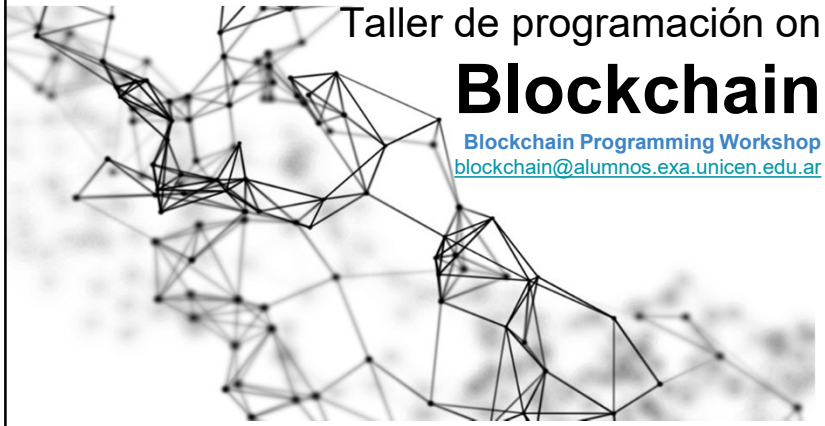
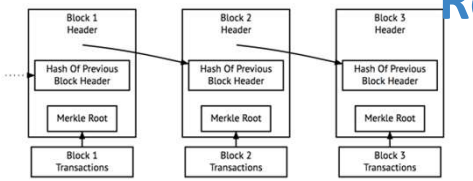


Taller de programación on

Blockchain

Blockchain Programming Workshop
blockchain@alumnos.exa.unicen.edu.ar

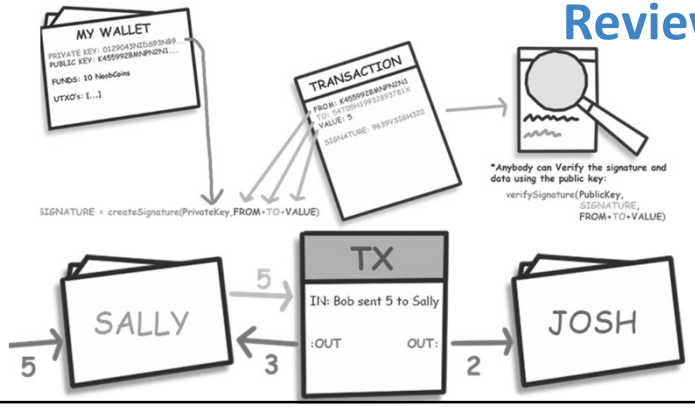
Blockchain Review



is a decentralized public database that keeps a permanent record of digital transactions.

It's a logfile storing an immutable record of all the digital transactions. This decentralized database is not controlled by a central administrator, but instead is a network of replicated databases (meaning each node in the network stores its own copy of the blockchain) that is shared and visible to anyone within network.

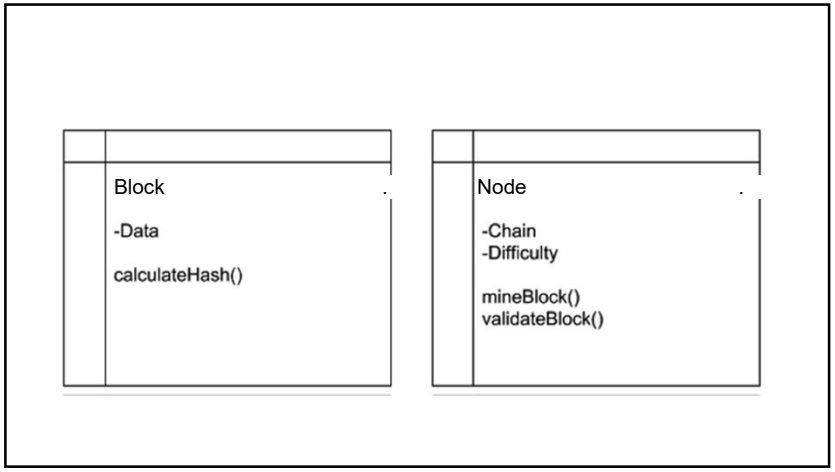
Review

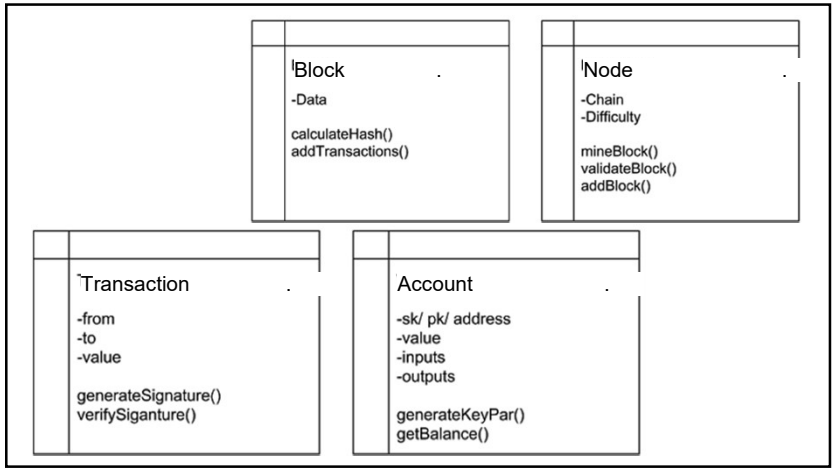


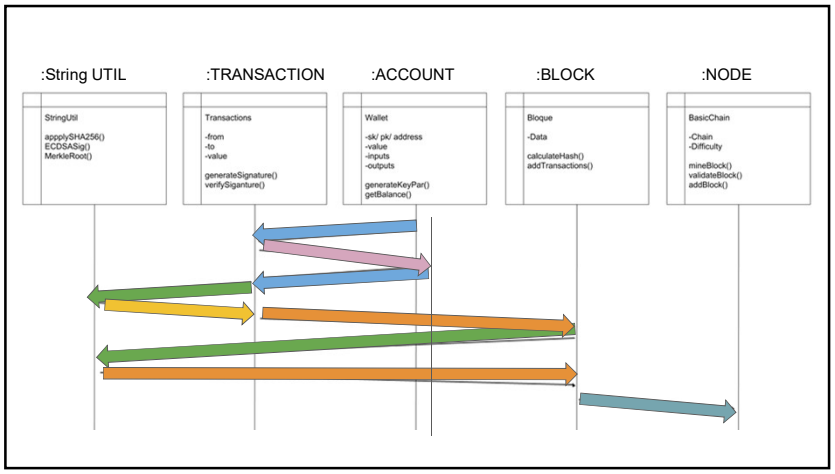
Trabajo Práctico

a) **Implementar en Java la estructura básica de una blockchain: transacciones, bloques, firmas digitales, nodos**
b) **Programar en Java los mecanismos básicos de validación de firma digital en transacciones y bloques.**
c) **Programar el proceso de seguimiento de balance de transacciones, no permitir transacciones en descubierto (sobre gasto).**

Voluntarios ?







:Schedule

1:

Introduction to Blockchain technology

2:

Peer-to-Peer Value Transfer System

3:

Blockchain as an application platform

4:

Smart contracts, Solidity and Web3

5:

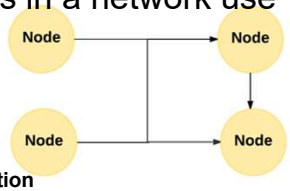
Tools for the safe development of Dapps

6:

Blockchain as a coordination platform

Protocol Layer

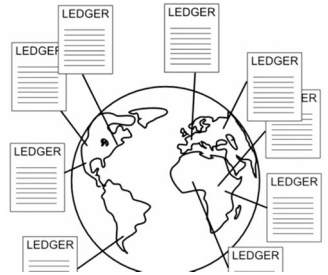
- special set of rules that nodes in a network use
- crypto economic rules



- **uses public key cryptography for authentication**
- **has economic incentives to ensure that the rules are followed**

Bitcoin (2009)

Is a cryptocurrency and payment system



Block rewards

Jan 2009 - Nov 2012: 50 BTC

Nov 2012 - Jul 2016: 25 BTC

Jul 2016 - Feb 2020*: 12.5 BTC

Feb 2020* - Sep 2023*: 6.25 BTC

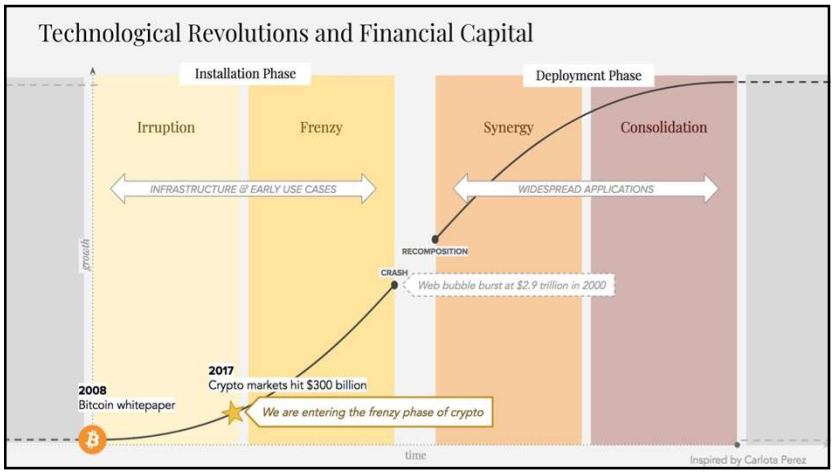
Economic incentive = Tokens

Objective: Maximize security of network

- Where "security" = compute power
- Therefore, super expensive to roll back changes to the transaction log

$$E(R_i) \ \alpha \ H_i * T$$

- E() = expected value
- **block rewards**
- hash power of actor = contribution to "security"
- **# tokens (BTC)** dispensed each block

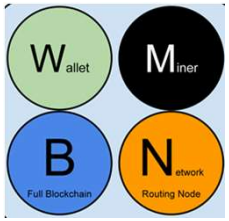


Nodes

Full-node client

Lightweight client

Third-party API client



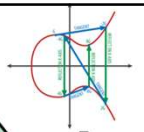
Wallets

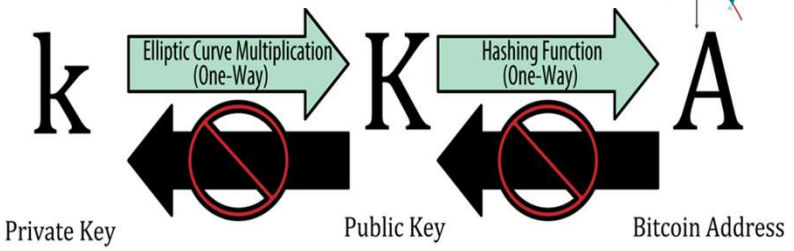
Desktop/Mobile/Web wallet

Paper wallet

Hardware wallet

Wallets Address





Kapoor, V., Abraham, V. S., & Singh, R. (2008). Elliptic curve cryptography. *Ubiquity*, *2008*(May), 7.
Hankerson, D., Menezes, A. J., & Vanstone, S. (2006). *Guide to elliptic curve cryptography*. Springer Science & Business Media.
Seroussi, G. (1999). Elliptic curve cryptography. In *Information Theory and Networking Workshop, 1999*(p. 41). IEEE.

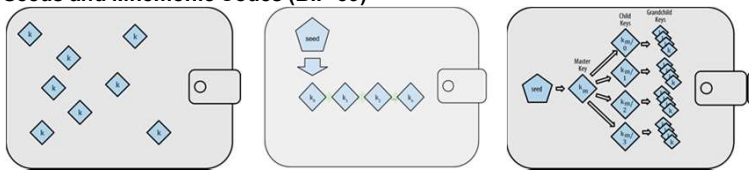
Wallet construction

Nondeterministic (Random) Wallets

Deterministic (Seeded) Wallets

HD Wallets (BIP-32/BIP-44)

Seeds and Mnemonic Codes (BIP-39)



Payment request QR code

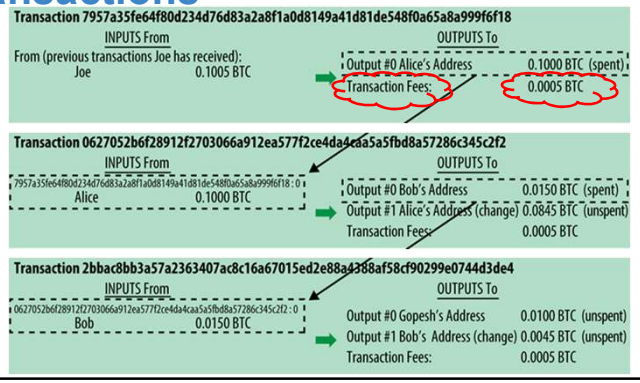
A bitcoin address: "1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA"

The payment amount: "0.015"

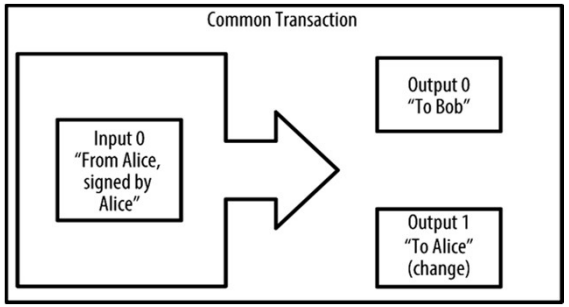
A label for the recipient address: "Bob's Cafe"

A description for the payment: "Purchase at Bob's Cafe"

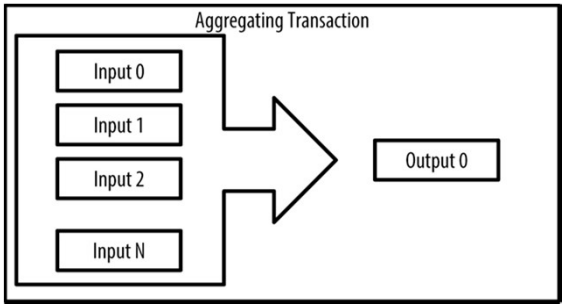
Transactions



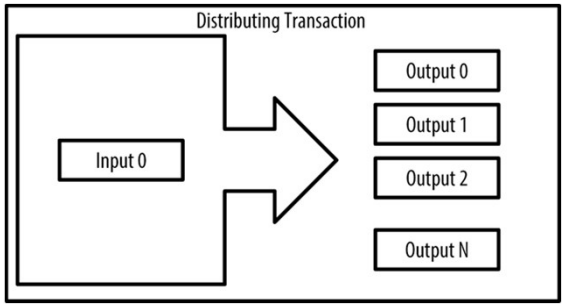
Balances



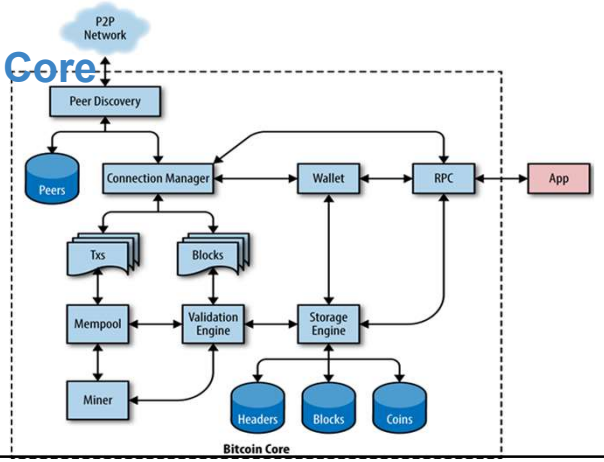
Input - 1 Output



1 Input - # Output

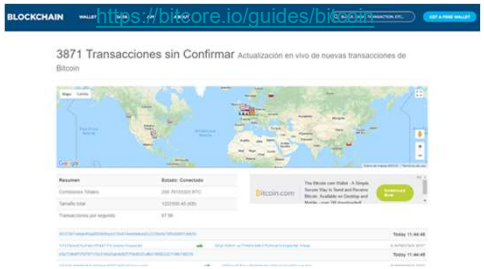


Bitcoin Core



Exploring Blocks and Transactions

https://blockchain.info/es/unconfirmed-transactions https://bitcore.io
https://blockchain.info/es



Exploring Transaction

$ bitcoin-cli getrawtransaction
0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2

0100000001186f9f998a5aa6f048e51dd8419a14d8a0f1a8a2836dd734d2804fe
65fa35779000000008b483045022100884d142d86652a3f47ba4746ec719bbfb
d040a570b1deccbb6498c75c4ae24cb02204b9f039ff08df09cbe9f6addac9602
98cad530a863ea8f53982c09db8f6e381301410484ecc0d46f1918b30928fa0e4
ed99f16a0fb4fde0735e7ade8416ab9fe423cc5412336376789d172787ec3457
eee41c04f4938de5cc17b4a10fa336a8d752adffffffff0260e3160000000000197
6a914ab68025513c3dbd2f7b92a94e0581f5d50f654e788acd0ef80000000000
01976a9147f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a888ac00000000

Exploring Transaction

$ bitcoin-cli getrawtransaction decoderawtransaction
0100000001186f9f998a5aa6f048e51dd8419a14d8a0f1a8a2836dd734d2804fe
65fa35779000000008b483045022100884d142d86652a3f47ba4746ec719bbfb
d040a570b1deccbb6498c75c4ae24cb02204b9f039ff08df09cbe9f6addac9602
98cad530a863ea8f53982c09db8f6e381301410484ecc0d46f1918b30928fa0e4
ed99f16a0fb4fde0735e7ade8416ab9fe423cc5412336376789d172787ec3457
eee41c04f4938de5cc17b4a10fa336a8d752adffffffff0260e3160000000000197
6a914ab68025513c3dbd2f7b92a94e0581f5d50f654e788acd0ef80000000000
01976a9147f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a888ac00000000

Exploring Transaction


```
{
 "txid": "0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2",
 "size": 258,
 "version": 1,
 "locktime": 0,
 "vin": [
  {
   "txid": "7957a35fe64f80d234d76d83a2...8149a41d81de548f0a65a8a999f6f18",
   "vout": 0,
   "scriptSig": {
    "asm":"3045022100884d142d86652a3f47ba4746ec719bbfbd040a570b1decc...",
    "hex":"483045022100884d142d86652a3f47ba4746ec719bbfbd040a570b1de..."
   },
   "sequence": 4294967295
  }
 ],
 "vout": [
  {
   "value": 0.01500000,
```


Exploring Transaction


```
 "vout": [
  {
   "value": 0.01500000,
   "n": 0,
   "scriptPubKey": {
    "asm": "OP_DUP OP_HASH160 ab68...5f654e7 OP_EQUALVERIFY OP_CHECKSIG",
    "hex": "76a914ab68025513c3dbd2f7b92a94e0581f5d50f654e788ac",
    "reqSigs": 1,
    "type": "pubkeyhash",
    "addresses": [
     "1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA"
    ]
   }
  },
  {
   "value": 0.08450000,
   "n": 1,
   "scriptPubKey": {
```


Exploring Transaction


```
  {
   "value": 0.08450000,
   "n": 1,
   "scriptPubKey": {
    "asm": "OP_DUP OP_HASH160 7f9b1a...025a8 OP_EQUALVERIFY OP_CHECKSIG",
    "hex": "76a9147f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a888ac",
    "reqSigs": 1,
    "type": "pubkeyhash",
    "addresses": [
     "1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK"
    ]
   }
  }
 ]
}
```


Exploring Block

$ bitcoin-cli getblock 0000000000000001b6b9a13b095e96db41c4a928b97ef2d944a9b3↵
1b2cc7bdc4


```
{
 "hash": "0000000000000001b6b9a13b095e96db41c4a928b97ef2d944a9b31b2cc7bdc4",
 "confirmations": 37371,
 "size": 218629,
 "height": 277316,
 "version": 2,
 "merkleroot": "c91c008c26e50763e9f548bb8b2fc323735f73577effbc55502c51eb4cc7cf2e",
 "tx": [
  "d5ada064c6417ca25c4308bd158c34b77e1c0eca2a73cda16c737e7424afba2f",
  "b268b45c59b39d759614757718b9918caf0ba9d97c56f3b91956ff877c503fbe",
  "04905ff987ddd4cfe603b03cfb7ca50ee81d89d1f8f5f265c38f763eea4a21fd",
  "32467aab5d04f51940075055c2f20bbd1195727c961431bf0aff8443f9710f81",
  "561c5216944e21fa29dd12aaa1a45e3397f9c0d888359cb05e1f79fe73da37bd",
[... hundreds of transactions ...]
  "78b300b2a1d2d9449b58db7bc71c3884d6e0579617e0da4991b9734cef7ab23a",
  "6c87130ec283ab4c2c493b190c20de4b28ff3caf72d16ffa1ce3e96f2069aca9",
  "6f423dbc3636ef193fd8898dfdf7621dcade1bbe509e963ffbff91f696d81a62",
```

Exploring Block


```
  "78b300b2a1d2d9449b58db7bc71c3884d6e0579617e0da4991b9734cef7ab23a",
  "6c87130ec283ab4c2c493b190c20de4b28ff3caf72d16ffa1ce3e96f2069aca9",
  "6f423dbc3636ef193fd8898dfdf7621dcade1bbe509e963ffbff91f696d81a62",
  "802ba8b2adabc5796a9471f25b02ae6aeee2439c679a5c33c4bbcee97e081196",
  "eaaf6a048588d9ad4d1c092539bd571dd8af30635c152a3b0e8b611e67d1a1af",
  "e67abc6bd5e2cac169821afc51b207127f42b92a841e976f9b752157879ba8bd",
  "d38985a6a1bfd35037cb7776b2dc86797abbb7a06630f5d03df2785d50d5a2ac",
  "45ea0a3f6016d2bb90ab92c34a7aac9767671a8a84b9bcce6c019e60197c134b",
  "c098445d748ced5f178ef2ff96f2758cbec9eb32cb0fc65db313bcac1d3bc98f"
 ],
 "time": 1388185914,
 "mediantime": 1388183675,
 "nonce": 924591752,
 "bits": "1903a30c",
 "difficulty": 1180923195.258026,
 "chainwork": "0000000000000000000000000000000000000000000000000934695e92aaf53afa1a",
 "previousblockhash": "000000000000002a7bbd25a417c0374cc55261021e8a9ca74442b01284f0569",
 "nextblockhash": "00000000000000010236c269dd6ed714dd5db39d36b33959079d78dfd431ba7"
}
```


Blockchain Scalability

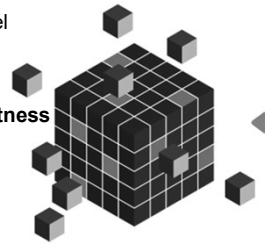
Transactions channel

Transactions format

Segregated Witness

Block limits

Mempool

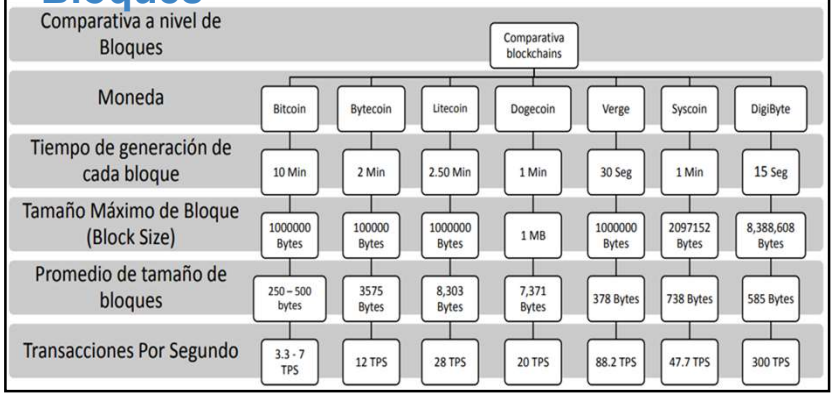


Average block time

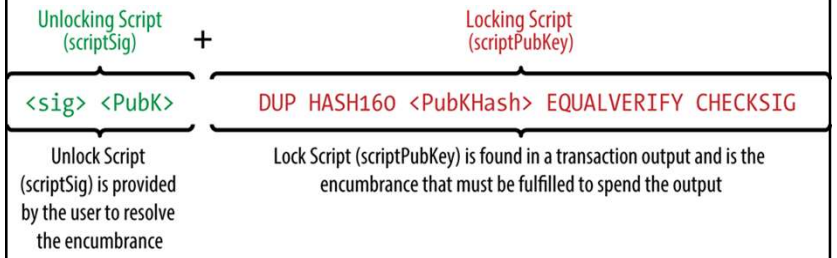
BTC: 10 minutes

ETH: 15 Seconds

Bloques

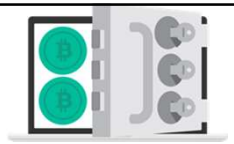


Transaction Format (Assembler Verification)



Segregated Witness

Signature advanced



Multisignature

Locking Script	2 PubKey1 PubKey2 PubKey3 PubKey4 PubKey5 5 CHECKMULTISIG
Unlocking Script	Sig1 Sig2

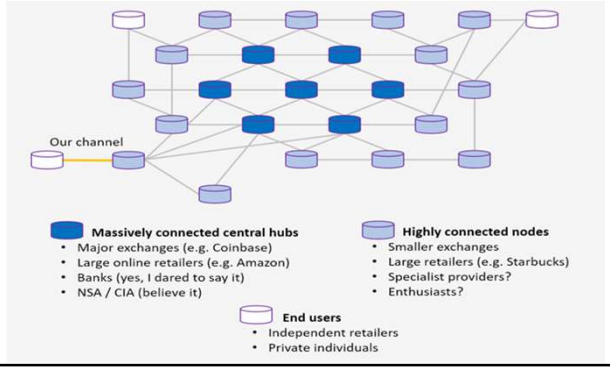
Pay-to-Script-Hash (P2SH)

Redeem Script	2 PubKey1 PubKey2 PubKey3 PubKey4 PubKey5 5 CHECKMULTISIG
Locking Script	HASH160 <20-byte hash of redeem script> EQUAL
Unlocking Script	Sig1 Sig2 <redeem script>

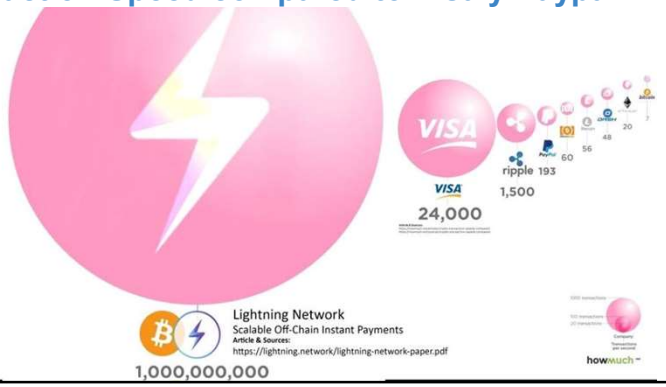
Multisignature by <Smart Contracts>

```
contract EscrowWithDelay(
  sender: PublicKey,
  recipient: PublicKey,
  escrow: PublicKey,
  delay: Duration,
  val: Value
) {
  clause transfer(sig1: Signature, sig2: Signature) {
    verify checkMultiSig([sender, recipient, escrow],
                         [sig1, sig2])
    unlock val
  }
  clause timeout(sig: Signature) {
    verify checkSig(sender, sig)
    verify older(delay)
    unlock val
  }
}
```

Routed Payment Channels (Lightning Network)



Transaction Speed compared to Visa y Paypal



CryptoNetwork

https://bitcoin.org/ https://www.bitcoinargentina.org