English Version

Proof of Concept Document – Anonymous and Decentralized Blockchain Project

Author: Théo Conte
Date of Birth: 10/01/2001
Place of Birth: Grenoble, France
Current Address: Villard-de-Lans, France
Date: 01/01/2025

Note: I speak and understand English very poorly. Please contact me in French for any inquiries or clarifications.

Project Overview

This blockchain project introduces an innovative architecture based on a hierarchical system of decentralized sub-blockchains. It aims to ensure maximum security, complete transaction anonymization, and modularity, allowing specific rules for each sub-blockchain. The primary objective is to create a system that is adaptable, scalable, and resistant to both large-scale attacks and quantum computing threats.

Disclaimer: This concept is currently theoretical but has been designed to be functional based on the proposed mechanisms. It is adaptable and can still be modified to enhance its security and efficiency further.

Sub-Blockchain Concept

Hierarchical Structure

- Each initial transaction is divided into smaller transactions that pass through **sub-blockchains**.
- These sub-blockchains communicate only with their "parent" blockchains, culminating in the main blockchain.
- The main blockchain handles proofs from sub-blockchains without revealing sender or receiver information.

Enhanced Security

- Miners in the sub-blockchains perform cryptographic proofs without accessing user data.
- Each sub-blockchain operates independently and can implement its own rules (e.g., fee management, validation speed, number of nodes required).

Role of Miners

- Miners are selected randomly and are periodically rotated to prevent centralization.
- They validate proofs based on their parent blockchains and local computations.
- Adding new miners involves a decentralized verification process through a collective consensus.

Transaction Anonymization

Pool and Mixer Usage

- A **transaction pool** collects multiple pending operations before processing.
- Transactions are randomly redistributed, preventing any miner or observer from linking a sender to a receiver.
- An integrated **mixer** ensures the fragmentation and recomposition of transactions randomly, achieving high anonymity.

No Personal Information Disclosure

- Miners and parent blockchains cannot access users' personal data.
- The system uses digital signatures and temporary identifiers for each transaction.

Security and Attack Resistance

Quantum-Safe Security

- The system uses post-quantum cryptography algorithms such as Dilithium and Kyber.
- These algorithms protect against quantum computer-based attacks.

Sub-Blockchain Robustness

- Breaking a sub-blockchain requires enormous computational power due to cryptographic isolation at each level.
- The resources needed to compromise the entire pyramid system are exponentially higher than for traditional blockchains like Bitcoin.

Benefits for States and Organizations

Financial Gains

- States and organizations adopting this system can earn royalties on transactions conducted within their sub-blockchains.
- By promoting widespread adoption, this could generate billions annually through microtransaction fees.

Modularity

- Each sub-blockchain can be customized according to user or institutional needs (e.g., compliance with local regulations or specific taxes).

Acknowledgments

I would like to thank **Micode**, **Hardisk**, and **Aypierre** for their inspiration. Their YouTube channels have been invaluable in understanding the importance of technological innovation and rigorous design in creating secure systems.

- https://www.youtube.com/channel/UCYnvxJ-PKiGXo_tYXpWAC-w
- https://www.youtube.com/@hardisk
- https://www.youtube.com/channel/UCA5sfitizqs1oEbB5KY4uKQ

Signature of the Author:
Théo Conte

Document de Preuve de Concept – Projet Blockchain Anonyme et Décentralisé

Auteur : Théo Conte
Date de naissance : 10/01/2001
Lieu de naissance : Grenoble, France
Adresse actuelle : Villard-de-Lans, France
Date : 01/01/2025

Note : Je parle et comprends très mal l’anglais. Merci de me contacter en français pour toute question ou précision.

Présentation du Projet

Ce projet de blockchain propose une architecture innovante basée sur un système hiérarchique de sous-blockchains décentralisées. L’objectif est de garantir une sécurité maximale, une anonymisation complète des transactions, et une modularité permettant des règles spécifiques pour chaque sous-blockchain.

Avertissement : Ce concept est actuellement théorique, mais il a été conçu pour être fonctionnel selon les mécanismes proposés. Il reste adaptable et peut encore être modifié pour renforcer sa sécurité et son efficacité.

Concept des Sous-Blockchains

Structure Hiérarchique

- Chaque transaction initiale est fragmentée en plusieurs petites transactions qui transitent par des **sous-blockchains**.
- Ces sous-blockchains communiquent uniquement avec leurs blockchains parentes, jusqu'à la blockchain principale.
- La blockchain principale gère uniquement les preuves des sous-blockchains sans divulguer les informations des expéditeurs ou des destinataires.

Sécurité Renforcée

- Les mineurs des sous-blockchains effectuent des preuves cryptographiques sans avoir accès aux données des utilisateurs.
- Chaque sous-blockchain a une structure indépendante et peut implémenter ses propres règles (exemple : gestion des frais, vitesse de validation, nombre de nœuds nécessaires).

Rôle des Mineurs

- Les mineurs sont sélectionnés de manière aléatoire et sont renouvelés périodiquement pour éviter toute centralisation.
- Ils valident les preuves basées sur leurs blockchains parentes et leurs propres calculs locaux.
- L'ajout de nouveaux mineurs passe par un processus de vérification décentralisé et consensuel.

Anonymisation des Transactions

Utilisation de Pools et Mixers

- Un **pool de transactions** regroupe plusieurs opérations en attente avant leur traitement.
- Les transactions sont redistribuées aléatoirement, empêchant tout mineur ou observateur de relier un émetteur à un destinataire.
- Un **mixer intégré** fragmente et recompose les transactions de manière aléatoire pour garantir un anonymat élevé.

Non-divulgation des Informations Personnelles

- Ni les mineurs, ni les blockchains parentes n'ont accès aux données personnelles des utilisateurs.
- Le système utilise des signatures numériques et des identifiants temporaires pour chaque transaction.

Sécurité et Résistance aux Attaques

Sécurité Quantique

- Le système repose sur des algorithmes de cryptographie post-quantique comme Dilithium ou Kyber.
- Ces algorithmes empêchent les attaques par des ordinateurs quantiques.

Robustesse des Sous-Blockchains

- Casser une sous-blockchain nécessite une puissance colossale due à l'isolement cryptographique entre chaque niveau.
- La quantité nécessaire pour compromettre tout le système pyramidal est exponentiellement supérieure à celle requise pour une blockchain classique comme Bitcoin.

Avantages pour les États et les Organismes

Gains Financiers

- Les États et organisations adoptant ce système pourront percevoir des redevances sur les transactions effectuées dans leur sous-blockchain.
- Une adoption massive pourrait générer des milliards d'euros chaque année grâce aux microfrais appliqués.

Modularité

- Chaque sous-blockchain peut être personnalisée en fonction des besoins des utilisateurs ou des institutions (par exemple : respect des réglementations locales ou imposition spécifique).

Remerciements

Je tiens à remercier **Micode**, **Hardisk**, et **Aypierre** pour leur inspiration. Leurs chaînes YouTube m'ont permis de mieux comprendre l'importance de l'innovation technologique et de la rigueur dans la conception de systèmes sécurisés.

- https://www.youtube.com/channel/UCYnvxJ-PKiGXo_tYXpWAC-w
- https://www.youtube.com/@hardisk
- https://www.youtube.com/channel/UCA5sfitizqs1oEbB5KY4uKQ

Signature de l'Auteur :
Théo Conte