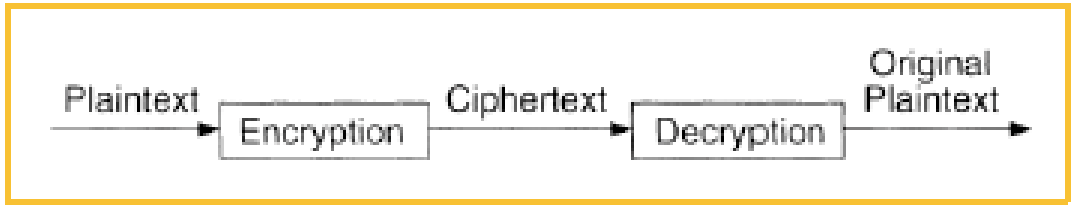
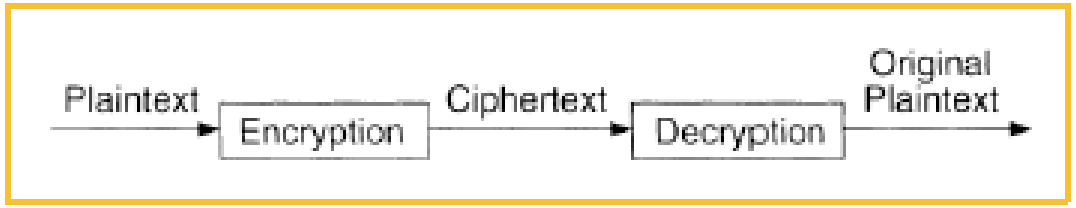
Cryptographie



Cryptographie



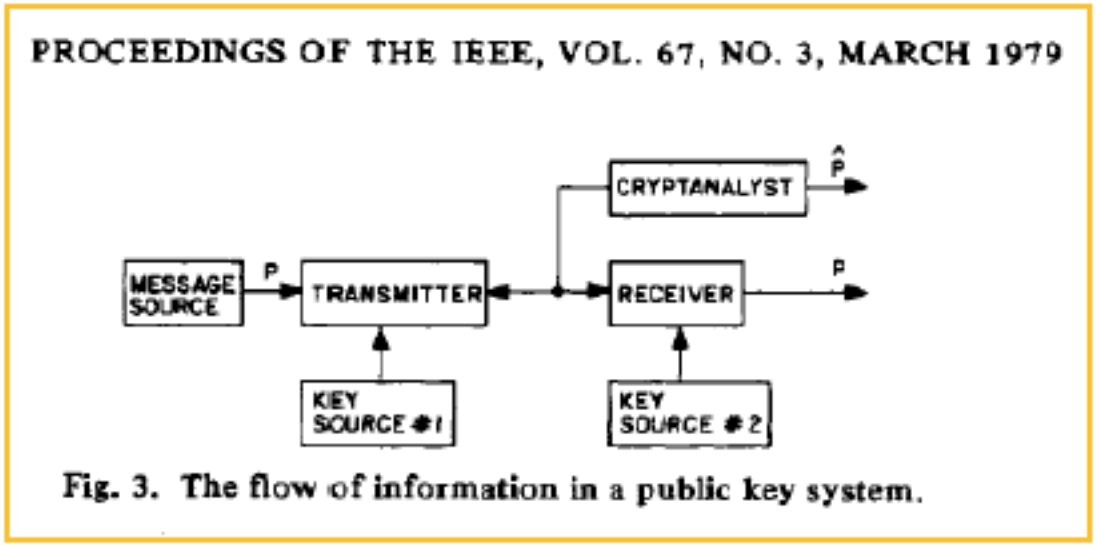


Fig. 3. The flow of information in a public key system.

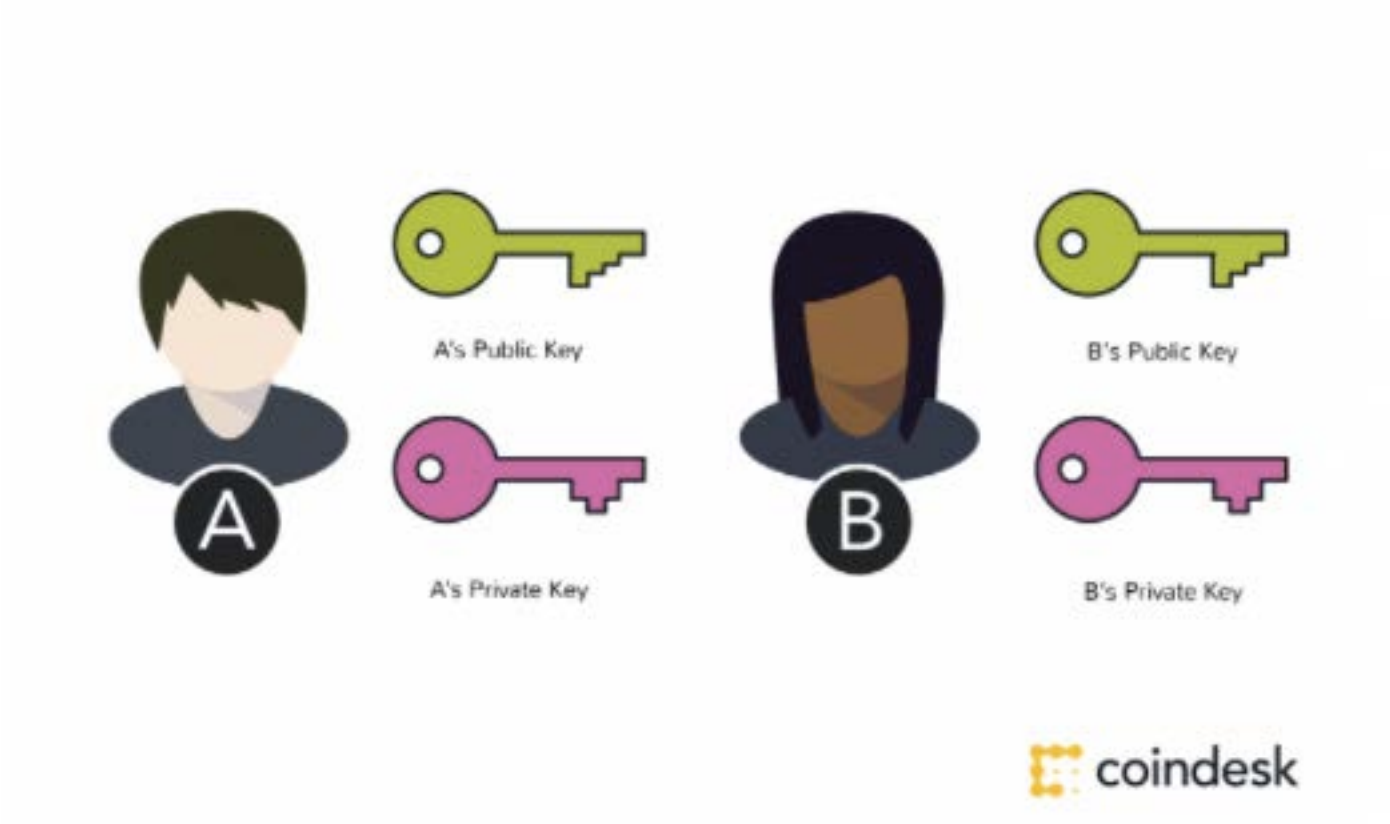
Chiffrement à clé publique

coindesk


http://coindesk.com
https://coindesk.com
SSL
certificate

Les tiers, des failles de sécurité

Chiffrement à clé publique



Règlement général sur la protection des données de l'Europe

- Très grande portée

Par « données personnelles », on entend toute information relative à une personne, que ce soit sur le plan personnel, professionnel ou public. Il peut s'agir d'un nom, d'une adresse domiciliaire, d'une photographie, d'une adresse électronique, d'information bancaire, de billets sur des sites Web de réseaux sociaux, de renseignements médicaux ou de l'adresse IP d'un ordinateur.

- Ce règlement s'applique aux entreprises établies en Europe et à toute entreprise dont les activités se rapportent à la définition des renseignements personnels des citoyens européens.

Règlement général sur la protection des données de l'Europe

- La bonne nouvelle

Protection de la vie privée par défaut ou dès la conception :

Il faut effectuer les activités de chiffrement et de déchiffrement localement et non au moyen d'un service à distance, car les clés et les données doivent demeurer sous le contrôle du responsable des données afin qu'on parvienne à assurer quelque protection que ce soit des renseignements.

Règlement général sur la protection des données de l’Europe

- La bonne nouvelle

Si le contrôleur de données assure le pseudonymat des données personnelles au moyen de politiques et mesures internes appropriées, on estime qu’elles sont rendues adéquatement anonymes et ne sont donc pas sujettes aux contrôles et peines du GDPR.

LPRPDE

- Harmonisée sur la législation européenne sur la protection des renseignements personnels.

Loi des É.-U.

- La liberté contractuelle

Non réglementée; on croit que les fournisseurs et consommateurs du marché libre choisiront le support le plus approprié.

Bitcoin

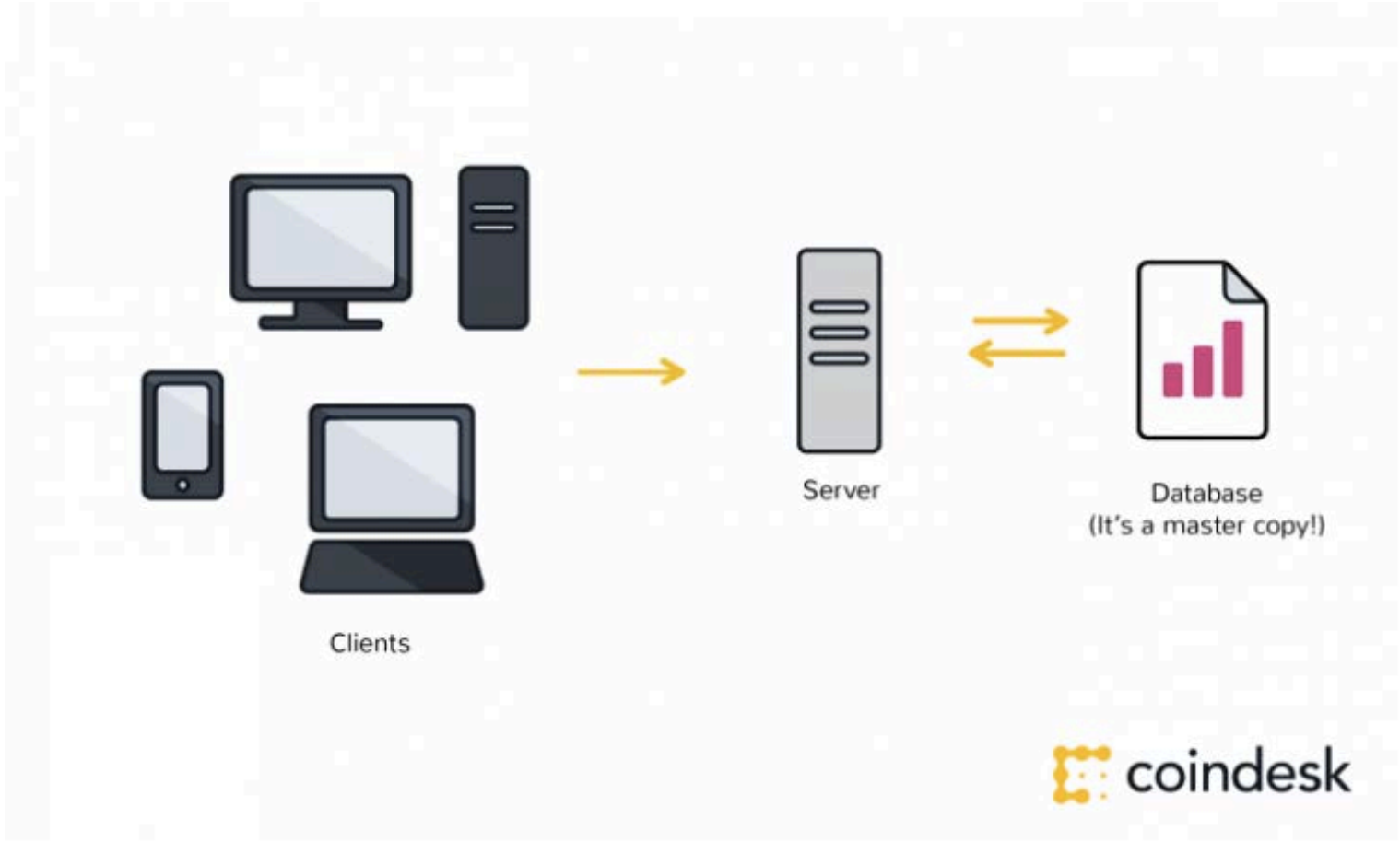
Bitcoin a entraîné la création d'un marché de portefeuilles numériques qui servent à gérer, à stocker et à générer des clés cryptographiques.

Authentification et autorisation

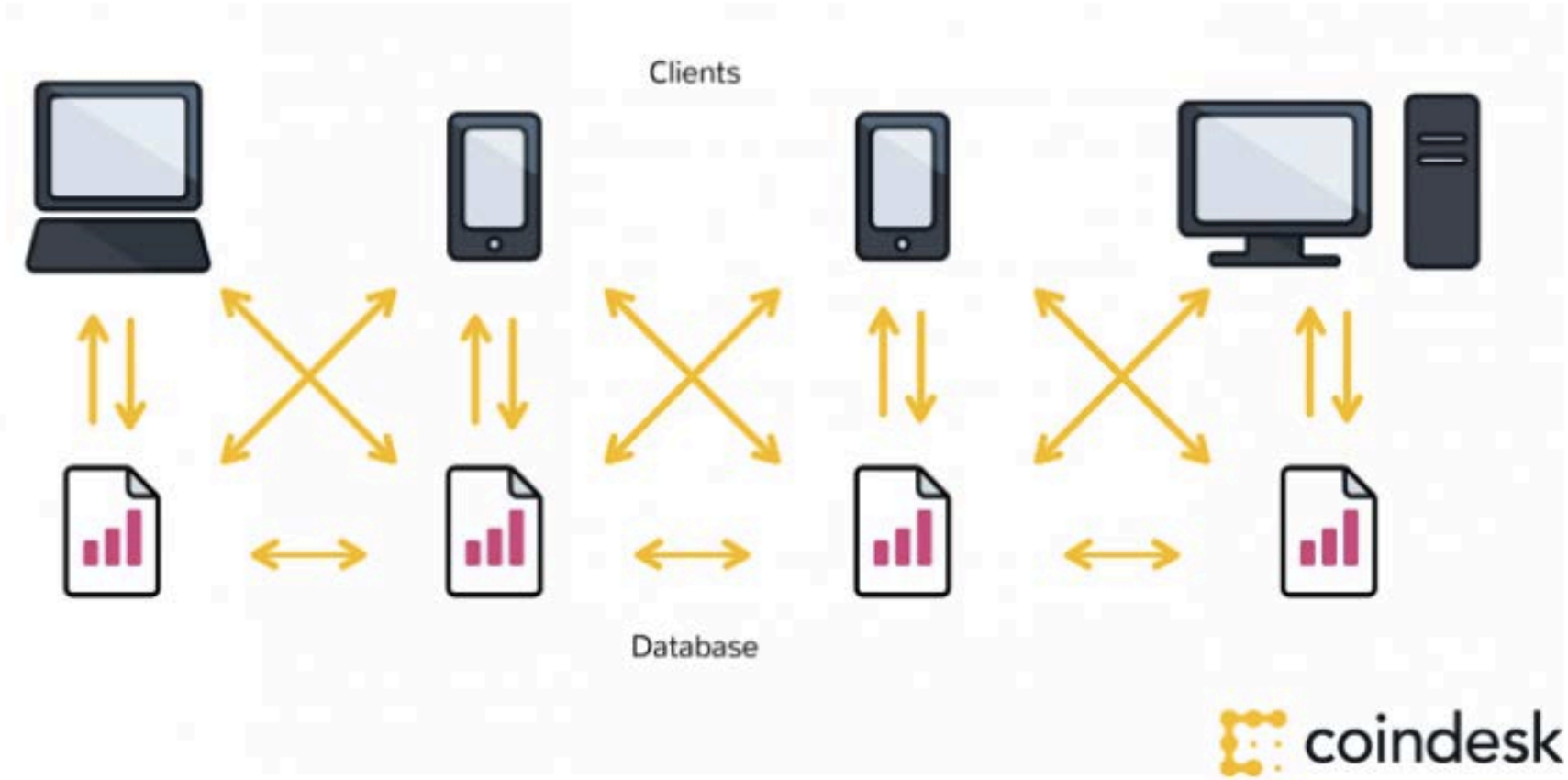
Créer et sécuriser des liens numériques

Réseau pair-à-pair

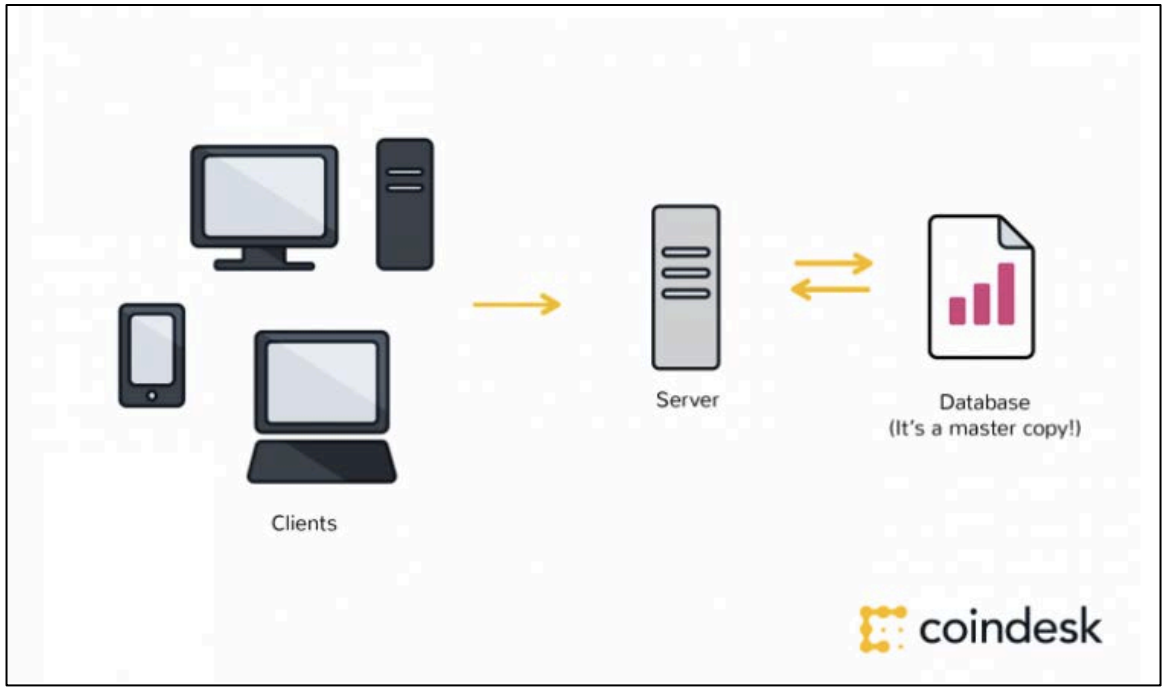
Fonctionnement actuel de l’Internet



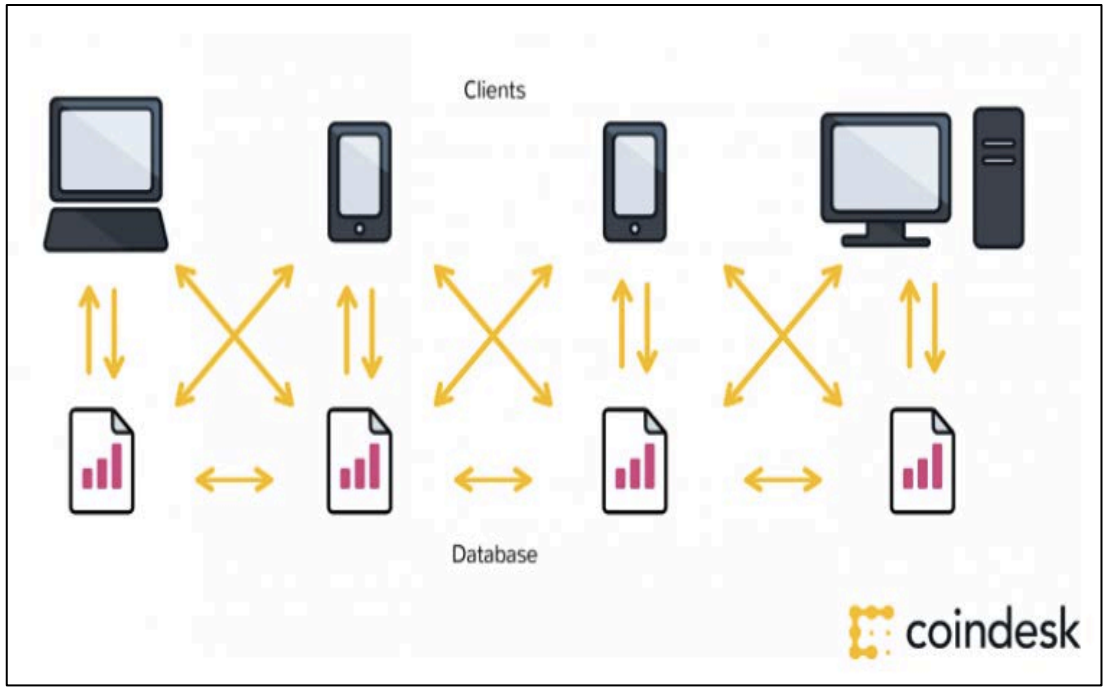
Réseau pair-à-pair



Réseau pair-à-pair

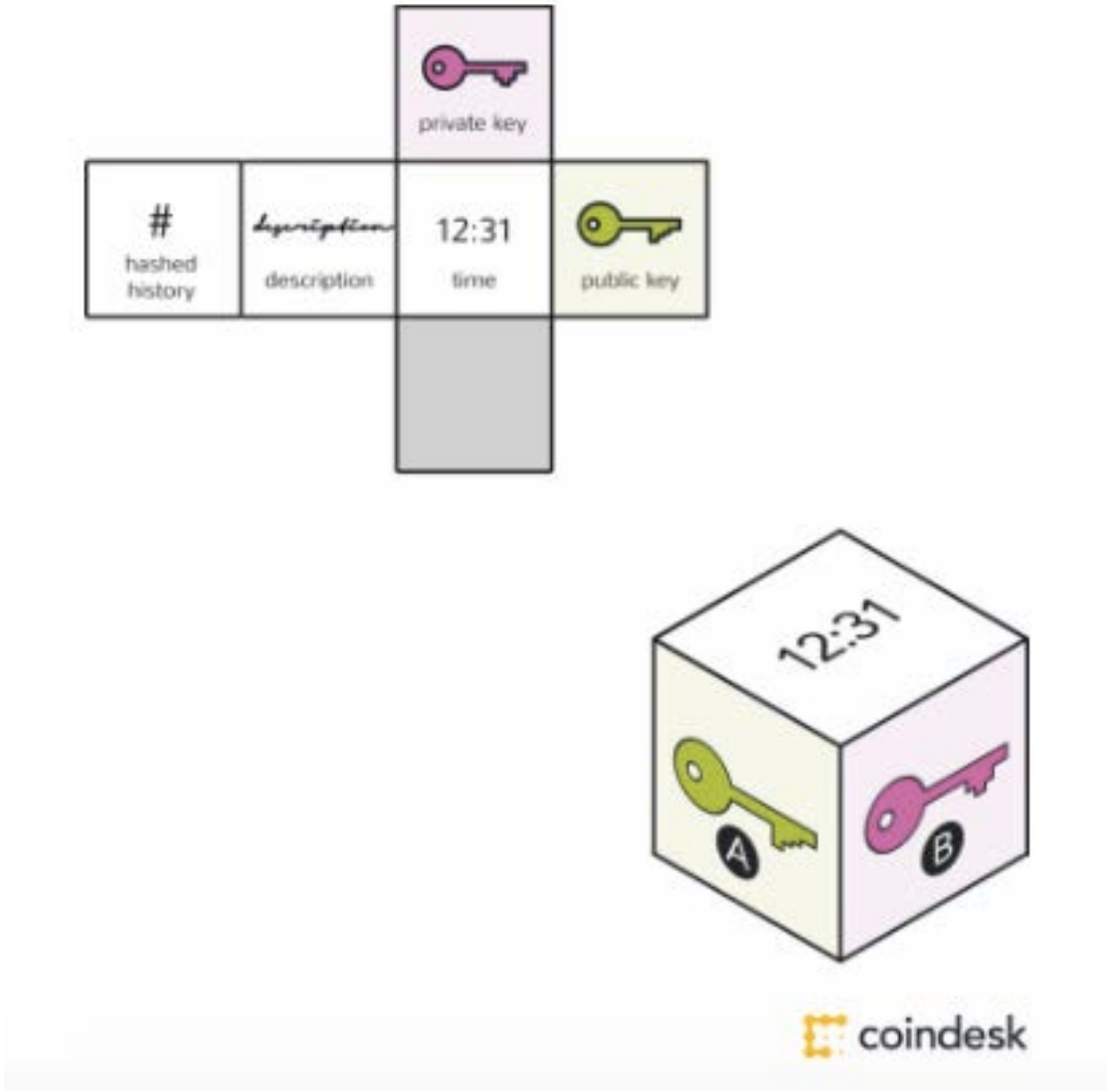


ou

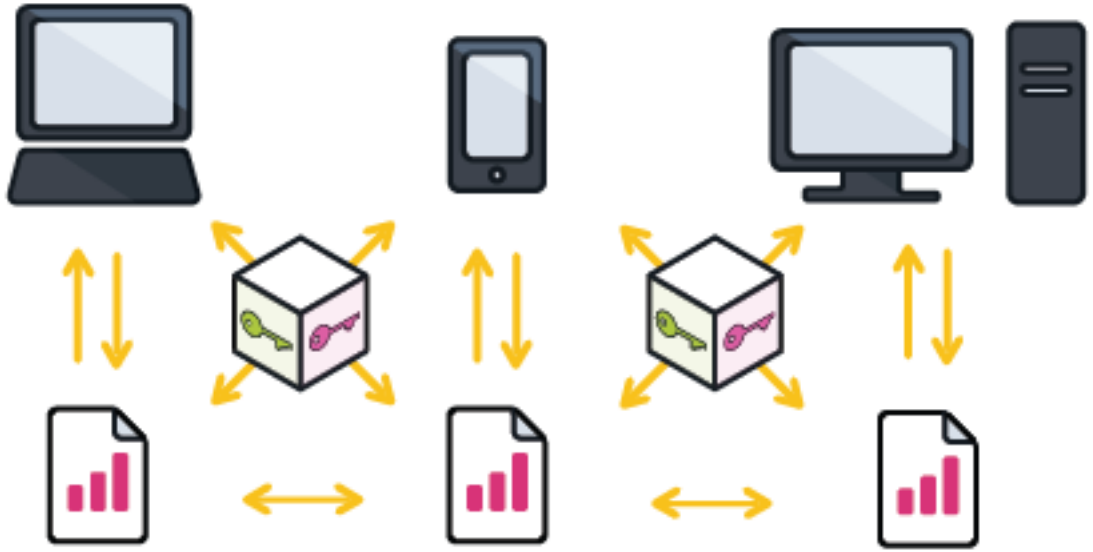


Autorisations

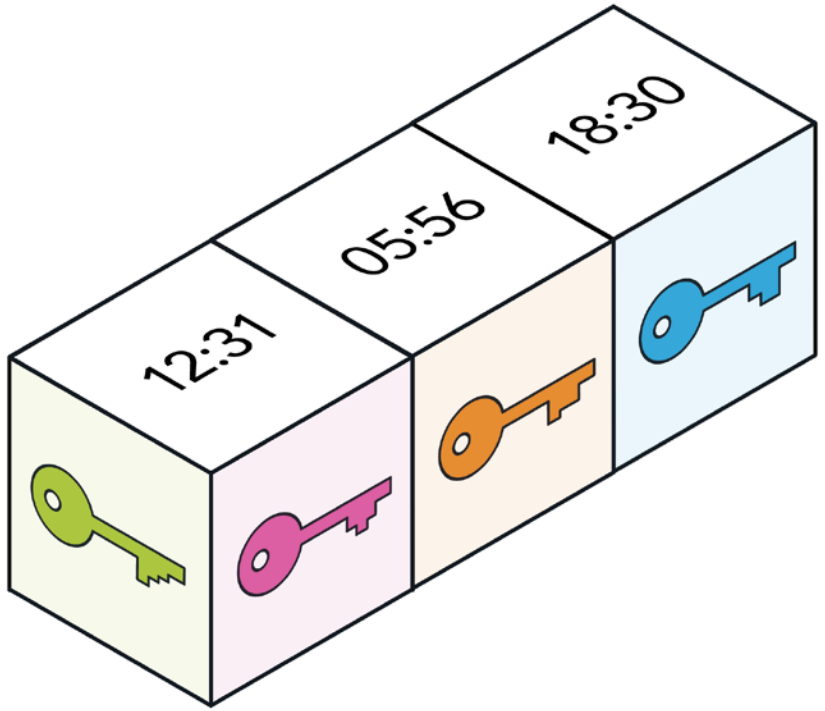
Autorisations



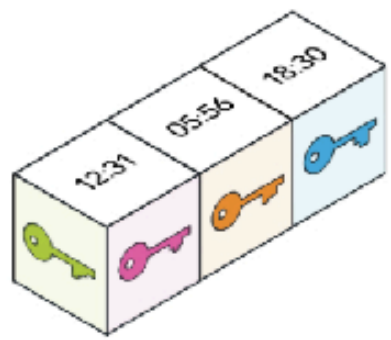
Autorisations



Chaîne de blocs



Blockchains are built from 3 technologies		
1. Public Key Cryptography	2. P2P Network	3. Program (the blockchain's protocol)
Cash vs. Plastic	Tree falls in a forest	Tragedy of the commons
Identity	System of Record	Platform



Conclusions

Chiffrement pour les particuliers et les machines

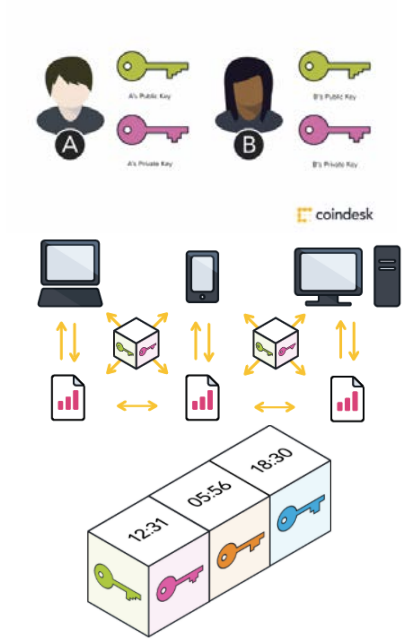
- Aucun tiers, respect de la protection des renseignements personnels

Sécurité décentralisée

- Absence de point de défaillance central

Créer et sécuriser des liens numériques

- Utile pour les particuliers et les machines



Mesures que le gouvernement peut prendre

Savoir quand ne pas constituer une autorité de certification.

- L'ajout même d'une AC pourrait compromettre le système.

Étudier la sécurité dès la conception

- Envisager l'adoption de matériel de chiffrement robuste.

Ne pas soumettre les outils de chiffrement préservant la protection des renseignements personnels au règlement à ce sujet.

- Le modèle opérationnel utilisé dans la plupart des transactions de chaînes de blocs publiques sert à limiter « l'aire d'exposition ».

Apprendre à vérifier le code fiduciaire.

- C'est-à-dire de parler aux cryptographes, à savoir les pirates.

Servir de nœud, traiter les cryptomonnaies et participer aux discussions de Codebase.