150 ING
la Argentina celebra su ingeniería
1870-2020

II Simposio de Informática

INDUSTRIA 4.0

08 al 16 DE JUNIO

2020

Contratos Inteligentes

Desafíos y Oportunidades en la Industria del Software

Mgtr. Mauro Argañaraz

abakus

UNCA
UNIVERSIDAD NACIONAL DE CATAMARCA

Tecnológico de Antioquia
Institución Universitaria

POLITÉCNICO COLOMBIANO
JAIME ISAZA CADAVID

Agenda

Parte I: Introducción

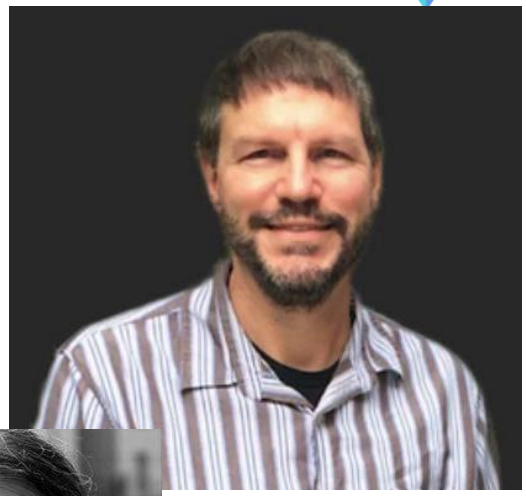
- Un poco de historia…
- ¿Qué es un Contrato Inteligente?
- Money Legos
- Ethereum

Parte II: Contratos Inteligentes

- Características
- Desafíos
- Desarrollo, Despliegue y Ejecución
- Stack
- Ciclo de Desarrollo
- Mainnet & Testnets
- Lenguajes de Programación
- Herramientas
- Comunidad

Un poco de historia…

- Acuñado en 1993 por el criptógrafo estadounidense **Nick Szabo**.
- Llevar las prácticas de la ley de contratos y las prácticas comerciales relacionadas hacia el diseño de protocolos de comercio electrónico entre extraños en internet.



@nickszabo4

- Creía que la especificación a través de una lógica clara, y una verificación o ejecución a través de protocolos podría constituir una mejora importante sobre los contratos legales tradicionales.
- No tuvo éxito debido a las limitaciones tecnológicas de ese momento.

@chaumdotcom

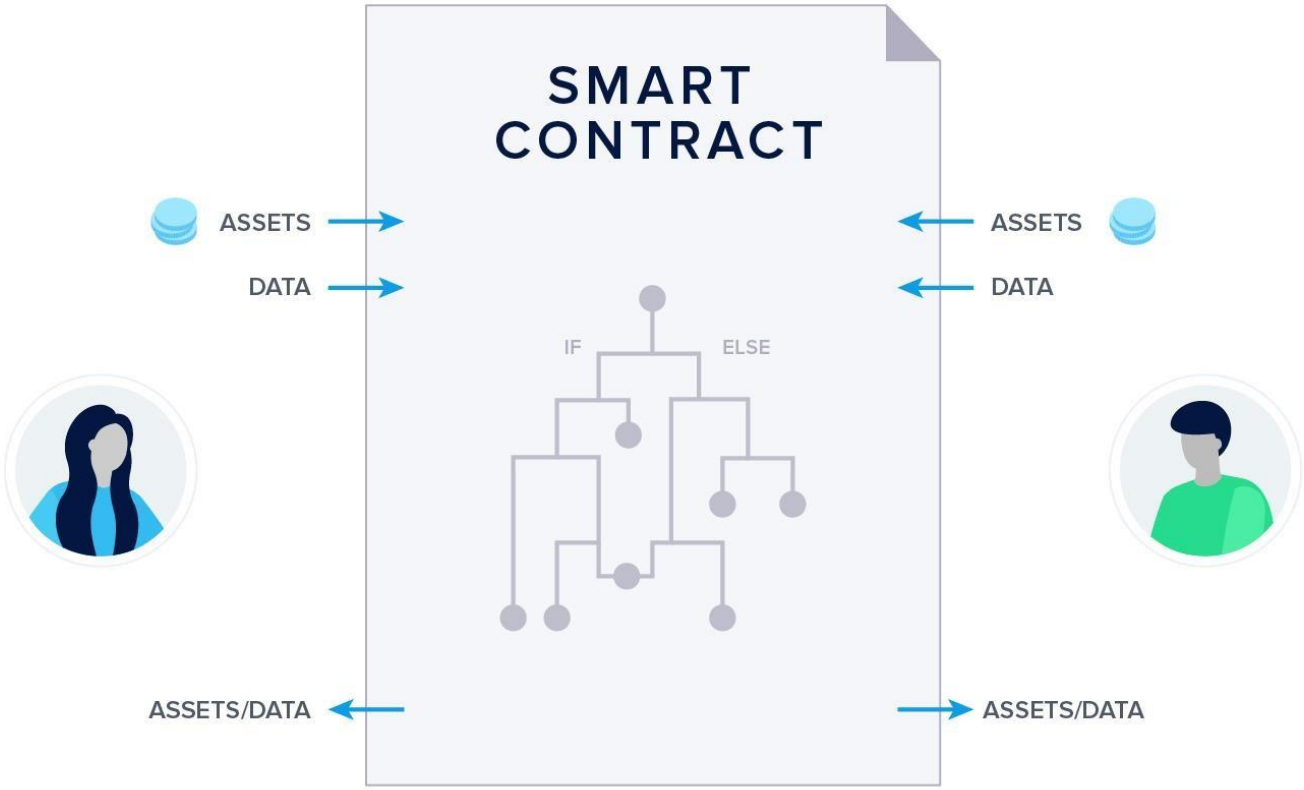
Un poco de historia…

- En 2008 se creó **Bitcoin** y cambió la situación. A pesar de que el Bitcoin solo estaba pensado para ser una herramienta financiera, su tecnología era útil.
- La primera generación de blockchains estaba enfocada en la transferencia de valor: Litecoin, Bitcoin Cash, Ripple

- En 2013 un desarrollador de Bitcoin, **Vitalik Buterin**, propuso aprovechar la red para ejecutar aplicaciones distribuidas. Su propuesta no fue aceptada.
- En 2015 junto a un grupo de desarrolladores puso en marcha **Ethereum**: la primera blockchain que implementaba con éxito los contratos inteligentes

@VitalikButerin

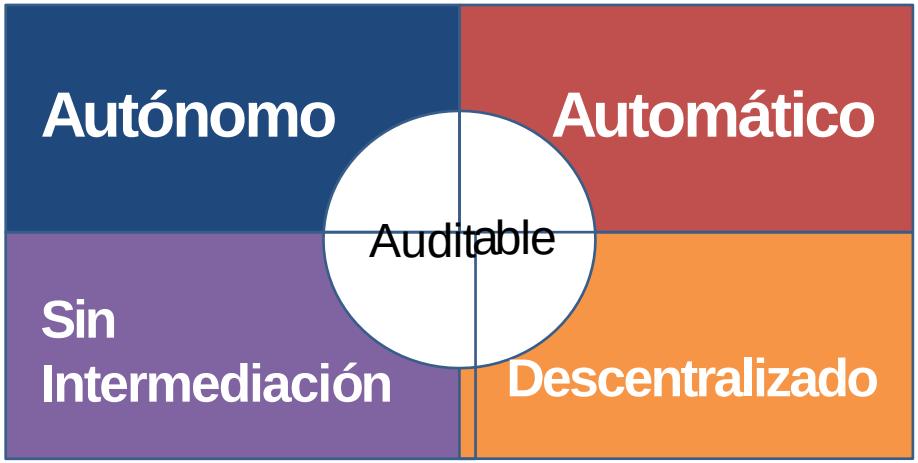
¿Qué es un Contrato Inteligente?



Son programas informáticos que facilitan, verifican y hacen cumplir la negociación y ejecución de contratos legales.

¿Qué es un Contrato Inteligente?

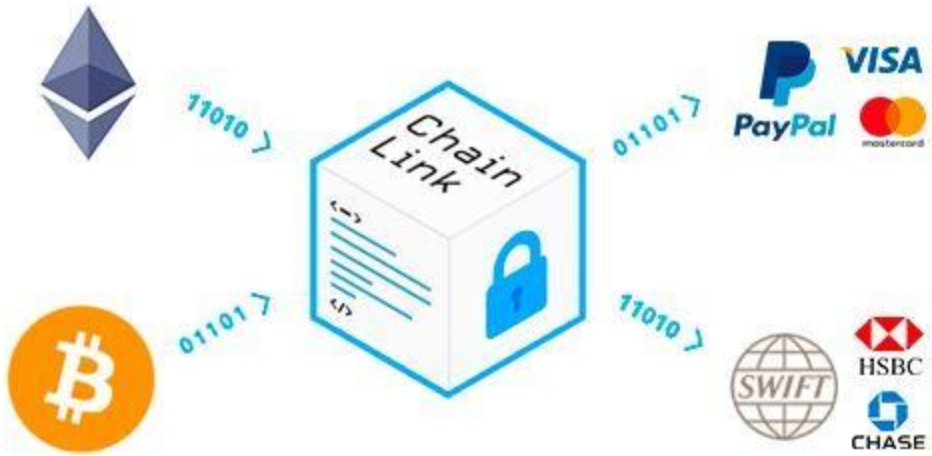
- Entidad **autónoma** que **automáticamente** lleva a cabo acciones específicas cuando se cumplen ciertas condiciones.
- Brinda un medio para interactuar con la cadena de bloques programáticamente, dando lugar al desarrollo de aplicaciones, juegos y plataformas usando la **blockchain** como base de datos. A estas aplicaciones se les conoce como **Dapps**.



Money Legos

- Monedas (Token ERC20: Stablecoins)
- Finanzas decentralizadas (DeFi: ahorros, prestamos, pooles de liquidez, DEXs)
- Derivados financieros (trading, sintéticos, leverage, futuros)
- NFT (Token ERC721: Coleccionables)
- Organizaciones descentralizadas (DAO)

Money Legos



- Fuentes de datos (Oráculos)
- Sistemas de votación
- Registros públicos y de títulos (Académico, Contribuyentes)
- Juegos (Decentraland, Gods Unchained)
- y miles de otras aplicaciones.

BLOCKCHAIN
FEDERAL ARGENTINA

Decentraland

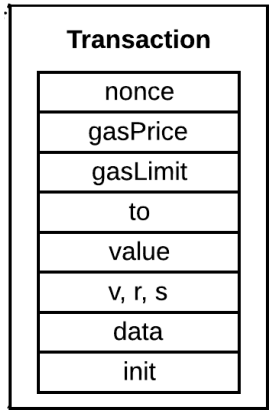
Ethereum

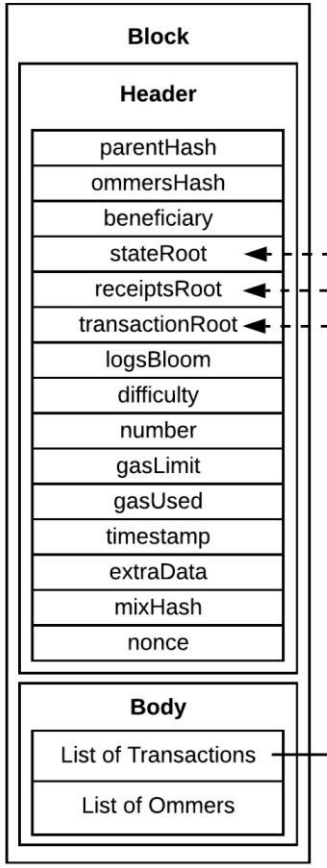
- Es una plataforma de computación distribuida basada en una blockchain de código abierto.
- Se utiliza para crear e implementar la funcionalidad de contratos inteligentes.
- Su token se llama ether (modelo inflacionario)
- Los desarrolladores pueden crear aplicaciones usando lenguajes de programacion amigables (Turing completo).
- El código fuente de alto nivel se compila a bytecode.
- El bytecode se ejecuta en una máquina virtual descentralizada.
- Año 2016: incidente de seguridad ETC -> ETH 1.0
- En curso: PoW -> PoS (ETH 2.0)

Ethereum

Transacciones

- Una solicitud para modificar el estado de la cadena de bloques
- Puede ejecutar código (contratos) que cambian el estado global
- Firmada por la cuenta de origen
- Tipos
  - Enviar valor de una cuenta a otra
  - Crear un contrato inteligente
  - Ejecutar el código de un contrato inteligente

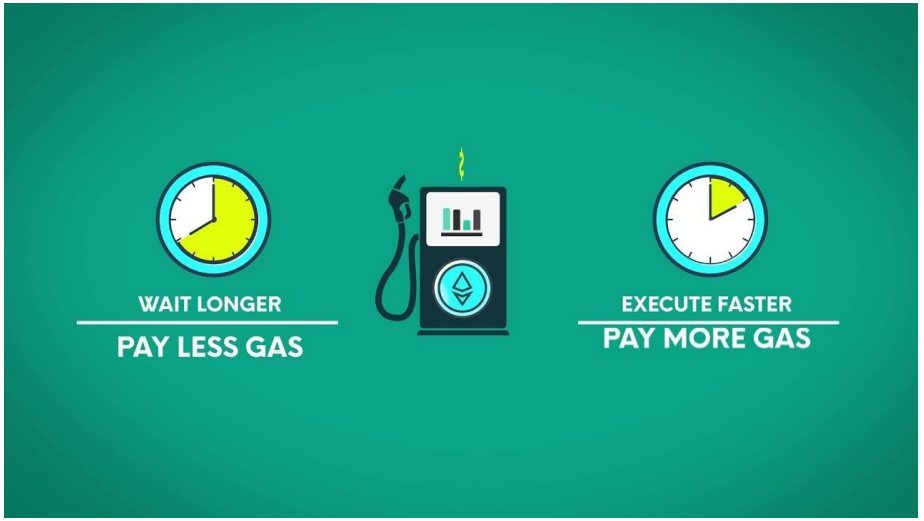




Ethereum

Uso de Gas

- El gas es el combustible que permite funcionar a la red
- La unidad de medida utilizada para representar el costo de correr operaciones en Ethereum



- Conceptos:
  - El **costo** de gas son las unidades de gas necesarias para correr cada operación
  - El **precio** del gas es el valor de una unidad de gas expresado en ether.
  - El **límite** de gas es la máxima cantidad de gas que uno está dispuesto a pagar en una transacción específica

Ethereum

Stats

- 100 millones de direcciones Ethereum.
- 40 millones de direcciones con saldo ETH (creciendo a 100k / día). 60 millones de cuentas del Bank of America.
- 400 mil direcciones diarias activas.
- Han superado el total de los primeros usuarios de Internet: 16 millones en 1995.

Características

- Código ejecutable
- Ejecución determinista
- Turing Complete
- Funciona como una cuenta externa
- Mantiene fondos
- Puede intereractuar con otras cuentas y contratos
- Almacena datos
- Se puede invocar a través de transacciones
- La ejecución de una instrucción tiene un costo (gas)
- Inmutable

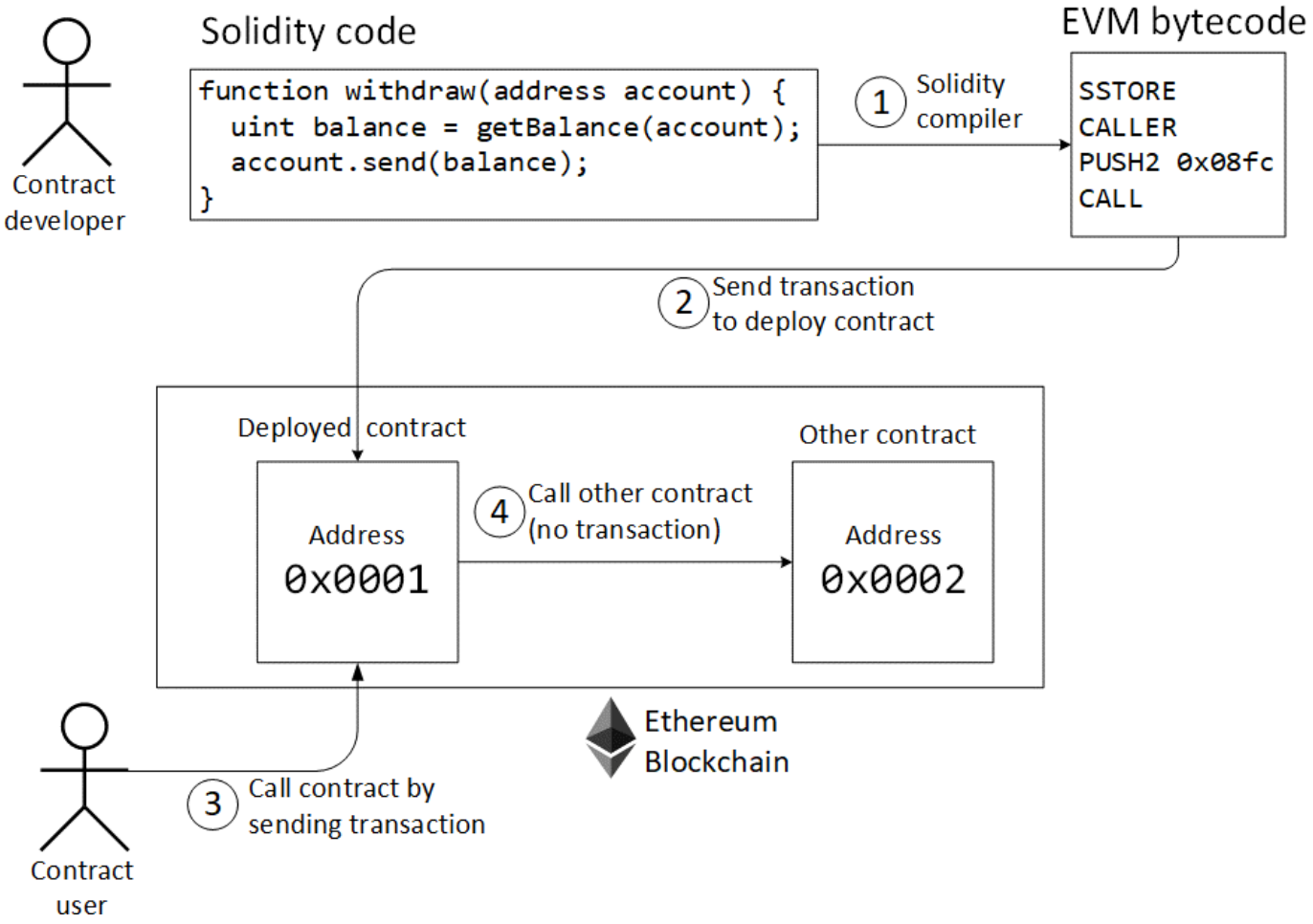
Desafíos

- **Entorno de ejecución desconocido**.
  Los desarrolladores no están acostumbrados a que su código sea ejecutado por una red global de nodos anónimos, sin una relación de confianza y con ánimo de lucro.
- **Nueva pila de software**.
  Compilador Solidity, EVM y la capa de consenso están en desarrollo, y aún se descubren vulnerabilidades de seguridad.
- **Habilidad muy limitada para arreglar contratos**.
  Contrasta con el proceso de desarrollo de software tradicional que promueve las técnicas iterativas.
- **Rápido ritmo de desarrollo**.
  Las compañías blockchain se esfuerzan por lanzar sus productos rápidamente, a menudo a expensas de la seguridad.

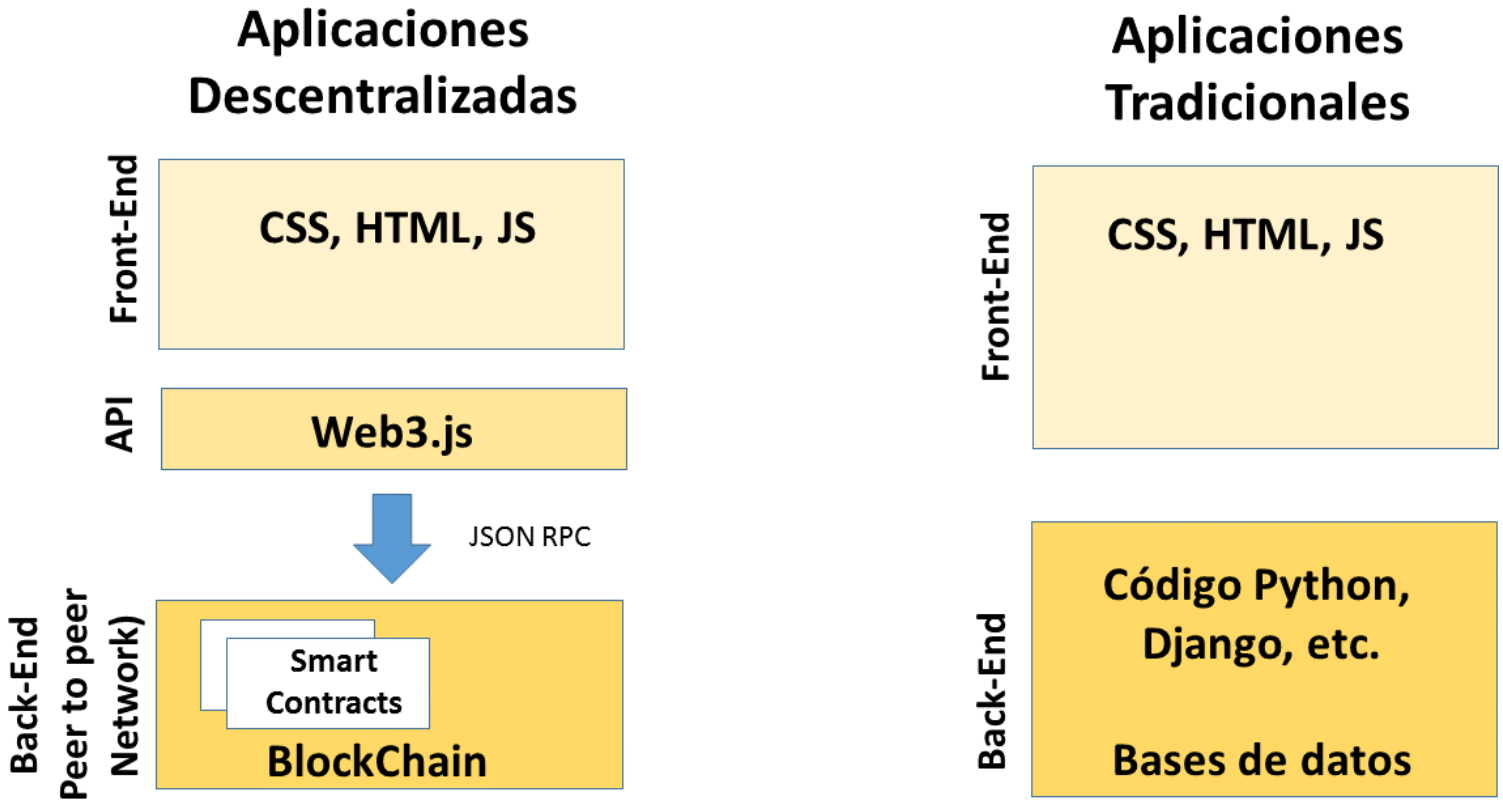
Desafíos

- **Atacantes anónimos financieramente motivados.**
  En comparación con muchos delitos cibernéticos, explotar contratos inteligentes ofrece:
  - mayores ganancias : los precios de las criptomonedas han aumentado rápidamente
  - facilidad para el cobro : el ether y los tokens se pueden comercializar instantáneamente
  - menor riesgo de castigo debido al anonimato y a la falta de legislación en la materia
- **Lenguaje de alto nivel subóptimo**.

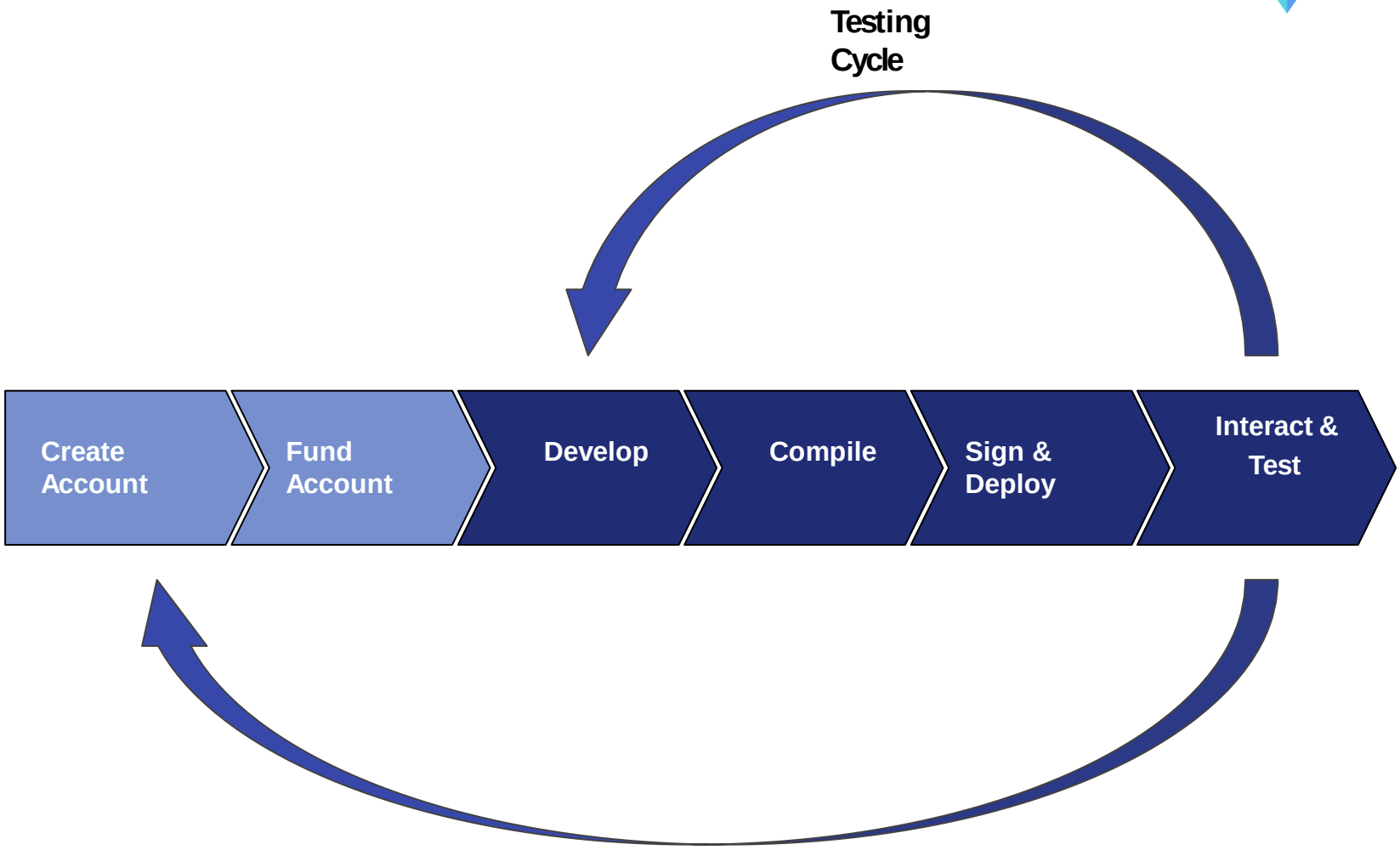
Desarrollo, Despliegue y Ejecución



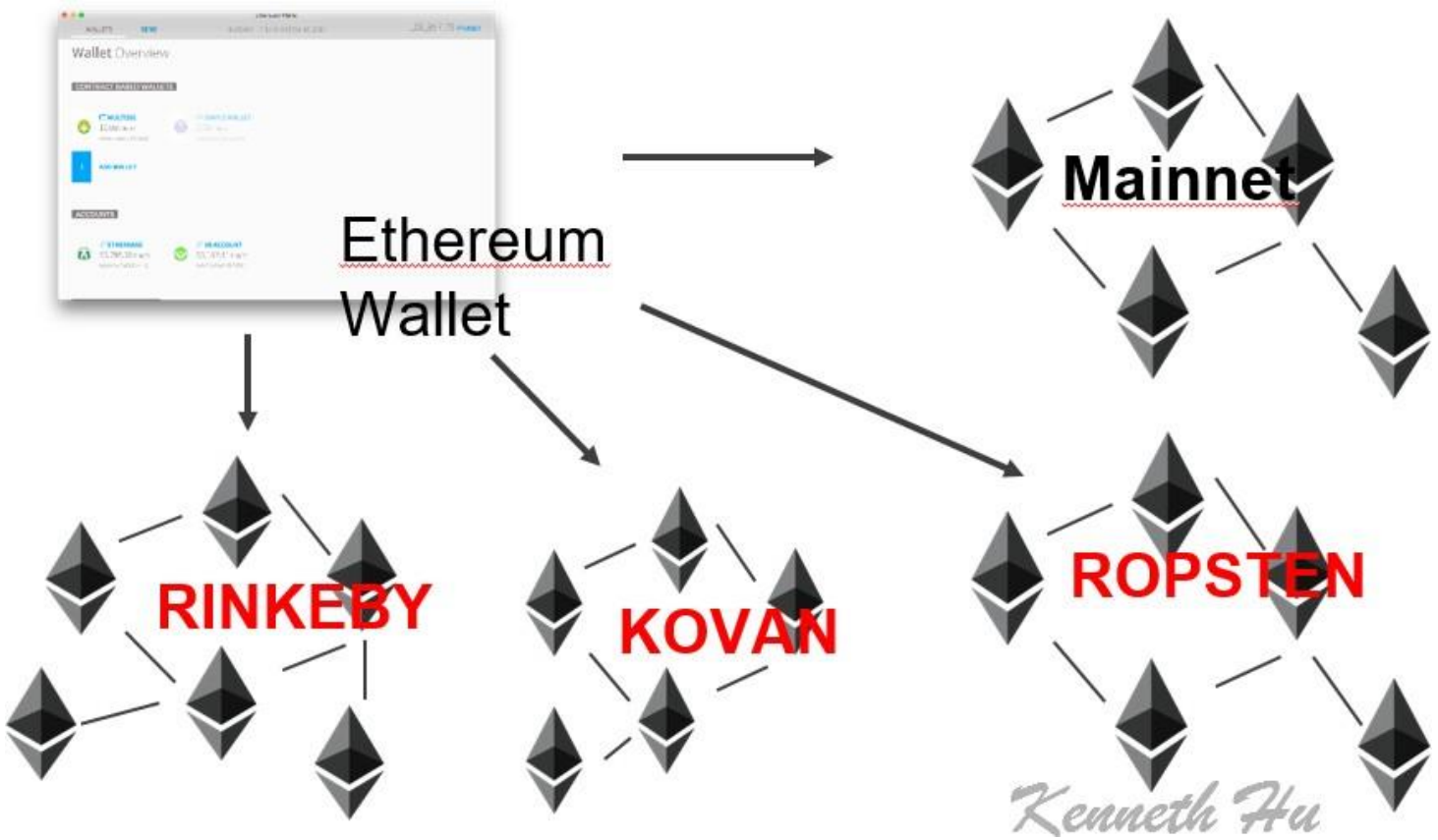
Stack


Aplicaciones Descentralizadas
Front-End
CSS, HTML, JS
API
Web3.js
JSON RPC
Back-End (Peer to peer Network)
Smart Contracts
BlockChain
Aplicaciones Tradicionales
Front-End
CSS, HTML, JS
Back-End
Código Python, Django, etc.
Bases de datos

Ciclo de Desarrollo



Mainnet & Testnets



Lenguajes de Programación

Solidity

- Lenguaje de alto nivel orientado a contratos
- Lo propuso Gavin Wood en 2014
- Similar a Javascript y C
- Soporta herencia, tipado estático y sobrecarga de métodos
- Tiene construcciones para interactuar con la plataforma Ethereum
- Actualmente versión 0.6.9

@solidity_lang

@gavofyork

Lenguajes de Programación

Vyper

- Prototipo basado en Python
- Orientado a mejorar aspectos de seguridad

Otros lenguajes

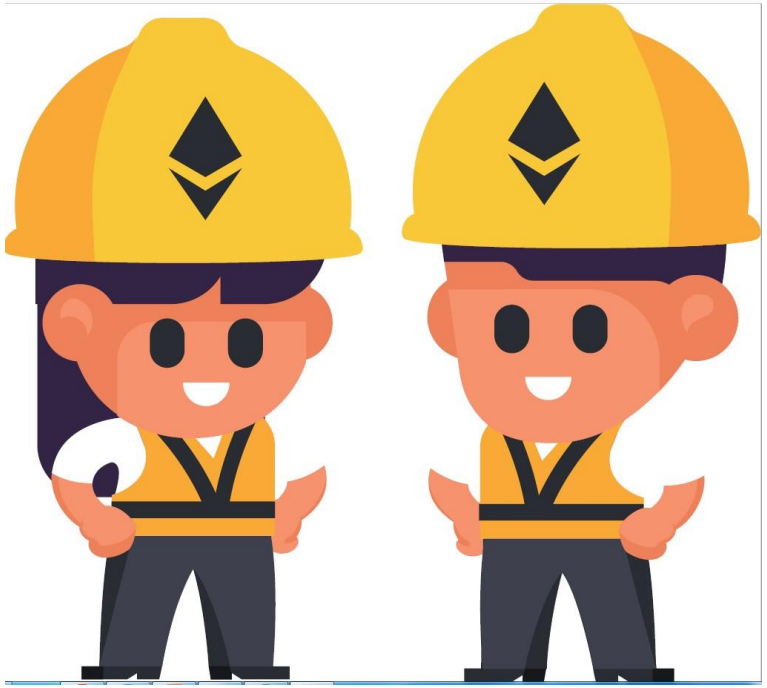
- Mutan (deprecated)
- Serpent (python)
- LLL (lisp)
- Bamboo
- Flint

Herramientas

- **Remix IDE**: Es un IDE para Solidity y Vyper basado en web, donde es posible escribir contratos, compilar, distribuir y ejecutar métodos de contratos en un navegador web. https://remix.ethereum.org
- **Metamask**: Es una extensión de Chrome que nos integra un nodo Ethereum en el navegador. Permite ejecutar e interactuar con la Blockchain de Ethereum con Javascript
- **Web3.js**: es la API que nos permite interactuar con la Blockchain desde el navegador

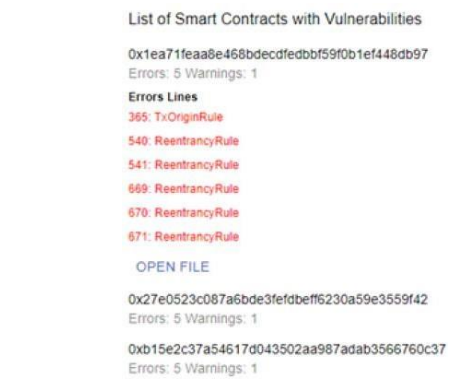
Setup: VS Code + Buidler

- VS Code
- Buidler (https://buidler.dev/)
  - Desarrollado por **Nomic Labs** (Patricio Paladino, Franco Zeoli)
  - Uso de plugins para unit testing, linting, gasreporter
  - Debug de código (EVM Buidler)



OpenBalthazar

- Es una herramienta web que realiza análisis léxicos y sintácticos para contratos implementados en la plataforma Ethereum.
- Lenguajes soportados: Solidity y Vyper.
- Método de análisis estático.
- Búsquedas de Bugs.
- Extensible
- Verificación automatizada.
- Integración con Etherscan.io



Comunidad

- EthereumBA.
- CryptoDevs ARG (Telegram).

- Dai & DeFi Latin America (Telegram)

- Ethereum Bogota 1er Meetup (06/06)
- EthereumBogota (Telegram)
- **Fundación Ethereum: Devcon 6 se realizará en Bogotá en 2021**

Caso de Exito

- https://compose.fi/
- Hackathon **HackMoney**
- **Bruno Balzani (**@brunitob**)** y **Daniel Fernandez**
- Una herramienta didáctica para conectar visualmente instrumentos DeFi y aprender sobre la composición.
- Un grafo se despliega y ejecuta como un contrato inteligente. No hay una base de datos central involucrada, solo escritura y lectura de datos de la blockchain.

II Simposio de Informática
INDUSTRIA 4.0

marganaraz@gmail.com

@mauro_arganaraz

https://www.linkedin.com/in/mauro-arga%C3%B1araz-3a5ba2174/

Enlace a la disertación virtual

https://www.youtube.com/watch?v=g7uLYsC1Qm0