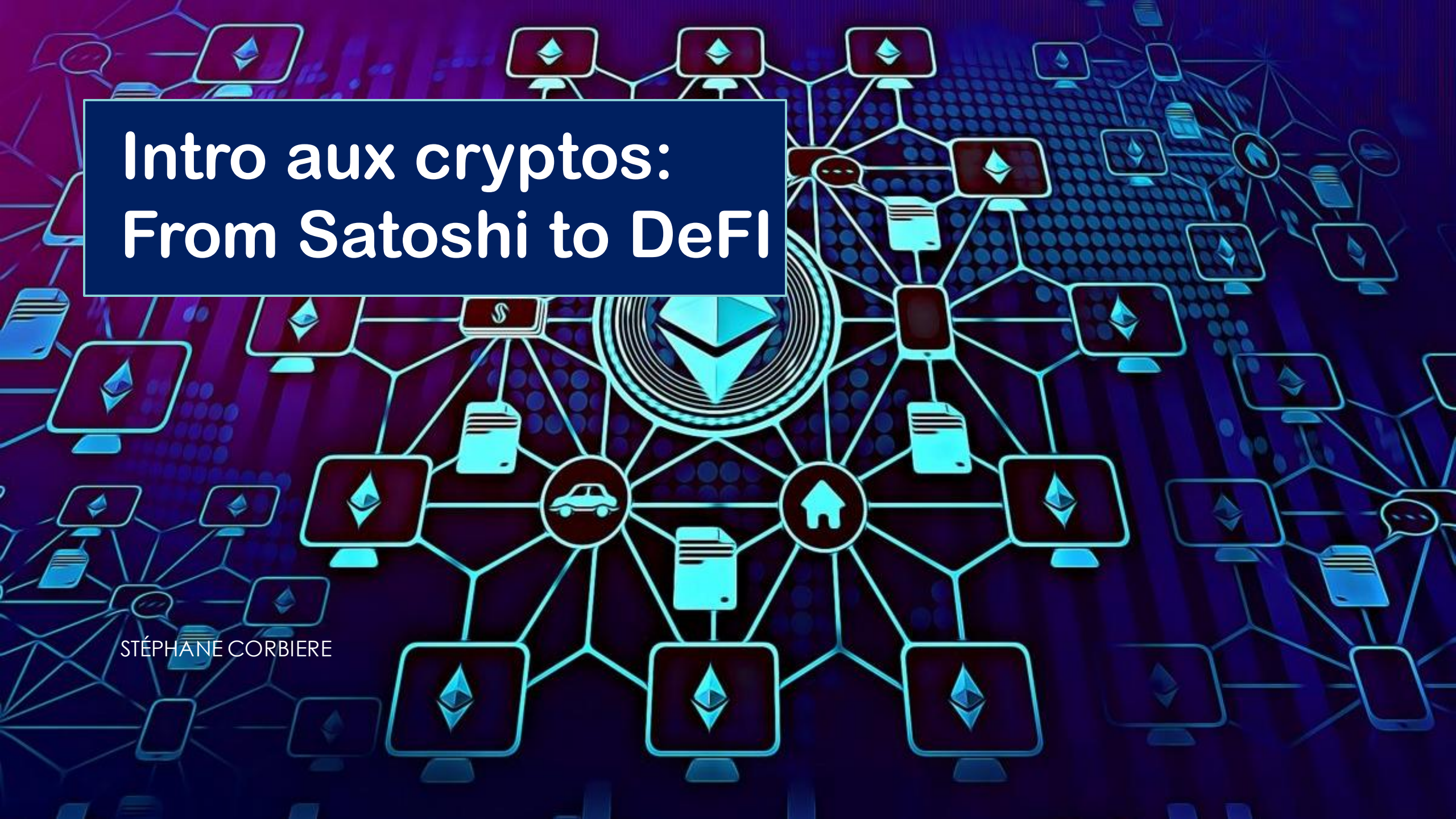
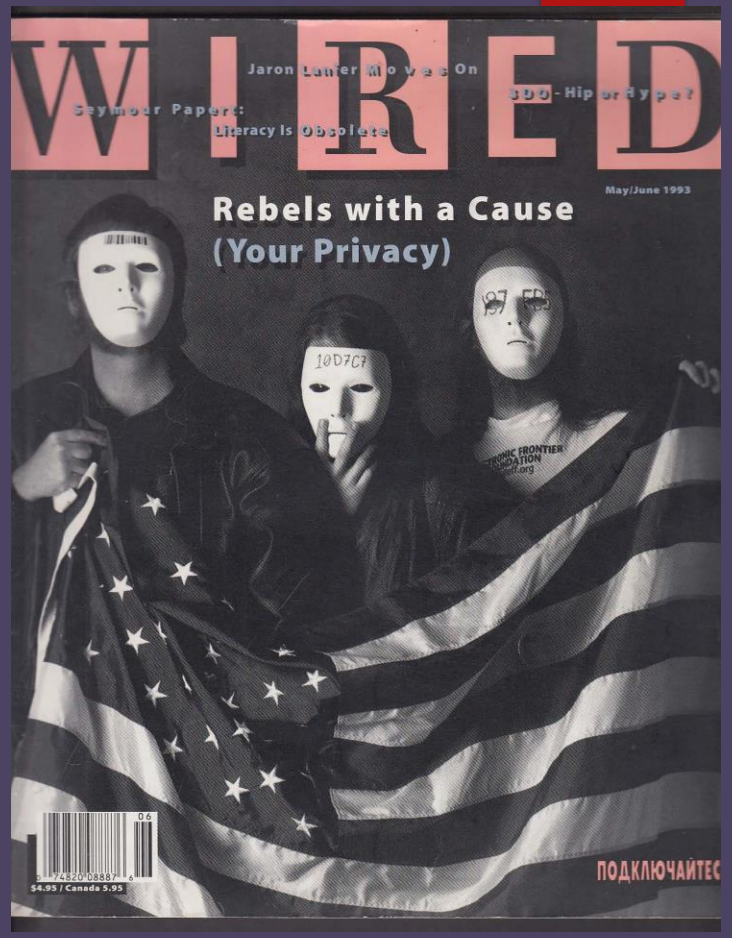


Intro aux cryptos: From Satoshi to DeFI

STÉPHANE CORBIERE

Les Cypherpunks

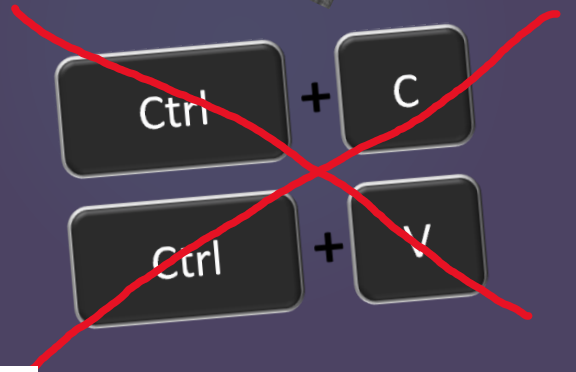
- Le mouvement Cypherpunk:
  - Création de la mailing list / forum en 92
  - Manifesto de Eric Hugues
  - De quelques centaines à plusieurs milliers de membres
- Avant Bitcoin:
  - DigiCash / eCash par David Chaum 83/89-98
  - G&SR / eGold par Douglas Jackson & Barry Downey 96-2008

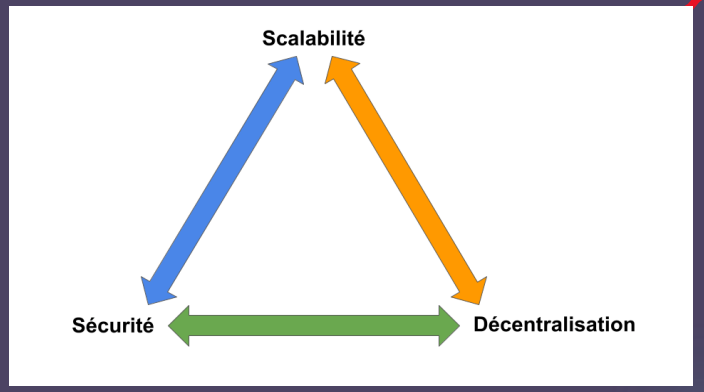


Cryptorebels – Steven Levy

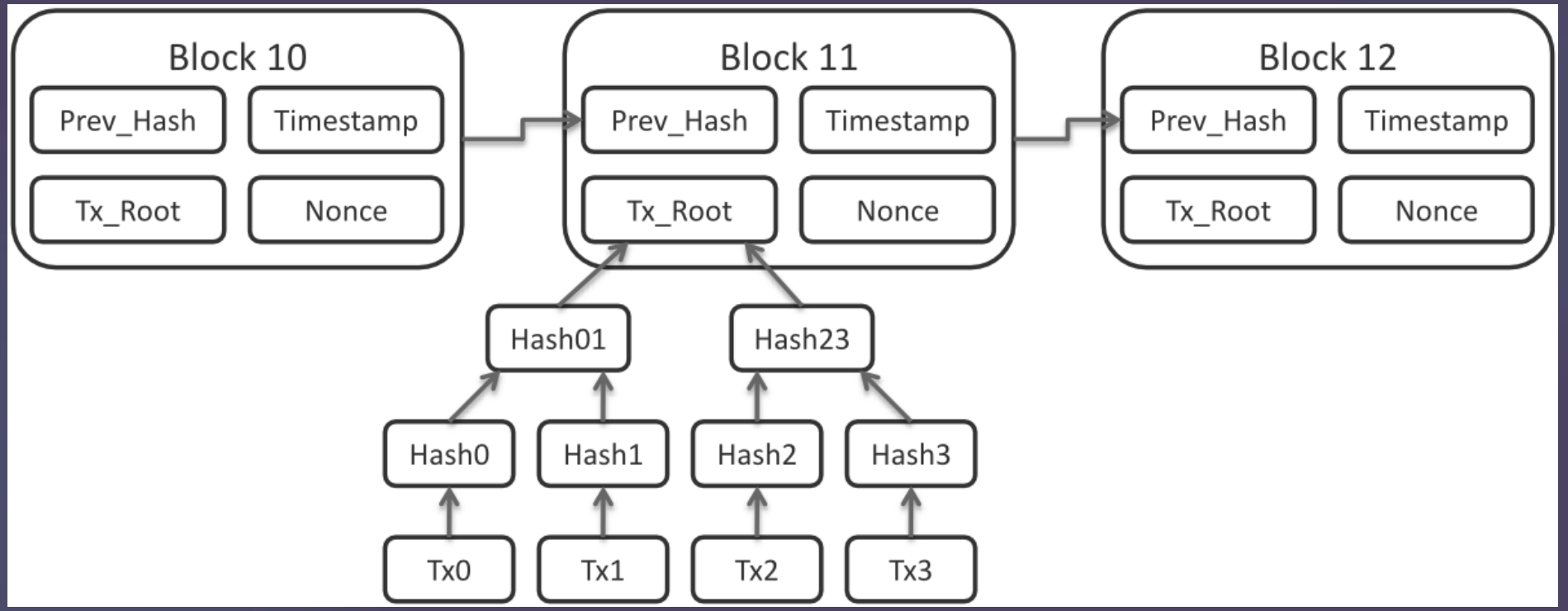
Satoshi Nakamoto & Bitcoin

- Satoshi = anonyme
- Bitcoin: a peer to peer electronic cash system
- Timestamp chain => Blockchain
  - Transactions dans des blocks d'infos
  - Décentralisation
- Consensus
- Trilemme des blockchains
- Utilisable par TOUT LE MONDE
- 1 sat = 1 BTC * 10^-9 (un milliardième)





Blockchain Bitcoin :



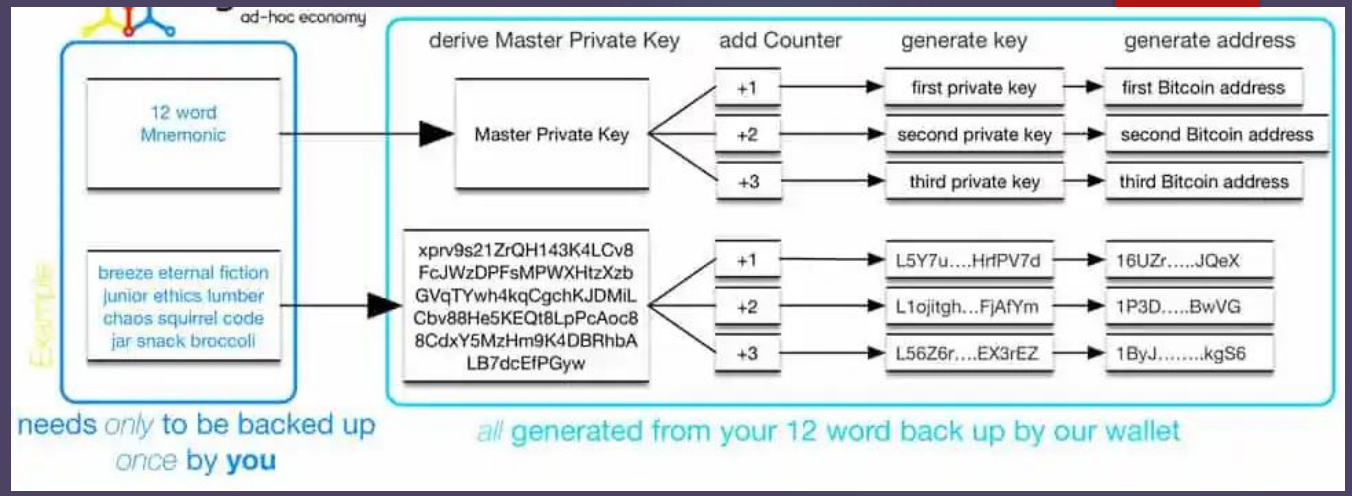
Les consensus & le minage

- Minage = UNIQUE moyen de créer des BTC

Consensus:

- Proof of Work: exemple d'un block BTC => confiance par le travail
- Proof of Stake: confiance collatéralisée
- ARCH, PoA etc...

Les wallets

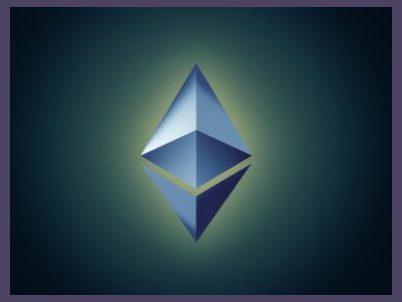


- Custodial / non-custodial
- Cryptographie asymétrique: clé publique, clé privée
- Phrase de récupération / mnemonic
- Clé publique clé privée
  - Addresses BTC
- Hot wallet / cold wallet / hardware wallet

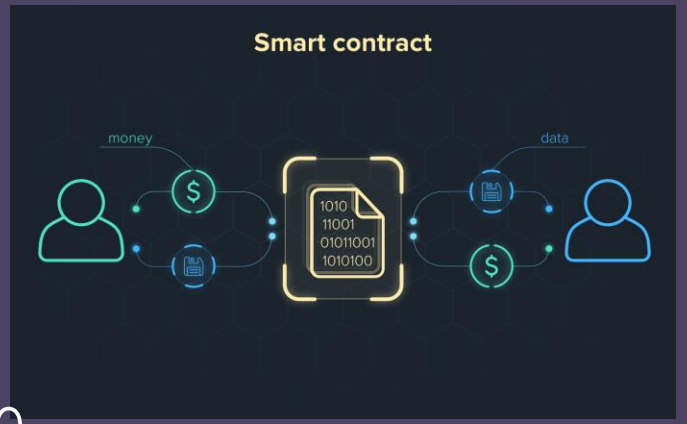
Les alternative-coins (altcoins)

- Copie de Bitcoin ?
  - -> Dogecoin / Litecoin / Bitcoin Cash ….
  - CMC en 2015: top 10
- Monero / Polkadot etc...
- Plein de shitcoins...

Ethereum & les blockchains d'infrastructure



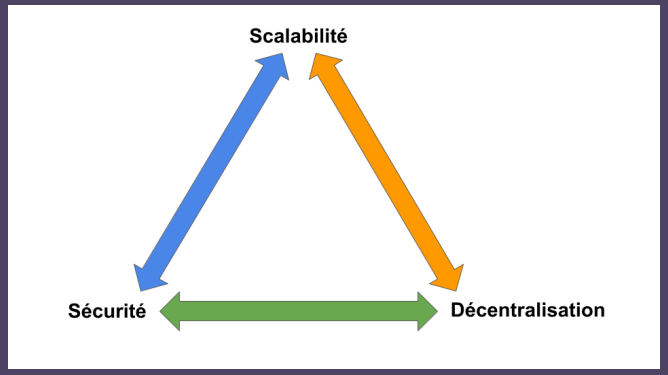
- 2014: Whitepaper, Vitalik Buterin & la Ethereum Fundation
- EVM: ethereum virtual machine
- Utiliser la blockchain pour des logiciels
  - Plus puissant que les scripts BTC
- Emergence des blockchains d'infrastructure, blockchain 2.0
- 1 wei = 10^-18 eth, 1 gwei = 1md wei



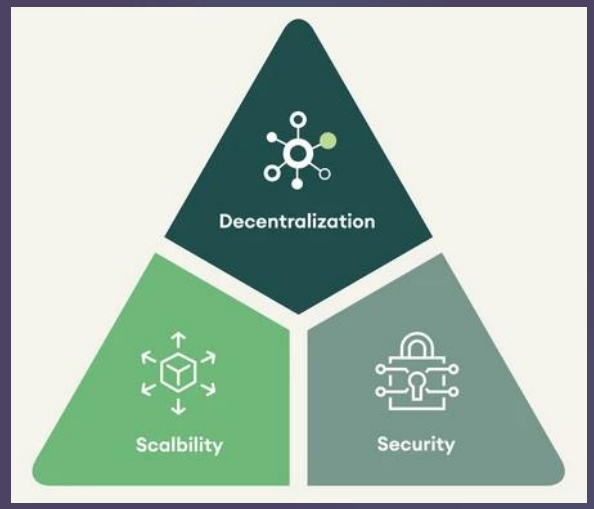
Les ethereum-killers

- Comme sur BTC a l'époque, des forks, des shitcoins...

- Meme problème du trilemme

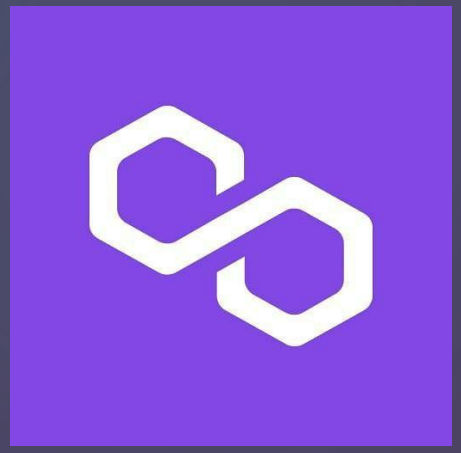


Les layers 2



- Augmenter la scalabilité: -cher, +rapide
  - En dépit du trilemme

- Sidechains, Rollups



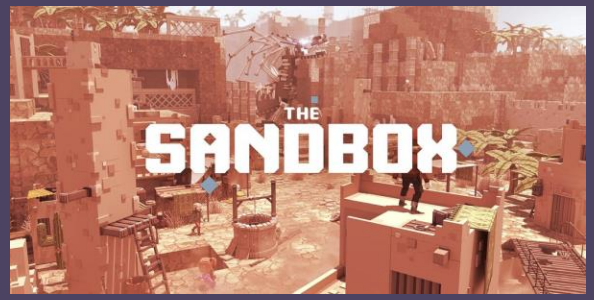
Les tokens

- Standards principaux:
  - ERC 20 => standard de tokens classiques
  - ERC 721 => standard pour des tokens non fongibles
  - ERC 1155 => amélioration pour les collections de NFT

Les NFTs

- De la propriété numérique
- L'art (spéculatif)
- Les P2E
- Metaverse
- La DeFi

RealT



Les stabblecoins

- Des tokens STABLES
- Tokens algorithmiques / collatéralisés
- Permet de swapper très rapidement de fiat a crypto en restant en crypto
  - Exemples: USDT, BUSD, USDC, agEUR, sEUR, PAXG...

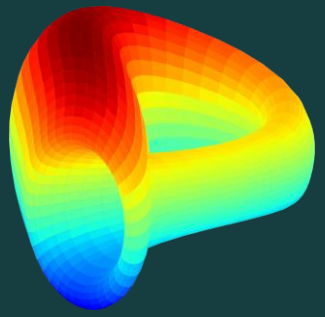
Globalisation de la décentralisation

- Décentralisation du stockage: IPFS => Filecoin / Aleph.im etc..

- Décentralisation de la puissance de calcul: Flux

- Emergence du Web 3.0
  - => Gouvernance décentralisée

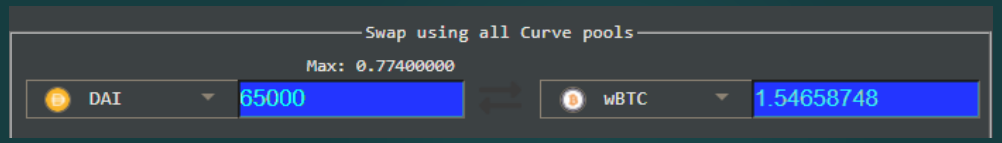
La Finance Décentralisée (DeFi)

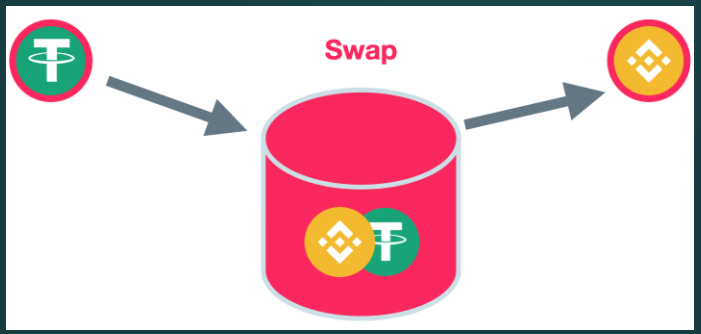


- Le futur (actuel) de la finance !
- Pas de pause des marchés, fonctionne H24
- Cut the greedy middleman
- Un marché décentralisé est inarrêtable
- Ouverture de la finance au peuple
- Trustless or Rekt

Les échangeurs décentralisés (Dex)

- Permet d'échanger un token contre un autre
- AMM
- Liquidity pools: bassins de tokens
- Frais faibles qui remunèrent les LPs
- Farming de LP => impermanent loss
- Gouvernance décentralisée



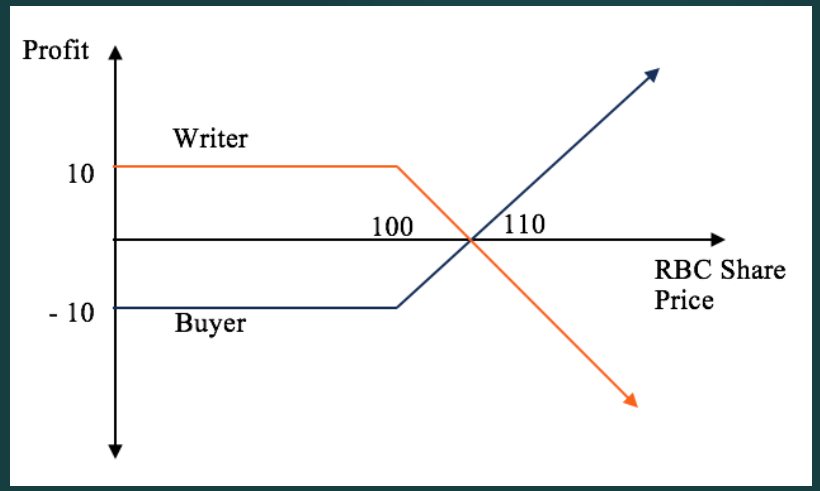


Les prêts collatéralisés
(lending / borrowing)

- N'importe qui peut emprunter OU prêter
- Emprunter avec un capital actif
- Yield Farming
- Des prêts FLASHs sans collatérals
  => flashloans

Les options & bonds

- Pure spéculation
- Effet de levier par contrat
- Puts & Call, strike price, expiration
- VOUS pouvez être writer & / ou buyer
- Bonds: sortes de prêts échangeables



Le DEV
Backend / frontend

- Backend: Solidity / python principalement
  - Vyper
- remix : all-in-one / vscode + plugins
- Framework: Truffle vs Hardhat
- Frontend: React avec ethers.js / web3.js
  - Permet la connection de wallets EVM compatibles

D.Y.O.R

Do Your Own Research

Merci !

(N.F.A)