IAO CRYPTO 2024

HASH FONCTION

Présenté par :

- EL FID NOUHAILA
- LEFORT Nomenjanahary Nuno

PLAN

Table de contenu

HISTOIRE

Contexte Historique

INTRODUCTION

C'est quoi fonction de hashage?

Correspondre un donnée taille variable en valeur numérique taille fixé, appelée HASH ou HACHE !

CARACTERISTIQUE HASH

DÉTERMINATION

UNIFORMITÉ

EFFICACITÉ

PRÉ-IMAGE RÉSISTANTE

RÉSISTANCE À LA SECONDE PRÉ-IMAGE

COLLISION

DIFFUSION

TAILLE FIXE

INTRODUCTION

ALGO POPULAIRE

MD5(Message Digit Algorithm 5)

SHA-256 (Secure Hash Algorithm 256bits)

BCRYPT

ARGON 2

UTILISATION

Verification integrite données

Extraction et stockage efficace données

Verification authenticite données

ATTAQUE - CONSEQUENCE

Attaques par Collision

Alteration données

Attaques par Dictionnaire

Perte de confiance

ATTAQUE - CONSEQUENCE

Force Brute

Violation intégrité

Attaques par Birthday

Révocation de certificats numériques

ATTAQUE - CONSEQUENCE

Attaques de Déni de Service

Compromission des protocoles cryptographiques

Avantage

INTÉGRITÉ DES DONNÉES

IDENTIFICATION UNIQUE

EFFICACITÉ

PROTECTION DES MOTS DE PASSE

COMPATIBILITÉ

QUESTION

Les fonctions de hachage sont-elles suffisantes pour la cryptographie ?

NON !

THYNK UNLIMITED

WHY?

Vulnérabilités aux Attaques

Limites Structurelles

Faiblesses dans la Pratique

APPLICATION

CRYPTO MONNAIES

BITCOIN

BITCOIN

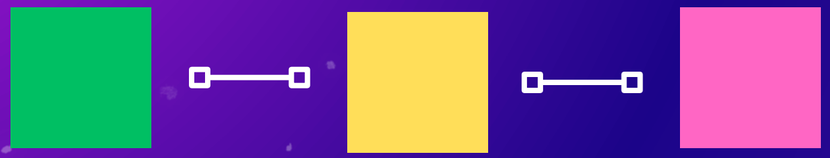
SHA-256

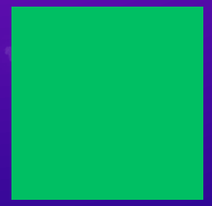
BLOCKCHAIN

ARBRE DE MERKLE

BITCOIN

BlockChain

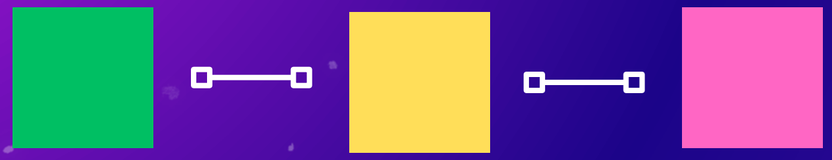


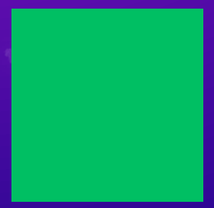


- Données Bitcoin: {De: A: Montant:}
- Hash block actuel
- Hash block précédent

BITCOIN

BlockChain





→ Données Bitcoin: {De: A: Montant:}

→ Hash block actuel

→ Hash block précédent

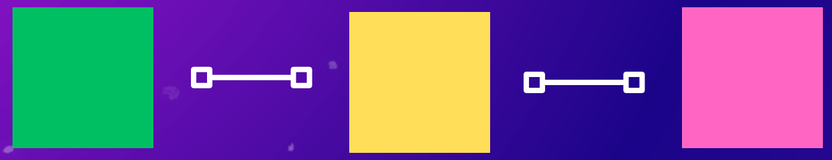
X6Y3

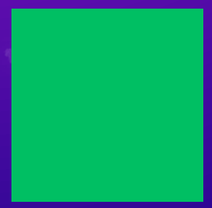
Hash: 1ZEF Hash: 6SDE Hash: Q95Z

PH0: 0000 PH1: 1ZEF PH2: 6SDE

BITCOIN

BlockChain





→ Données Bitcoin: {De: A: Montant:}

→ Hash block actuel

→ Hash block précédent

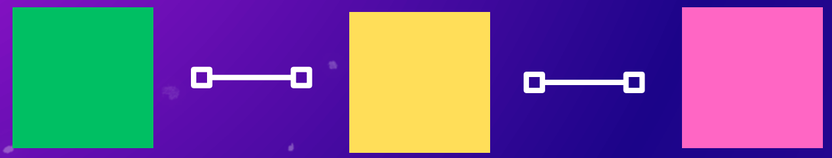
X6Y3

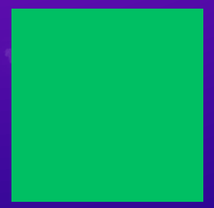
Hash: 1ZEF Hash: ~~6SDE~~ Hash: Q95Z

PH0: 0000 PH1: 1ZEF PH2: 6SDE

BITCOIN

BlockChain





→ Données Bitcoin: {De: A: Montant:}

→ Hash block actuel

→ Hash block précédent

X6Y3

Hash: 1ZEF Hash: ~~6SDE~~ Hash: Q95Z

PH0: 0000 PH1: 1ZEF PH2: 6SDE

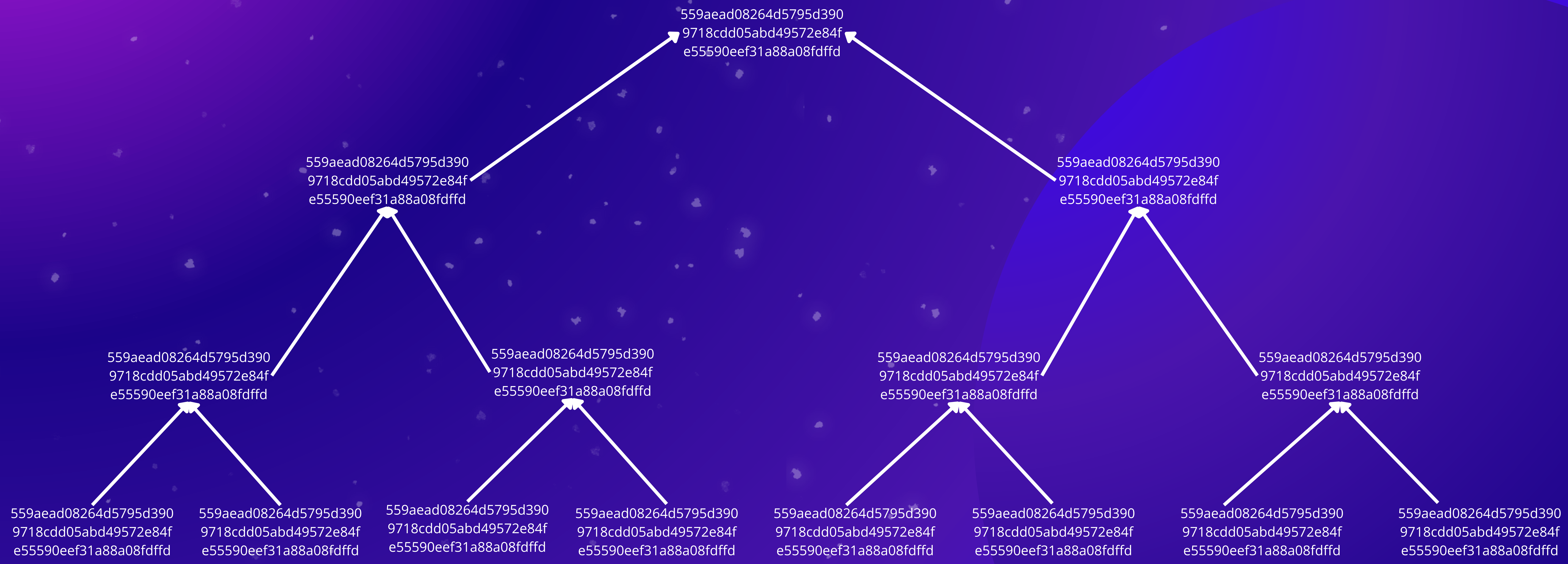
SOLUTION

PROOF OF WORK
10MIN/BLOCK

DISTRIBUTION
P2P NETWORK

BITCOIN

Arbre de Merkle



BITCOIN

Racine de Merkle

COMPLEXITE

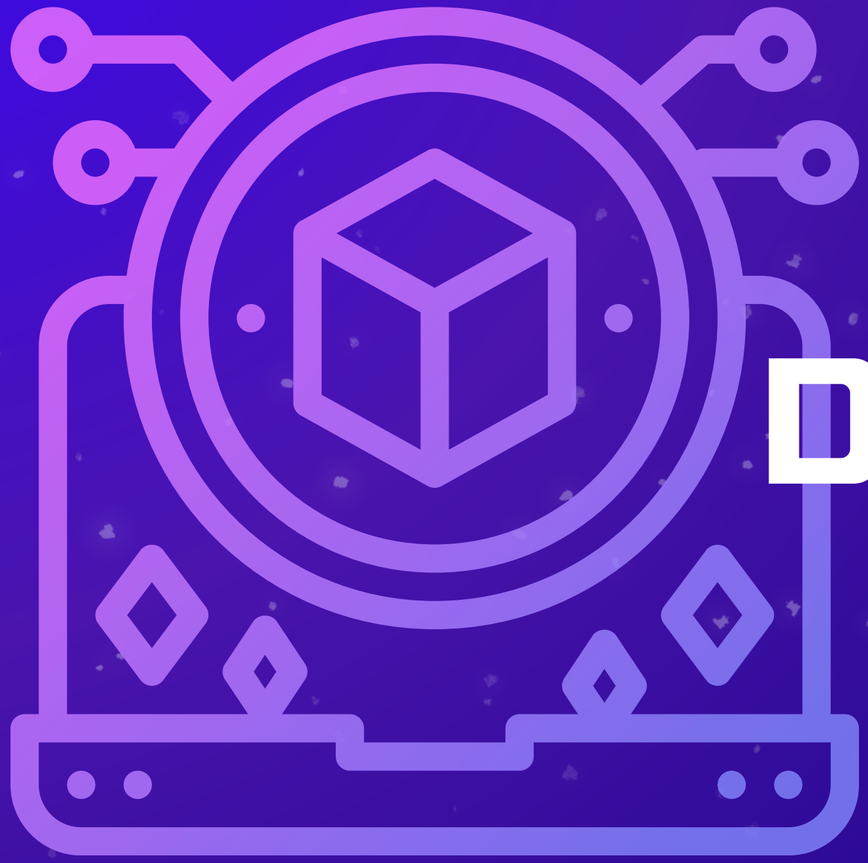
MD5 : 320 ns – 128 bytes

SHA-256 : 600 ns –256 bytes

BCRYPT: 4kb – 8kb

ARGON 2: 64 kb

DEMONSTRATION



DEMONSTARTION

CONCLUSION

QUESTIONS

DES QUESTIONS ?