



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

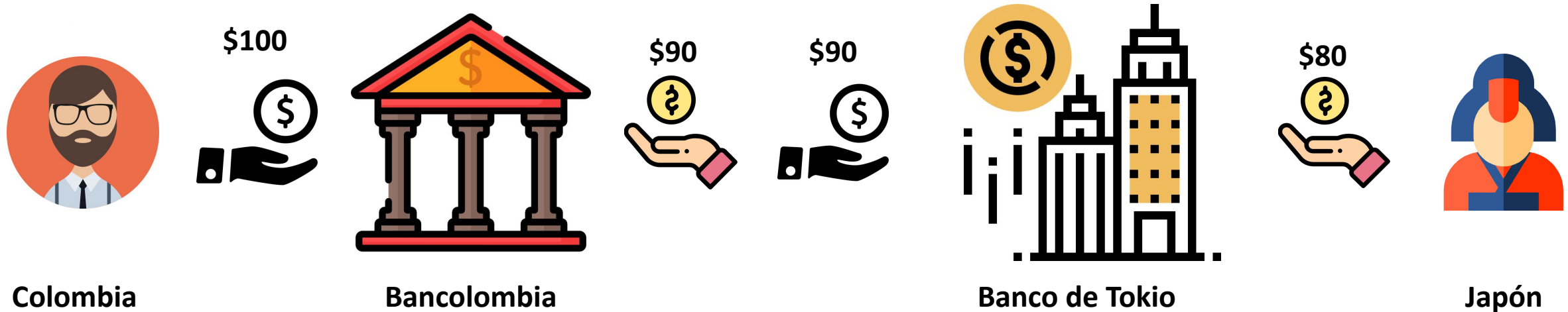
MACC



Tabla de contenido

1. Sistema bancario tradicional
2. Que es blockchain
3. Visualización de transacciones en Bitcoin
4. Topología lógica de una blockchain
5. Cadena de bloques

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!

¿Podemos confiar en la seguridad de un banco?

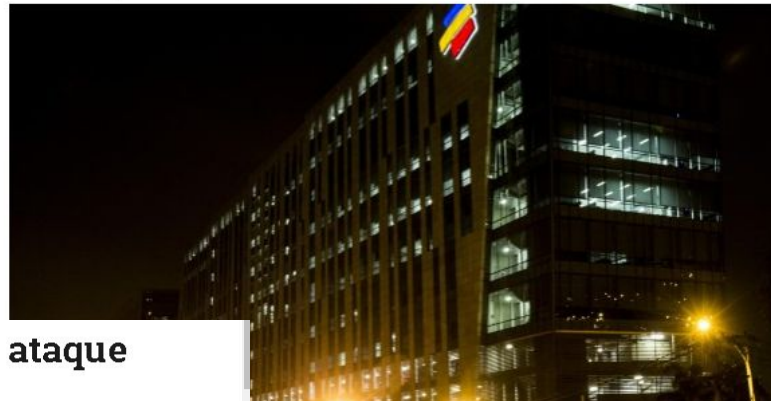
ORGANIZACIÓN CRIMINAL



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

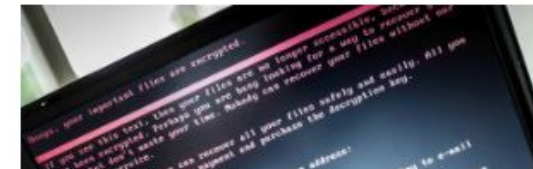


El robo del siglo que no alcanzó a ser



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

¿La **seguridad** ofrecida por un banco es suficiente?

¿Los **costos** del sistema bancario son accesibles?

¿Los **tiempos de comunicación** entre bancos pueden ser mejorados?

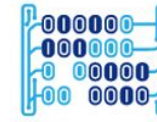
Bancolombia restableció todos los canales que durante este presentado **fallas a nivel nacional**, según lo reportaron una gran des sociales.

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

E. CAMHAJI | 18/05/2018 · 19:05 CEST



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 Lupu/ Reuters



¿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!

¿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!

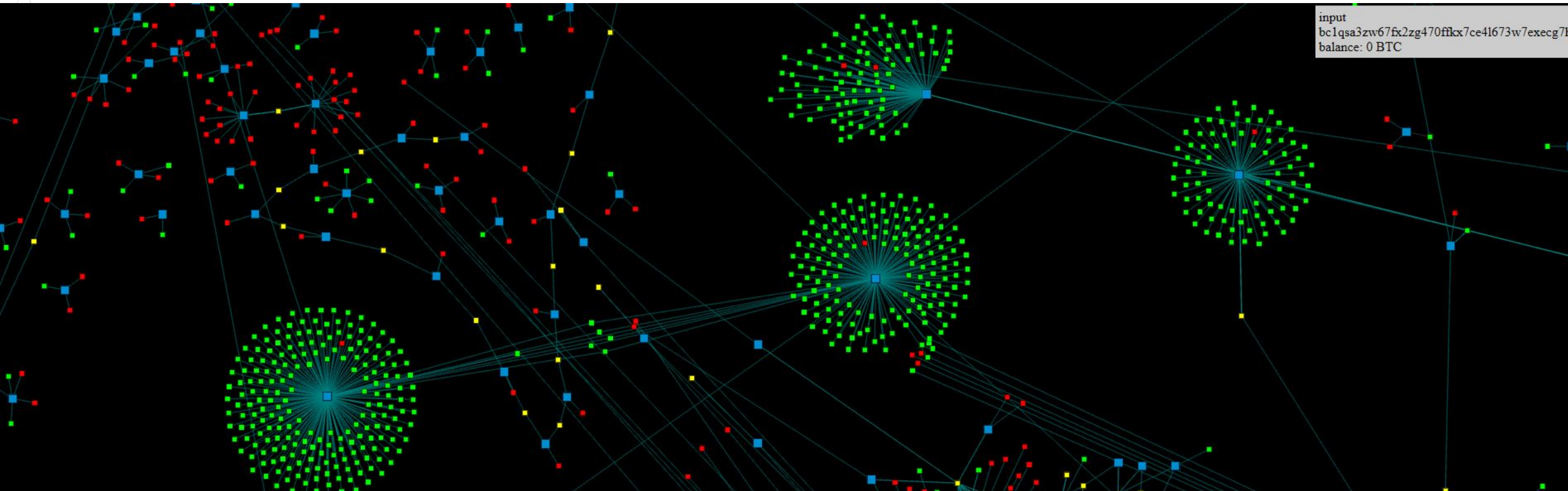
¿Es seguro?

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**

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

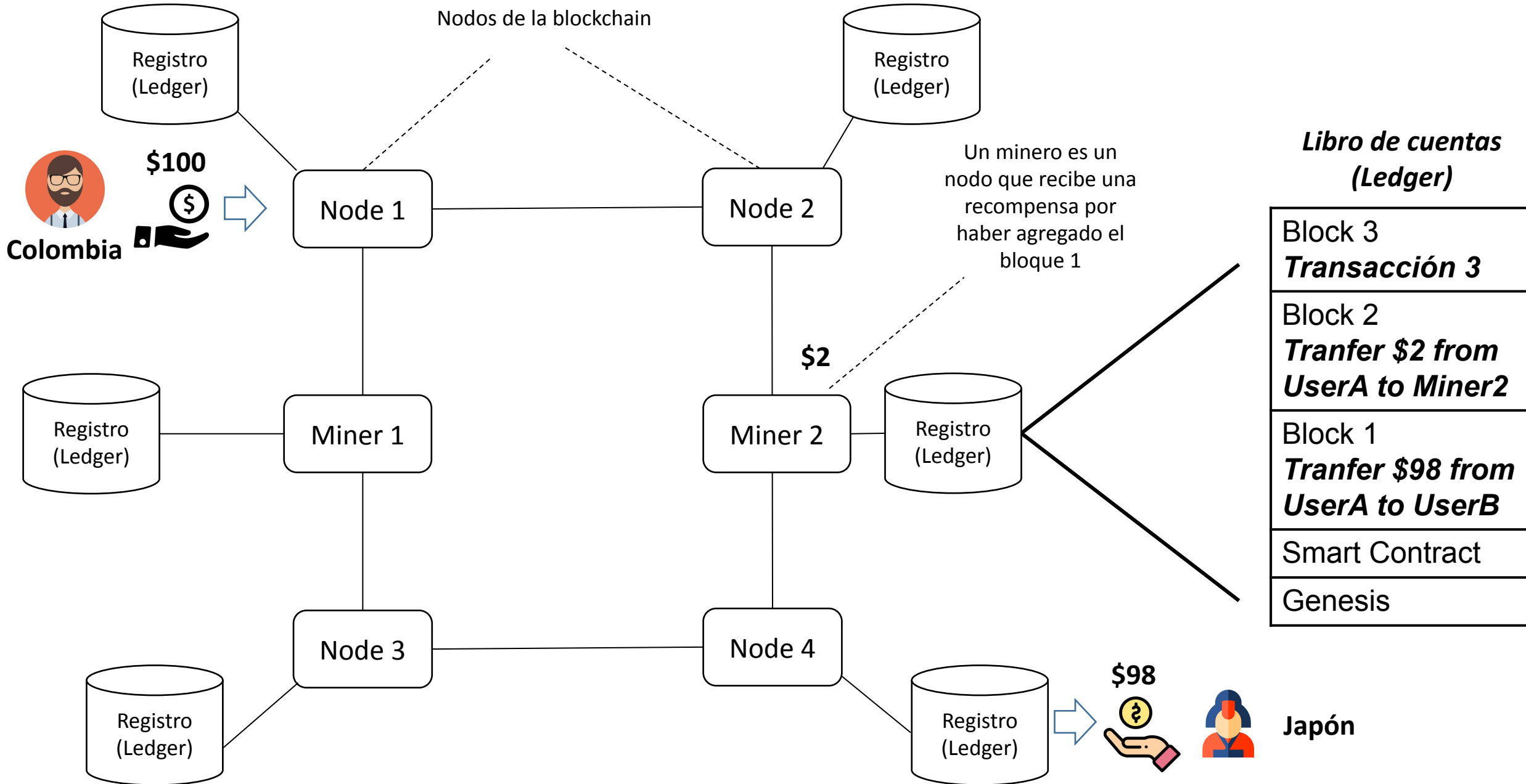


<http://dailyblockchain.github.io/>

Red: output
Green: input

Blue: transaction
Yellow: input+output

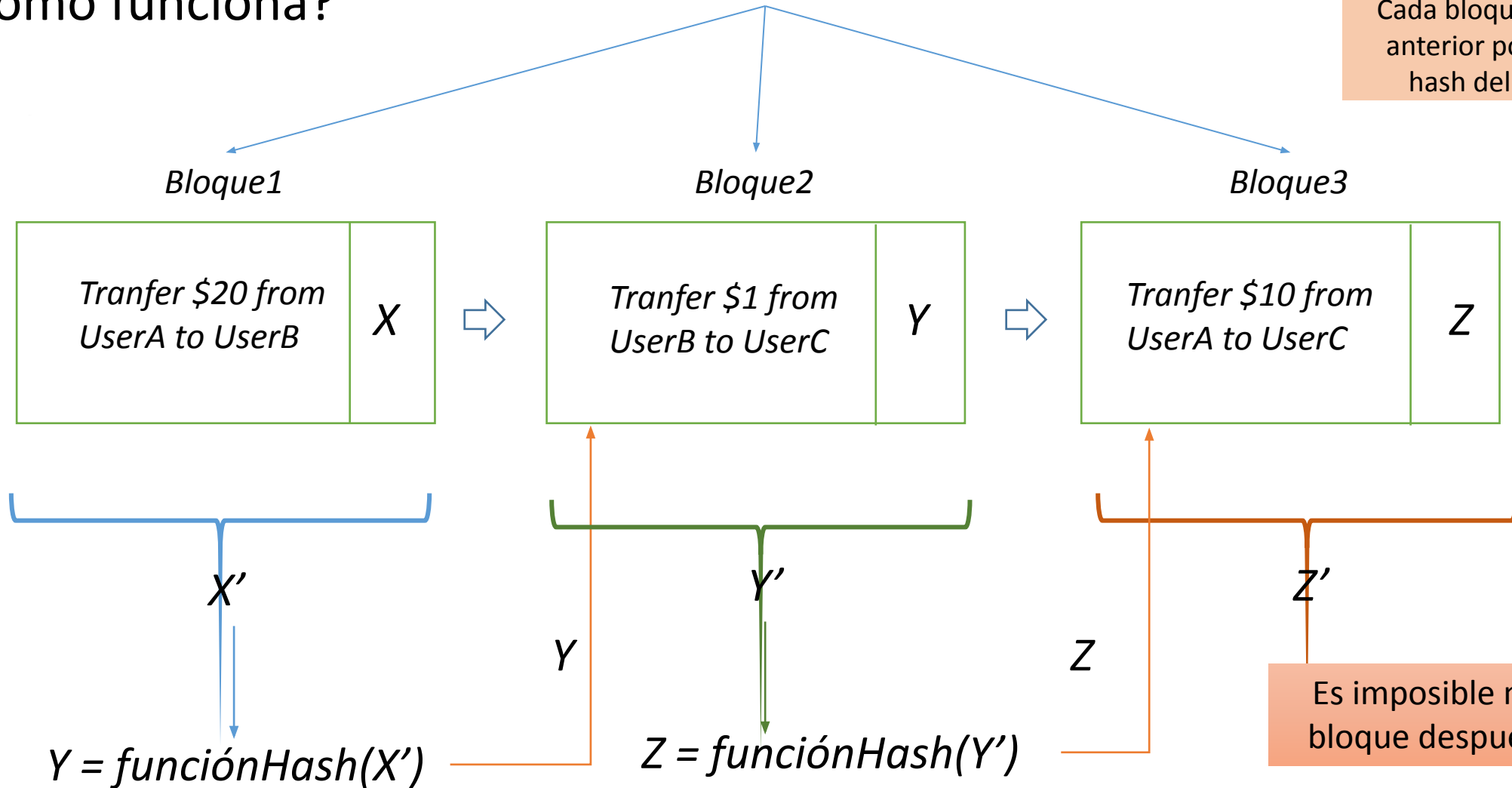
Ejemplo de transacción interbancaria usando nodos de una blockchain



¿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

$Y = AA47F8215C6F30A0DCDB2A36A9F4168E$

$Z = FEF7185DD6E69D561BC286F3FE6E391F$

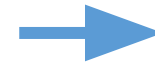
A parte de utilizar blockchain para transferencias de dinero, ¿Qué otros usos puede tener?

✓ Voto electrónico



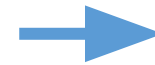
Cuido de que los datos NO sean modificados

✓ 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

- **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

Blockchain para la construcción de Ciudades Inteligentes y Seguras

Use cases of Blockchain technology in Smart Cities

COMMUNITY

- TOURISM
- HEALTHCARE
- DAILY USERS
- FOUNDATION
- VETERANS
- EDUCATION

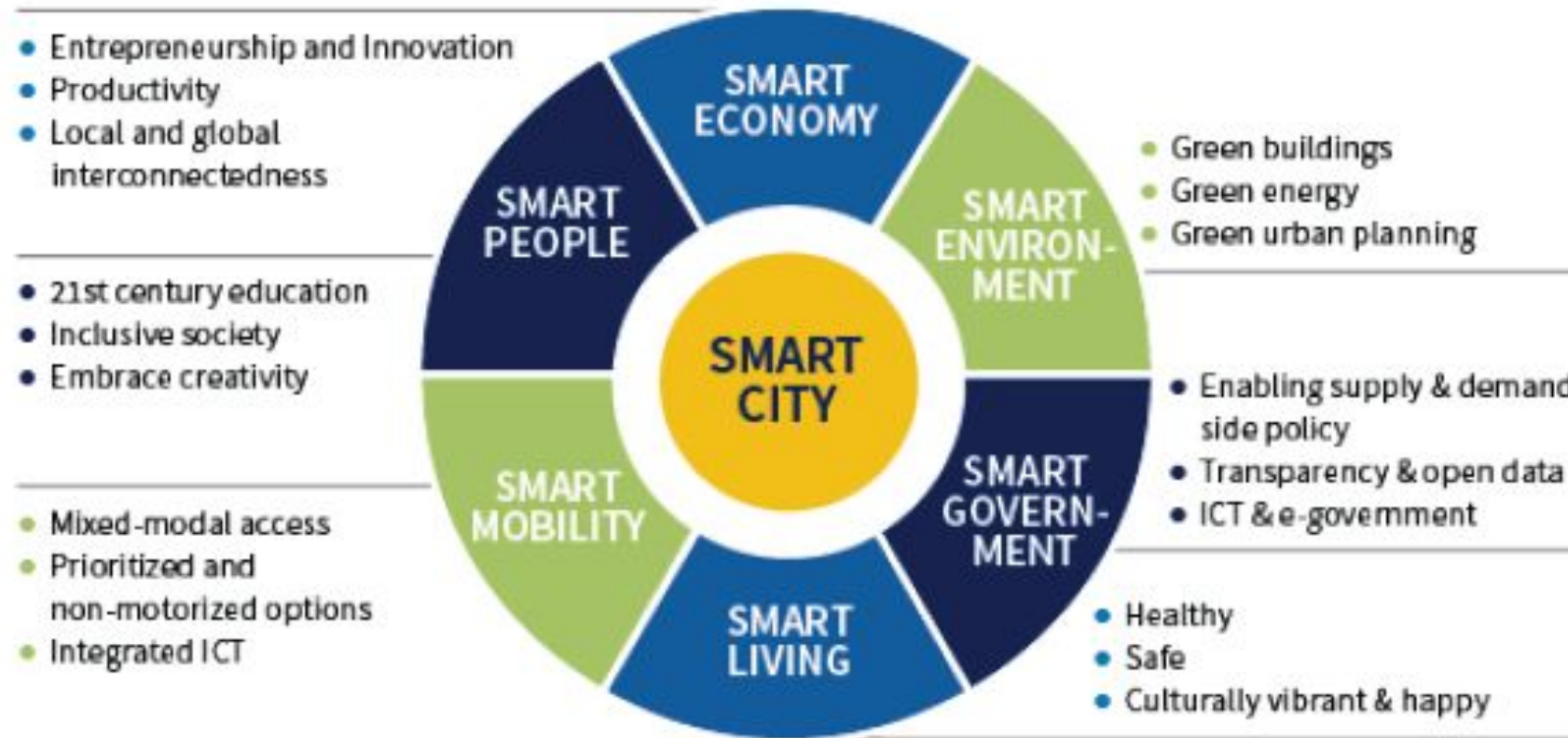
BUSINESS

- JOB
- GLOBALIZATION
- BRI
- SMALL-MEDIUM ENTERPRISES
- iGLOBE

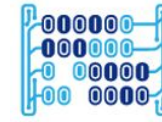
GOVERNMENT

- DIGITAL GOVERNANCE
- JOB
- DATA CONTROL
- IMMIGRATION
- BRAIN GAIN

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

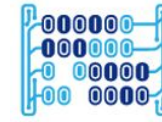


Las seis dimensiones de una Smart City



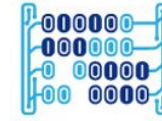
¿Cual de las siguientes NO es una característica del sistema bancario tradicional?

- 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



¿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

MACC

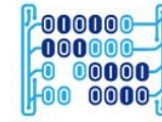
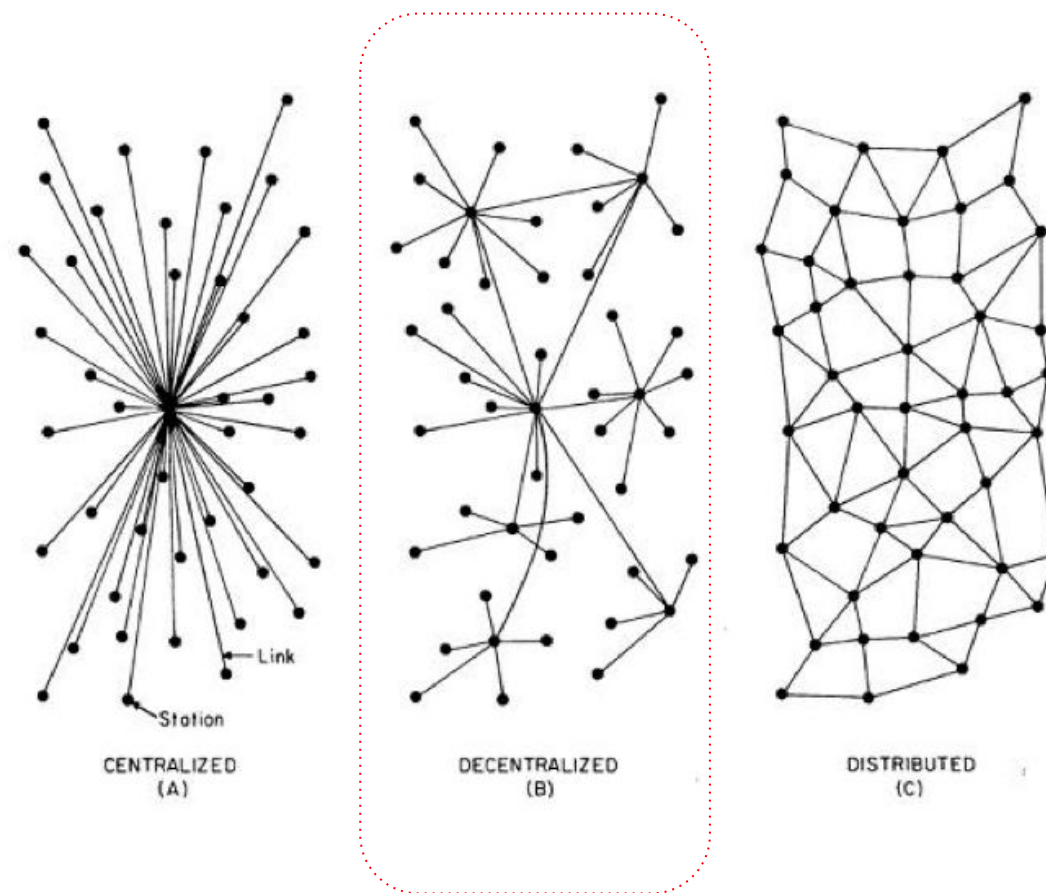


Tabla de contenido

1. DAPP: Aplicaciones distribuidas
2. Marketplace
3. Creación de una *Wallet*
4. Creación de una DAPP

¿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)

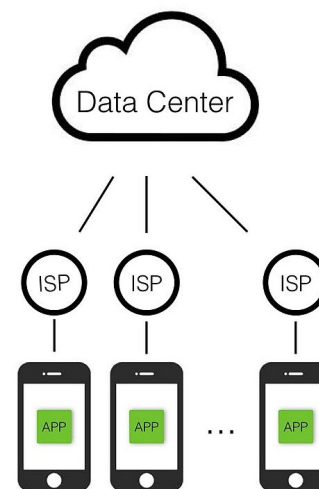


Similar al grafo de nodos observado en:
<http://dailyblockchain.github.io/>

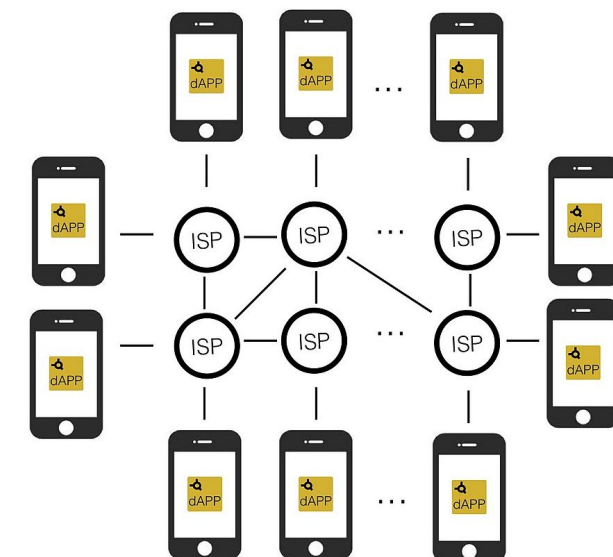
¿Que es una Dapp?

- 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 aplicación 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/>

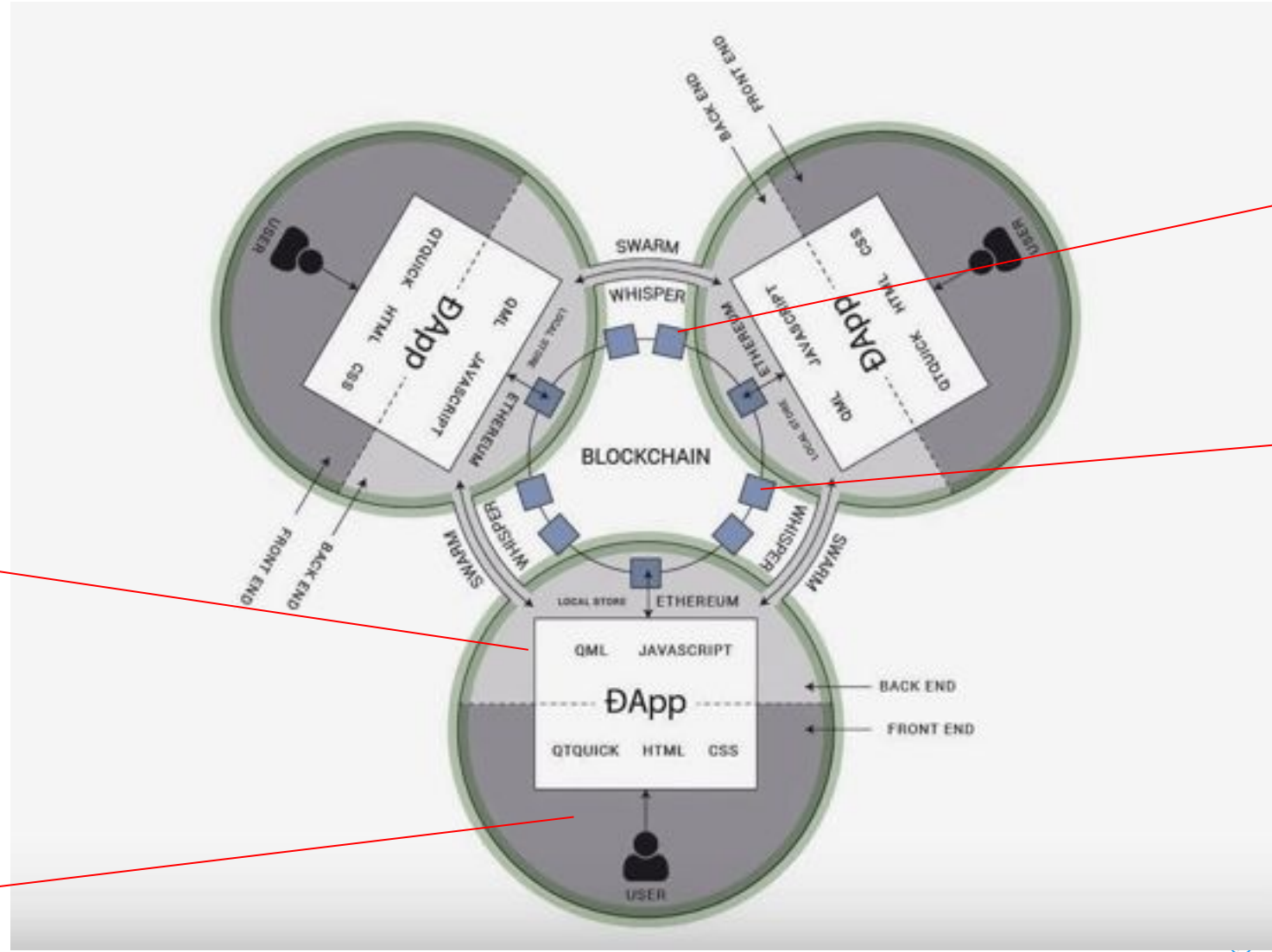
Apps



dApps



Componentes de una DApp



El backend define la interacción con la blockchain (Ethereum)

El frontend define la interfaz GUI al usuario en cada nodo

Ethereum interconecta a cada uno de los nodos

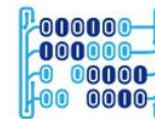
Ethereum almacena la información de la DApp de manera criptográfica



Marketplace de DApps



Universidad del
Rosario



MACC
Matemáticas Aplicadas y
Ciencias de la Computación

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

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

Mail - Daniel O... Daniel board -... Calendar - Dan... Curso de Prog... Your Projects -... Certificación I... Tasks Home P...

DappRadar Rankings Portfolio NFTs DeFi Reports Blog Search... EN ▾

Top Blockchain Dapps

All Protocols **ETH** EOS TRON IOST ONT ThunderCore VeChain NEO
WAX Steem Hive BORA BSC NEW Polygon NEW Flow NEW Other

All Categories Games DeFi Gambling Exchanges Collectibles Marketplaces Social Other High-Risk

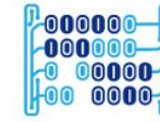
Only New Dapps 24H 7D 30D

	CATEGORY	PROTOCOL	BALANCE	USERS	VOLUME	ACTIVITY
Ad	Games	LITECOIN	\$43.25k	644 +6.27%	\$169.94	
1	Exchanges	ETH	\$408.84B	40.40k -17.70%	\$832.06M	
2	DeFi	ETH	\$6.38k	3.09k -17.54%	\$61.47M	
3	Exchanges	ETH	\$4.95B	2.97k -13.07%	\$383.54M	
4	Marketplaces	ETH	\$3.56k	1.79k -18.45%	\$563.69k	
5	Marketplaces	ETH	\$31.32k	1.49k -15.79%	\$1.56M	
6	Games	ETH	\$4.85M	1.34k +31.96%	\$111.67k	

Marketplace de DApps



Universidad del
Rosario



MACC
Matemáticas Aplicadas y
Ciencias de la Computación

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

Browser address bar: <https://www.dapp.com/dapps/ethereum>

Navigation: **dapp** Topic Dapp Ranking Market Earn

Blockchain filters: All **Ethereum** Binance BSC EOS TRON Neo Steem TomoChain IOST Terra Vexanium ICON WAX
Chiliz Hive McashChain Matic ThunderCore DRK Zilliqa Fuse

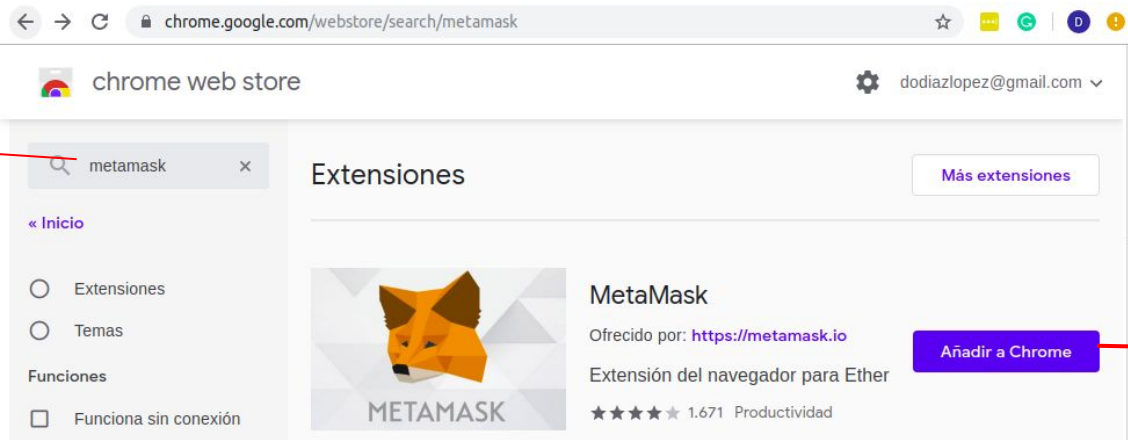
Category filters: All Gambling Game Exchange Finance Social Marketplace Utilities Others High-risk All 24 hours

#	Dapp	Category	Blockchain	24Hr Users	24hr Transactions	24Hr Volume	Social Signal
AD	HEX	High-risk	Ethereum	285 -35.37% ↓	437 -36.02% ↓	0.00 USD -100.00% ↓	3,966 -13.65% ↓
TOKEN	1 Uniswap V2	Exchange	Ethereum	45.49K 10.91% ↑	173.29K 10.98% ↑	1.25B USD 12.97% ↑	17,223 27.29% ↑
	2 dYdX	Exchange	Ethereum	105 -29.53% ↓	475 -21.36% ↓	1.13B USD 33.98% ↑	3,804 42.47% ↑
TOKEN	3 SushiSwap	Exchange	Ethereum	2.70K 2.08% ↑	14.93K 3.25% ↑	422.20M USD -1.71% ↓	2,528 -61.10% ↓
TOKEN	4 MakerDAO	Finance	Ethereum	5.00K 17.84% ↑	9.28K 31.79% ↑	408.38M USD 415.43% ↑	4,038 11.89% ↑

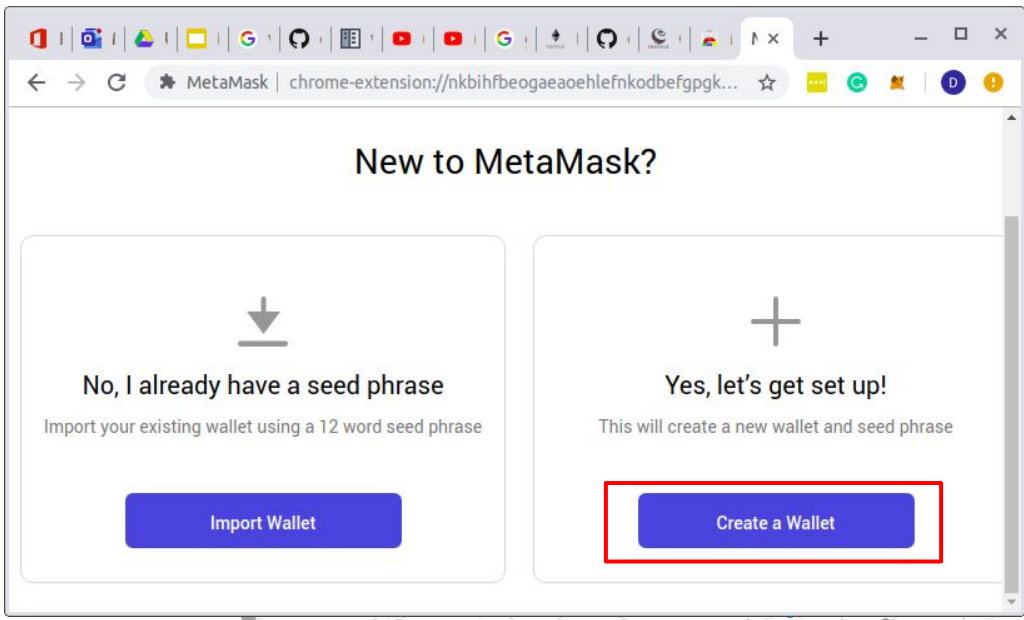
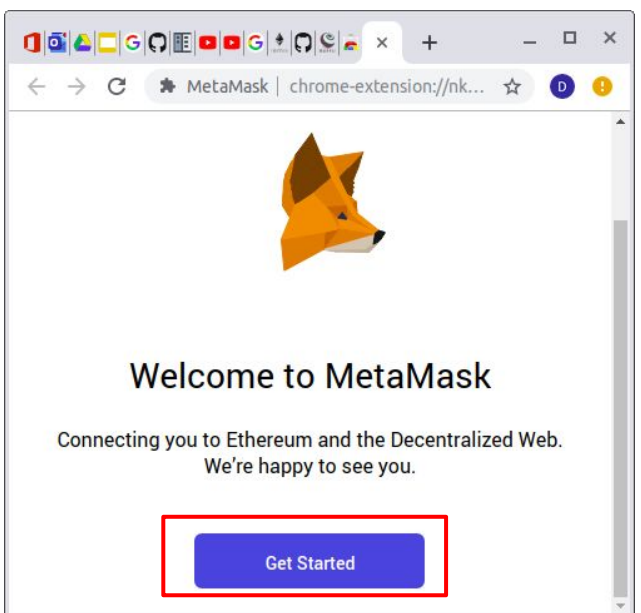
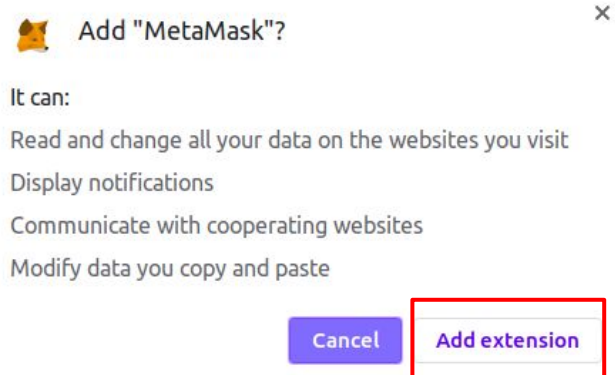
Antes de usar una Dapp necesitamos una wallet



Buscar Metamask



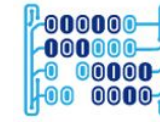
Seleccionar Añadir Metamask a Chrome



Antes de usar una Dapp necesitamos una wallet



Universidad del
Rosario



MACC
Matemáticas Aplicadas y
Ciencias de la Computación



Help Us Improve MetaMask

MetaMask would like to gather usage data to better understand how our users interact with the extension. This data will be used to continually improve the usability and user experience of our product and the Ethereum ecosystem.

MetaMask will..

- ✓ Always allow you to opt-out via Settings
- ✓ Send anonymized click & pageview events
- ✓ Maintain a public aggregate dashboard to educate the community
- ✗ **Never** collect keys, addresses, transactions, balances, hashes, or any personal information
- ✗ **Never** collect your full IP address
- ✗ **Never** sell data for profit. Ever!

No Thanks

I agree



< Back

Create Password

New Password (min 8 chars)

.....

Confirm Password

.....



I have read and agree to the [Terms of Use](#)

Create



Secret Backup Phrase

Your secret backup phrase makes it easy to back up and restore your account.

WARNING: Never disclose your backup phrase. Anyone with this phrase can take your Ether forever.



CLICK HERE TO REVEAL SECRET WORDS

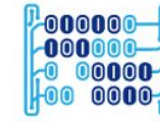
Remind me later

Next

Antes de usar una Dapp necesitamos una wallet

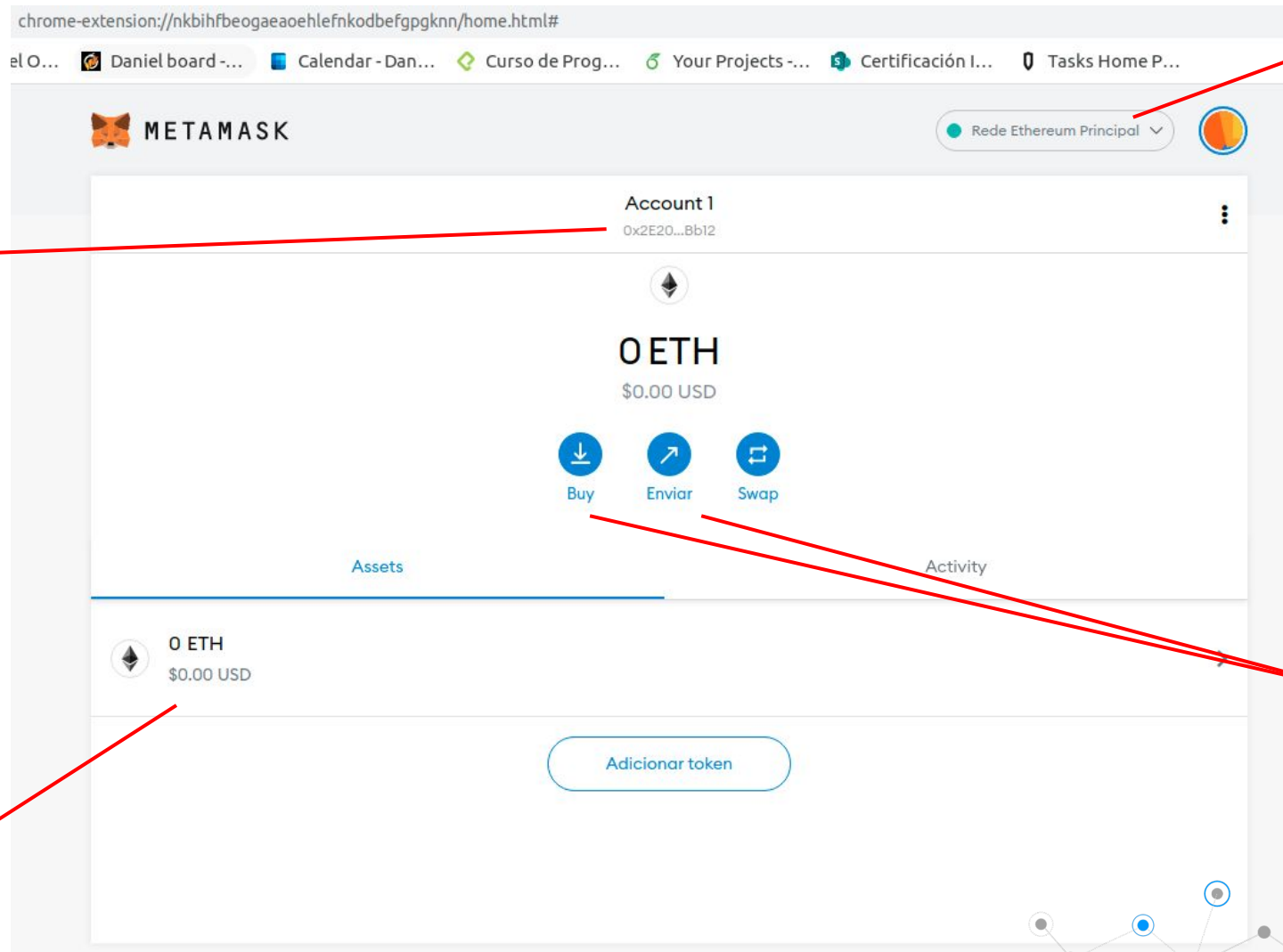


Universidad del
Rosario



MACC
Matemáticas Aplicadas y
Ciencias de la Computación

Ya tenemos nuestra cuenta/wallet de blockchain



Esta es una nuestra dirección de wallet, ya esta dirección nos pueden transferir dinero!

Esta es la red a la cual está conectada nuestra wallet

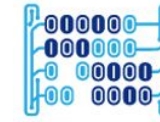
Podemos ponerle dinero a nuestra wallet o transferir dinero desde nuestra wallet

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



Buy



Enviar



Torneira de Testes

Obtenha Ether em uma torneira
para Ropsten

Obter Ether

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

https://faucet.ropsten.be

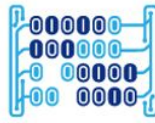
Ropsten Ethereum Faucet

Enter your testnet account address

0x2E2095a408A1e611BcFE8aaB29B8787F00daBb12

Send me test Ether

Antes de usar una Dapp necesitamos una wallet



The screenshot shows the 'Coin Flip' game interface on dice2.win. The game is set to a 50.00% winning chance. The current bet is 0.10 ETH, and the winning bet pays 1.96x. A jackpot of 1.048 ETH is available with a 0.1% chance. The game history table on the right shows previous bets and results.

Player	Bet	Result	Score
0x7b0f32	0.05	5	0.099
0xfdc84c	0.10	5	0.196
0xfdc84c	5.00	5	885
0xfdc84c	0.10	5	589
0xfdc84c	5.00	5	727
0xfdc84c	1.00	5	1.978
0xfdc84c	5.00	5	174
0xfdc84c	17.00	5	33.658
0xfdc84c	1.00	5	733
0xfdc84c	3.10	5	6.136
0xfdc84c	0.10	5	170
0xfdc84c	5.00	5	29
0xfdc84c	0.10	5	0.196
0xfdc84c	13.10	5	25.936
0xfdc84c	5.00	5	887

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



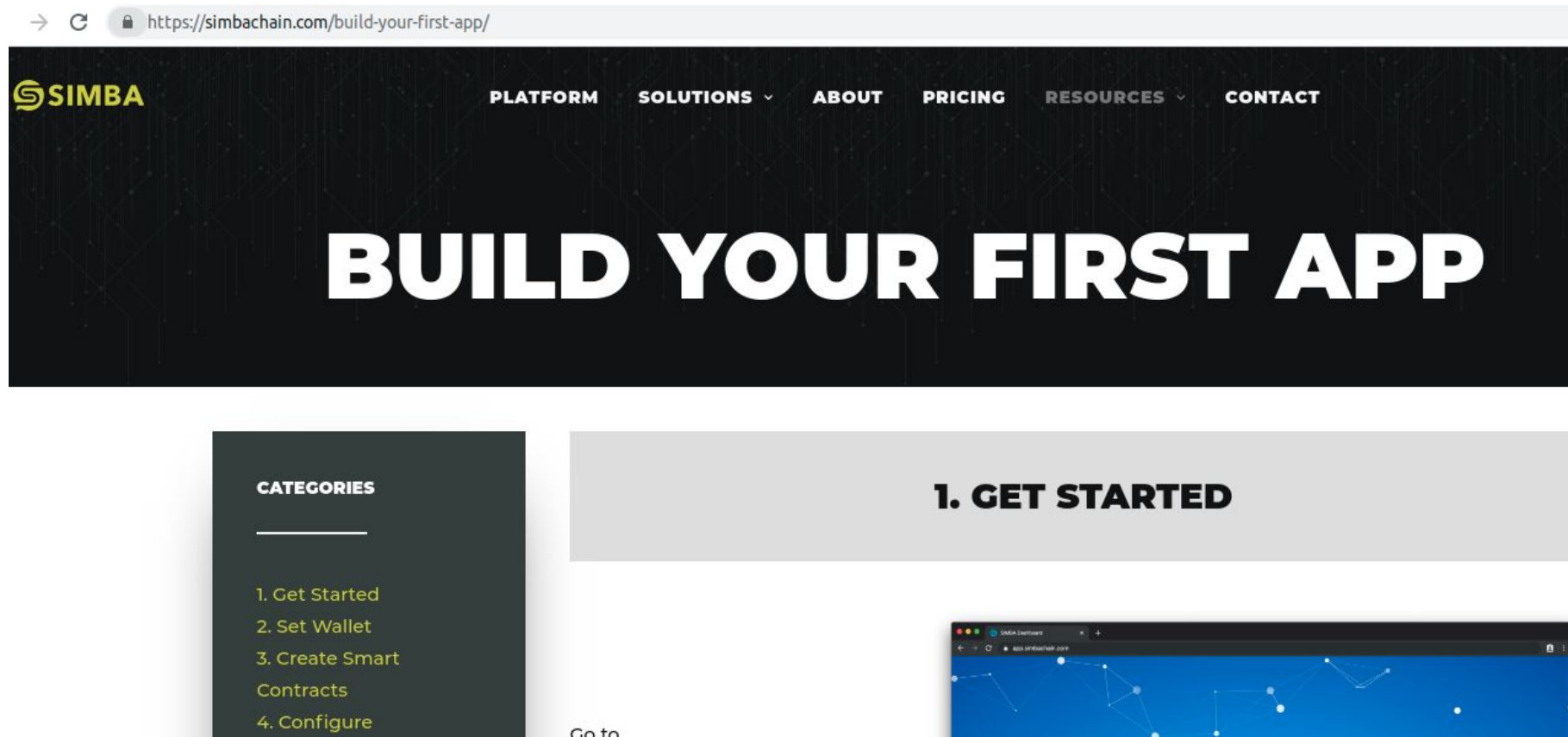
MACC
Matemáticas Aplicadas y
Ciencias de la Computación

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

The screenshot shows the SIMBA Chain website interface. The browser address bar displays `https://simbachain.com`. The website header includes the SIMBA logo and navigation links: PLATFORM, SOLUTIONS, ABOUT, PRICING, RESOURCES, and CONTACT. A yellow button labeled "LOGIN/SIGNUP" is positioned in the top right corner. The main content area features a large black box with the text: "SIMPLE WAY TO DEVELOP POWERFUL BLOCKCHAIN APPS". Below this text are two buttons: "USE CASES >" and "TRY SIMBA NOW >". The background of the website shows a laptop displaying a dashboard with a blockchain diagram and a chatbot window. The chatbot window contains the text: "SIMBA Chain Hi 😊 Have a look around! Let us know if you have any questions."

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/>



→ <https://simbachain.com/build-your-first-app/>

SIMBA PLATFORM SOLUTIONS ABOUT PRICING RESOURCES CONTACT


BUILD YOUR FIRST APP

CATEGORIES

1. Get Started
2. Set Wallet
3. Create Smart Contracts
4. Configure

1. GET STARTED

Go to





Universidad del
Rosario



MACC



HINNT

¡Gracias!

