

Une Introduction technique à Bitcoin

Concepts et outils pour expérimenter rapidement

Un problème résolu

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshi@gmx.com
www.bitcoin.org

La double dépense
→ d'un objet numérique
sans tiers de confiance

Un protocole solution

Éléments clés

Protocole : Ensemble de règles suivies par un réseau afin de transmettre des messages produisant un service.

- Messages : TRANSACTIONS
- Transmission : NŒUDS (Clients)
- Vérification (*et encrage*) des messages : MINAGE
- Utilisateurs : ADRESSES



Vocabulaire

Quelques notes

- Satoshi (sat) : plus petite unité monétaire.
- BTC : Notation monétaire (€,\$,£,...)
- $1 \text{ BTC} = 100\,000\,000 \text{ sats}$ (10^8)
- $1\text{€} = 1500 \text{ sats}$
- UTXO : Unspent Transaction Output (Sortie de transaction non dépensée)
- Txid: Transaction Identifier
- HMAC: Hash-Based Message Authentication
- Timestamp : Horodatage

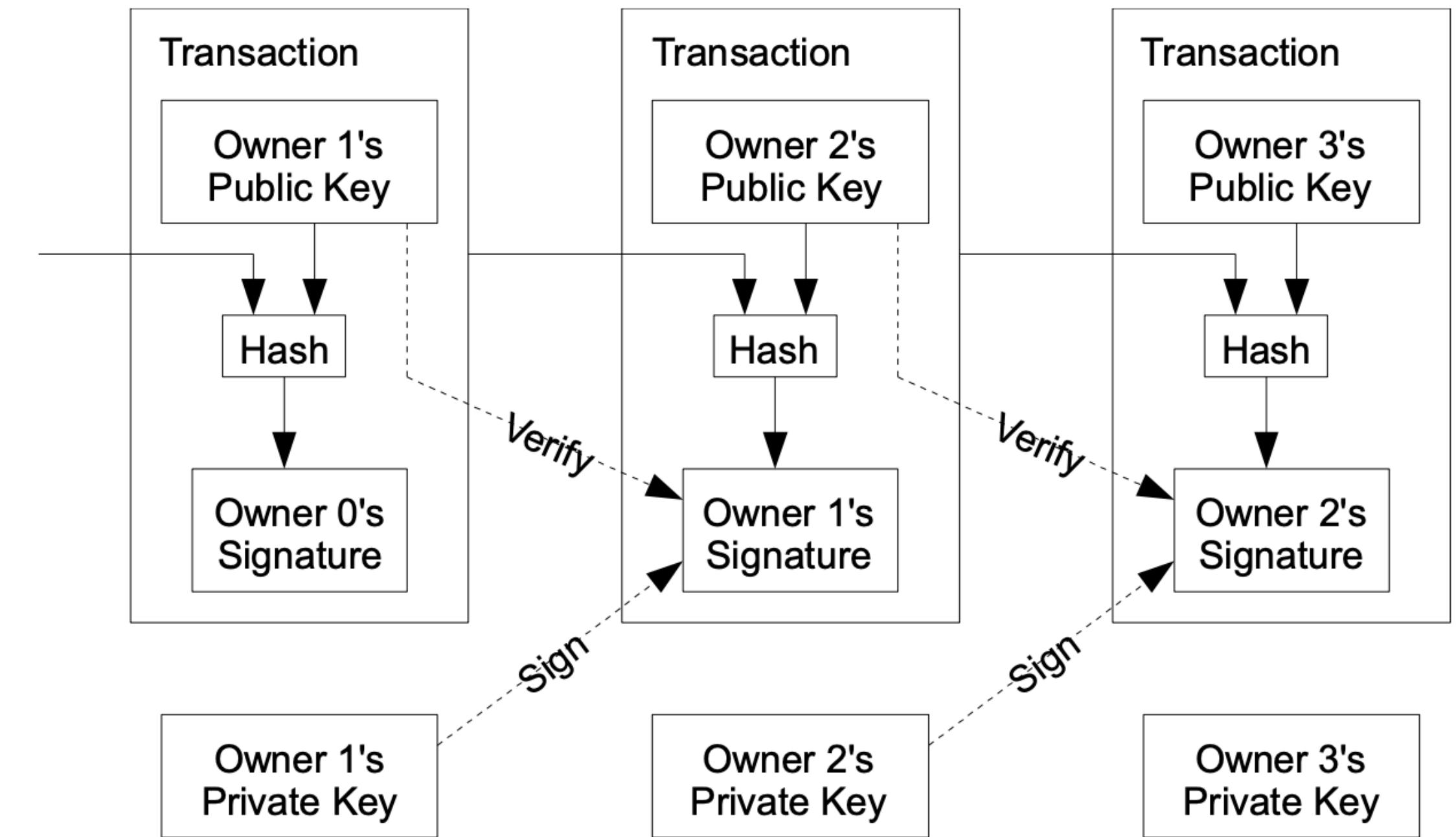
Hash

Détails sur les fonctions de hachage

- **Fonction de Hachage cryptographique:** Prend en entrée une quantité arbitraire de données et produit une sortie de taille fixe, appelée le **Hash** (ou empreinte).
 - Déterminisme
 - Rapidité de calcul
 - Effet avalanche
 - Resistance aux collisions
 - Résistance à la pré-image
- Md5, SHA-1, **SHA-256**, SHA-512, **RIPEDM-160**,... Expérimenter: [emn178](#)

Transactions

Une suite de signatures...



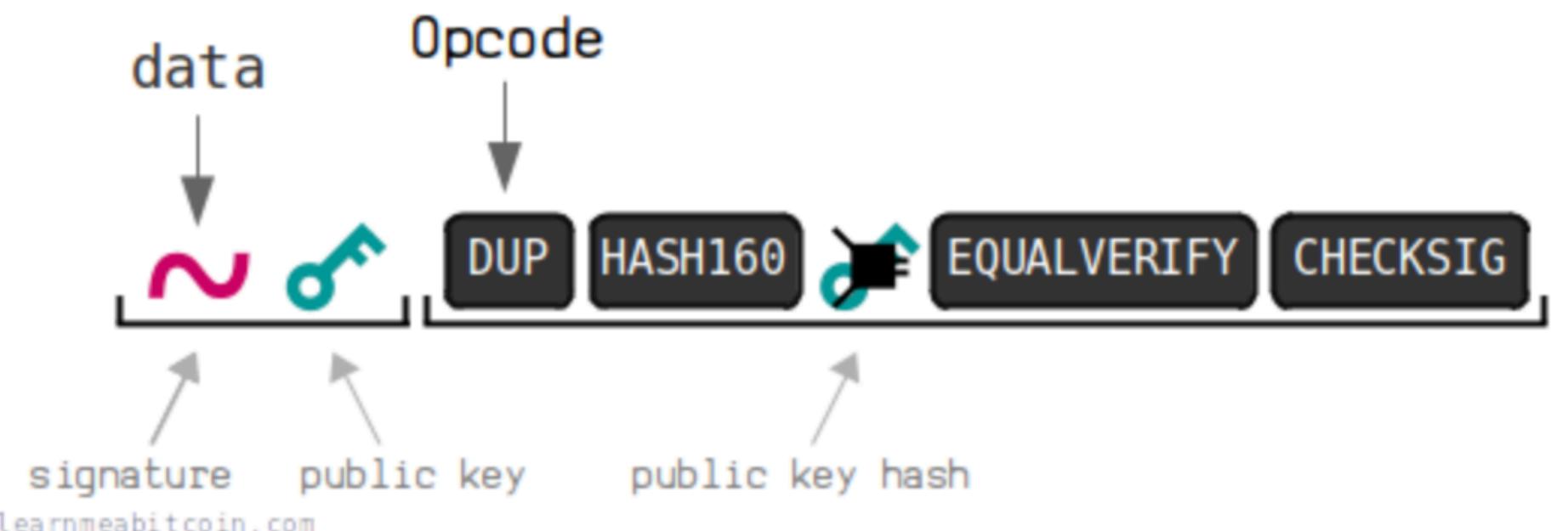
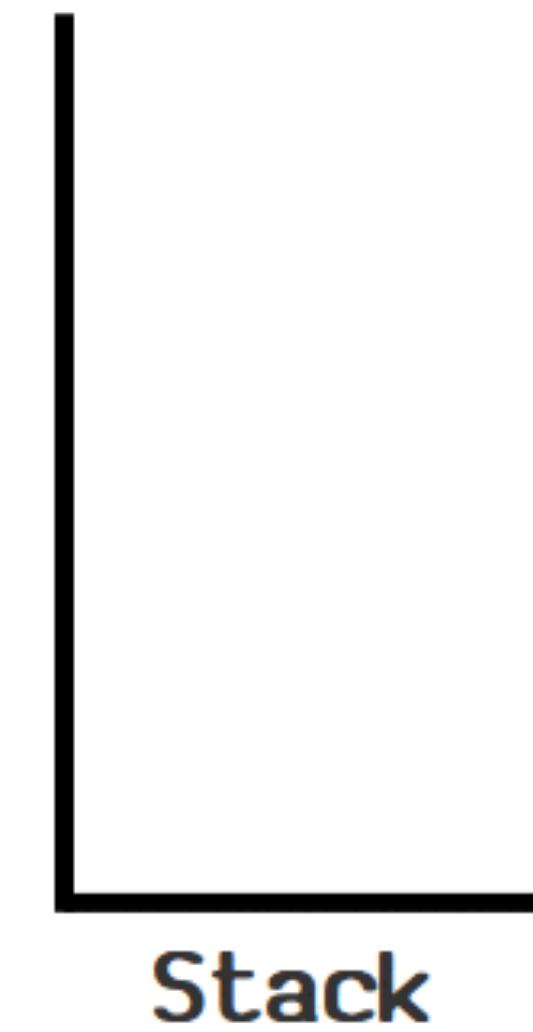
... du script...

Exécution de la transaction

- Un script c'est :

- Des **OP_CODEs** : fonctions simples pour opérer sur de la donnée.
- Des **données** : des clés publiques, des signatures, etc.

- Langage : Bitcoin Script (stack-based)



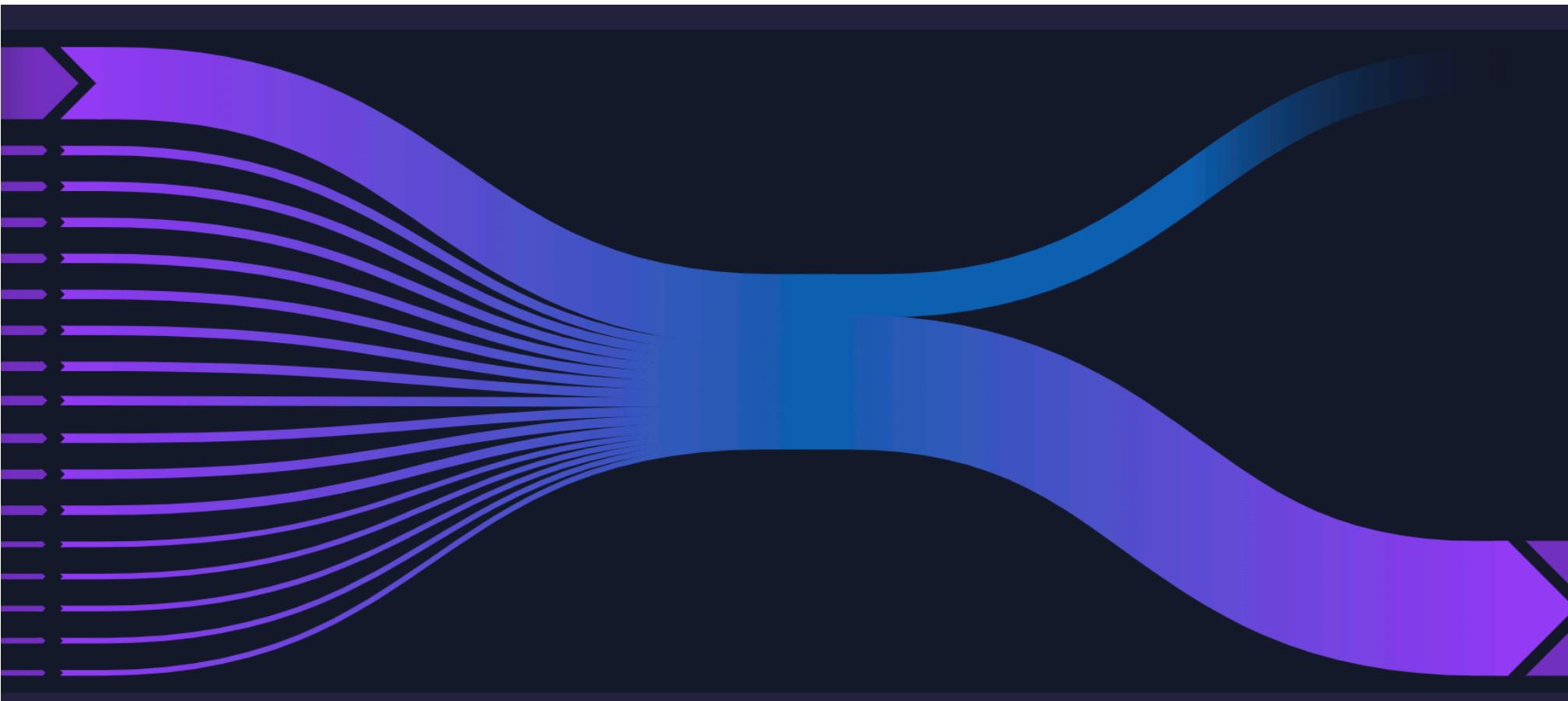
... et des entrées, sorties

LE BUT ?

Envoyer de l'argent !

En "simulant" du Cash

Txid: 777651b5a8b960be8496f5706470972f88fcb76f36b4953934db420b4898d341



TXID = HASH256([version][inputs][outputs][locktime])

```
{  
  "txid": "777651b5a8b960be8496f5706470972f88fcb76f36b4953934db420b4898d341",  
  "hash": "08dca35406dfba05cd8fac55f07c1616f85257eb8efdb67c4657513a3968bf35",  
  "version": 2,  
  "size": 2957,  
  "vsize": 1586,  
  "weight": 6344,  
  "locktime": 0,  
  "vin": [  
    {  
      "txid": "3d758cb22aa35eba351988bda0ff32f28ab63392c02560cc75730454cd36bf75",  
      "vout": 6,  
      "scriptSig": {  
        "asm": "0014d1bbb6f6a888ed8522743f0eacda53ba79c978d",  
        "hex": "160014d1bbb6f6a888ed8522743f0eacda53ba79c978d"  
      },  
      "txinwitness": [  
        "3044022059556736519c11af5d90b4113d296b8d5384b898998bde7677fc532004f8acf0220364e25c4a67cf61f56fba61a6ac218be1d0610f9dc1acfeecb242cdc766faf4601",  
        "03683d8ba54d5231d2520d4502fe8b128112473dbc7ace0d56975c9623cc33140d"  
      ],  
      "sequence": 4294967293  
    },  
    {  
      "txid": "3d758cb22aa35eba351988bda0ff32f28ab63392c02560cc75730454cd36bf75",  
      "vout": 4,  
      "scriptSig": {  
        "asm": "0014d1bbb6f6a888ed8522743f0eacda53ba79c978d",  
        "hex": "160014d1bbb6f6a888ed8522743f0eacda53ba79c978d"  
      },  
      "txinwitness": [  
        "3044022020fb3433a07486a716f10b8bcfa9baf881fc9ced6400859a394caf8b5c48d8c02205843a456c7affb25cf11bddb62df546304d9f3d8e9dd5d33c42ed6f33804458b01",  
        "03683d8ba54d5231d2520d4502fe8b128112473dbc7ace0d56975c9623cc33140d"  
      ],  
      "sequence": 4294967293  
    },  
    "vout": [  
      {  
        "value": 0.00020660,  
        "n": 0,  
        "scriptPubKey": {  
          "asm": "0 a5e132b2a9380f38ab82a93d6eb3e1a8e1145278",  
          "desc": "addr(bc1qhsn9v4f8q8n32uz4y7kavlp4rs3g5nc6wk03a)#wv2lsx4k",  
          "hex": "0014a5e132b2a9380f38ab82a93d6eb3e1a8e1145278",  
          "address": "bc1qhsn9v4f8q8n32uz4y7kavlp4rs3g5nc6wk03a",  
          "type": "witness_v0_keyhash"  
        }  
      }  
    ]  
}
```

Un autre GIF

Détails des éléments des données d'une raw transaction



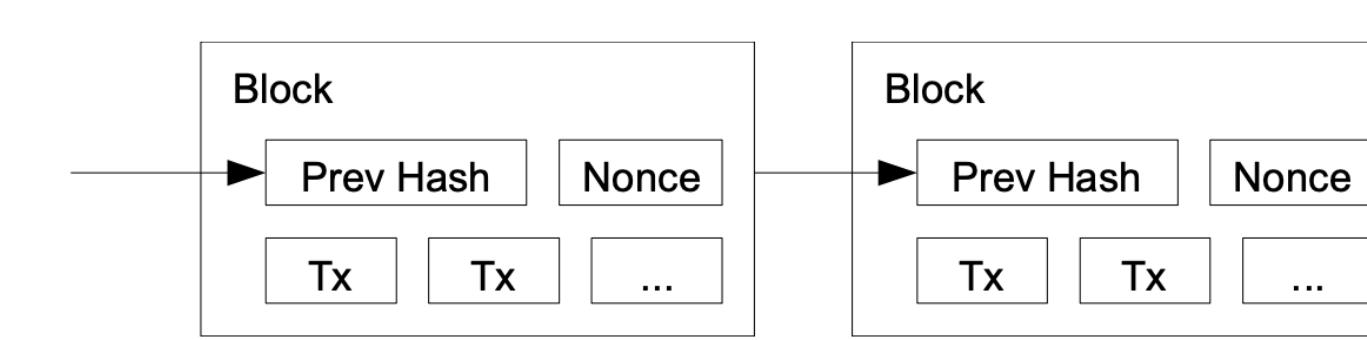
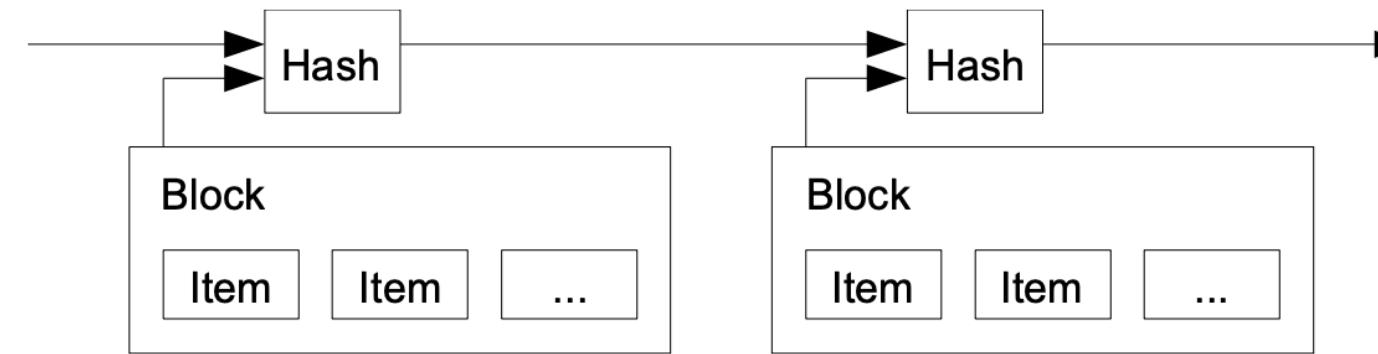
Bitcoin-core

Client Bitcoin

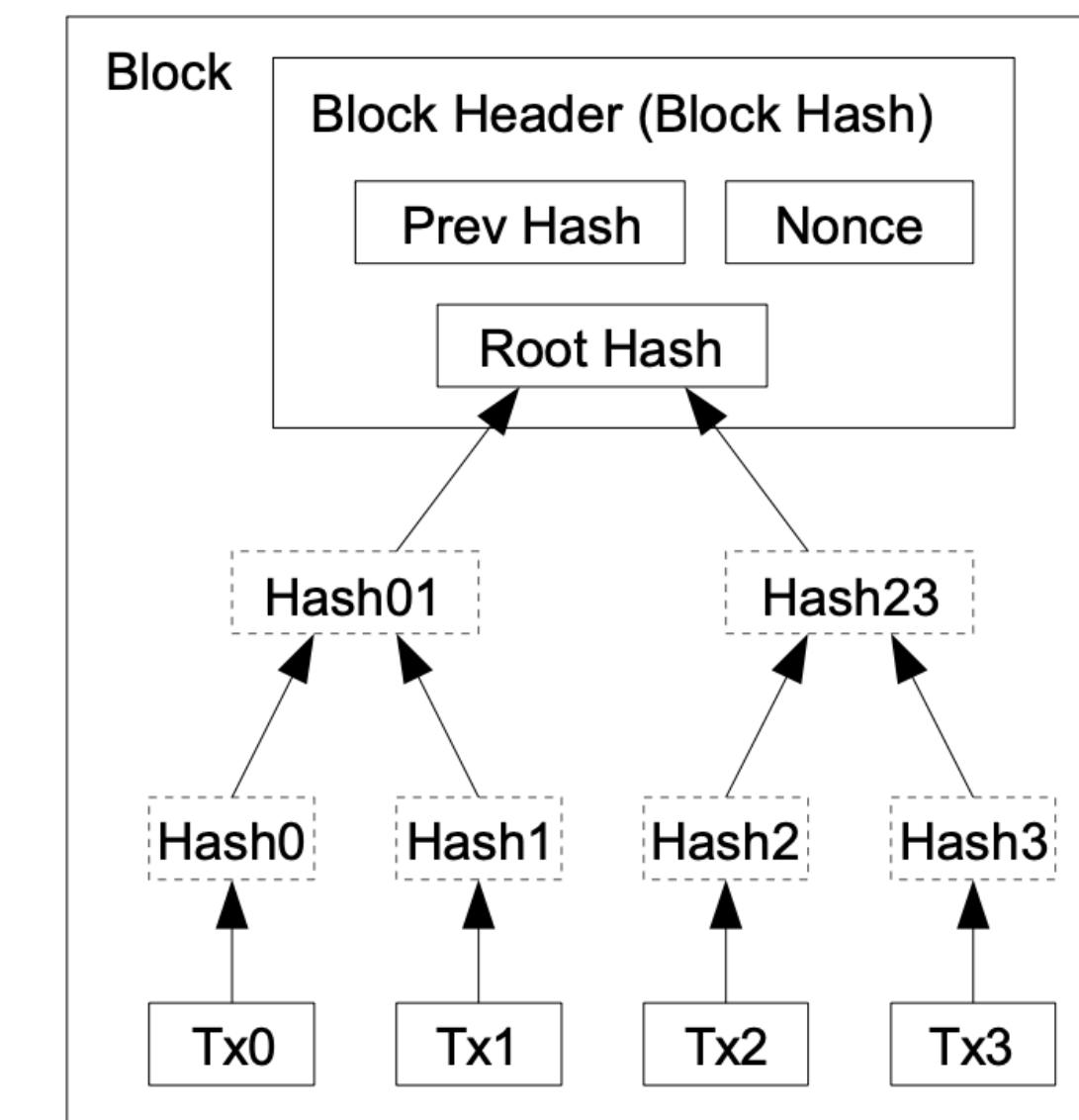
- Github officiel: <https://github.com/bitcoin/bitcoin>
- Pour pouvoir utiliser le client il faut que le *daemon* tourne : bitcoind
 - La configuration : [bitcoin-core config generator](#)
- Ligne de commande: bitcoin-cli
 - Premières commandes: `bitcoin-cli getblockchaininfo`, `bitcoin-cli getnetworkinfo`

Du timestamp server à Bitcoin

Construction des blocs



Nonce: Number used once

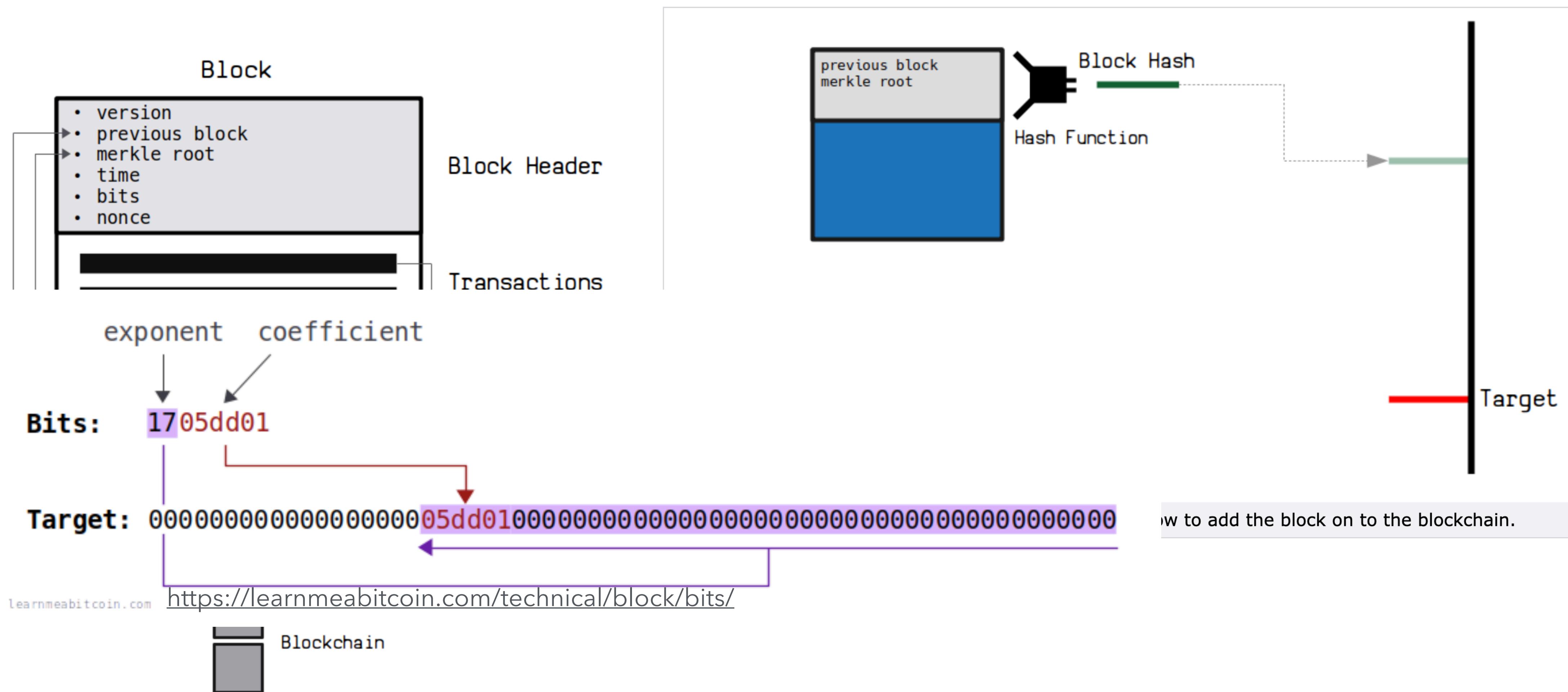


Transactions Hashed in a Merkle Tree

Commande à tester : `bitcoin-cli getblocktemplate '{"rules": ["segwit"]}'`

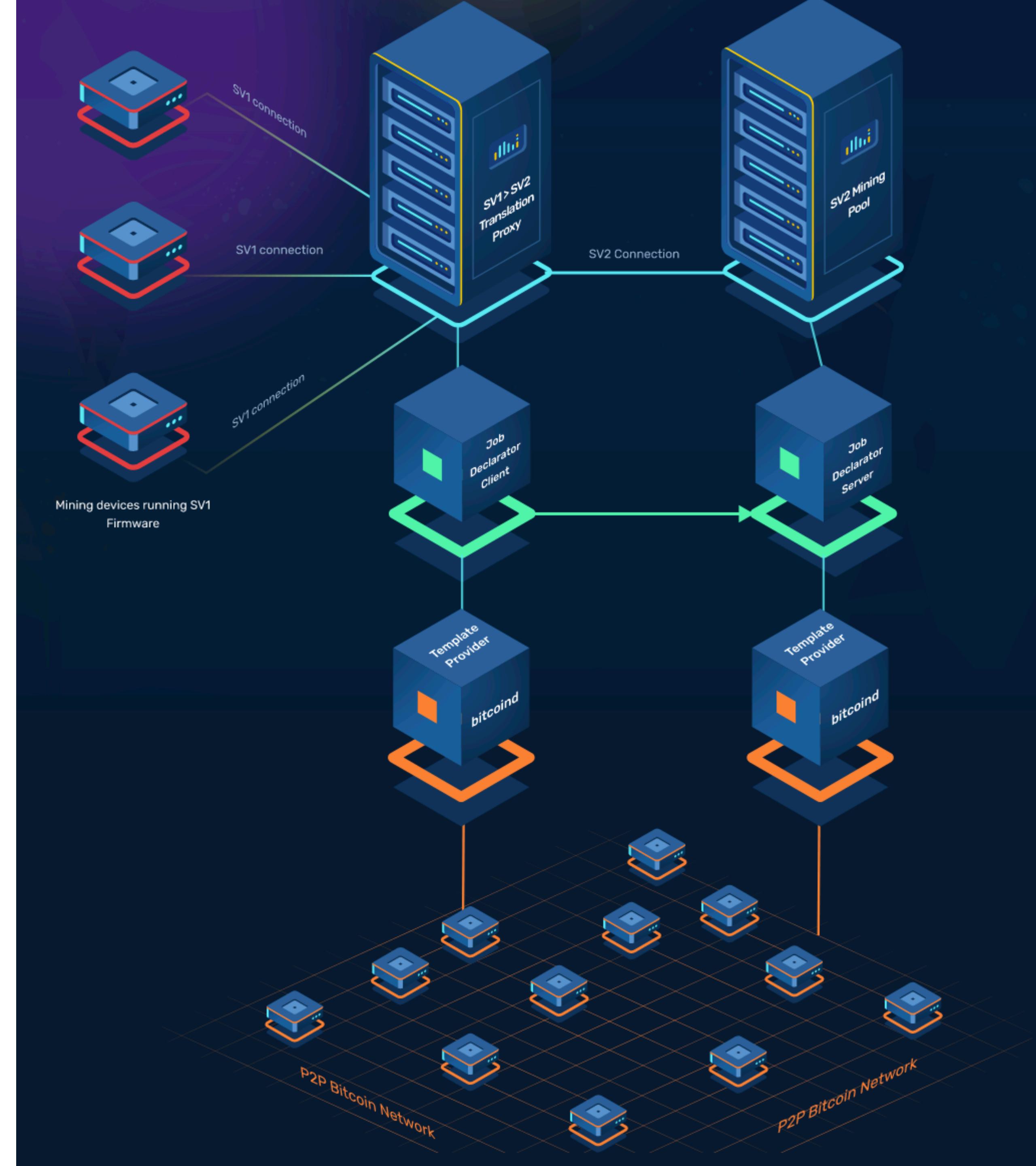
Comment on mine?

Chercher la Nonce



Outils & pools

- Miner avec cpu → Exemple de code:
cpuminer -> cpuminer.c 1.1073
- Stratum Protocol : coordonner le mining dans des pools.
- Hardware: ASICs Antminer



Mining & écologie

Quels sont les problèmes ?

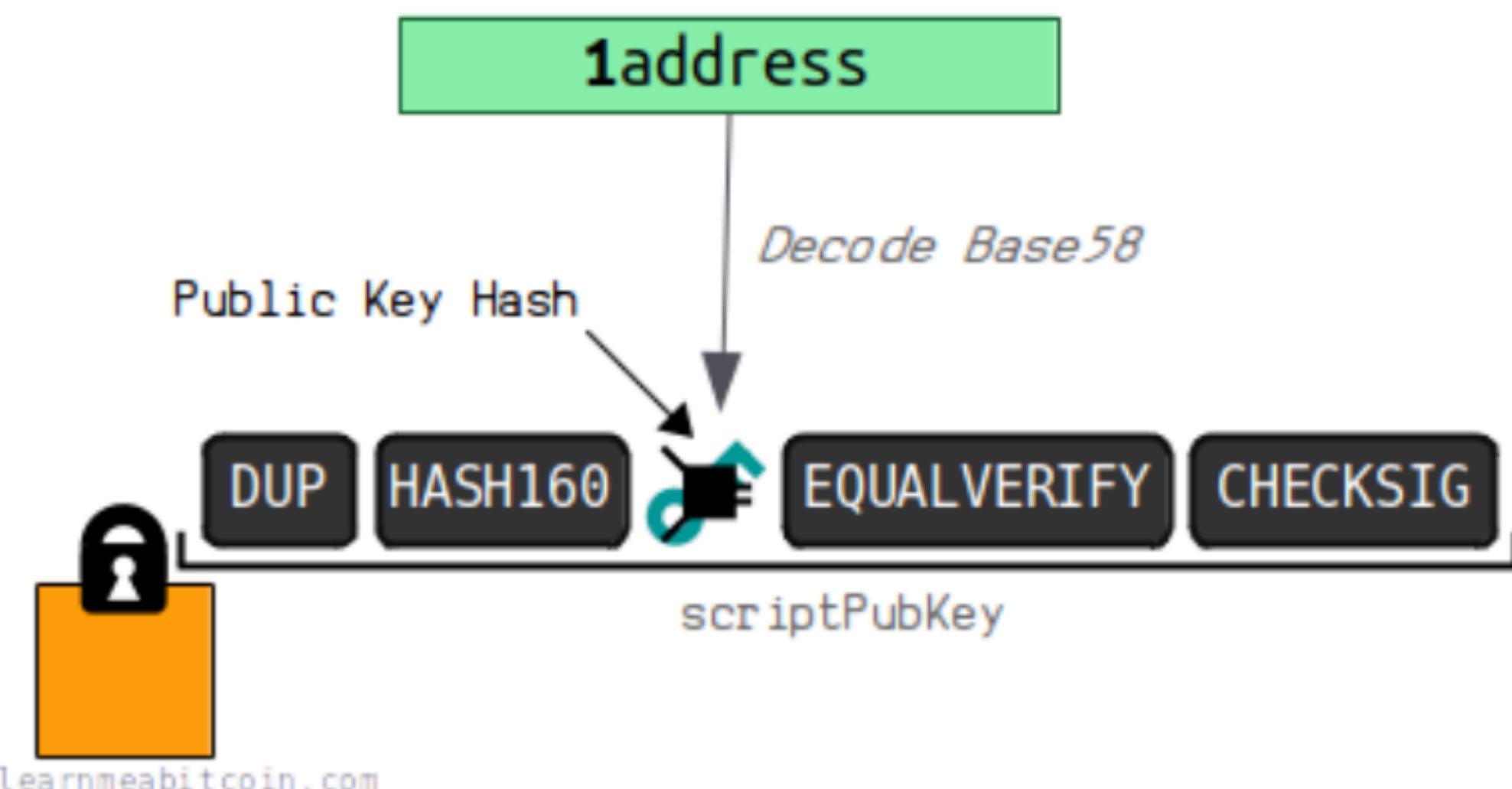
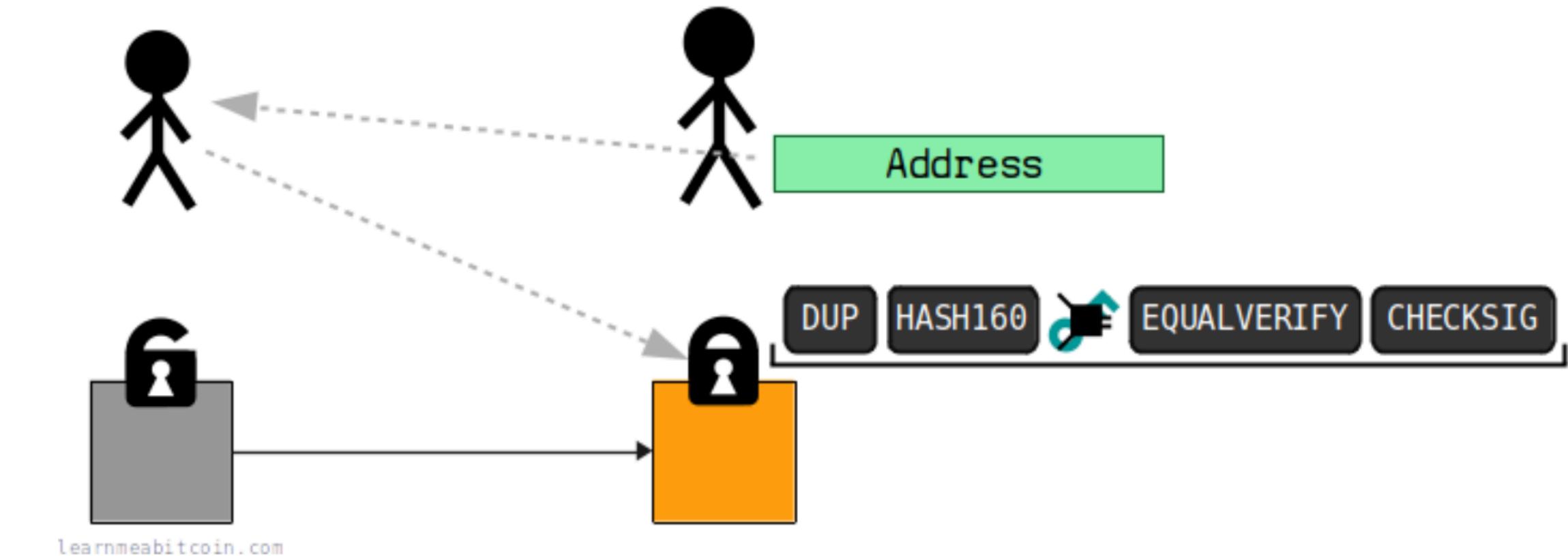
- Trop d'utilisation de l'électricité ?
 - Consomme PLUS que LA BELGIQUE
 - Quid des data centers ?
- Que disent les industriels ?
- ASICs Antminer !
 - Chauffage + Bitaxe



Adresse

Définition

- Représente un **script de verrouillage** particulier
- Désigne un encodage *user-friendly* du hash de la clé publique ou celui du script



Les types d'adresses

P2PKH
Base58

Example P2PKH Address:

1CYY8sHqgicPWd3b7jujH85hKvRUNdfZMH

34 characters

Example P2PKH ScriptPubKey:

ASM Hex

OP_DUP
OP_HASH160
OP_PUSHBYTES_20
7ea044e7a765e1febde4d3e2a87bcfc288c5687e
OP_EQUALVERIFY
OP_CHECKSIG

P2SH
Base58

Example P2SH Address:

3LVUiA3GM79B9nbrMXzPp4MWz1nSh4nGqt

34 characters

Example P2SH ScriptPubKey:

ASM Hex

OP_HASH160
OP_PUSHBYTES_20
ce3bc22f62fa552ade63f76b40b1c69e9d6155d9
OP_EQUAL

P2WPKH
Bech32

Example P2WPKH Address:

bc1qdwlv8cdqkvuqqy4v4f9817gpf46ct8ddw08qqn

42 characters

Example P2WPKH ScriptPubKey:

ASM Hex

OP_0
OP_PUSHBYTES_20
6bbec3e1a0b3380092acaa4a7ff9014d75859dad

P2WSH
Bech32

Example P2WSH Address:

bc1qnkfmv3yqfl98guple4p3p7ek9sc222esz95j9fyuzy2pqy8ydxxxqpyvluq

62 characters

Example P2WSH ScriptPubKey:

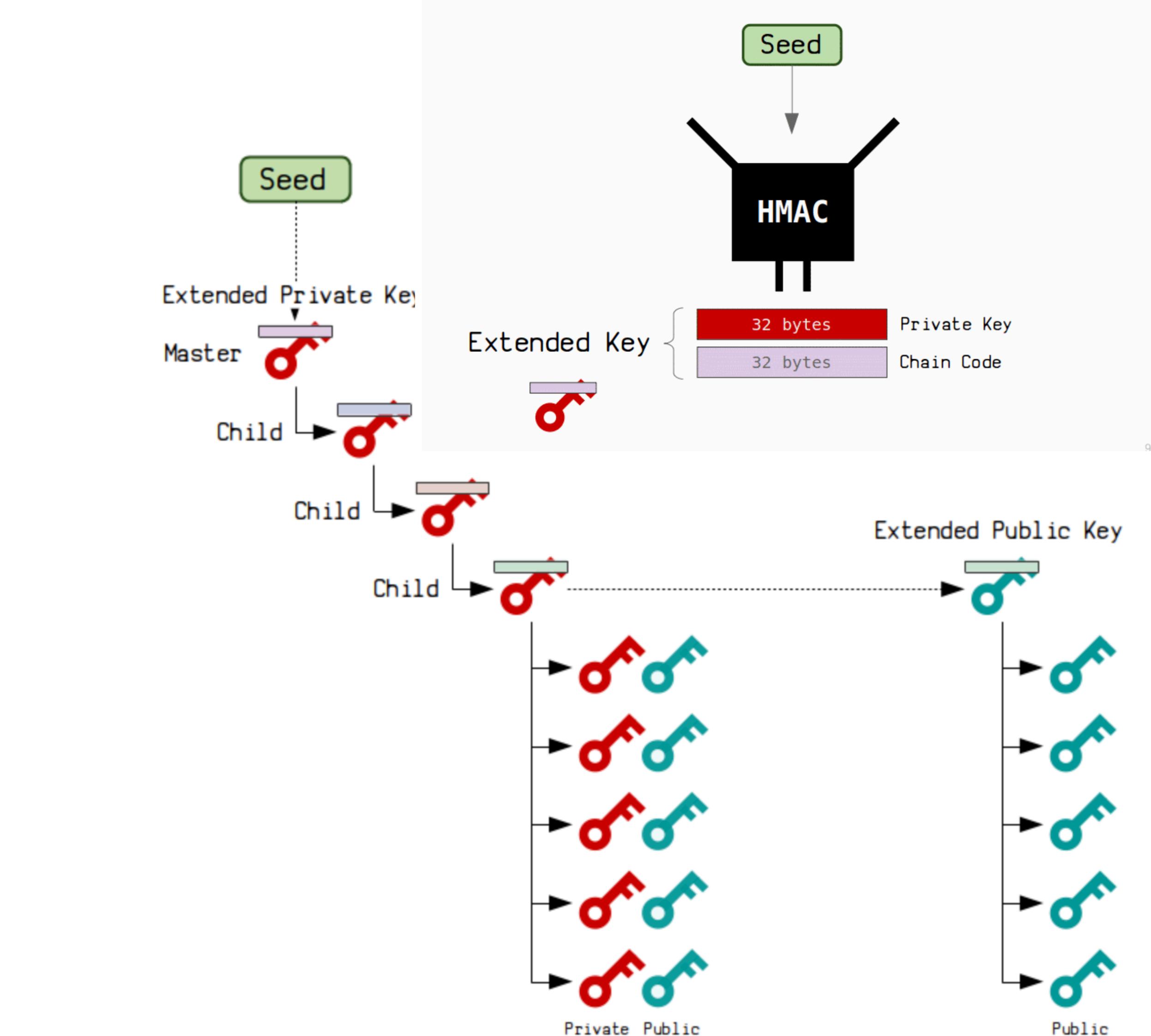
ASM Hex

OP_0
OP_PUSHBYTES_32
9d93b644804fc74703fc4310fb362c30a52b30116922a49c11141010e4698c

Les Wallets

Une infinité d'adresses

- A partir d'une **SEED** on dérive les clés publiques/privées correspondantes
- On appelle cela les **HD Wallets**
Hierarchical Deterministic Wallets
- Expérimentation: iancoleman.io/bip39

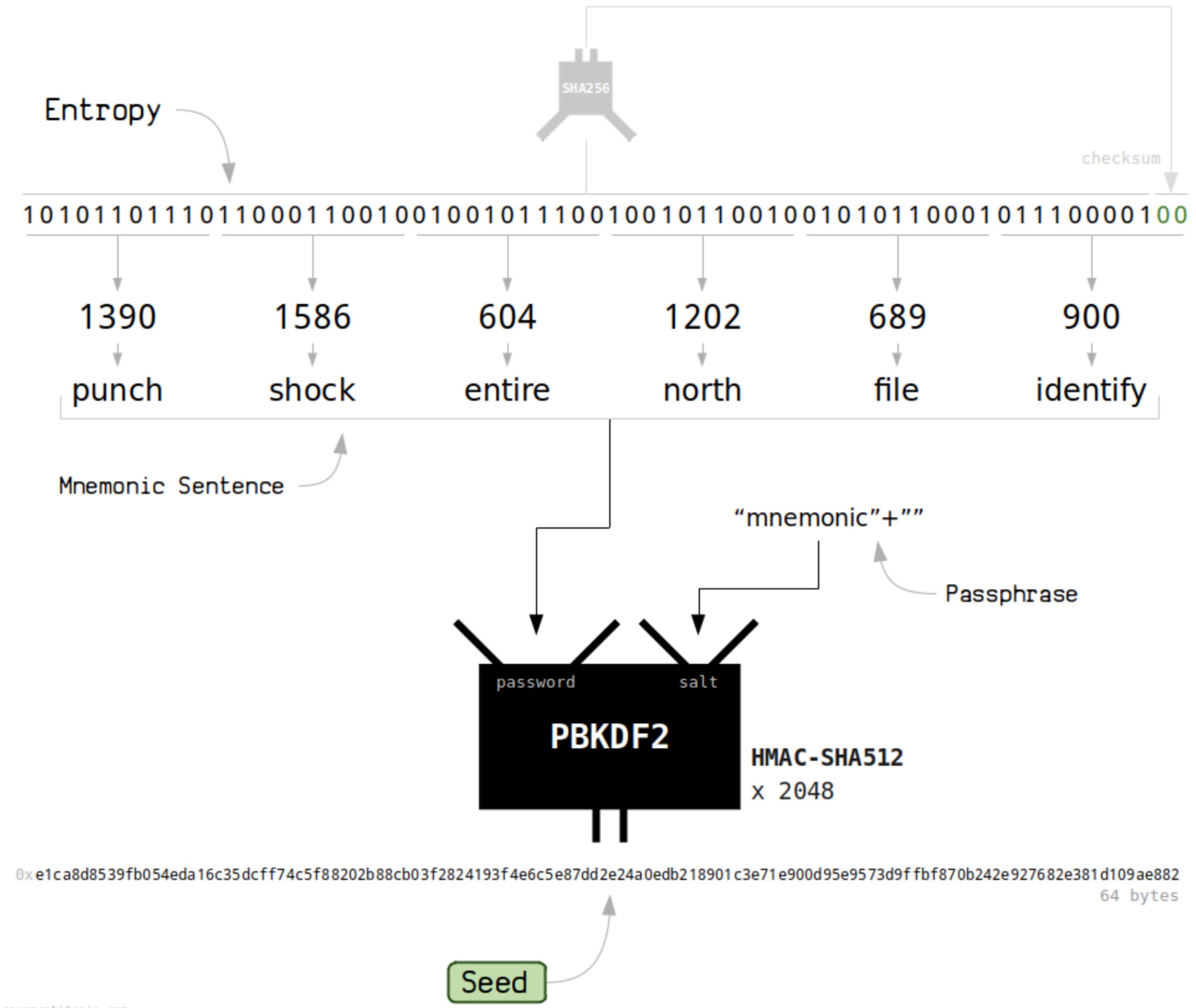


learnmeabitcoin.com

SEED

Du binaire à la phrase

- Une **SEEDPHRASE** désigne le MOT DE PASSE contenant entre 12 et 24 mots déverrouillant toutes les adresses associées
- Expérimentation: iancoleman.io/bip39



Des transactions
Dans des blocs
En réseau

Merci à tous
pour l'accueil 😊

QUESTIONS ?
Réponses !



Références

Pour aller plus loin

LUDOVIC LARS

L'ÉLÉGANCE DE BITCOIN

HISTOIRE, ENJEUX ET PRINCIPES

PRÉFACE DE JACQUES FAVIER



- LA BIBLE ! <https://learnmeabitcoin.com/>
- Tutoriel transactions (en python) par [Chaincodelabs](#) : [bitcoin-tx-tutorial](#)
- Forum officiel: <https://bitcointalk.org/index.php>
- Documentation API Mempool : <https://mempool.space/docs/faq>
- Exemple [bitcoinjs-lib](#): [p2tr bitcoin-js examples](#)
- Crate (Rust) bitcoin : <https://crates.io/crates/bitcoin>
- Cours bitcoin Rust de Chaincodelabs : <https://btcde-my.thinkific.com/>
- Discussions & Newsletters: [Delving Bitcoin](#), [Bitcoin optech](#)

KONSENSUS
NETWORK