Properties of BlockChains : Security and vulnerabilities

> **Resources :**
> - Satoshi White Paper 2008-1.pdf
> - White Paper Bitcoin traduit en Français par COIN24.pdf
> - Session 1 (2026) Introduction to Blockchain.pptx
> - Session 2 (2026) Crypto Assets.pptx

Why security is important :

- If there is value, there are criminals

Some report can be found at Chainalysis - forensics company specialized in blockchains.

Ransomware are way older than I thought. The first one were paid in dollars send to a postal box.

La blockchain est un registre distribué (*distributed ledger*)

La blockchain = des registres d'activité sur un compte. chaque page conserve les transactions et le solde. La page suivante contiendra le solde de la page précédente etc.

Avec les sites https://www.blockchain.com/explorer/ et https://etherscan.io/ il est possible de retracer les transactions de n'importe quel portefeuille de crypto (ETH et BTC). La **transparence** semble être au cœur de la blockchain.

Il est possible de tracker en mettant en commun les informations. Pour éviter cela, des entreprises ou des bloc dédié permettent d'obfusquer les transactions.

Pour chaque BTC ou ETH il y a des subdivisions pour être plus précis notamment dans les frais.

Pour le BTC, lors d'une transaction c'est en fait la totalité du solde qui est transmis, la partie à payer est soustraite puis le reste est renvoyé au portefeuille d'origine.

C'est comme le rendu monnaie au supermarché. On donne plus et le reste nous est rendu. Le but est d’empêcher la double dépense et contrôler que le portefeuille dispose bien des fonds.

Sécuriser une blockchain

Arrivé à consensus. la tolérance à l'erreur Byzantine (Byzantine Fault Tolerance). Il est nécessaire d'avoir une tolérance à l'erreur dans le cas ou un nœud est hors-ligne, compromis ou défectueux.

> Un seul glitch du BTC en 2013 causé par une mise à jour qui n'a pas été adoptée universellement.

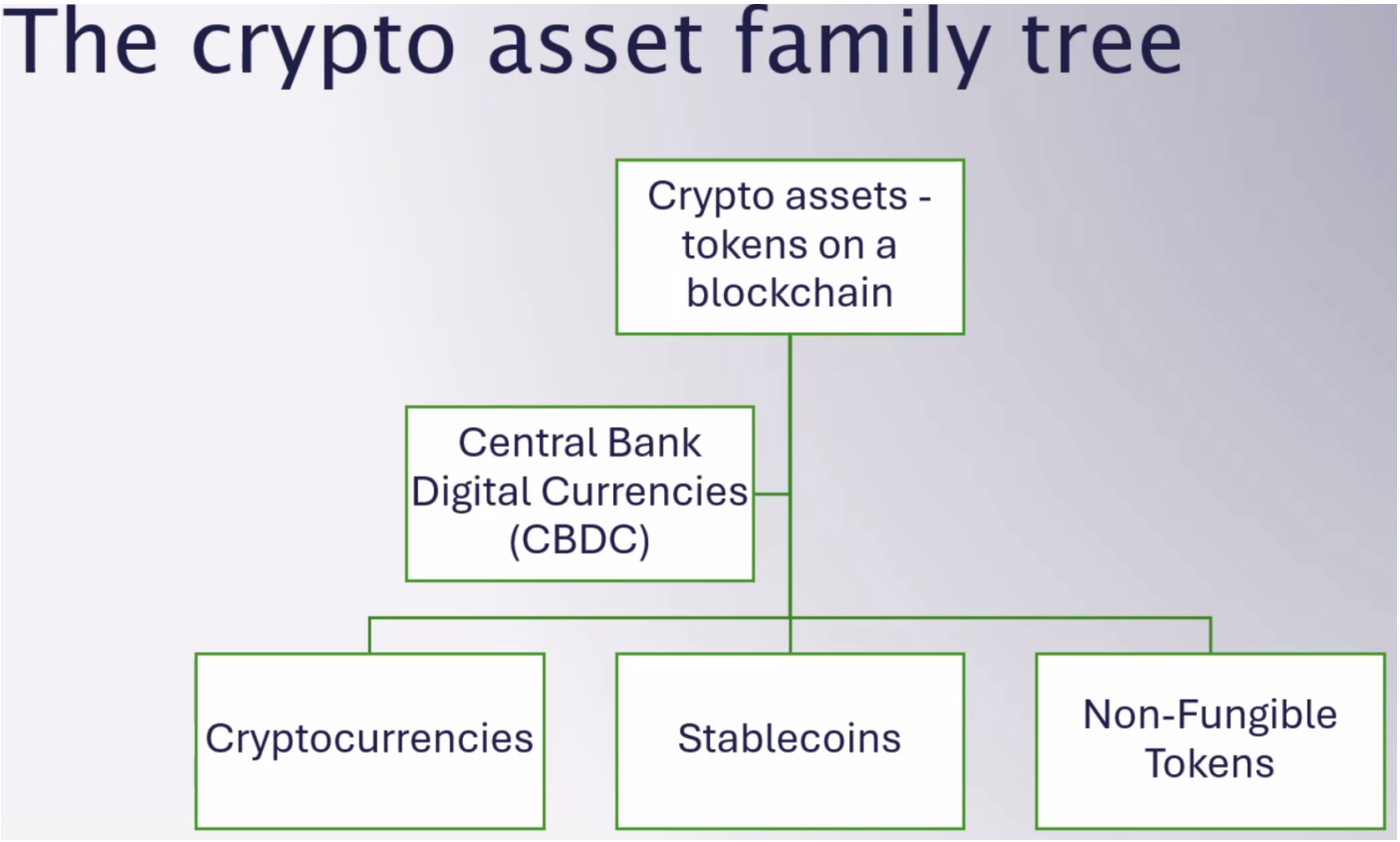
> Algorithme de Shor : risque de cassage de la cryptographie non post-quantique

Le risque principale d'attaque est le risque des 51%, ou la majeure partie de la chaine est contrôlée par un acteur.

Crypto Assets - Qu'est-ce et comment sont-ils protégés

En 2013, on recensait 66 cryptomonnaies. En 2025 il en existe plus de 10 000. Beaucoup d'autres ont été créer et ont fais faillite. Ils sont connus comme des poussières (dust).

Les familles sont regroupé en arborescence



Les devises digitale de banque centrales. Seulement 3 sont lancée et en utilisation.

https://www.atlanticcouncil.org/cbdctracker/

Les NFTs sont parfois associés à des événements du monde physique comme le bat token pour le concert de Dolly Parton en 2022.

La protection des cryptos assets

Un portefeuille est l'identité sur la blockchain. Une portefeuille différents peut être nécessaire pour chaque chaine.

Comme pour n'importe quelle clé privée, si elle est perdue ou volée elle est irrécupérable. Mais une phrase de passe créer à la création de la clé privé permet de la récupérer.

https://minuteluxe.com/sothebys-personnage-numerique-nft-vendu-11-millions/

https://www.cointribune.com/mark-cuban-victime-dun-piratage-crypto-de-pres-de-900-000/

https://www.crypto-france.com/sim-hijacking-poursuite-at-t-vol-crypto-monnaies/

Les contrats intelligents

Qu'est-ce ce que c'est ? Ce ne sont pas des contrats et ils ne sont pas intelligents □□ c'est simplement un terme.

C'est tout simplement l'automatisation d'un asset. Le nom à été choisi par Vitalic (joueur de WoW, fondateur d'ETH) en se basant sur le travail de Szabo (1994).

> Cours de programmation pour apprendre Solidity et apprendre à créer une NFT
> https://cryptozombies.io/
> Apprendre Solidity peut être une bonne compétence pour travailler dans la crypto

Outil d'audit automatisés

Des outils comme Manticore, Mythril, Lighcross ou Slither permettent d'audit un contrat intelligent. Pour trouver un contrat intelligent, il faut se rendre sur EtherScan et dans la partie contrat il est possible de copier le code source du contrat intelligent.

https://github.com/gsfyrakis/lightcross

Revision #8
Created 23 March 2026 07:58:53 by Marc
Updated 25 March 2026 11:06:02 by Marc