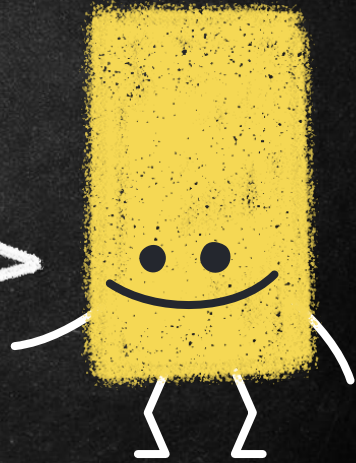
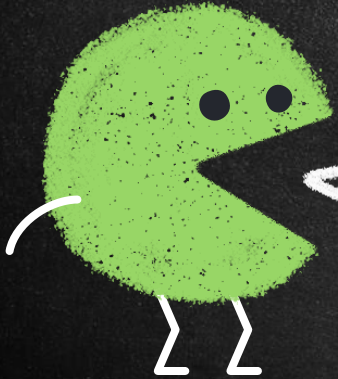
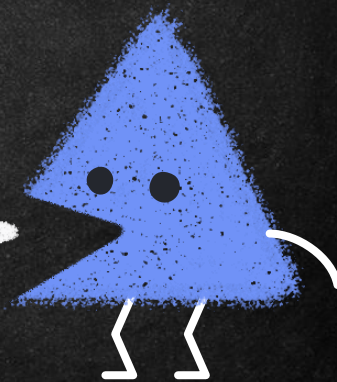


SÉCURITÉ DES DONNÉES
A2021/H2022
BLOCKCHAIN



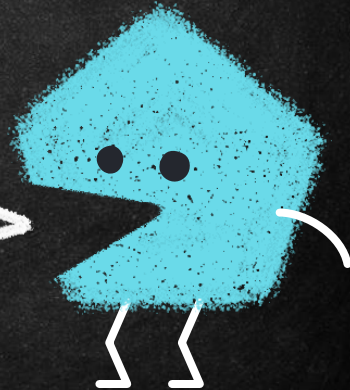
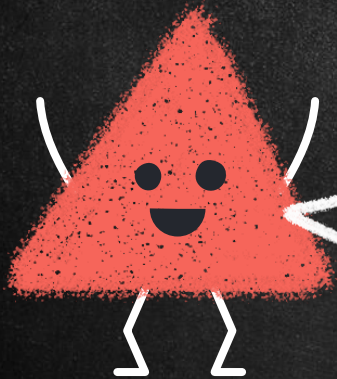
PLAN DE LA SÉANCE

- Concepts
- Fonctionnement
- Utilisations
- Proof of Work vs Proof of Stake
- Codons un peu



CONCEPTS

<https://txstreet.com/>



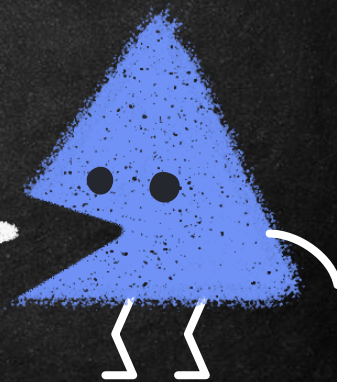
CONCEPT GÉNÉRAL

- Base de données publique et distribuée
 - Nœud du réseau
- Les données sont sauvegardé dans des blocs
- Les blocs sont liés dans un chaine via des outils cryptographiques cryptographie

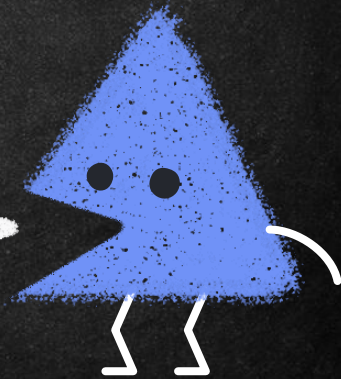


TERMES

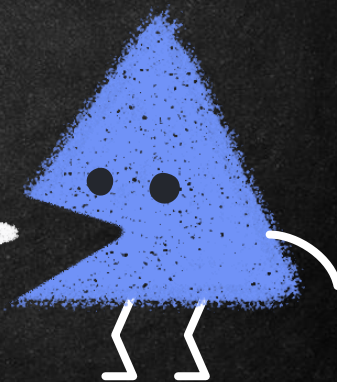
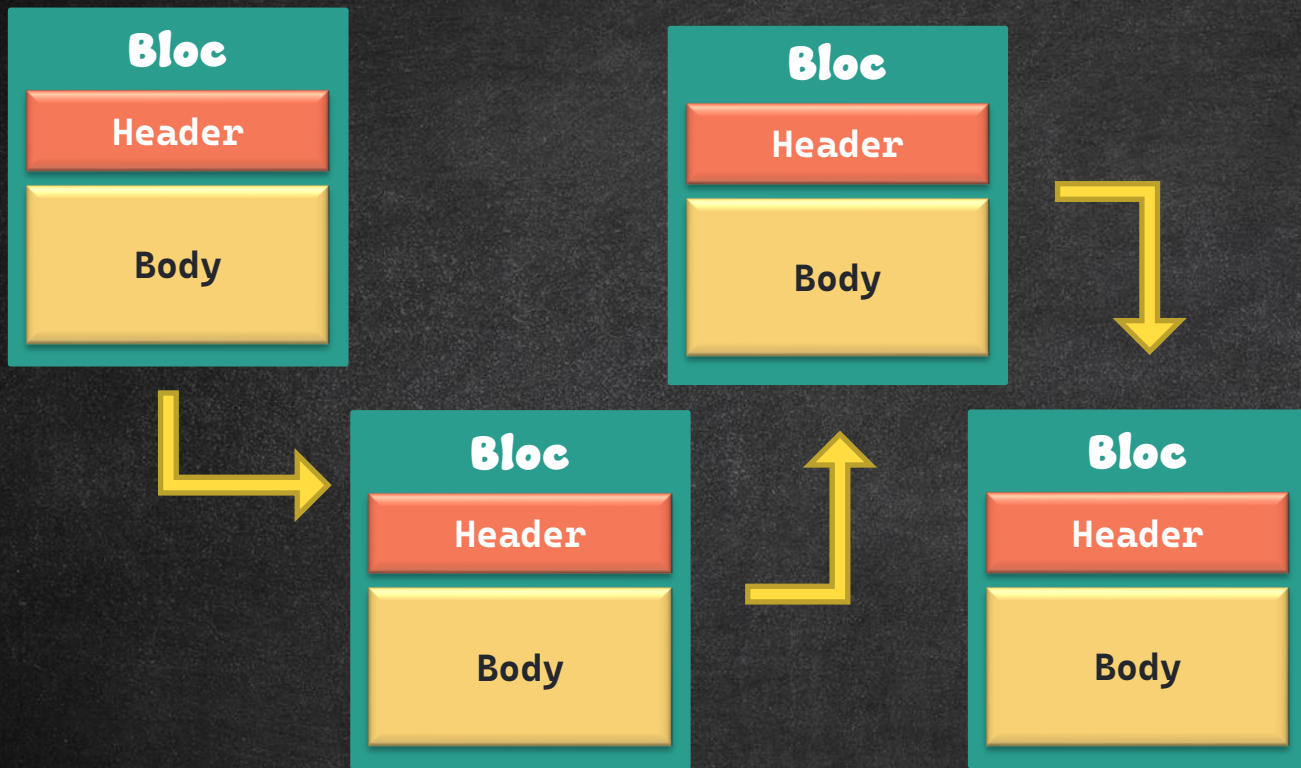
- Block
- Chain
- Merkle Root
- Node
- Mining (proof-of-work vs proof-of-stake)
- Fork
- Smart Contract



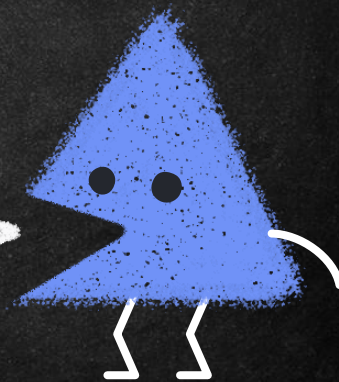
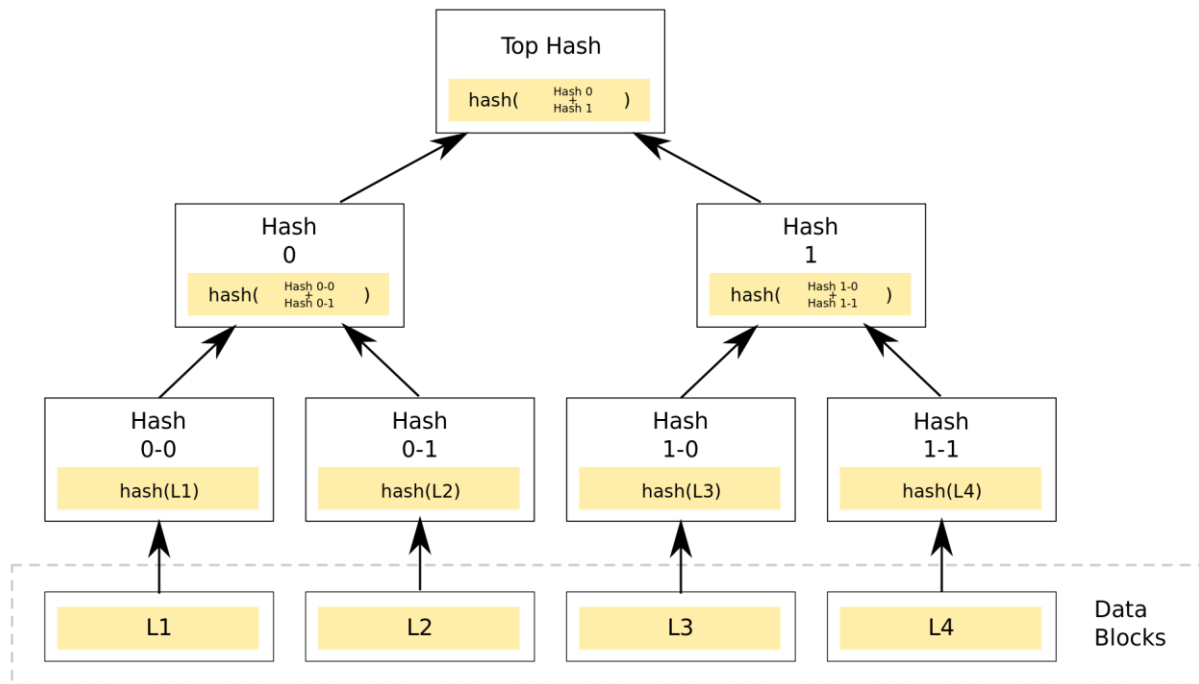
BLOCK



CHAIN

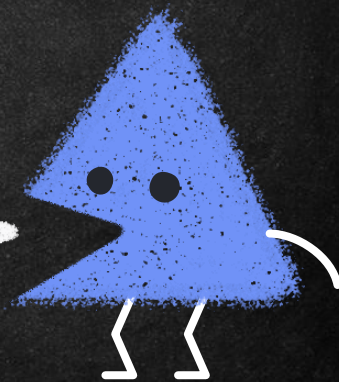


MERKLE ROOT



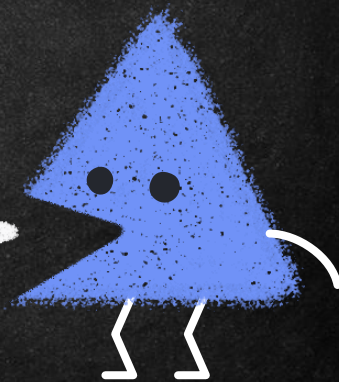
NODE

- Nœud du système distribué qui:
- Possède une copie de la blockchain
 - Accepter de nouveaux blocs
 - Valider le nouveau bloc et la blockchain



PROOF-OF-WORK ET MINING

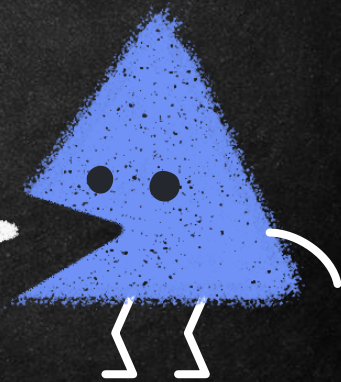
- Défi cryptographique prouvant l'effort nécessaire
- Chaque essaie à la même probabilité de solutionner le défi
- En général, trouver un hash respectant un certain critère arbitraire ($< x$, commence par 0xffff)
- La multiplication du nombre d'essai est la manière de gagner la course
- Les pirates doivent avoir 51% de force de travail disponible sur le réseau



POW – LE PROBLÈME

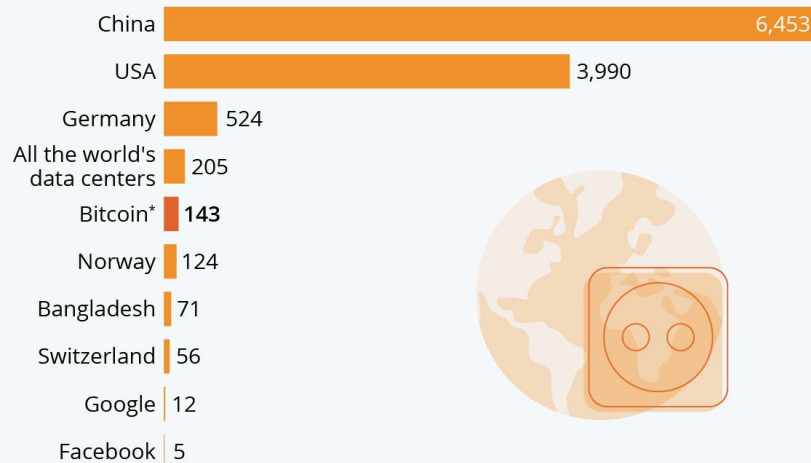
- L'énergie nécessaire au processus devient un enjeu important
 - Environ 0,55% de toute l'énergie mondial sur une base annuelle
 - Environ l'énergie nécessaire à l'état de Washington par année
 - En progression de 10x dans les 5 dernières années
- Certaines sources d'énergie sont non renouvelable (charbon)

<https://www.nytimes.com/interactive/2021/09/03/climate/bitcoin-carbon-footprint-electricity.html>



Bitcoin Devours More Electricity Than Many Countries

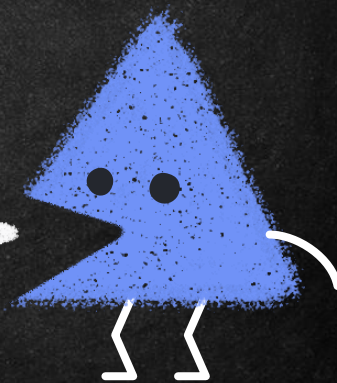
Annual electricity consumption in comparison (in TWh)



* Bitcoin figure as of May 05, 2021. Country values are from 2019.
Sources: Cambridge Centre for Alternative Finance, Visual Capitalist

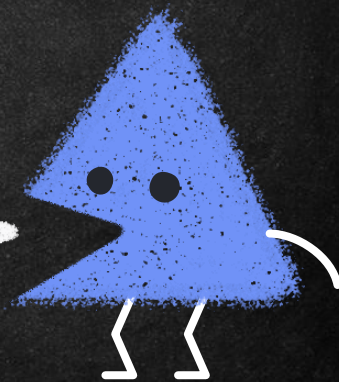


statista



PROOF-OF-STAKE ET FORGING

- Les nœuds du réseaux souhaitant être validateur mettre en jeu un montant de cryptomonnaie.
- Ce montant est gage de leur honnêteté et peut être retiré si un comportement non autorisé est détecté
- Les pirates doivent posséder et mettre en jeu 51% de toute la cryptomonnaie

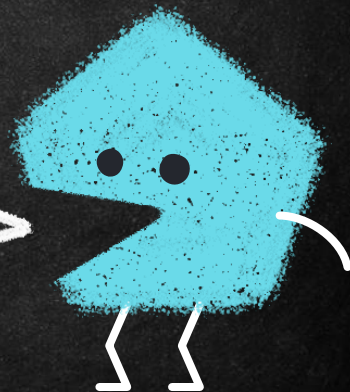
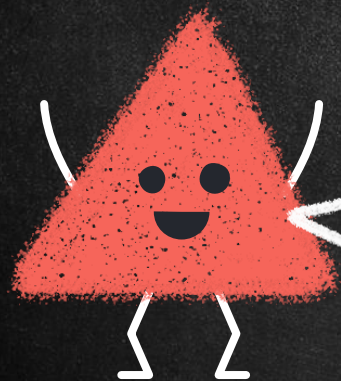


FORGING

→ À compléter

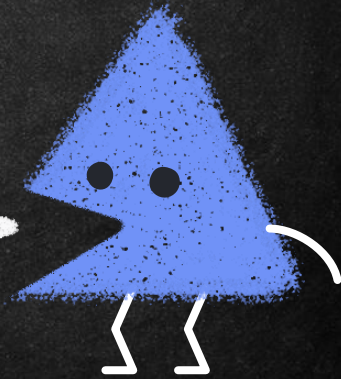


CRYPTOMONNAIE



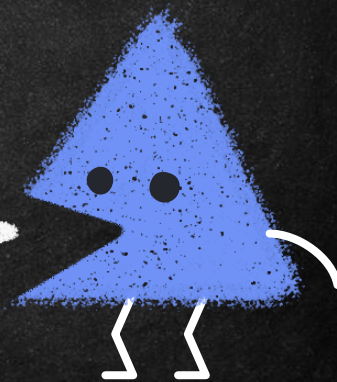
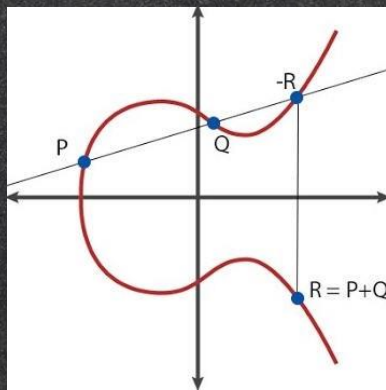
BITCOIN (BTX/XBT)

- 3 janvier 2009
- Satoshi Nakamoto
- Sous-unité: 1 / 100 000 000 satoshi (1 satoshi = 0,00000001)
- Proof-of-Work
- SHA256
- Un bloc au +/- 10 minutes
- Récompense 6,25 BTC jusqu'à mars 2024 et divisé par 2 au +/- 4ans
- Quantité maximale: 20 999 999,977



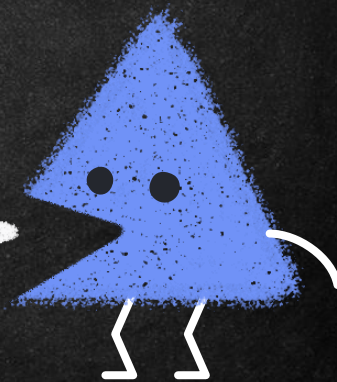
ADRESSE ET SIGNATURE

- L'adresse est générée en hashant la clé publique de l'utilisateur avec les algorithmes SHA256 et RIPEMD-160
- Clé privée et publique générées avec ECDSA
- Les hash ajout un niveau de protection si ECDSA devient vulnérable, il faudrait défaire 2 méthodes de hash.



UTXO

- Unspent transaction output
- Chacun des UTXO représente une pièce (coin) avec une valeur
- Chacun des UTXO représente la chaîne de propriétaire de cette pièce



UTXO OUTPUT ET INPUT

→ Output

- Pièce verrouillée pouvant être dépensée

→ Input

- Pièce sur le point d'être dépensée et devant être déverrouillée

→ Le processus de verrou est fait via un langage de script



100\$



[0x171]

0\$

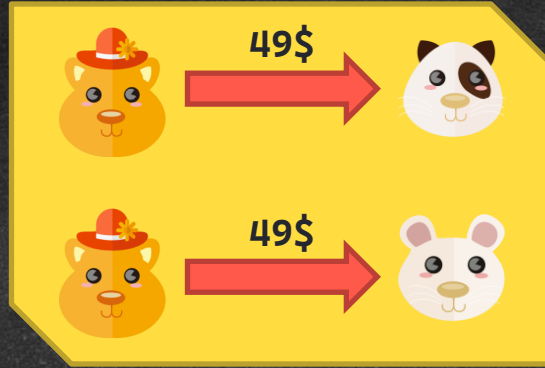


[0xabc]

0\$



[0x123]



```
{  
  inputs: [0xbdf1],  
  outputs: [  
    {value: 49, owner: 0xabc},  
    {value: 49, owner: 0x123},  
    {value: 2, owner: 0x171}  
  ],  
  sigs: [0x171]  
}
```

Hash: 0xbdf1
value: 100
owner: 0x171
is_spent: false

100\$



[0x171]

0\$

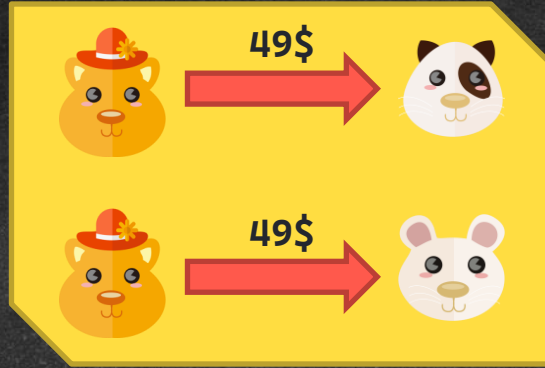


[0xabc]


0\$



[0x123]




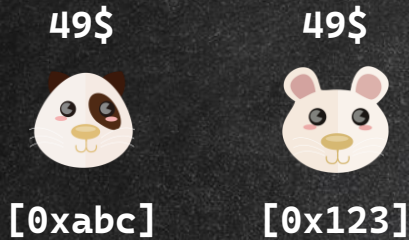
```
{
  inputs: [0xbdf1],
  outputs: [
    {value: 49, owner: 0xabc},
    ✓ {value: 49, owner: 0x123},
    {value: 2, owner: 0x171}
  ],
  sigs: [✓]
}
```


 `apply_transaction() {`
 //1. Vérifier toutes les signatures de la transaction
 //2. Vérifier que les inputs non dépensés
 //3. Vérifier que $\Sigma(\text{inputs}) \geq \Sigma(\text{outputs})$
 //4. Mettre à jour les inputs
 //5. Ajouter les nouveaux outputs
`}`

Hash: 0xbdf1
 value: 100
 owner: 0x171
 is_spent: false ✓



```
{
  inputs: [0xbdf1],
  outputs: [
    {value: 49, owner: 0xabc},
    {value: 49, owner: 0x123},
    {value: 2, owner: 0x171}
  ],
  sigs: []
}
```



 `apply_transaction() {`
//1. Vérifier toutes les signatures de la transaction
//2. Vérifier que les inputs non dépensés
//3. Vérifier que $\Sigma(\text{inputs}) \geq \Sigma(\text{outputs})$
//4. Mettre à jour les inputs
//5. Ajouter les nouveaux outputs
`}`

Hash: 0xbdf1
value: 100
owner: 0x171
is_spent: **true**

Hash: 0xcc85
value: 49
owner: 0xabc
is_spent: false

Hash: 0x34de
value: 49
owner: 0x123
is_spent: false

Hash: 0x1911
value: 2
owner: 0x171
is_spent: false

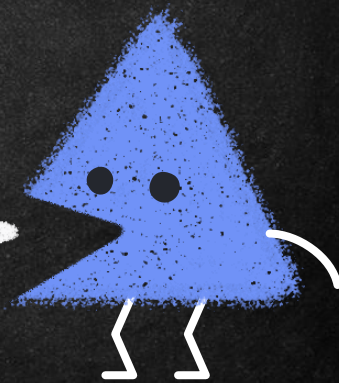
UTXO SCRIPT

- Modèle de pile
- Pas de boucle
- <https://en.bitcoin.it/wiki/Script>



PAY TO PUBKEY HASH (P2PKH)

- Objectif: Envoyer des fonds à une clé publique
- Utiliser le hash de la clé publique pour sauver de l'espace
- Output: scriptPubKey (Pkscript):
 - Instruction comment vérifier la signature d'une clé publique hashée
- Input: scriptSig: signature, clé publique



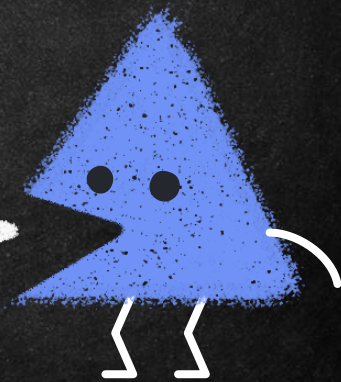
PAY TO PUBKEY HASH (P2PKH)

ScriptPubkey (Output)	ScriptSig (Input)
OP_DUP OP_HASH160 [H(pubkey)] OP_EQUALVERIFY OP_CHECKSIG	[signature] [pubkey]



UTXO SCRIPT

→ Transaction: 0xeff1694bd...b873ef0af3b



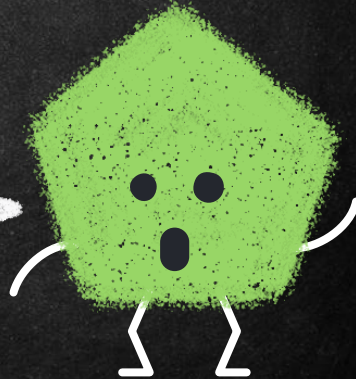
UNSPENDABLE OUTPUT

OP_RETURN

ANYONE CAN SPEND OUTPUT

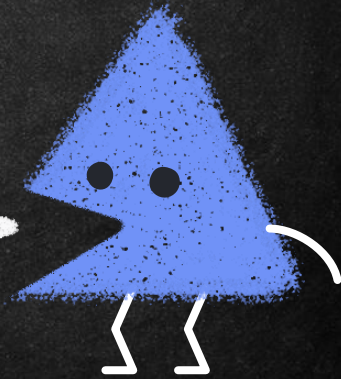
OP_TRUE

AUTRES



ETHEREUM

- 30 juillet 2015
- Vitalik Buterin
- 1/100 000 000 Gwei et 10^{-18} Wei
- Proof-of-Work → Proof-of-Stake
- Ethash
- Un bloc au +/- 15 secondes
- Récompense 2 ETH par bloc
- Quantité maximale: Infini



SMART CONTRAT

- Partie fondamentale d'Ethereum
- Programme informatique s'exécutant dans la blockchain
- Semblable à un contrat dans le monde réel
- Exécution automatique
- Résultats prédictibles



ETHEREUM 2.0

- [Beacon Chain](#)
- Passage de Proof-of-Work à Proof-of-Stake
 - Ethereum 1.0 devient un shard
- 64 shards (blockchain) en parallèle
- Epoch, Slots, crosslink
 - Chaque slot = 12 seconds
 - Possibilité pour crosslink un shard
 - Chaque Epoch = 32 slots => 6,4 minutes



ETHEREUM 2.0

- Pour chaque *slot* d'un epoch
 - un proposeur et comité de minimum 128 validateurs pour le block du beacon chain
- Pour chacun des crosslink d'un shards
 - Même principe
- Un attaquant a 1/mille milliards de contrôler 2/3 d'un comité

