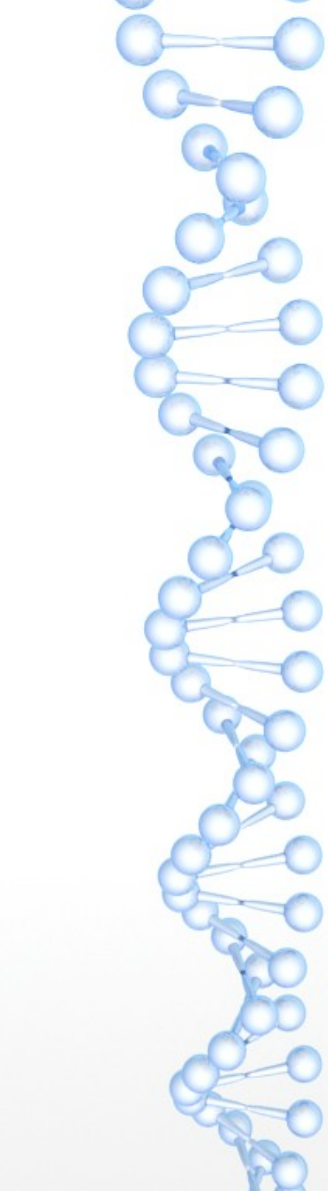
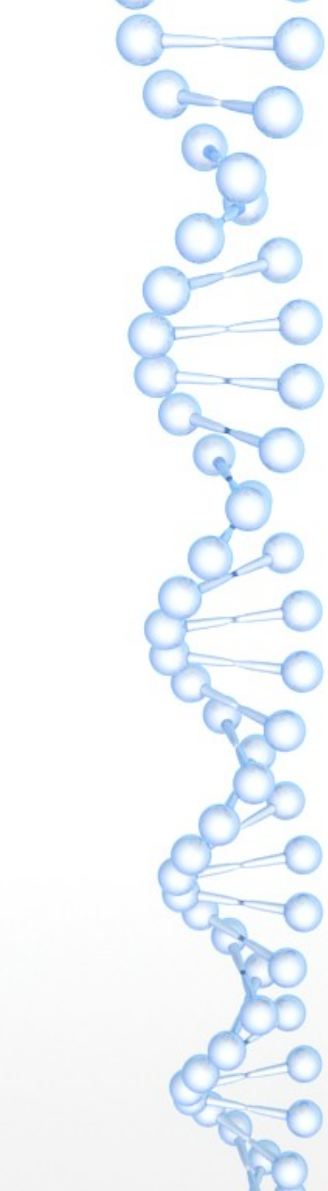


La Cryptographie dans la Ğ1

Tout ce que vous avez voulu savoir sur la Cryptographie dans la June sans jamais oser le demander !

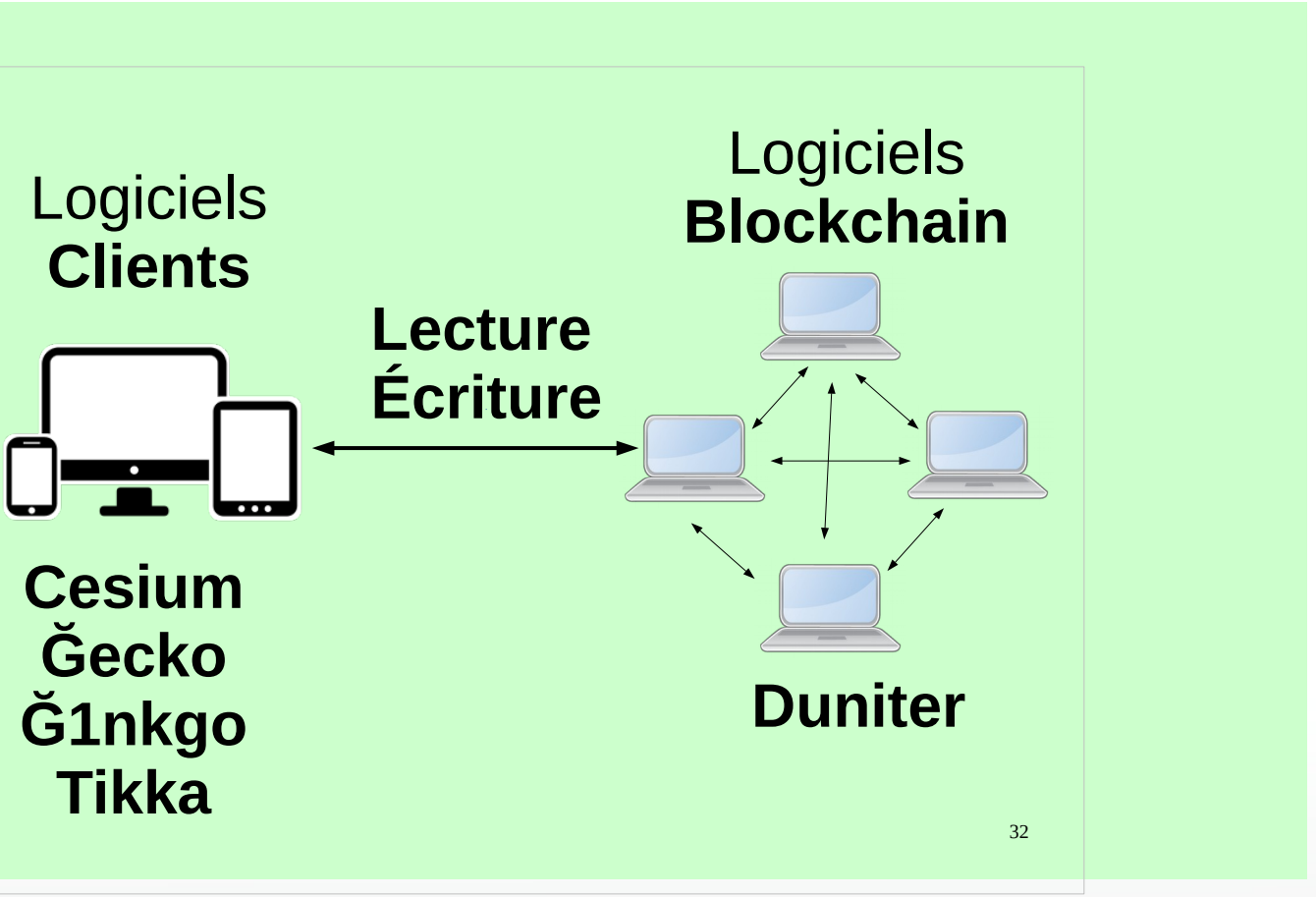


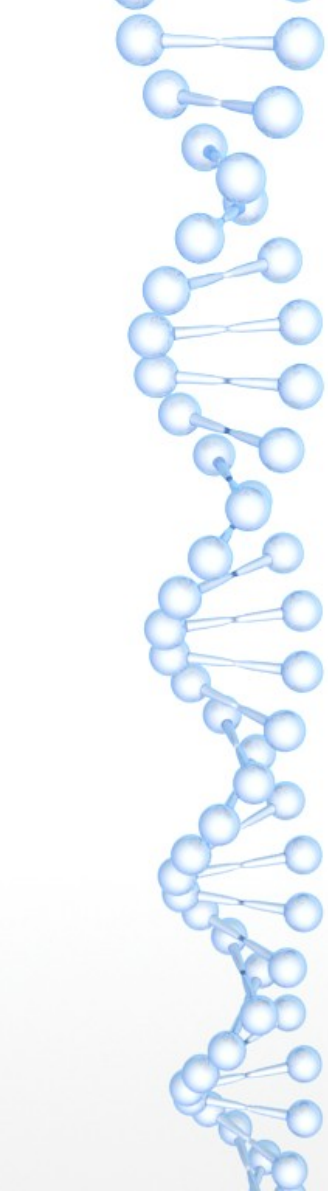
- La June est une **Crypto- Monnaie**.

- Les comptes et virements sont stockés dans une ***Blockchain.***

- **Blockchain :** grand livre des transactions stocké sur le « réseau des logiciels **Duniter** »

- Les logiciels « clients » lisent et écrivent dans la **Blockchain** en communiquant avec **Duniter**.

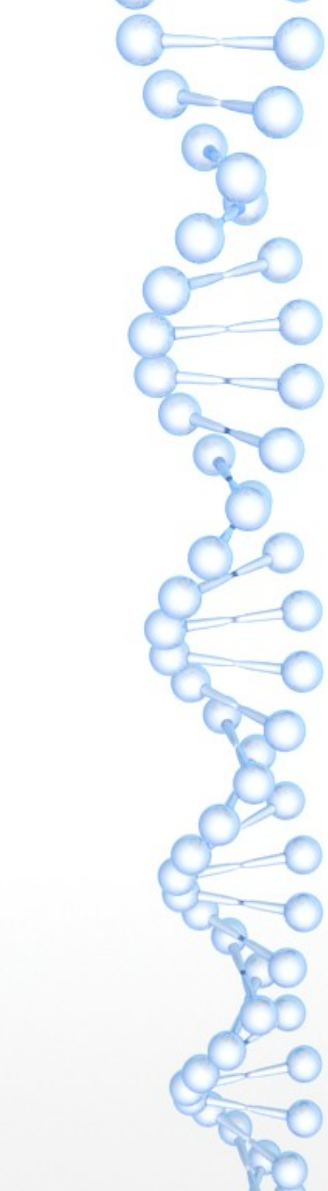

Logiciels
Clients
Logiciels
Blockchain
Lecture
Écriture
Cesium
Ğecko
Ğ1nkgo
Tikka
Duniter
32



• Pour communiquer avec **Duniter**, les logiciels clients envoient des **commandes**.

• Les logiciels clients peuvent lire le contenu de la **Blockchain** qui est **publique**.

• Les **commandes** de **lecture** ne nécessitent pas de sécurité particulière.

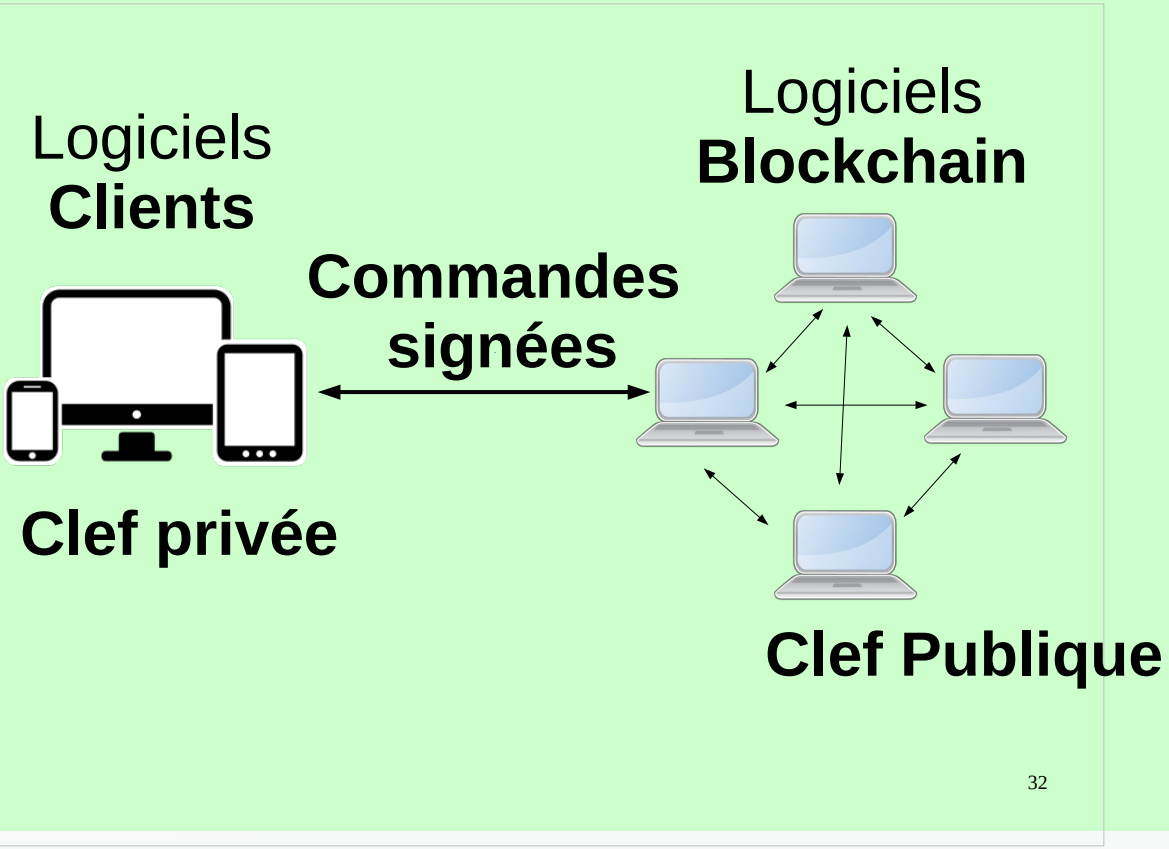


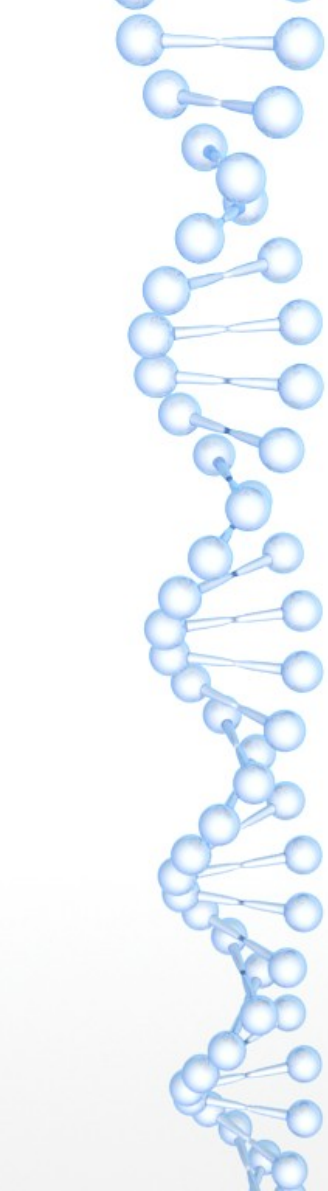
• Pour **écrire** dans la **Blockchain**, il faut envoyer des commandes « **signées** » à **Duniter**.

• C’est là que la **Cryptographie** intervient.

• On utilise des « **Trousseaux de Clefs Cryptographiques** ».

• **Trousseau de Clef Cryptographiques** :
2 Clefs (**Clef Privée** + **Clef Publique**)


Logiciels
Clients
Logiciels
Blockchain
Commandes
signées
Clef privée
Clef Publique
32

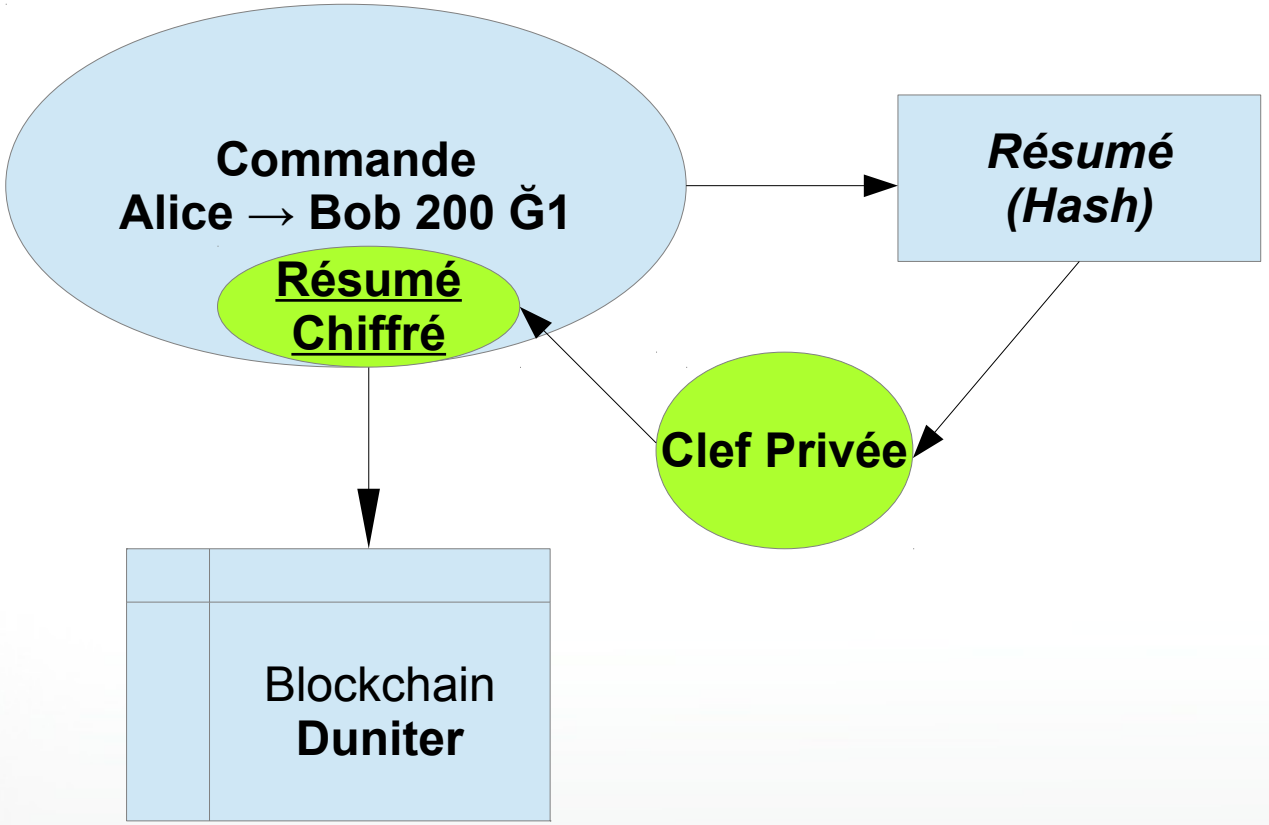


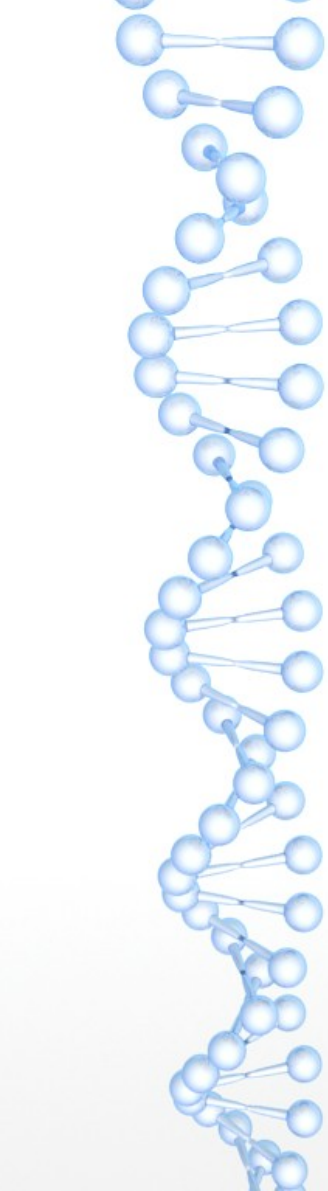
• **Signature :** résumé (**Hash**) d’un message, chiffré avec une **Clef Privée**.

• **Message :** *Virement de Alice → Bob de 200 Ğ1*
• **Résumé :** *a2f56ghU8uHAg45klm6*
• **Signature :** *bh73f74d5e263d4f78924dc*

•**Message signé** envoyé à **Duniter :**
Virement de Alice → Bob de 200 Ğ1
bh73f74d5e263d4f78924dc

Signature de commande





- **Vérification de Signature** par **Duniter :**

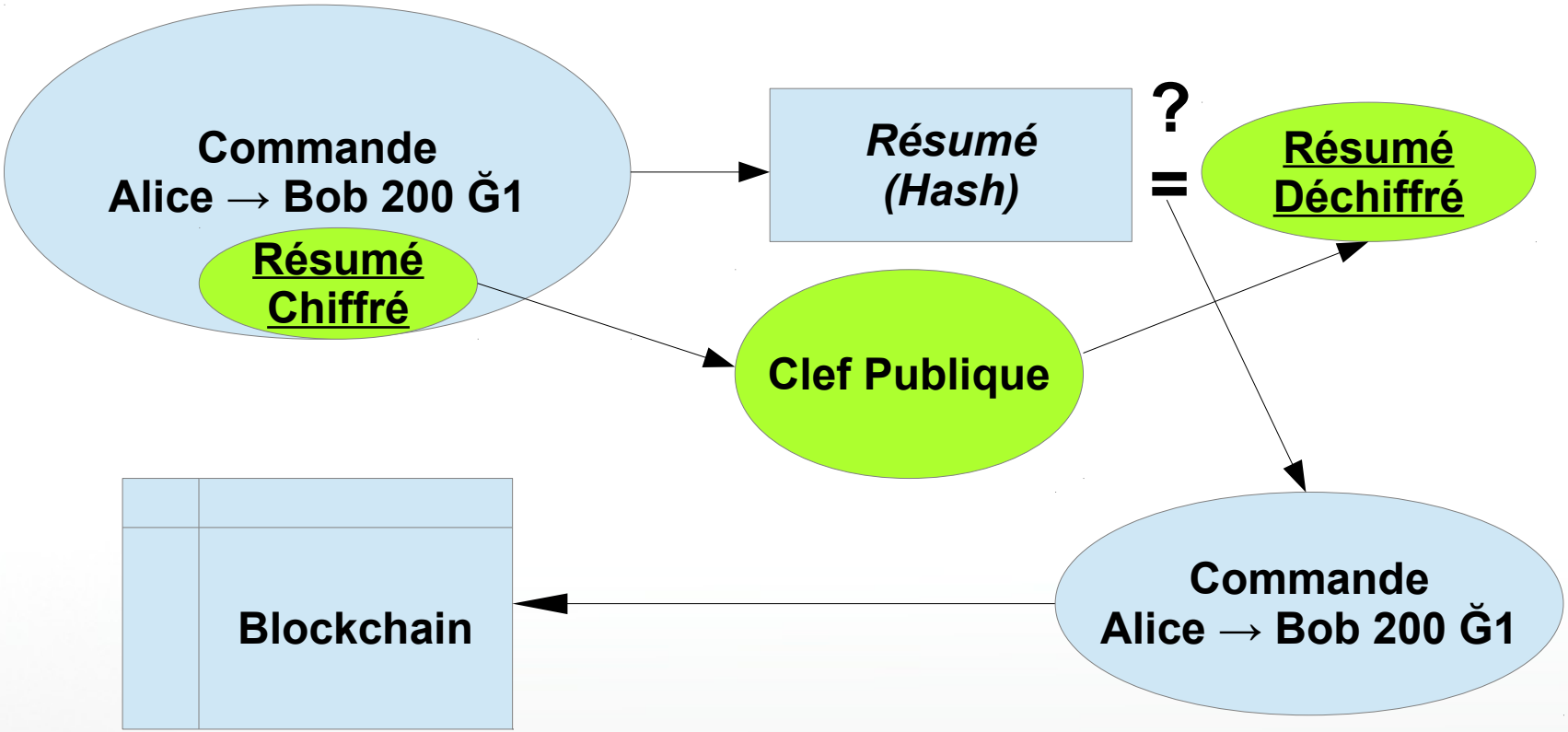
- Déchiffrer le **Résumé** avec la **Clef Publique**.

- Si réussite, alors l’auteur du message est bien le possesseur de la **Clef Privée**.

- **Duniter** génère aussi le **Résumé** du message.

- **Résumé Duniter = Résumé déchiffré ?**

Vérification de Signature par Duniter



Création d’un Trousseau de Clef

• **Phrase de récupération :** suite de 12 mots **UNIQUE** générée par le logiciel client.

`bottom drive obey lake curtain smoke basket hold race lonely fit walk`

• L’utilisateur doit noter, et protéger sa **Phrase** qui doit rester **privée**.

Création d’un Trousseau de Clef

• Génération d’une **Graine (seed) unique** à partir de la **Phrase de Récupération.**

`fac7959dbfe72f052e5a0c3c8d6530f202b02fd8f9f5ca3580ec8deb7797479e`

• Le logiciel doit protéger la **Graine** qui doit rester **privée**.

Création d’un Trousseau de Clef

• Génération d’une **Clef Privée unique** à partir de la **Graine.**

??????????????????????????????

• Le logiciel doit protéger la **Clef Privée** qui doit rester **privée**.

Création d’un Trousseau de Clef

• Génération d’une **Clef Publique unique** à partir de la **Clef Privée.**

`46ebddef8cd9bb167dc30878d7113b7e168e6f0646beffd77d69d39bad76b47a`

• Le logiciel doit afficher la **Clef Publique** pour les humains afin d’identifier le compte.

Création d’un Trousseau de Clef

- Encodage de la **Clef Publique** en une **Adresse de Compte unique.**

5DfhGyQdFobKM8NsWvEeAKk5EQQgYe9AydgJ7rMB6E1EqRzV

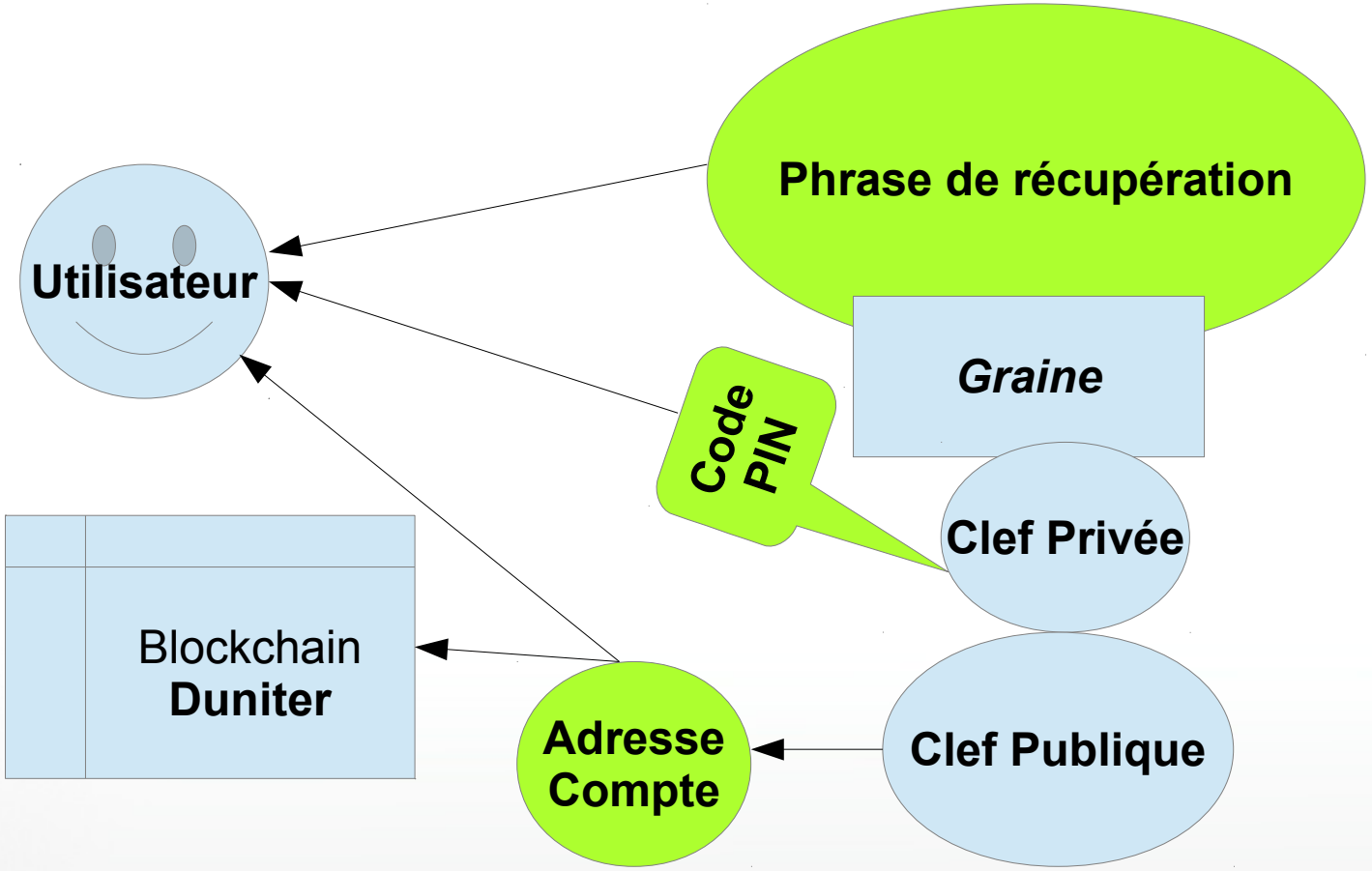
Stocker et Protéger la Clef Privée

• Chiffrement de la **Clef Privée** avec un **CODE PIN.**

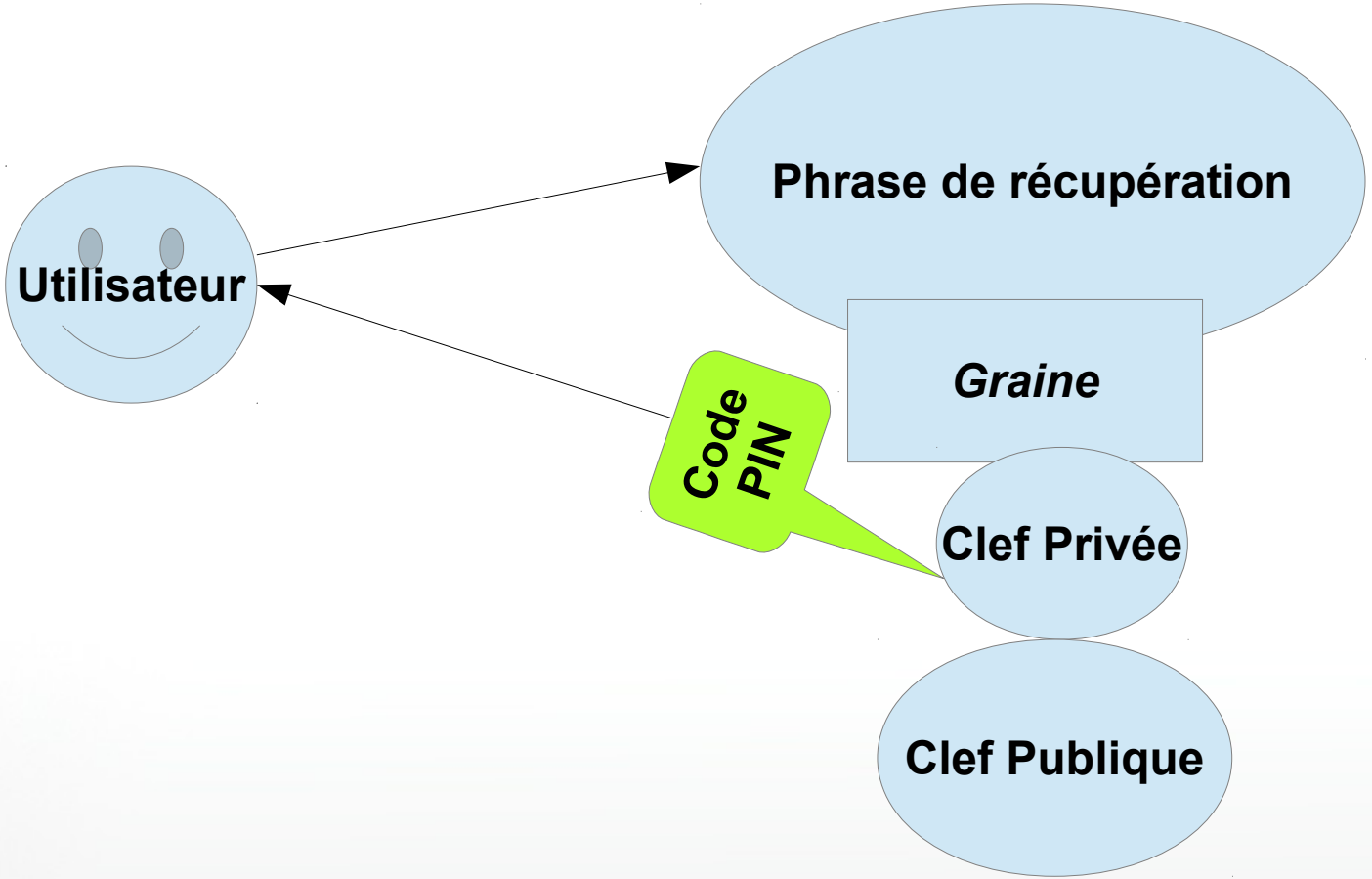
• **La Clef Privée** est stockée **chiffrée.**

• **Impossible d’utiliser la Clef Privée sans le CODE PIN !**

Création de Compte



Récupération du Compte



Coffre Fort et Comptes Dérivés

- **Compte Racine** : un Compte généré seulement avec la **Phrase de Récupération**.

- **Compte Dérivé** : un Compte généré par la **Phrase de Récupération** suivi d'un **Chemin de Dérivation**.

Coffre Fort et Comptes Dérivés

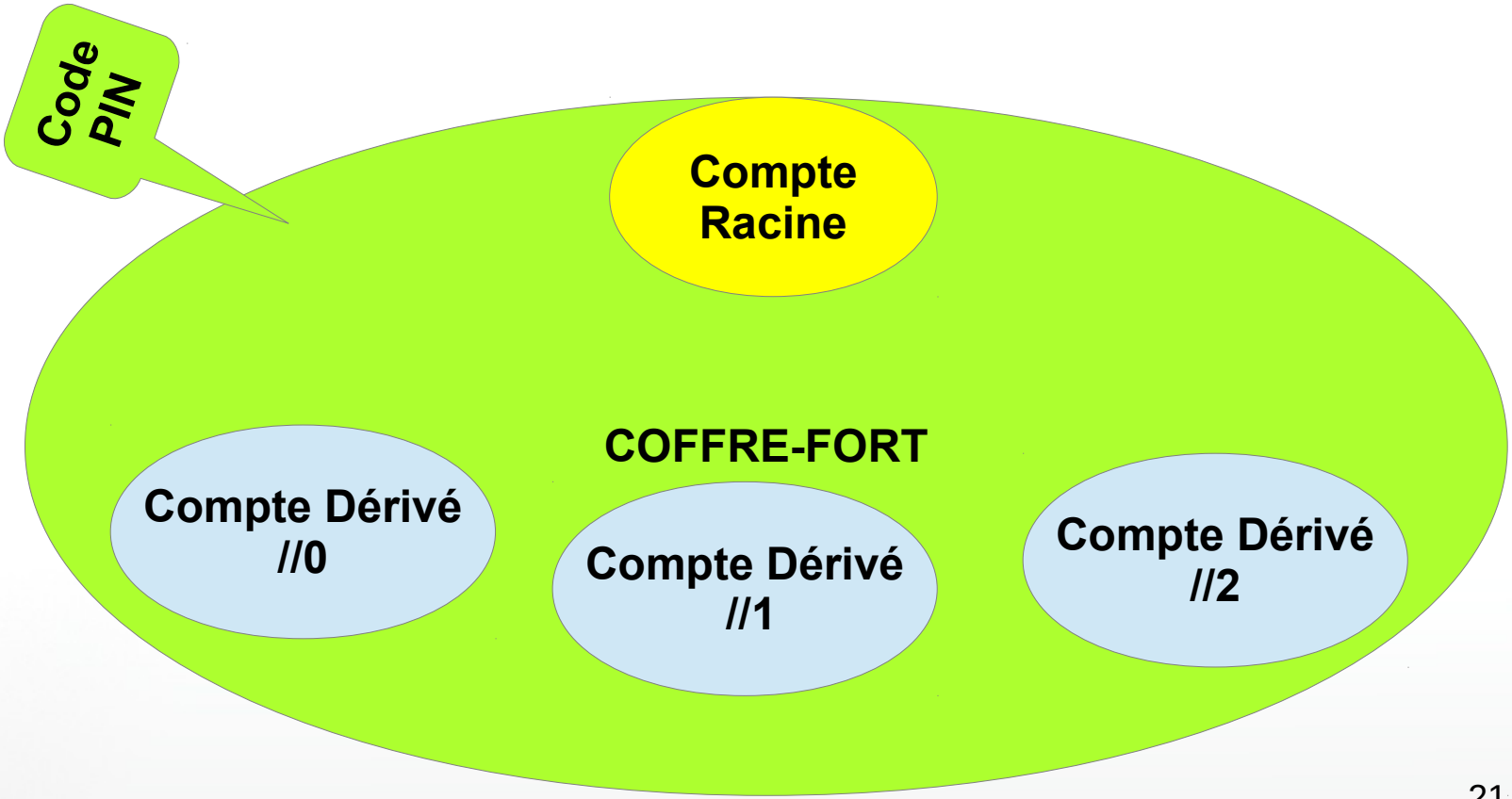
- **Phrase de Récupération d'ALICE :** suite de 12 mots **UNIQUE** suivi par le chemin //ALICE.

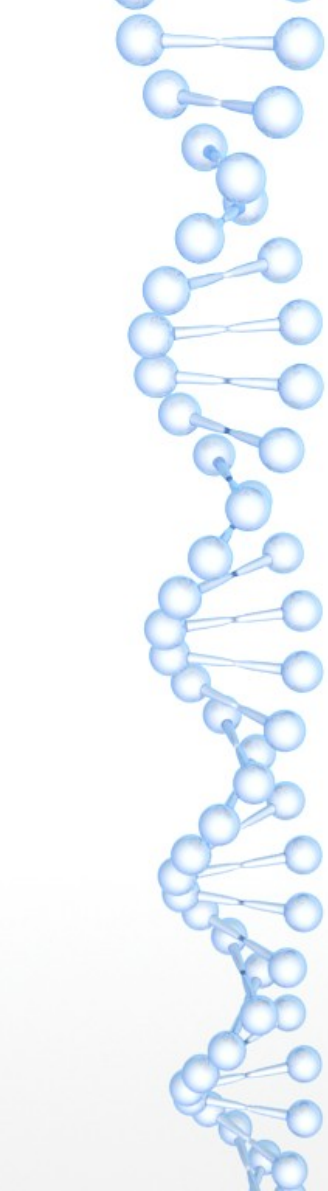
```
bottom drive obey lake curtain smoke basket hold
race lonely fit walk//Alice
```

- Nouvelle **Graine, Clef Privée, Clef Publique**.

- **Duniter** utilise des **Chemins de Dérivation** simples sur un chiffre : //0, //1, //2, etc...

Un **Coffre-Fort** est l'ensemble des comptes issus d'une même **Phrase de Récupération**





La Cryptographie dans la Ğ1

Merci de votre attention !

Merci à **Maaltir** pour le résumé de cryptographie et à **Nicolas80** pour les exemples !

Présentation créée par Vit, Mai 2025.