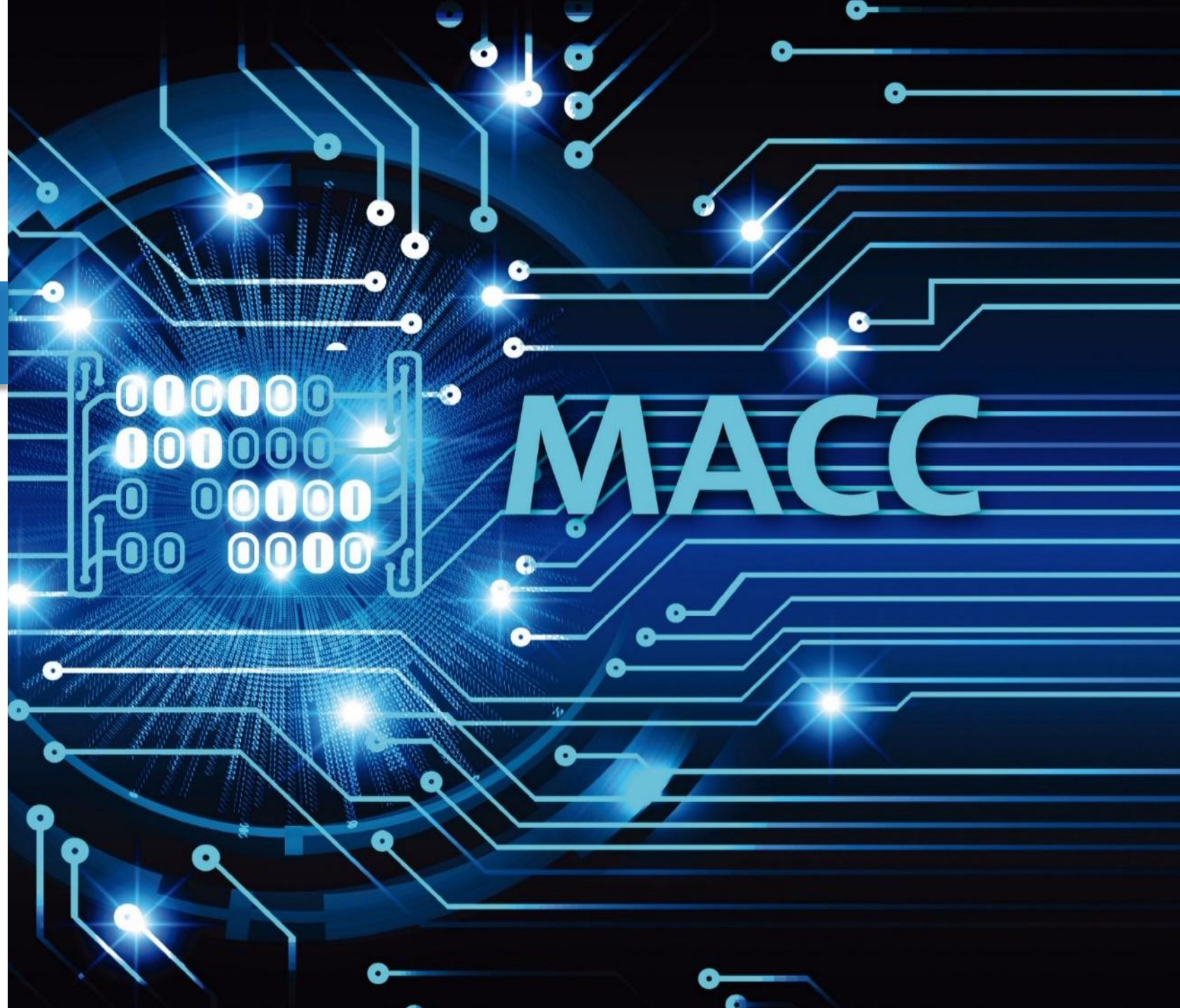
Universidad del Rosario

MACC
Matemáticas Aplicadas y Ciencias de la Computación

Introducción a Blockchain



Daniel Orlando Díaz López, PhD

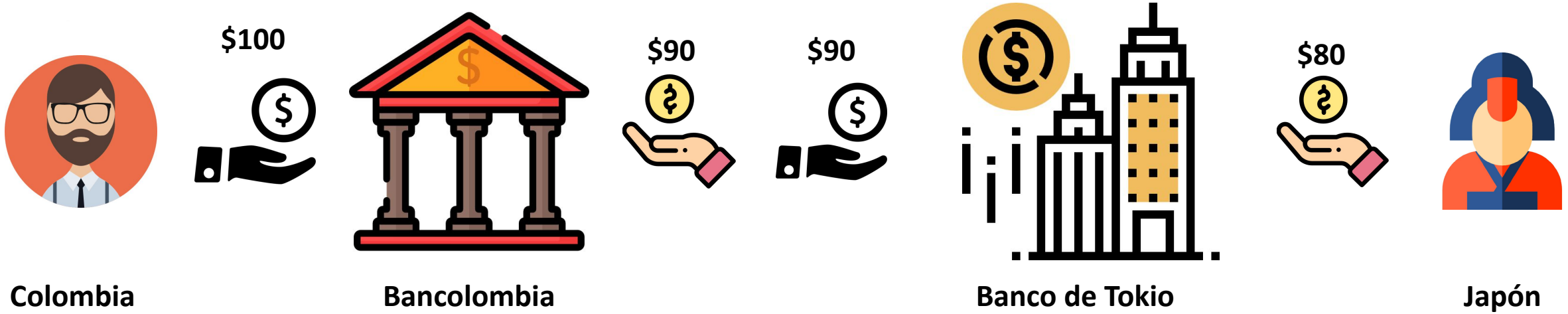
Profesor principal
Departamento MACC
Universidad del Rosario
danielo.diaz@urosario.edu.co

Tabla de contenido

Sistema Bancario Tradicional

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

Ejemplo de transacción interbancaria usando el Sistema Bancario Tradicional



Problemas

- Se paga una comisión por cada transacción
- Transacciones nacionales entre distintos bancos tardan 1 día
- Transacciones internacionales pueden tardar hasta 5 días
- El banco lleva un registro de todas las transacciones y ese registro es susceptible de ser atacado
- El banco se convierte en un objetivo atractivo para un cibercriminal

¡El banco nos da una sensación de **seguridad/confianza** por la cual pagamos una comisión!

Sistema Bancario Tradicional

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

¿Podemos confiar en la seguridad de un banco?

ORGANIZACIÓN CRIMINAL

Así 'hackeó' cuentas bancarias en 27 países la red de Babá, el nigeriano

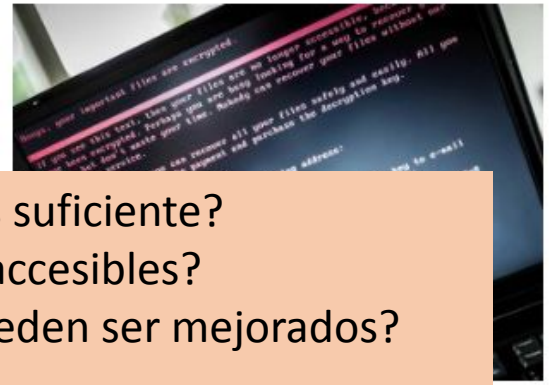
JOSÉ ANTONIO HERNÁNDEZ | 19/06/2018 · 12:48 CEST

Bancolombia presentó fallas a nivel nacional en pleno día de quincena

El robo del siglo que no alcanzó a ser

Judicial 18 Dic 2014 - 12:25 PM
Por: Redacción Judicial

Un grupo de hackers logró traspasar $160.000 millones a unas 360 cuentas de Bancolombia. Debido a los controles internos de la entidad, los ladrones sólo tuvieron acceso al 4% de lo que se planeaban apropiar.



Banco de Malta cierra operaciones por ataque cibernético

En el incidente informático los cibercriminales transfirieron dine

Comentar 1
Facebook
Twitter
Guardar
Enviar
Linkedin

Además de suspender sus operaciones, el banco de La Valetta cerró sus sucursales y cajeros en la isla mediterránea y desactivó su sitio web.
Foto: Darrin Zammit Lupi/ Reuters

Bancolombia restableció todos los canales que durante este presentado **fallas a nivel nacional**, según lo reportaron una gran des sociales.

¿La **seguridad** ofrecida por un banco es suficiente?
¿Los **costos** del sistema bancario son accesibles?
¿Los **tiempos de comunicación** entre bancos pueden ser mejorados?

El mayor ciberatraco en la historia de México mantiene en vilo al sistema bancario

E. CAMHAJI | 18/05/2018 · 19:05 CEST

Sistema Bancario Tradicional

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

¿Qué pasaría si el control de las transacciones no estuviese a cargo de una organización bancaria sino de múltiples componentes (nodos de una red)?

- ✔ El registro de las transacciones estaría almacenado entre múltiples nodos
- ✔ No pagaríamos altas comisiones por transacción
- ✔ Las transacciones serían (casi) inmediatas entre usuarios independiente de la ubicación geográfica
- ✔ Un cibercriminal tendría que atacar un porcentaje importante de nodos (>50%) para vulnerar el sistema

¡Blockchain permite que no hayan intermediarios y que aún así exista un control total sobre el estado de las transacciones!

Blockchain

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

¿Que es?

- Cada usuario tiene una copia de las transacciones (base de datos)
- La información de las transacciones se encuentra ahora distribuida y es controlada por todos los usuarios

¡No hay una autoridad central!

¿Es seguro?

Si, porque dado que la información es controlada por los usuarios, se requeriría que el 51% de los usuarios fueran atacados (Muy difícil)

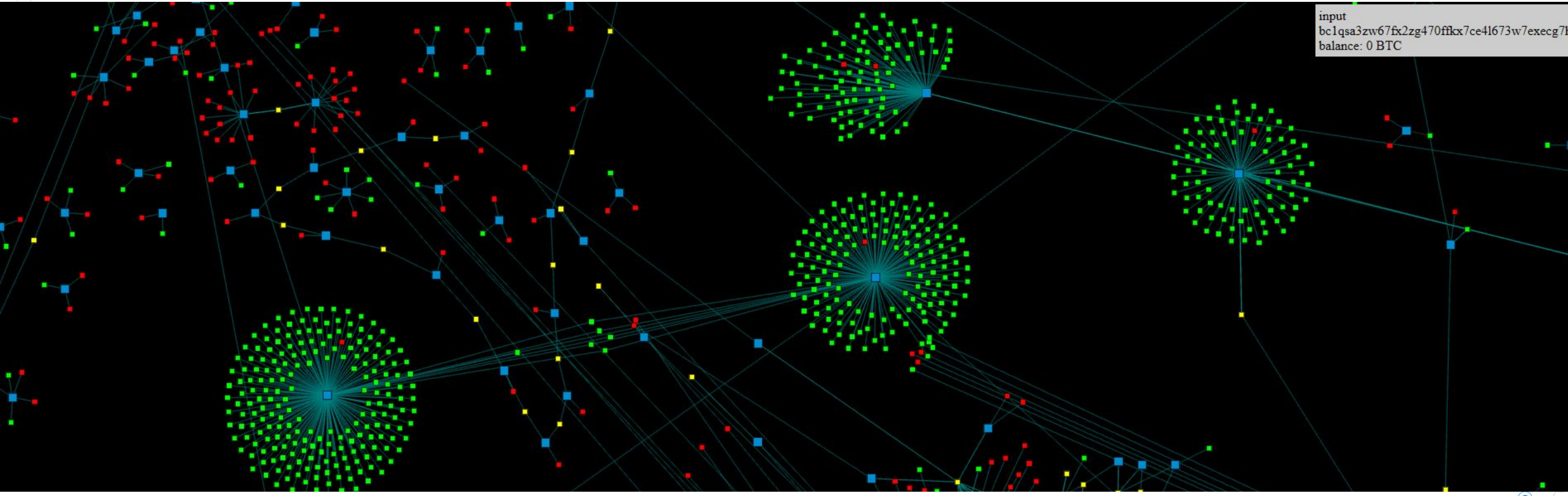
¿Puedo poner mas dinero en mi cuenta?

Inicialmente si, pero la cada transacción será validada por otros usuarios por lo que un incremento no justificado de dinero no sería aprobado y el cambio sería rechazado

Blockchain

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

¿Cómo luce una blockchain? -> Transacciones de Blockchain Bitcoin en tiempo real:

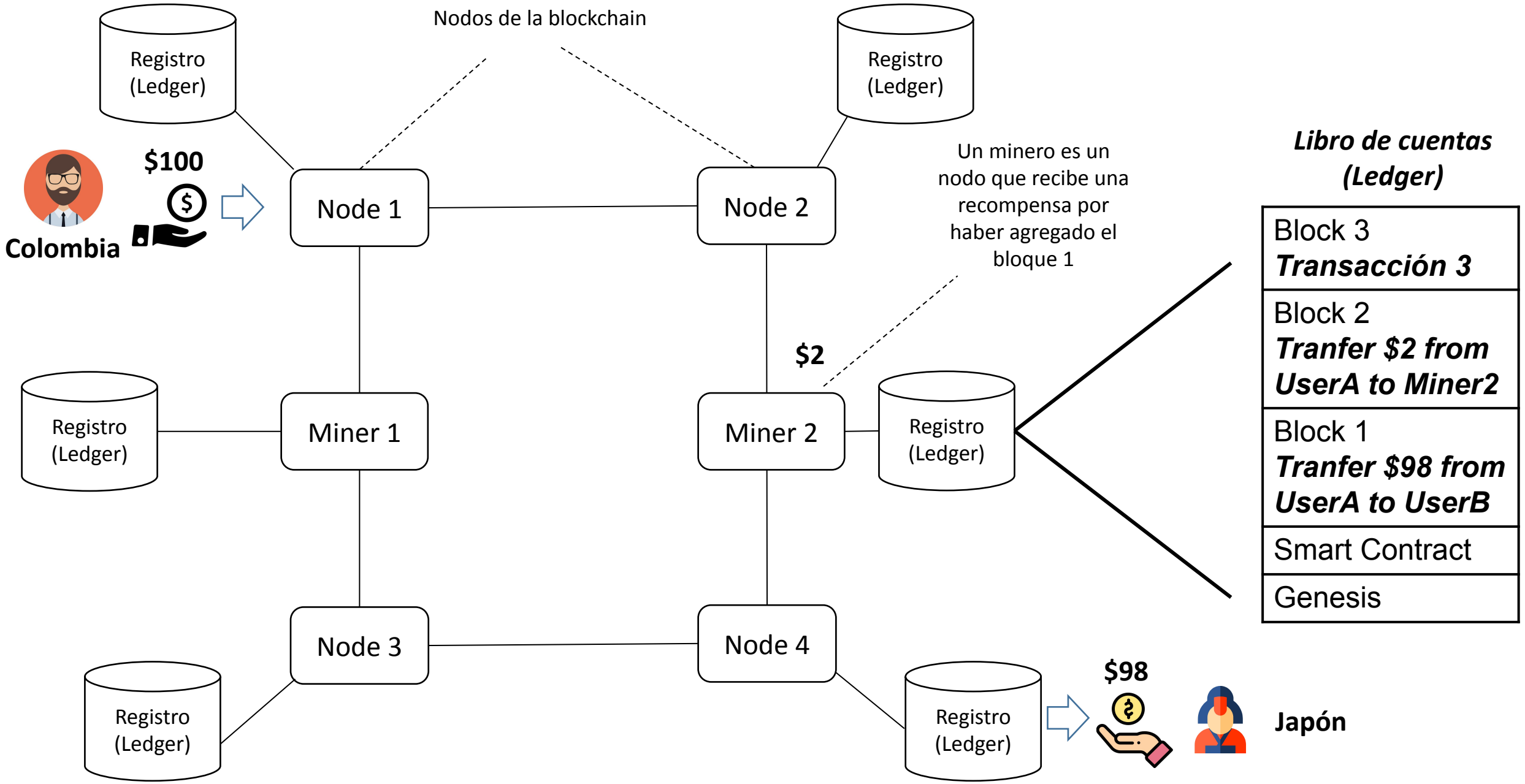


http://dailyblockchain.github.io/

Red: output
Green: input

Blue: transaction
Yellow: input+output

Ejemplo de transacción interbancaria usando nodos de una blockchain



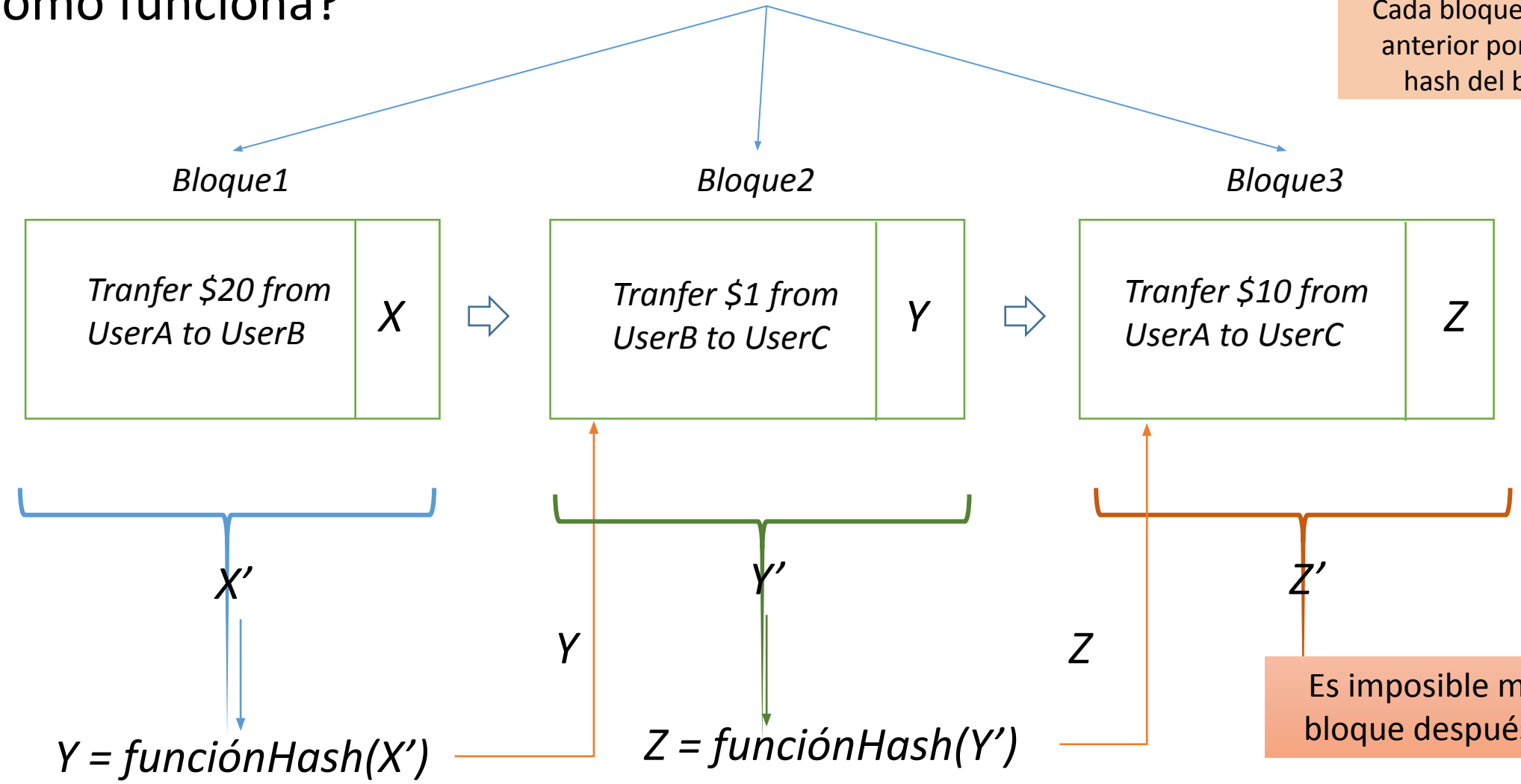
Blockchain

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

¿Cómo funciona?

Blockchain = Cadena de Bloques

Cada bloque está vinculado al anterior por medio del valor hash del bloque anterior



Es imposible modificar un bloque después de creado

Y = AA47F8215C6F30A0DCDB2A36A9F4168E

Z = FEF7185DD6E69D561BC286F3FE6E391E

Usos de Blockchain

A parte de utilizar blockchain para transferencias de dinero, ¿Qué otros usos puede tener?

- ✔ Voto electrónico → Cuido de que los datos NO sean modificados
- ✔ Autenticación de usuarios → Registro la actividad de los usuarios
- ✔ Bolsas de inversión → Visualizo los ingresos hacia un mismo destino

- Tipos de blockchain
  - Pública: Cualquiera puede unirse a la blockchain (e.g. Bitcoin)
  - Privada: El acceso a la blockchain es restringido solo a ciertos nodos

Usos de Blockchain

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

- Tipos de blockchain
  - Pública: Cualquiera puede unirse a la blockchain (e.g. Bitcoin)
  - Privada: El acceso a la blockchain es restringido solo a ciertos nodos

A parte de utilizar blockchain para transferencias de dinero, ¿Qué otros usos puede tener?

✔ Voto electrónico → Cuido de que los datos NO sean modificados

✔ Autenticación de usuarios → Registro la actividad de los usuarios

✔ Bolsas de inversión → Visualizo los ingresos hacia un mismo destino

Usos de Blockchain

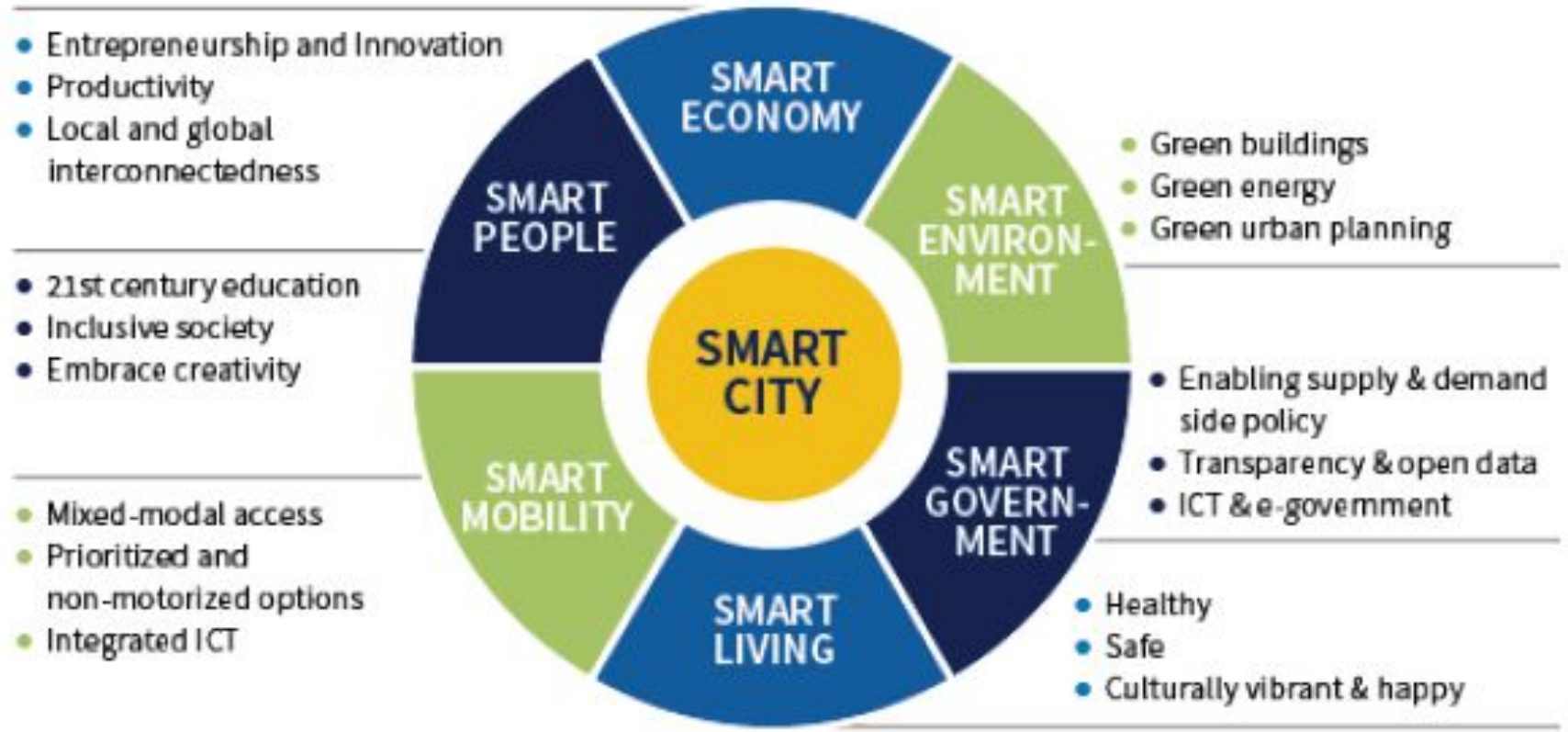
Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

Blockchain para la construcción de Ciudades Inteligentes y Seguras

Usos de Blockchain

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

¿Que tipo de Dapps (Aplicaciones de Blockchain) podemos pensar para una Ciudad Inteligente y Segura?



Las seis dimensiones de una Smart City

¿Cual de las siguientes NO es una característica del sistema bancario tradicional?

a) Las transacciones pueden tardar hasta 5 días
b) El sistema bancarios es infalibles ante ciberataques
c) El registro de las transacciones está centralizado
d) Los bancos reciben ingresos por la función de intermediación

Blockchain

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

¿Cual de la siguientes es una característica de Blockchain?

a) Las transacciones en blockchain son demoradas pero seguras
b) Cualquier usuario de la blockchain puede contaminar los datos
c) El registro de las transacciones es distribuido en n sitios
d) Es fácil de atacar porque los bloques están desprotegidos

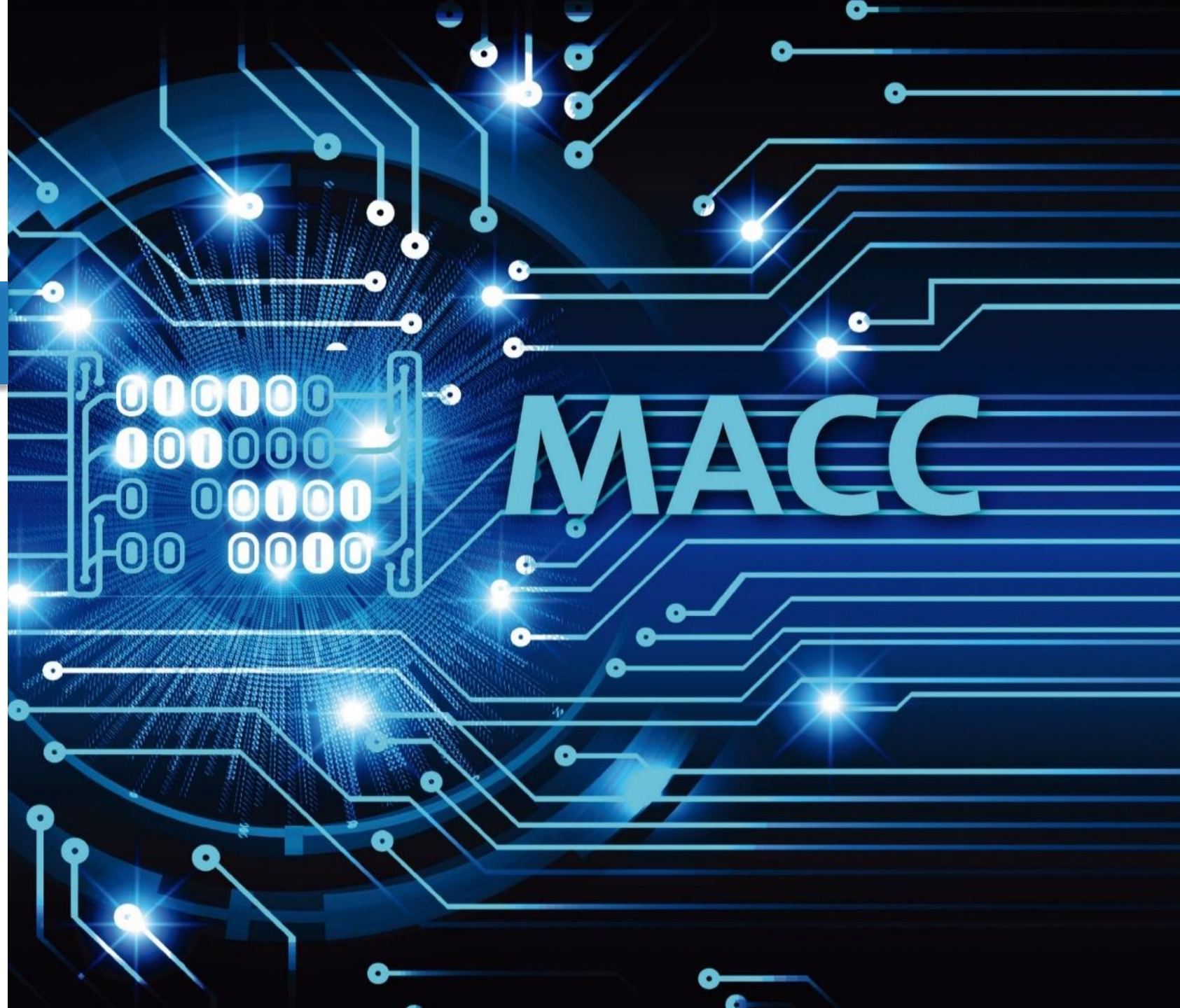
Una cadena de bloques es/contiene:

a) Bloques vinculados por medio de una función matemática
b) Los datos de contacto de los usuarios de la blockchain
c) Datos de las transacciones asociadas a un único usuario
d) Conjunto de bloques que pueden ser modificables

Universidad del Rosario

MACC
Matemáticas Aplicadas y Ciencias de la Computación

Dapps, seguridad y consenso



Daniel Orlando Díaz López, PhD

Profesor principal
Departamento MACC
Universidad del Rosario
danielo.diaz@urosario.edu.co

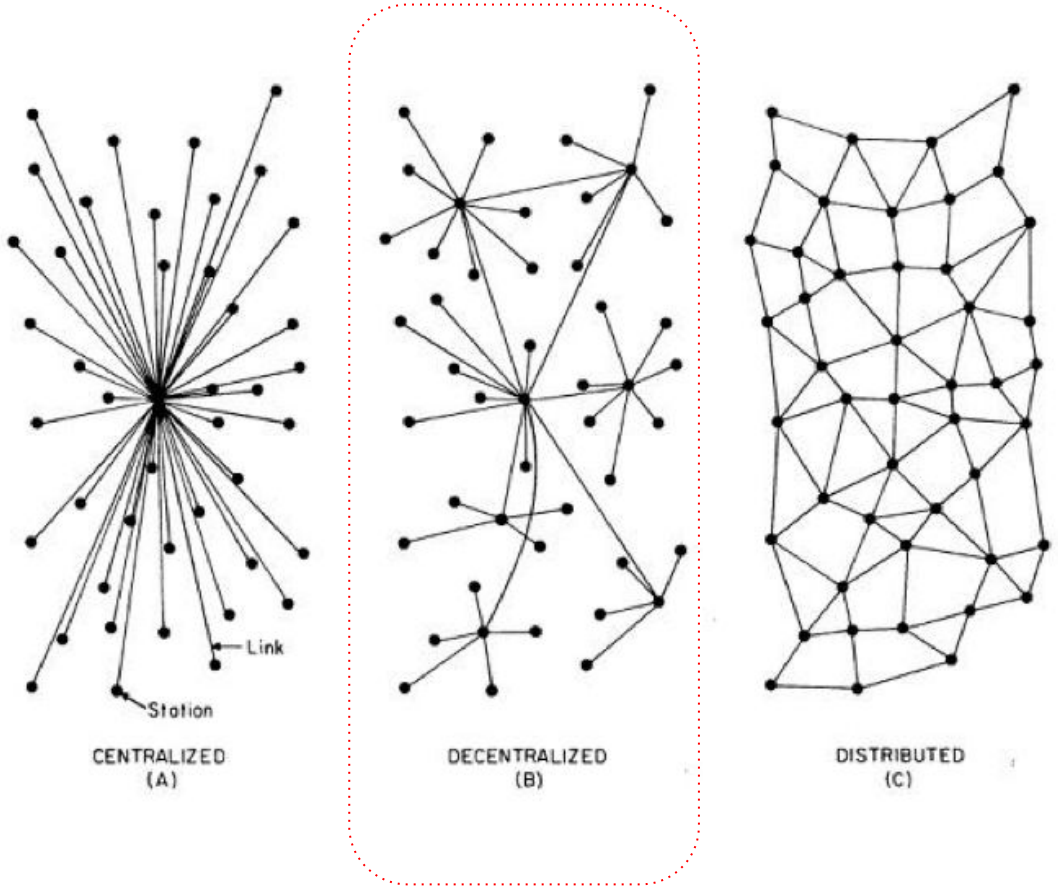
Tabla de contenido

Dapp

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

¿Que es una Dapp?

- DApp = dApp = Dapp = dapp = **Decentralized Application**
- Aplicación que se ejecuta sobre un **sistema de computación distribuido** (e.g. los nodos de una Blockchain como Ethereum o Bitcoin)



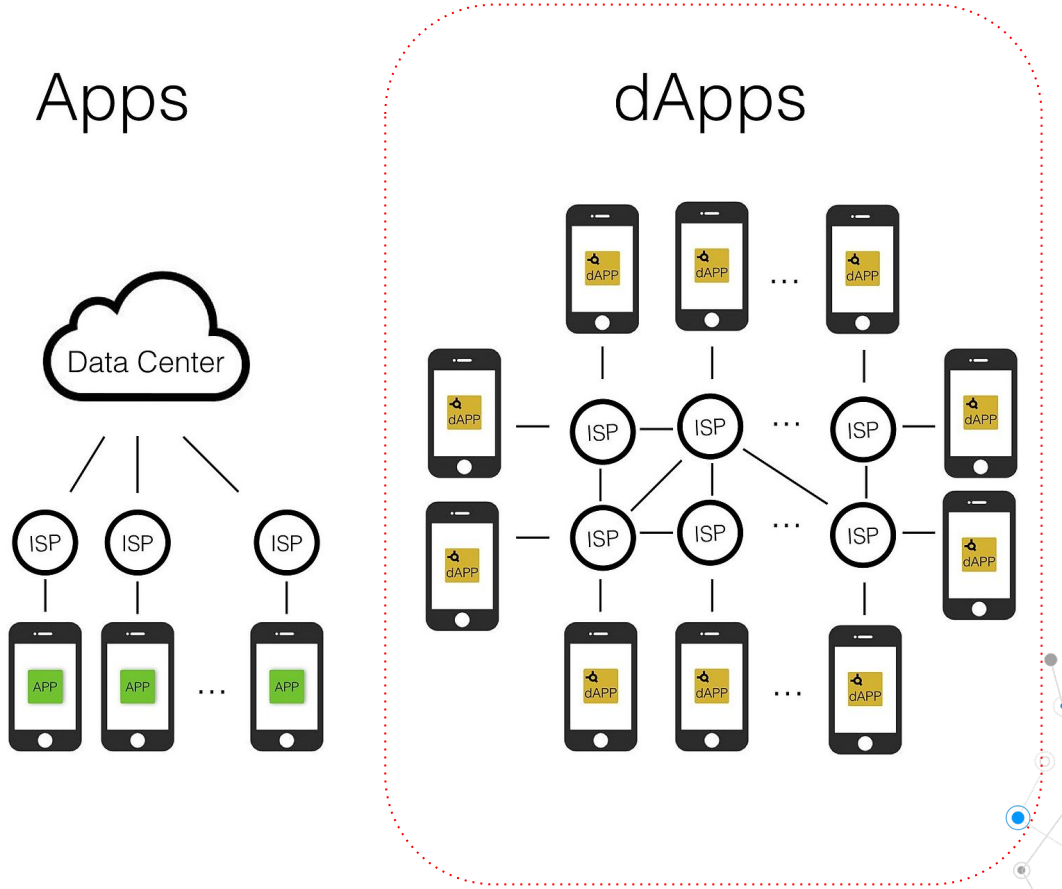
Similar al grafo de nodos observado en:
http://dailyblockchain.github.io/

Dapp

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

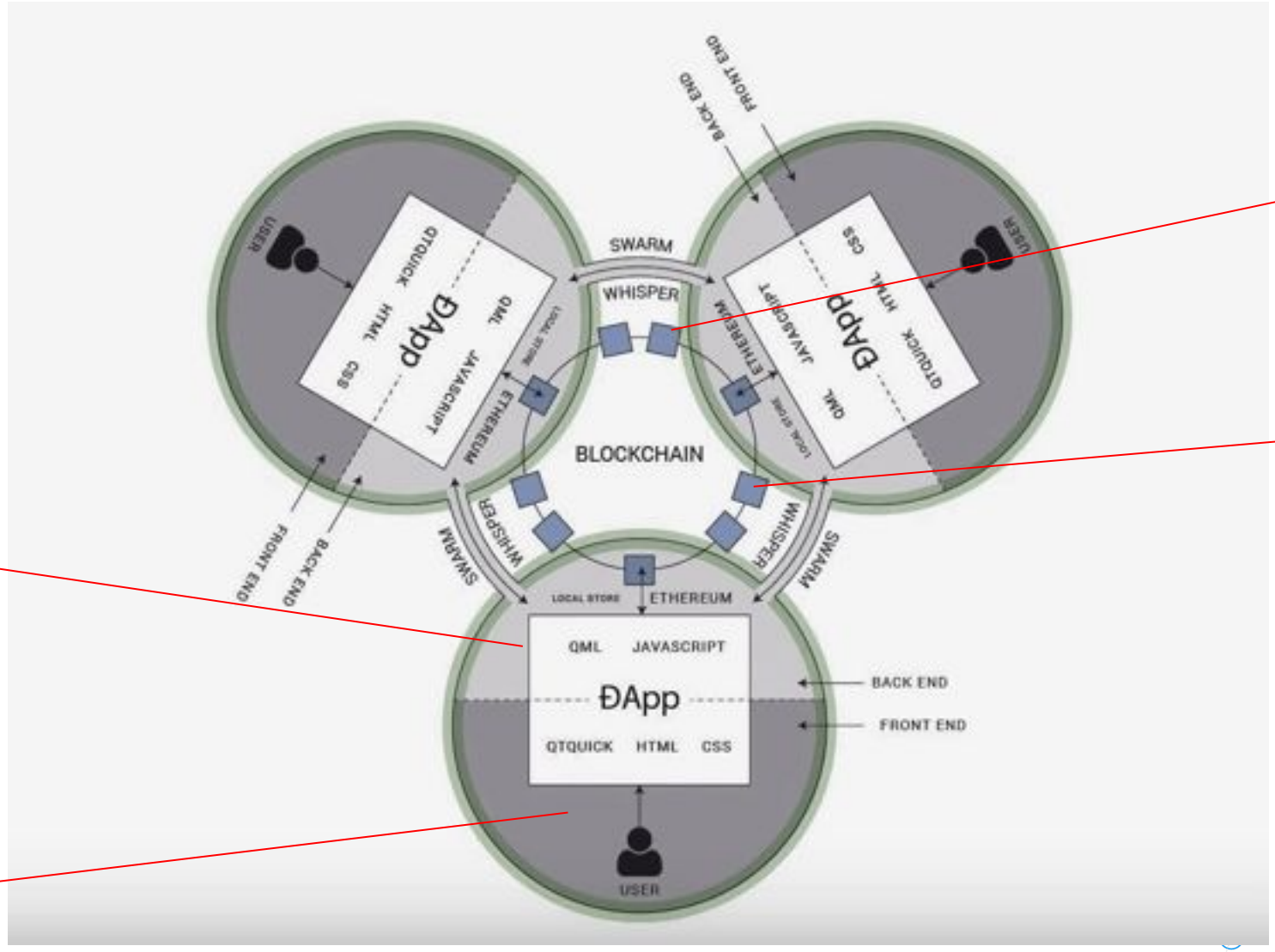
¿Que es una Dapp?

- En una Dapp no hay un servidores almacenados en datacenters que contienen la lógica principal de la aplicación
- En una Dapp la lógica de la aplicacioń está distribuida en todos los nodos por igual en forma de **smart contract**
- Todos los nodos de la blockchain almacenan una copia del smartcontract
- Así todos los nodos ejecutan el **mismo código** y el control de la aplicación no depende de un servidor
    - https://dappradar.com/rankings/protocol/eth
    - https://www.dapp.com/search/



Componentes de una DApp

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación



Ethereum interconecta a cada uno de los nodos

Ethereum almacena la información de la DApp de manera criptográfica

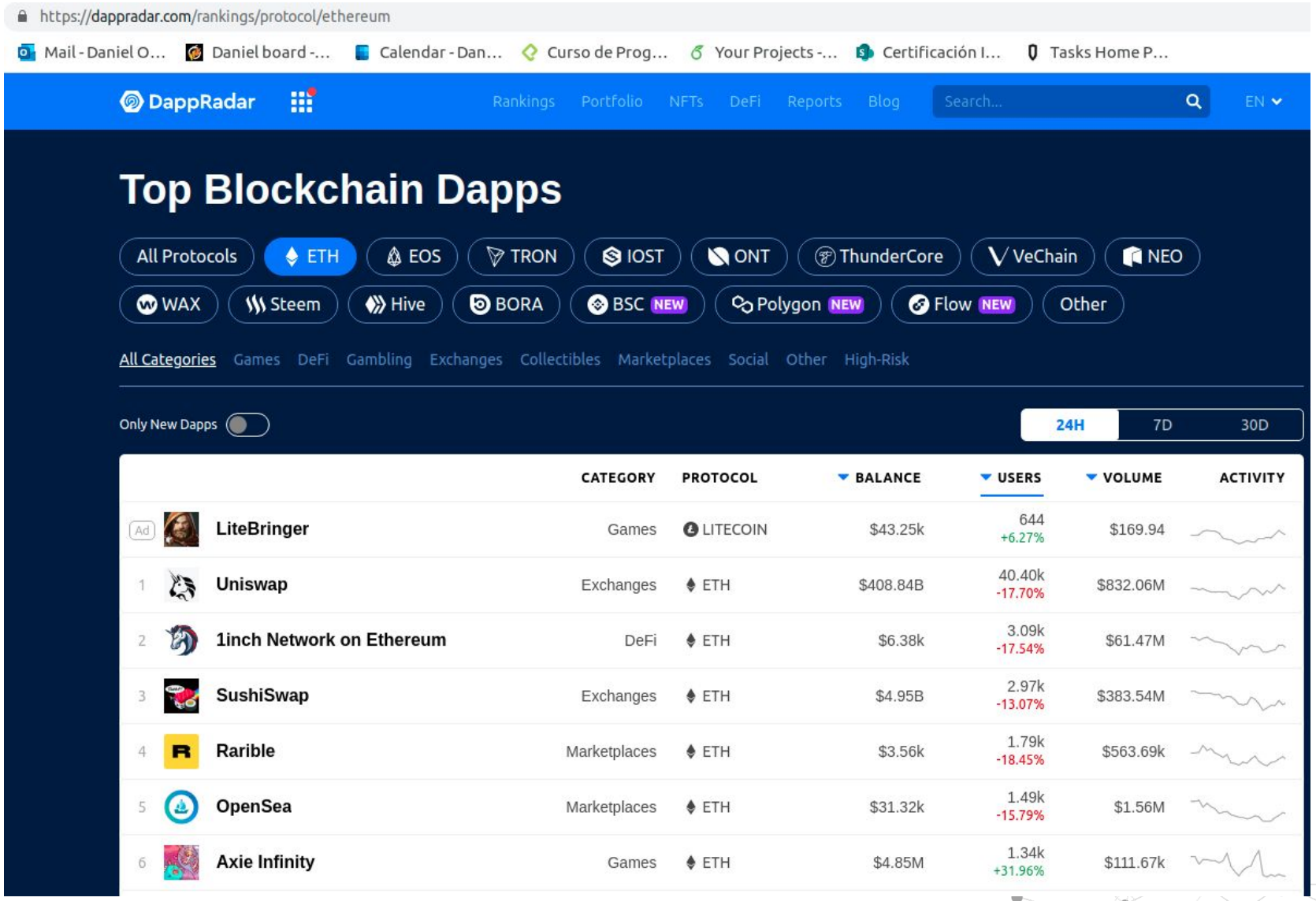
El backend define la interacción con la blockchain (Ethereum)

El frontend define la interfaz GUI al usuario en cada nodo

Marketplace de DApps

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

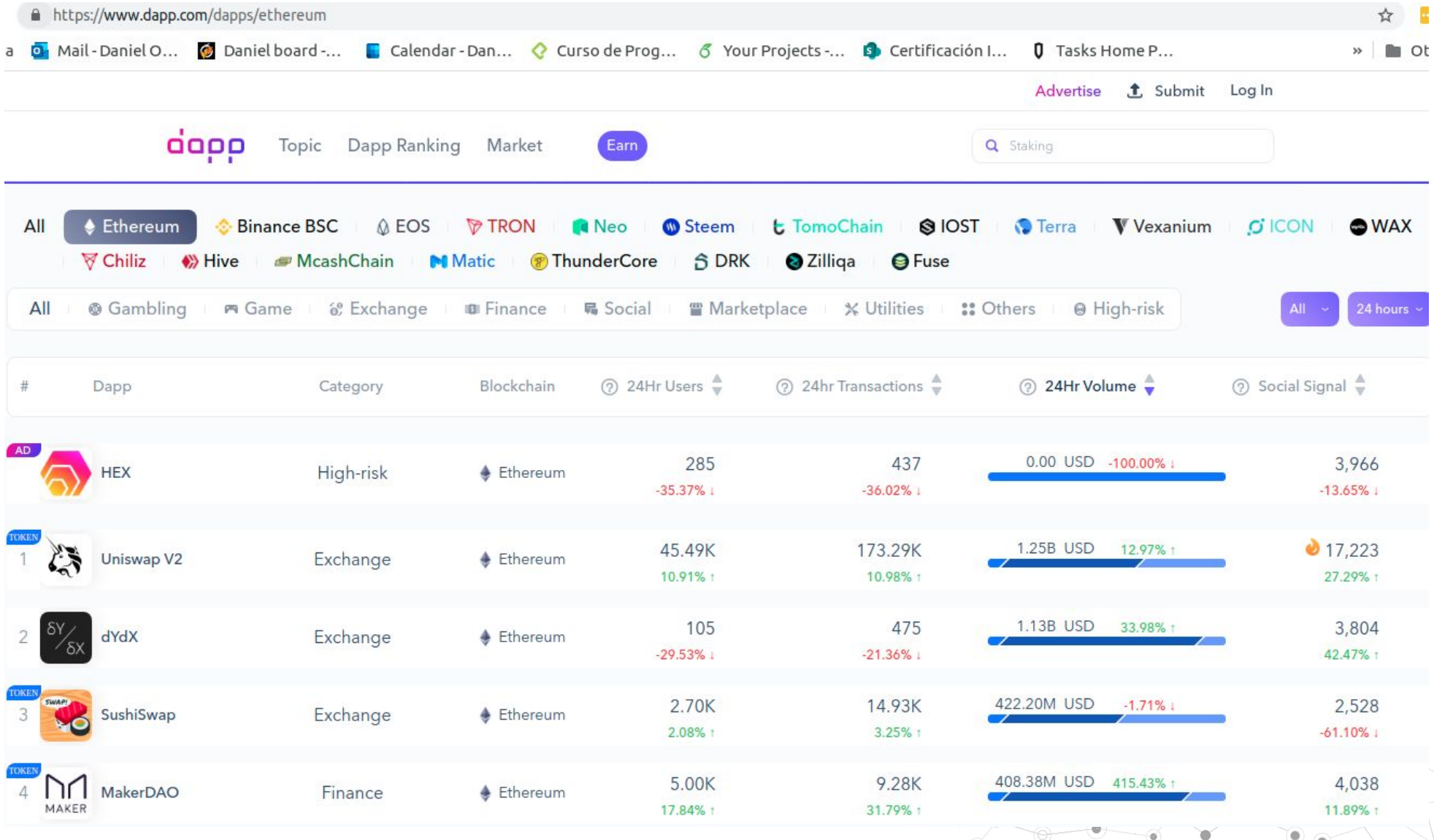
https://dappradar.com/rankings/protocol/ethereum



Marketplace de DApps

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

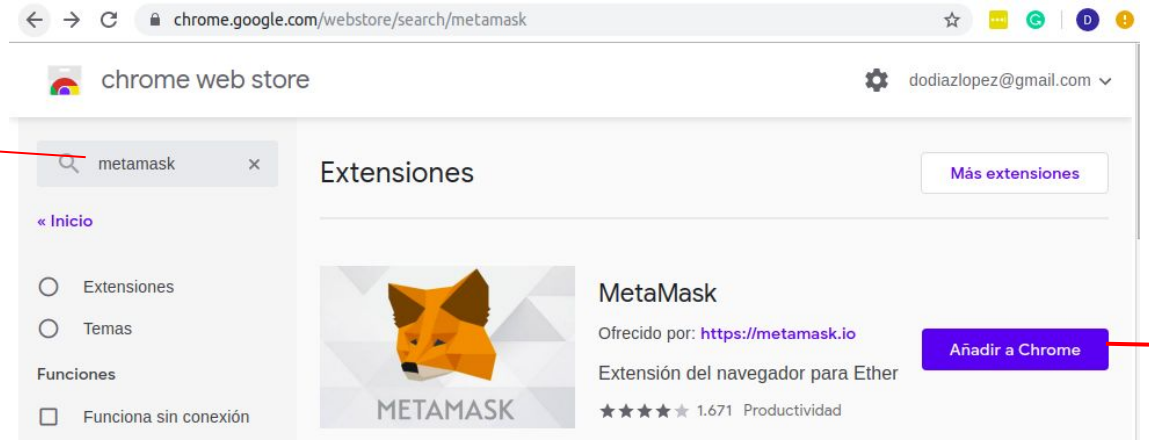
https://www.dapp.com/dapps/ethereum



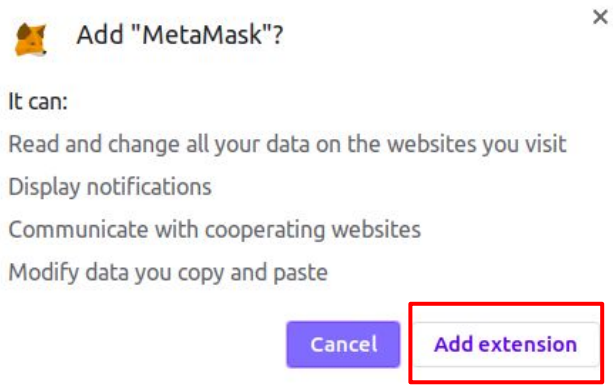
Antes de usar una Dapp necesitamos una wallet

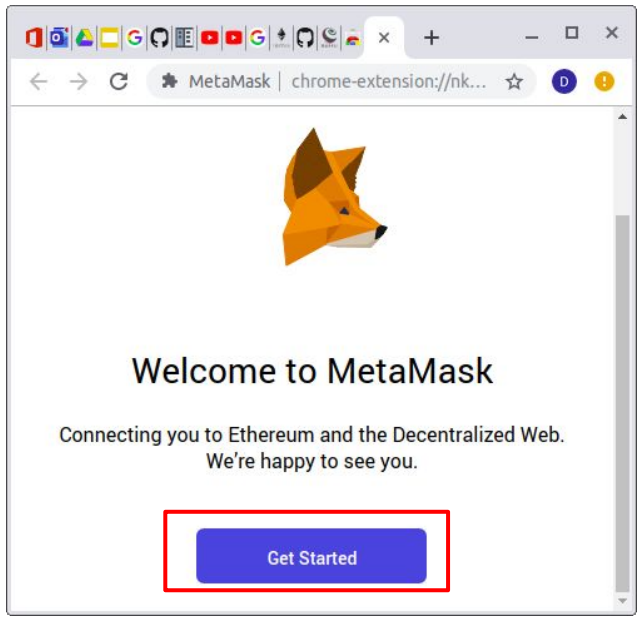
Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

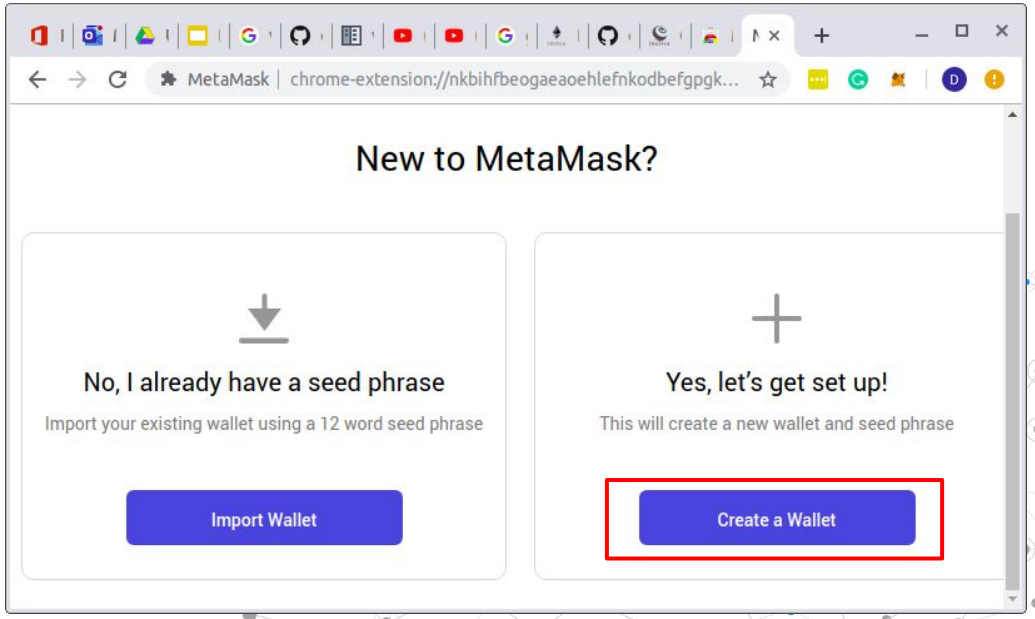
Buscar Metamask



Seleccionar Añadir Metamask a Chrome

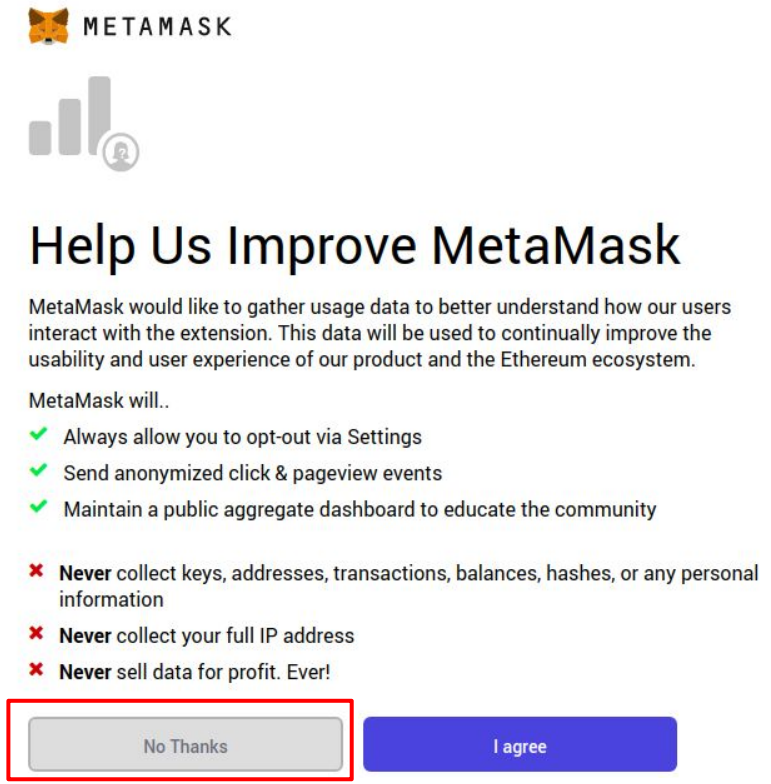


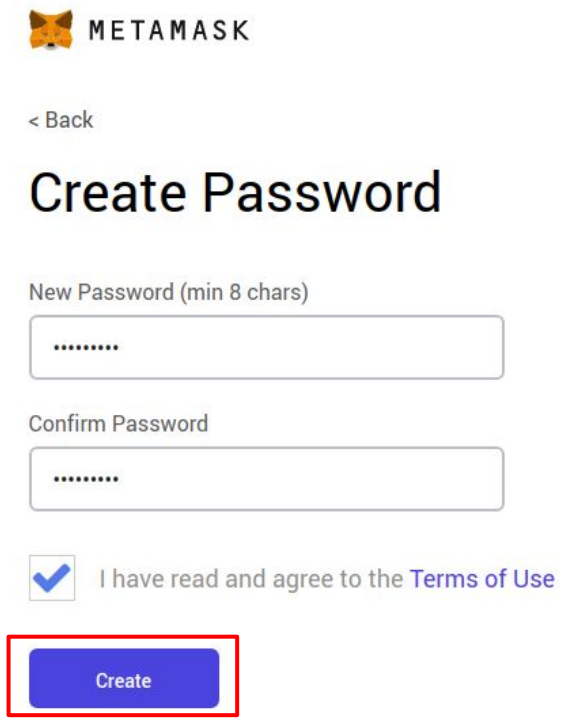


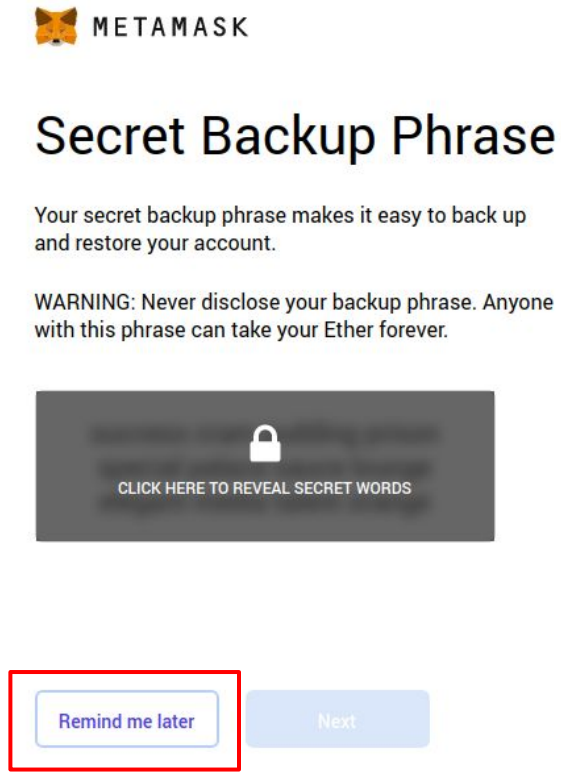


Antes de usar una Dapp necesitamos una wallet

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación



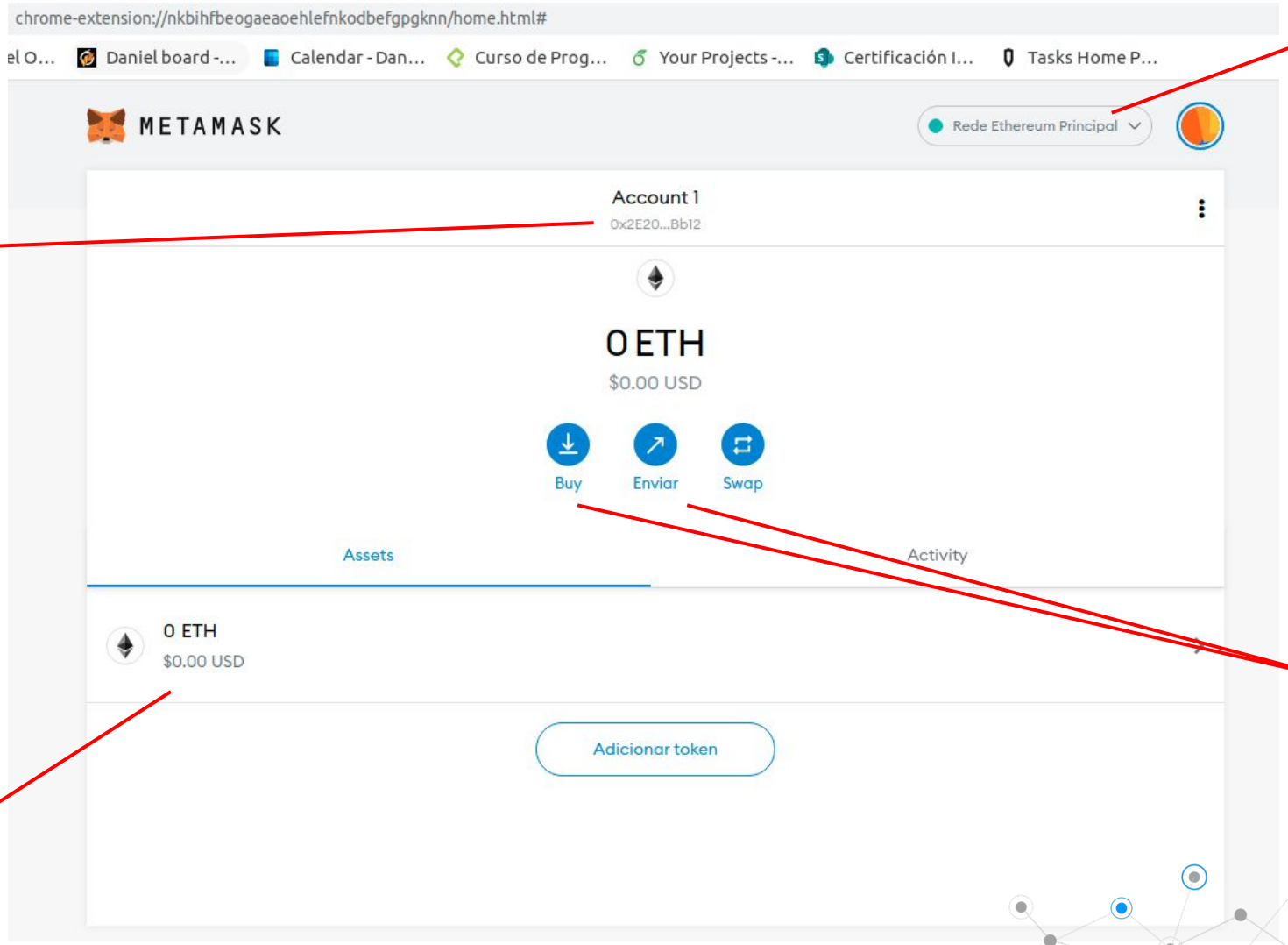




Antes de usar una Dapp necesitamos una wallet

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

Ya tenemos nuestra cuenta/wallet de blockchain



Esta es una nuestra direccion de wallet, ¡a esta dirección nos pueden transferir dinero!

Esta es la red a la cual está conectada nuestra wallet

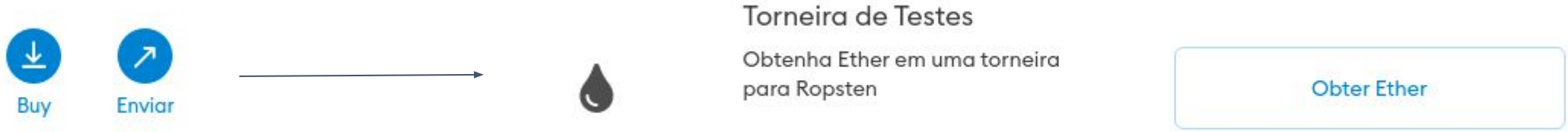
Podemos ponerle dinero a nuestra wallet o transferir dinero desde nuestra wallet

Este es nuestro saldo (0 ETH en este momento)

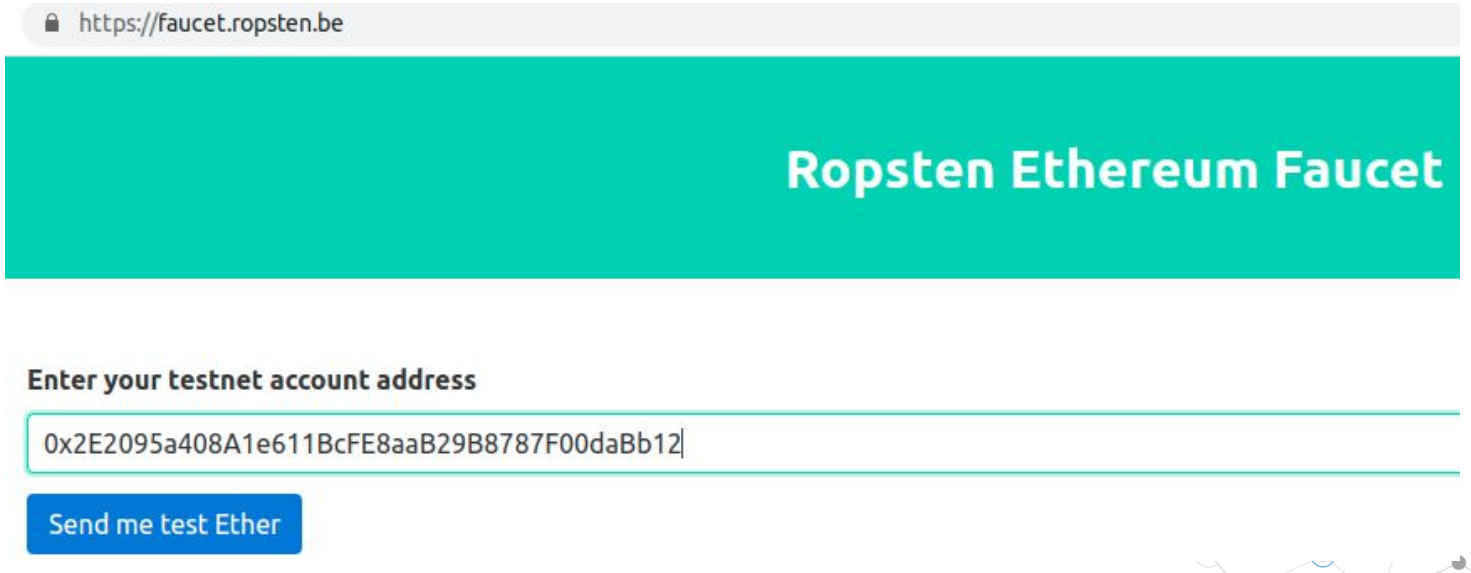
Antes de usar una Dapp necesitamos una wallet

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

Ahora debemos ingresar dinero en nuestra wallet

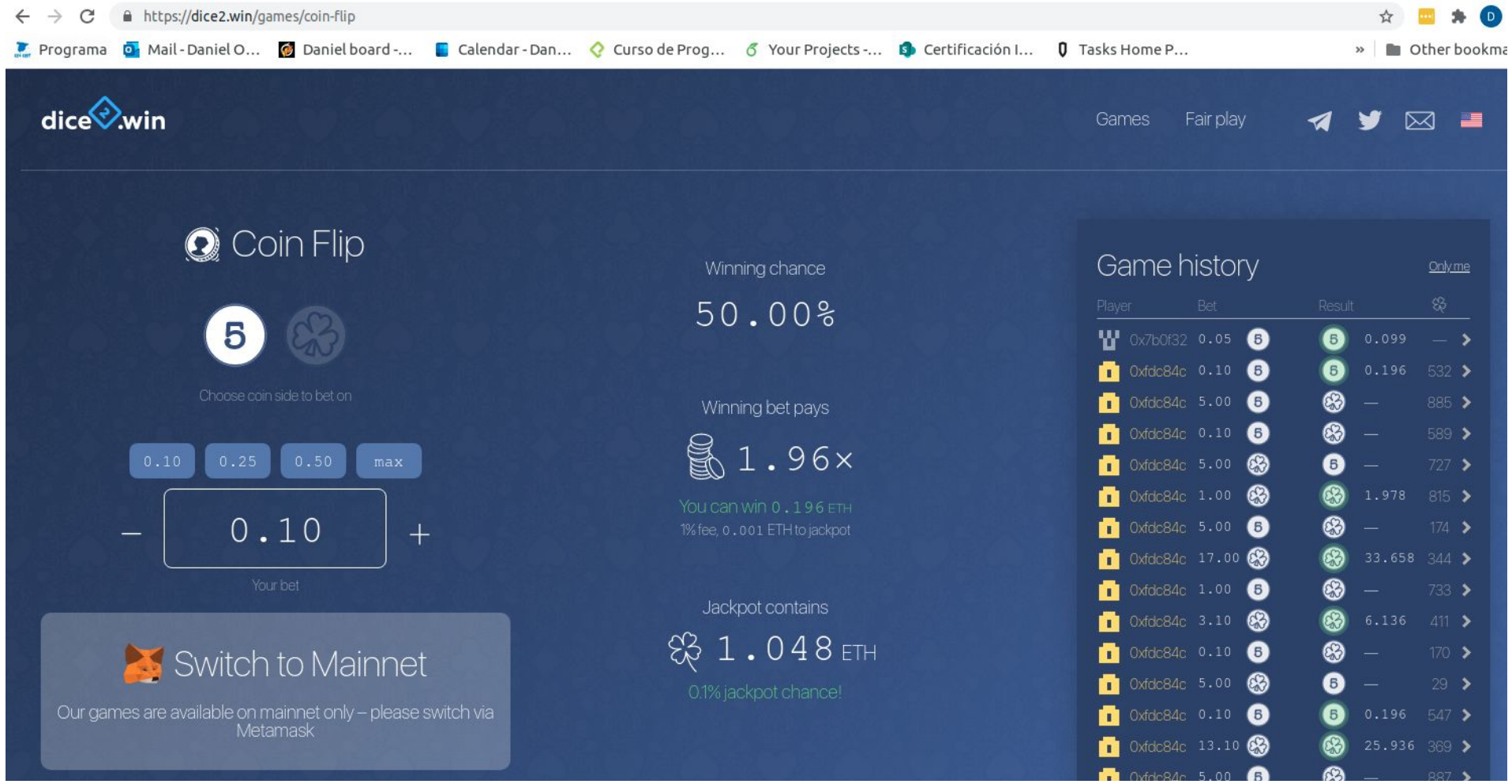


Si el website https://faucet.metamask.io/ esta caído podemos obtener ethers de prueba de aquí:



Antes de usar una Dapp necesitamos una wallet

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación



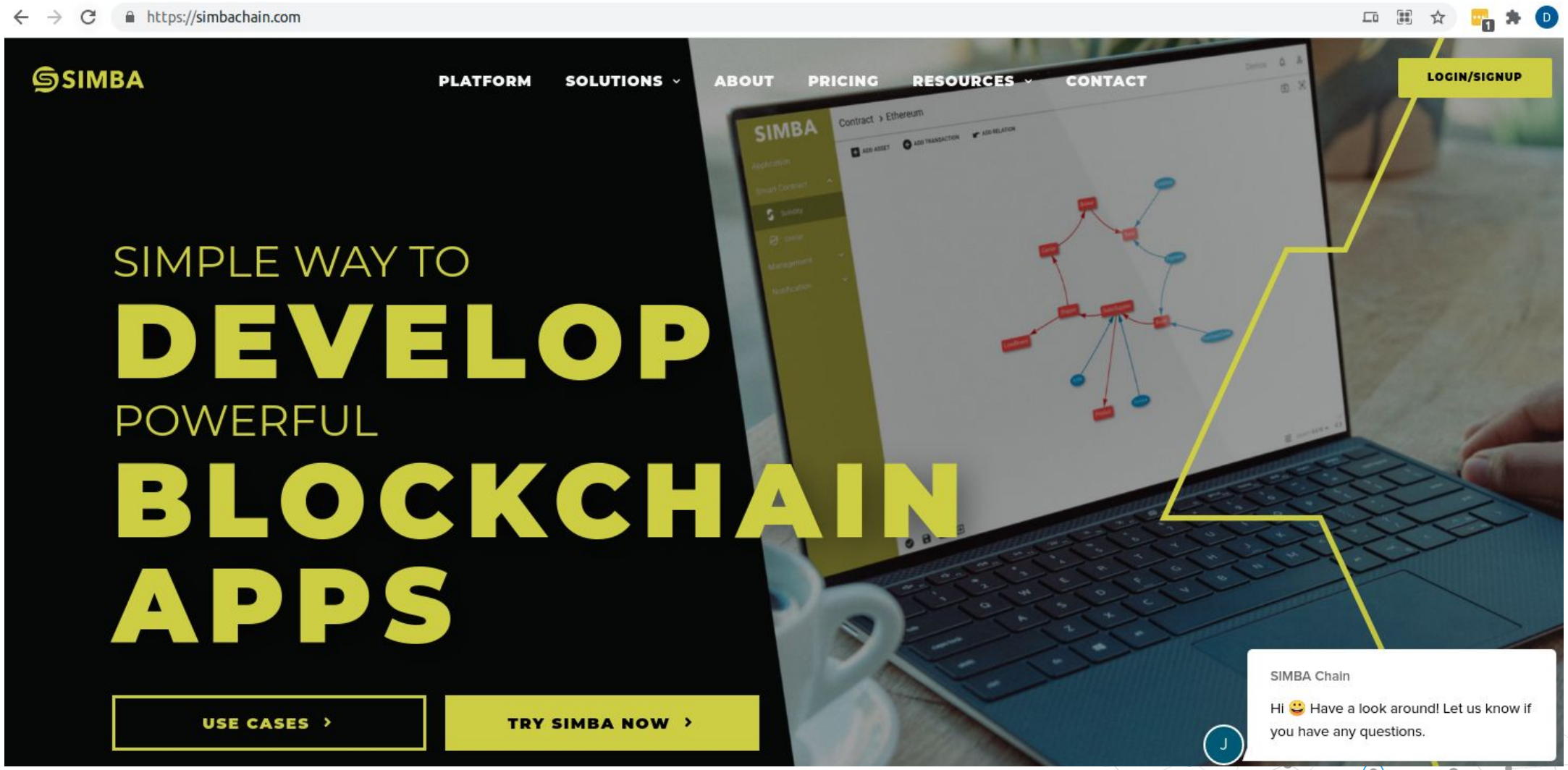
Algunas dapps solo funcionan en la Mainnet y no permiten el uso de redes de prueba como Ropsten, Kovan, etc

¿Podemos encontrar una dapp que funcione con la red de pruebas de Ropsten?

Creación de una Dapp

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

Vamos a utilizar una blockchain implementada como servicio (Blockchain As a Service)

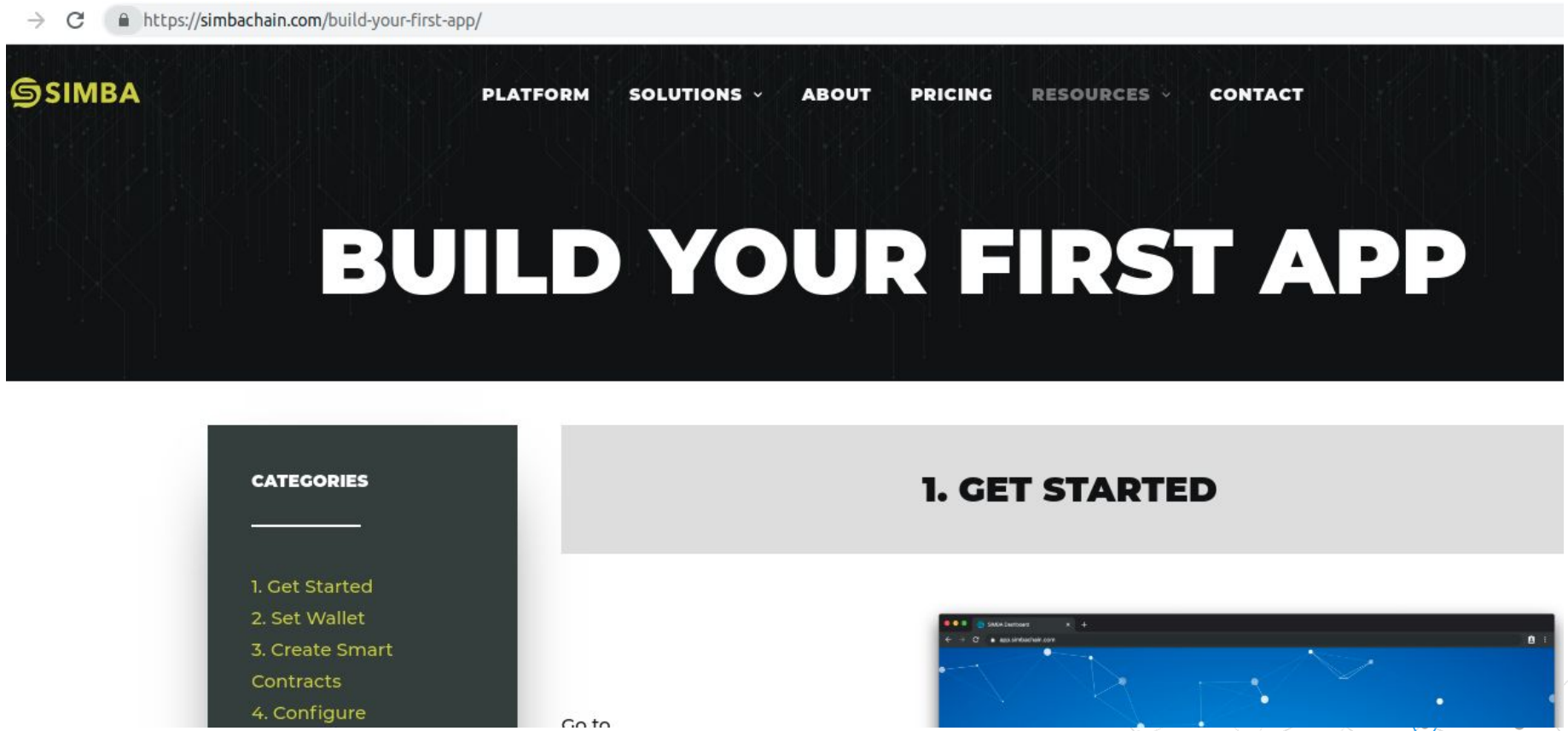


Creación de una Dapp

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

Pasos a seguir:

1. Leer el documento SIMBA-Chain-Capabilities.pdf
   a. ¿Donde se almacenan los datos en SIMBA Chain?
   b. ¿Cuales blockchains son soportadas por SIMBA Chain?
2. Seguir los pasos para construir nuestra primera APP descritos en https://simbachain.com/build-your-first-app/



Universidad del Rosario | MACC | HINNT

¡Gracias!