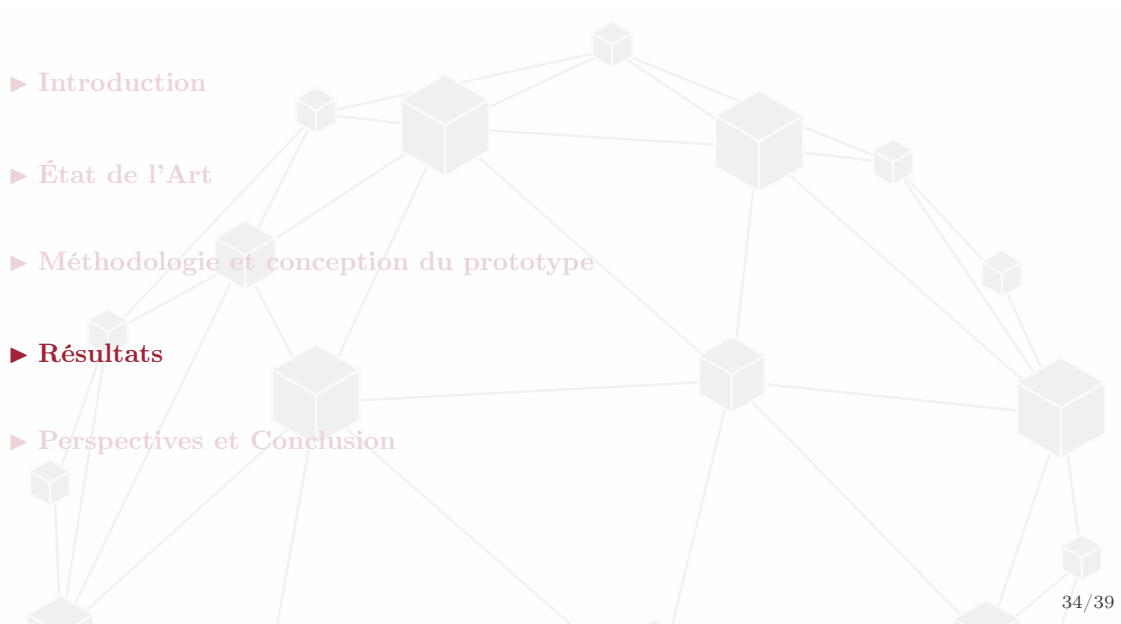
Figure – Processus détaillé avec les Merkle Trees

Développement des interfaces utilisateur

- Interface KYC
- Interface du Mixeur (Phantom ETH)

Mise en place du relayer de transactions

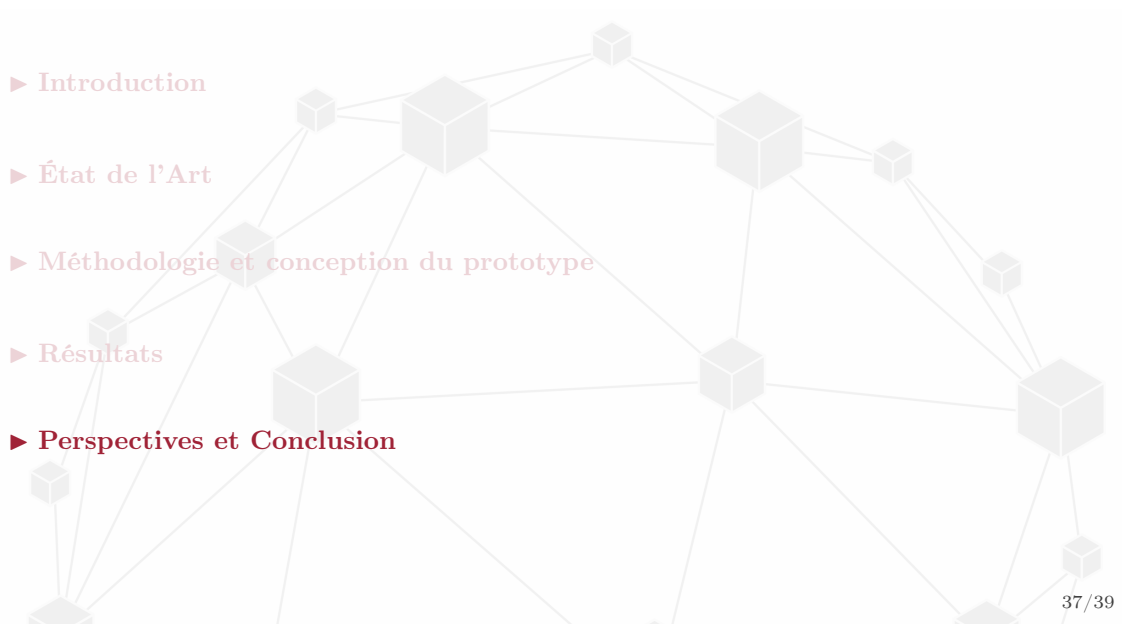
- Réception des informations du retrait
- Estimation des frais de gaz
- Signature de la transaction

- 
- A network diagram is overlaid on the slide, consisting of several gray 3D cubes connected by thin gray lines. The cubes are arranged in a complex, interconnected pattern across the slide, with some cubes being larger than others. The diagram serves as a background for the table of contents.
- ▶ Introduction
 - ▶ État de l'Art
 - ▶ Méthodologie et conception du prototype
 - ▶ **Résultats**
 - ▶ Perspectives et Conclusion

DÉMO

Caractéristiques	Phantom ETH	Tornado Cash
Fonctionnalités		
Anonymisation des transactions	✓	✓
Vérification KYC intégrée	✓	×
Whitelisting en cascade	✓	×
Support multi-denominations	×	✓
Technique		
Utilisation de zk-SNARK	✓	✓
Arbre de Merkle on-chain	✓	✓
Relayeurs décentralisés	×	✓
Nullifier hash	✓	✓
Conformité		
Conformité réglementaire	✓	×
Traçabilité KYC	✓	×
Protection vie privée	✓	✓
Expérience Utilisateur		
Interface simplifiée	✓	✓
Gestion des notes	✓	✓

Figure – Comparaison entre Phantom ETH et Tornado Cash

- 
- A network diagram is overlaid on the slide content. It consists of several gray 3D cubes of varying sizes connected by thin gray lines. The cubes are arranged in a non-linear fashion, with some acting as central hubs and others as peripheral nodes. The lines represent connections between these nodes, forming a complex web that spans the width and height of the slide.
- Introduction
 - État de l'Art
 - Méthodologie et conception du prototype
 - Résultats
 - Perspectives et Conclusion

- Support cross-chain
- Support de dénominations personnalisés
- Décentralisation du Relayeur
- Coût en Gaz

CONCLUSION