

Taller de programación on

Blockchain

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

Blockchain

Review

The diagram illustrates a blockchain structure with three blocks. Each block is represented as a box containing a 'Block X Header' (where X is 1, 2, or 3). Inside each header box, there is a 'Hash Of Previous Block Header' and a 'Merkle Root'. Below the header box is a box for 'Block X Transactions'. Arrows indicate the flow of data: from 'Block 1 Transactions' to 'Block 1 Merkle Root', from 'Block 1 Merkle Root' to 'Block 1 Hash Of Previous Block Header', from 'Block 1 Hash Of Previous Block Header' to 'Block 2 Hash Of Previous Block Header', from 'Block 2 Transactions' to 'Block 2 Merkle Root', from 'Block 2 Merkle Root' to 'Block 2 Hash Of Previous Block Header', from 'Block 2 Hash Of Previous Block Header' to 'Block 3 Hash Of Previous Block Header', from 'Block 3 Transactions' to 'Block 3 Merkle Root', and from 'Block 3 Merkle Root' to 'Block 3 Hash Of Previous Block Header'. A dashed arrow points to the 'Hash Of Previous Block Header' of Block 1.

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.

MY WALLET

PRIVATE KEY: 0129043NDS0P09R
PUBLIC KEY: K4509P0ANPNZNG...
FUNDS: 10 NeoCoins
UTXOs: [...]

TRANSACTION

FROM: K4509P28NPN2NI
TO: 04T09N4P999937B1A
VALUE: 5
SIGNATURE: 9L3PVS55H3D0

Review

*Anybody can Verify the signature and data using the public key:

verifySignature(PublicKey, SIGNATURE, FROM-TO-VALUE)

SALLY

TX

IN: Bob sent 5 to Sally
OUT: 3

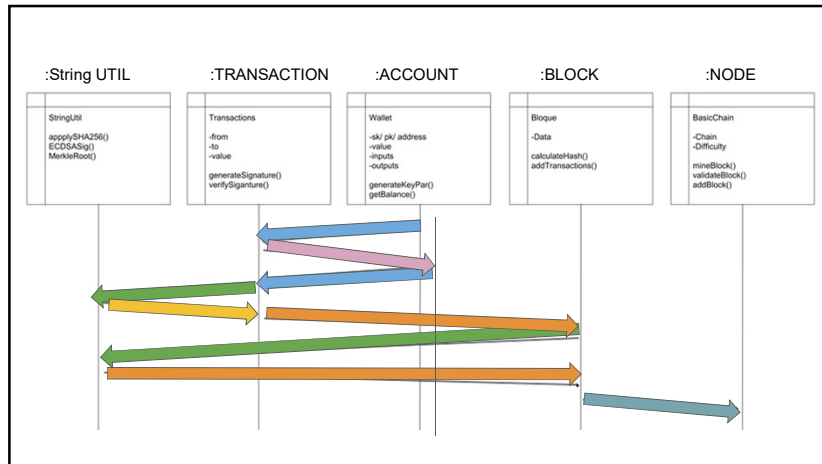
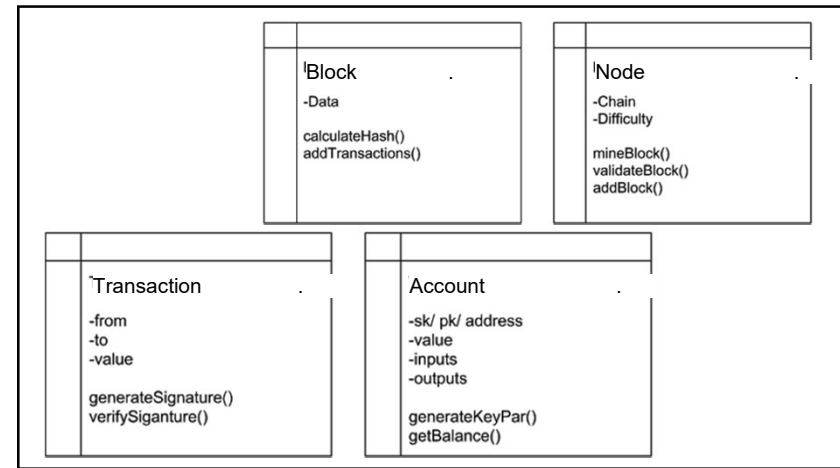
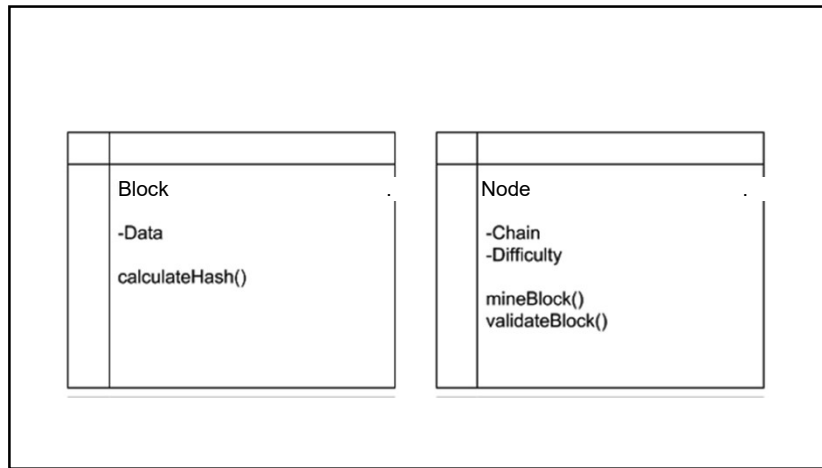
JOSH

2

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 ?

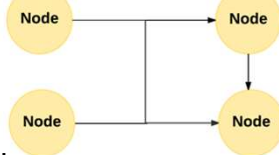


:Schedule

- 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

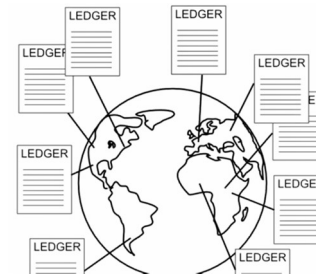
- special set of rules that nodes in a network use
- crypto economic rules



- 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

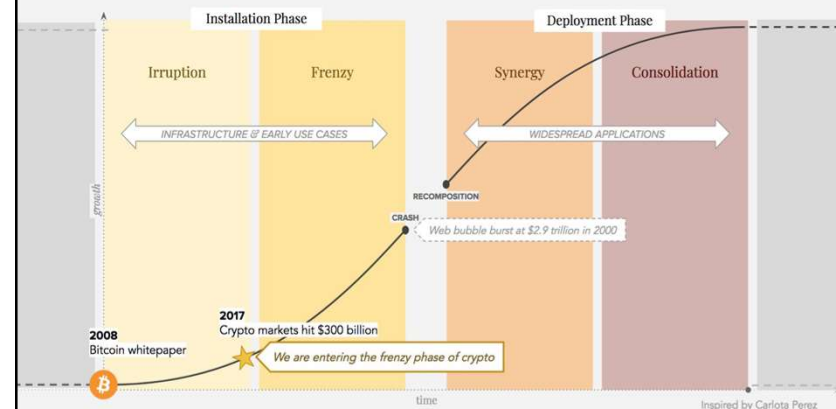
Objective: Maximize security of network

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

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

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

Technological Revolutions and Financial Capital

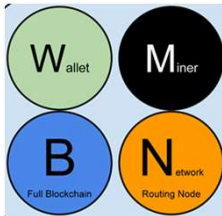


Nodes

Full-node client

Lightweight client

Third-party API client



Wallets

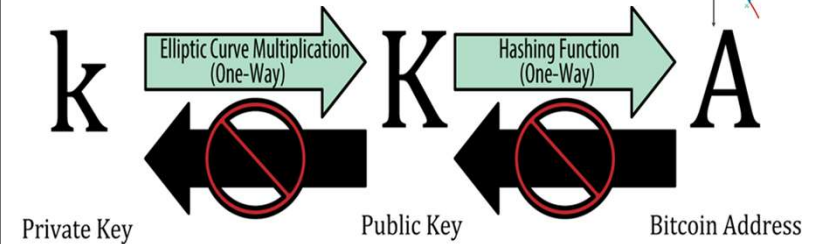
Desktop/Mobile/Web wallet

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.

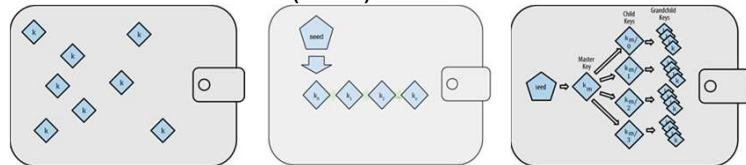
Wallet construction

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"

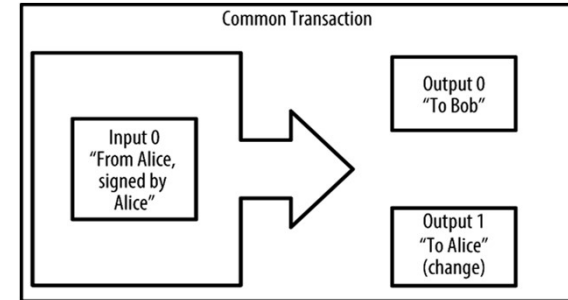
A label for the recipient address: "Bob's Cafe"

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

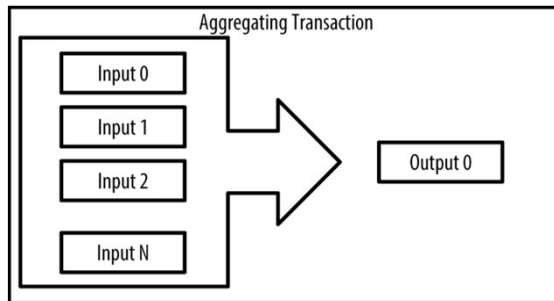
Transactions

Transaction 7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18	
INPUTS From	OUTPUTS To
From (previous transactions Joe has received): Joe 0.1005 BTC	Output #0 Alice's Address 0.1000 BTC (spent)
	Transaction Fees: 0.0005 BTC
Transaction 0627052b6f28912f2703066a912ea577f2ce4da4c6a5a5fbd8a57286c345c2f2	
INPUTS From	OUTPUTS To
7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18 : 0 Alice 0.1000 BTC	Output #0 Bob's Address 0.0150 BTC (spent)
	Output #1 Alice's Address (change) 0.0845 BTC (unspent)
	Transaction Fees: 0.0005 BTC
Transaction 2bbac8bb3a57a2363407ac8c16a67015ed2e88a4388af58cf90299e0744d3de4	
INPUTS From	OUTPUTS To
0627052b6f28912f2703066a912ea577f2ce4da4c6a5a5fbd8a57286c345c2f2 : 0 Bob 0.0150 BTC	Output #0 Gopesh's Address 0.0100 BTC (unspent)
	Output #1 Bob's Address (change) 0.0045 BTC (unspent)
	Transaction Fees: 0.0005 BTC

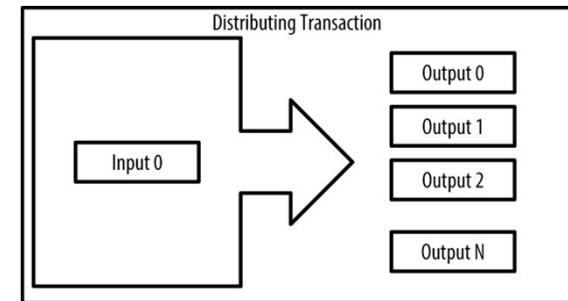
Balances

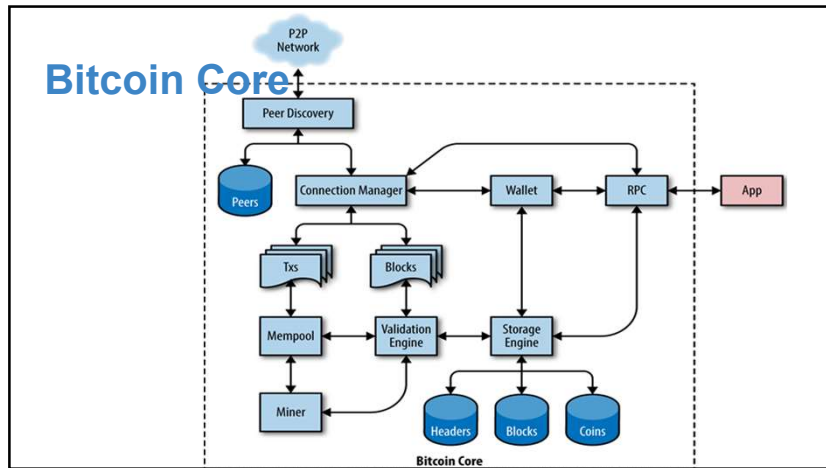


Input - 1 Output



1 Input - # Output





Exploring Blocks and Transactions

<https://blockchain.info/es/unconfirmed-transactions>
<https://blockchain.info/es>

<https://bitcore.io>

<https://bitcore.io/guides/bitcoin.html>



Exploring Transaction

\$ bitcoin-cli getrawtransaction

0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2

```
0100000001186f9f998a5aa6f048e51dd8419a14d8a0f1a8a2836dd734d2804fe
65fa35779000000008b483045022100884d142d86652a3f47ba4746ec719bbfb
d040a570b1deccbb6498c75c4ae24cb02204b9f039ff08df09cbe9f6addac9602
98cad530a863ea8f53982c09db8f6e381301410484ecc0d46f1918b30928fa0e4
ed99f16a0fb4fde0735e7ade8416ab9fe423cc5412336376789d172787ec3457
eee41c04f4938de5cc17b4a10fa336a8d752adffffff0260e31600000000000197
6a914ab68025513c3dbd2f7b92a94e0581f5d50f654e788acd0ef80000000000
01976a9147f9b1a7fb68d60c536c2fd8aeea53a8f3cc025a888ac00000000
```

Exploring Transaction

\$ bitcoin-cli getrawtransaction decoderawtransaction

```
0100000001186f9f998a5aa6f048e51dd8419a14d8a0f1a8a2836dd734d2804fe
65fa35779000000008b483045022100884d142d86652a3f47ba4746ec719bbfb
d040a570b1deccbb6498c75c4ae24cb02204b9f039ff08df09cbe9f6addac9602
98cad530a863ea8f53982c09db8f6e381301410484ecc0d46f1918b30928fa0e4
ed99f16a0fb4fde0735e7ade8416ab9fe423cc5412336376789d172787ec3457
eee41c04f4938de5cc17b4a10fa336a8d752adffffff0260e31600000000000197
6a914ab68025513c3dbd2f7b92a94e0581f5d50f654e788acd0ef80000000000
01976a9147f9b1a7fb68d60c536c2fd8aeea53a8f3cc025a888ac00000000
```

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": {
      "asm": "OP_DUP OP_HASH160 7f9b1a...025a8 OP_EQUALVERIFY OP_CHECKSIG",
```

Exploring Transaction

```
{
  "value": 0.08450000,
  "n": 1,
  "scriptPubKey": {
    "asm": "OP_DUP OP_HASH160 7f9b1a...025a8 OP_EQUALVERIFY OP_CHECKSIG",
    "hex": "76a9147f9b1a7fb68d60c536c2fd8aeea53a8f3cc025a888ac",
    "reqSigs": 1,
    "type": "pubkeyhash",
    "addresses": [
      "1Cddi9KFAatwczBwBttQcwXYCpvK8h7FK"
    ]
  }
}
```

Exploring Block

\$ bitcoin-cli getblock 000000000000001b6b9a13b095e96db41c4a928b97ef2d944a9b341b2cc7bdc4

```
{
  "hash": "000000000000001b6b9a13b095e96db41c4a928b97ef2d944a9b31b2cc7bdc4",
  "confirmations": 37371,
  "size": 218629,
  "height": 277316,
  "version": 2,
  "merkleroot": "c91c008c26e50763e9f548bb8b2fc323735f73577effbc55502c51eb4cc7cf2e",
  "tx": [
    "d5ada064c6417ca25c4308bd158c34b77e1c0eca2a73cda16c737e7424afba2f",
    "b268b45c59b39d759614757718b9918caf0ba9d97c56f3b91956ff877c503fbc",
    "04905ff987dd4cfe603b03cfb7ca50ee81d89d1f8f5f265c38f763ee4a21fd",
    "32467aab5d04f51940075055c2f20bbd1195727c961431bf0aff8443f9710f81",
    "561c5216944e21fa29dd12aaa1a45e3397f9c0d888359cb05e1f79fe73da37bd",
    "... hundreds of transactions ..."
  ],
  "txs": [
    "78b300b2a1d2d9449b58db7bc71c3884d6e0579617e0da4991b9734cef7ab23a",
    "6c87130ec283ab4c2c493b190c20de4b28ff3caf72d16ffa1ce3e96f2069aca9",
    "6f423dbc3636ef193fd8898dfdf7621dcade1bbe509e963ffbf91f696d81a62",
    "802ba8b2ed4ba5706e047449fb02ae6e9e2439e529e5a22e4fbb9e987e084406"
```

Exploring Block

```

"78b300b2a1d2e9449b58db7bc71c3884d6e0579617e0da4991b9734cef7ab23a",
"6c87130ec283ab4c2c493b190c20de4b28ff3caf72d16ffa1ce3e9672069ac9a",
"6f423dbcc3636fe193fd889d87f7621dcade1bffe509e963ffbf91f69d681a62",
"802b8a2adabc65796a9471f25b02a6eaae2439c67c9a533c4bbccc9e7e081196",
"eaa6fa0d8588d9ad4ad1c092539bd571dd8af30635c152a3b0e8b61e67d1a1a1a",
"6e7abcb6bd5e2cac169821afc51b20712744b29a841e769b75218759b9a8d8",
"d3895a5a6a1bfd35037cb7776b2d86797abb7a06630f05d0327d85805da5a2ac",
"45ea0a3f6016d2bb90ab92c34a7aac9767671a8a849b9ccce6c1906197c134b",
"0c98445d748ced5f178f27f9f67258cbec9eb32c0fc65d0b313bcbac13c3c98f"
],
"time": 1388185914,
"mediantime": 1388183675,
"nonce": 924591752,
"bits": "1903a30c",
"difficulty": 1180923195.258026,
"chainwork": "00000000000000000000000000000000000000000000000000934a5e92aaf53afa1a",
"previousblockhash": "00000000000000000000002a7b25da417c0374cc555261021e8a9ca74442b01284f0569",
"nextblockhash": "00000000000000000000010236c269dd6ed714dd5db39d36b33959079d78dfd431ba7"
}

```

Blockchain Scalability

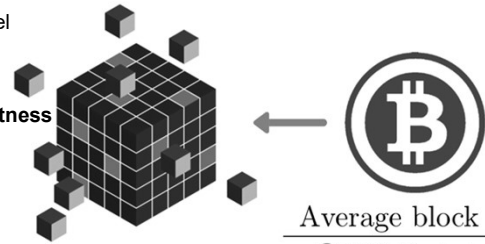
Transactions channel

Transactions format

Segregated Witness

Block limits

Mempool



Average block time

● BTC: 10 minutes

◆ ETH: 15 Seconds

Bloques

Comparativa a nivel de Bloques

Comparativa a nivel de Bloques	Comparativa blockchains						
Moneda	Bitcoin	Bytecoin	Litecoin	Dogecoin	Verge	Syscoin	DigiByte
Tiempo de generación de cada bloque	10 Min	2 Min	2.50 Min	1 Min	30 Seg	1 Min	15 Seg
Tamaño Máximo de Bloque (Block Size)	100000 Bytes	10000 Bytes	100000 Bytes	1 MB	100000 Bytes	2097152 Bytes	8,388,608 Bytes
Promedio de tamaño de bloques	250 – 500 bytes	3575 Bytes	8,303 Bytes	7,371 Bytes	378 Bytes	738 Bytes	585 Bytes
Transacciones Por Segundo	3.3 - 7 TPS	12 TPS	28 TPS	20 TPS	88.2 TPS	47.7 TPS	300 TPS

Transaction Format (Assembler Verification)

Unlocking Script (scriptSig)

+

Locking Script
(scriptPubKey)

<sig> <PubK>

DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG

Unlock Script
(scriptSig) is provided
by the user to resolve
the encumbrance

Lock Script (scriptPubKey) is found in a transaction output and is the encumbrance that must be fulfilled to spend the output

Segregated Witness

Signature advanced



Multisignature

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

Pay-to-Script-Hash (P2SH)

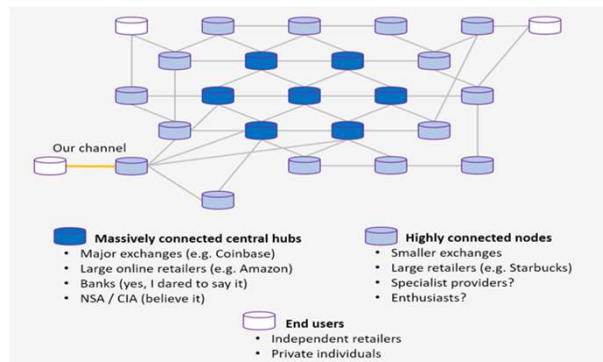
Redeem Script	2 PubKey1 PubKey2 PubKey3 PubKey4 PubKey5 5 CHECKMULTISIG
Locking Script	HASH160 <20-byte hash of redeem script> EQUAL
Unlocking Script	Sig1 Sig2 <redeem script>



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



