

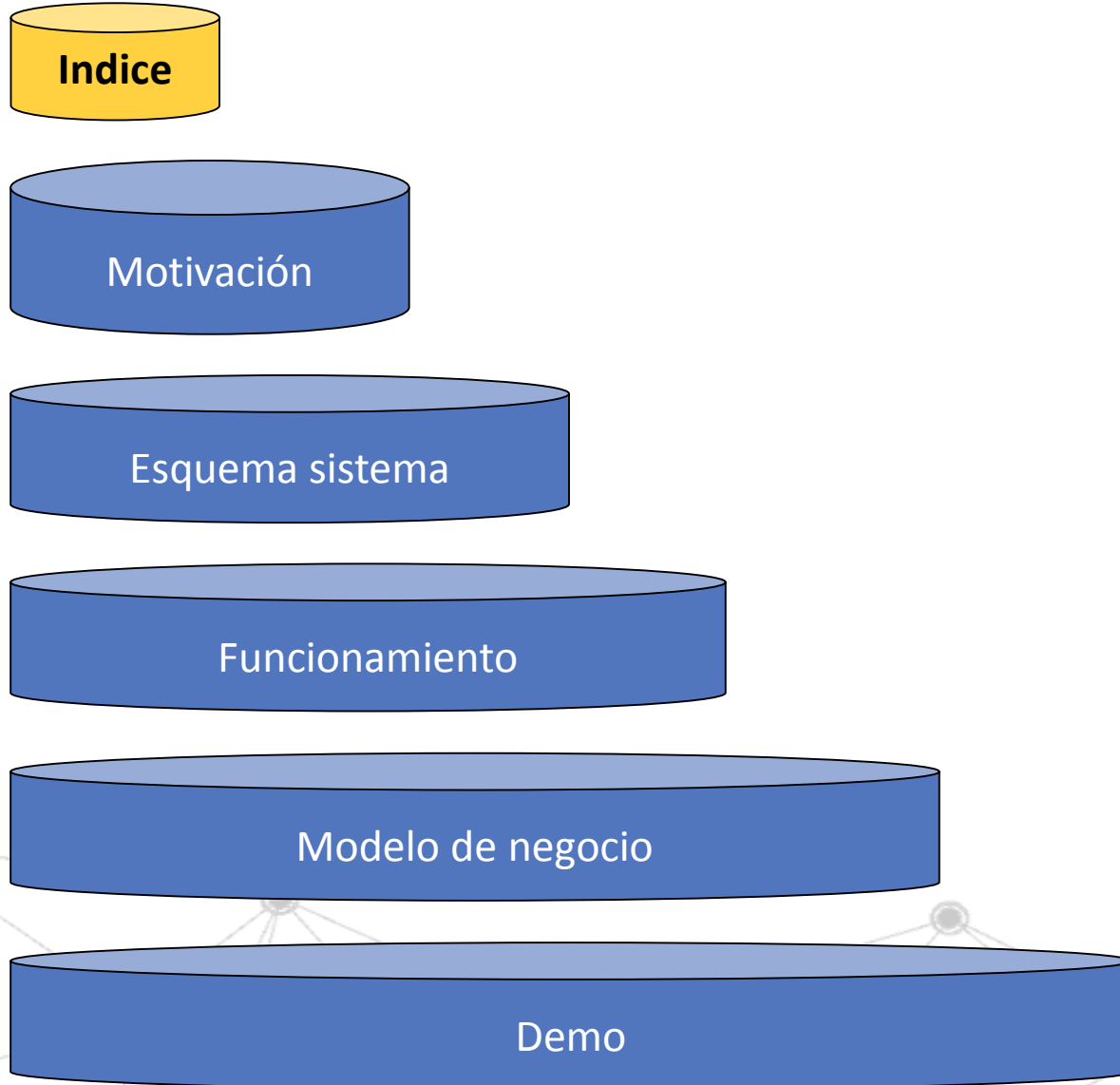
Sistema para el desarrollo de redes de sensores
gestionado desde dispositivo inteligente con
almacenamiento y compra de datos empleando blockchain



Javier Fraile Pérez de Arilucea



Indice



Motivación



Arduino + SesNe + ethereum

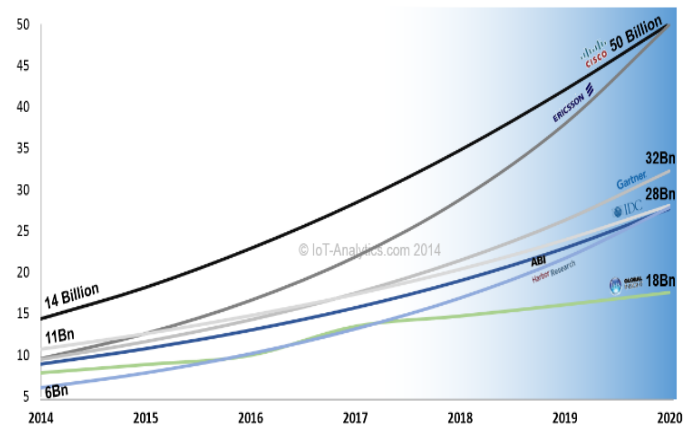
Motivación

IoT + Blockchain

IoT Analytics - Quantifying the connected world

Global IoT/IoE device forecasts

of worldwide connected devices² (in Billion)



Source	Date	CAGR ¹ 2014-'20
CISCO	2013	23%
ERICSSON	2010	-
Gartner	2013	23%
IDC	2014	17%
Harbor Research	2014	29%
ABI Research	2014	21%
IHS	2014	14%

Note: Some forecasts only for specific years, in that case all other years in between are extrapolated based on the corresponding growth rate; Ericsson does not specify today's number of connected devices - therefore: Average of all other studies assumed as starting point in 2014.
1. CAGR = Compound annual growth rate 2. Connected devices includes all autonomous connected things (every forecaster has own definition) - does NOT include computers, mobile devices, tablets
Sources: Cisco, Ericsson, ABI Research, Gartner, IHS, IDC, Harbor Research, IoT-Analytics.com

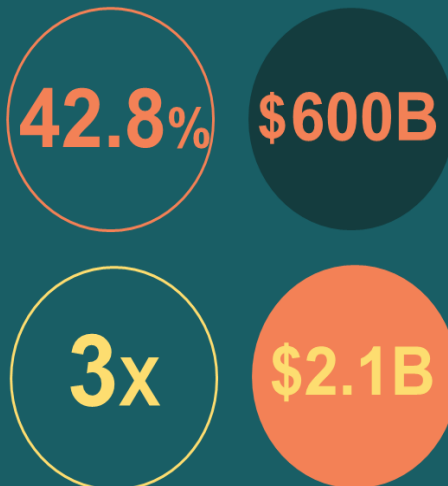
El uso de blockchain aumentará un 42,8% para el año 2020

Las oportunidades laborales se multiplicaron por 3 de 2017 a 2018

50.000 millones de dispositivos conectados para el año 2020

55% de los dispositivos orientados al mundo empresarial

The Power of the Blockchain Movement



What Data Says?

- The Blockchain space is predicted to expand by 42.8% by 2020.
- 600 Billion was the size of the entire cryptocurrency market by the end of 2017
- Blockchain related LinkedIn jobs tripled from 2017 to 2018
- Global spending on blockchain solutions in 2018 equals to \$2.1 Billion.

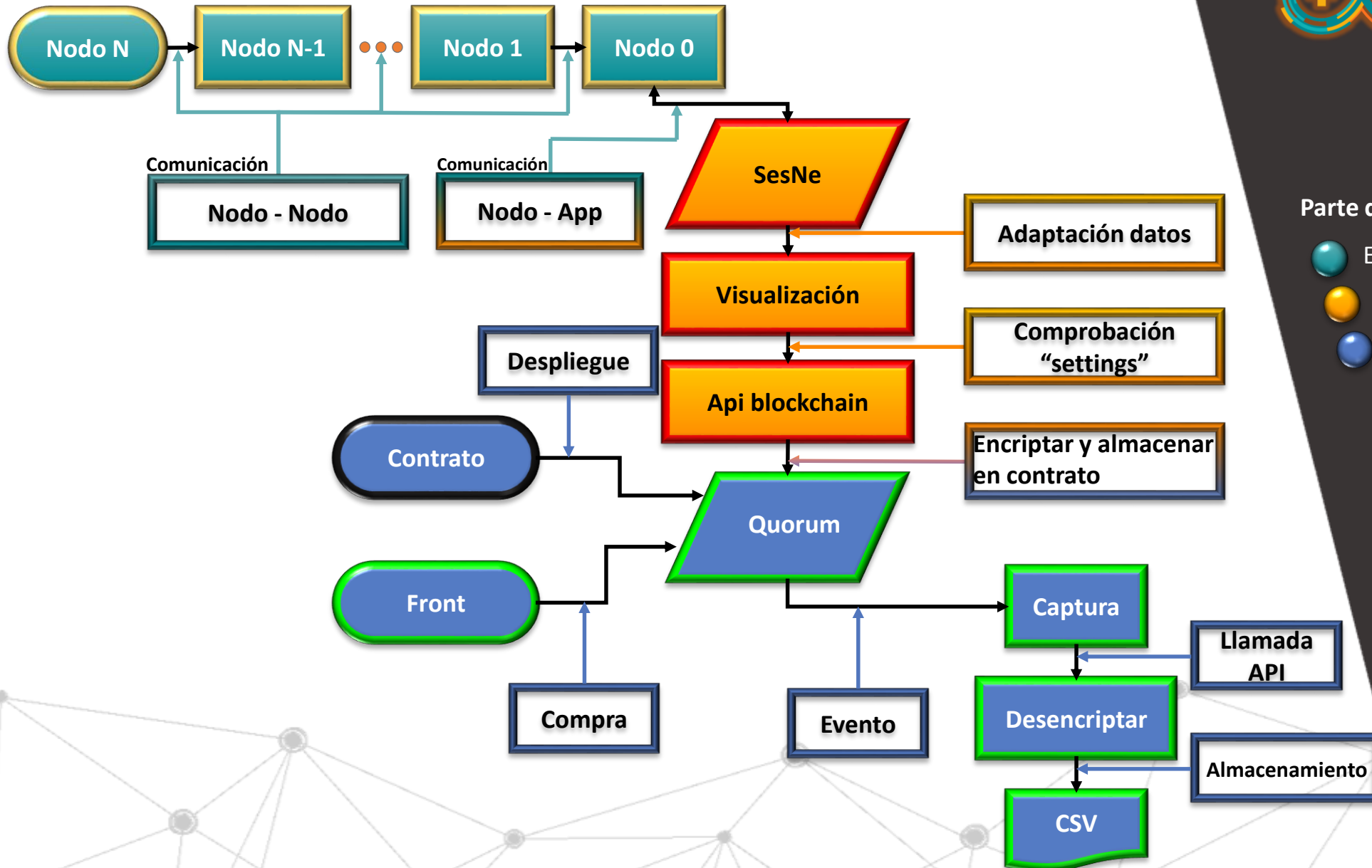


Esquema sistema



Arduino + SesNe + ethereum

Esquema del sistema



Parte del sistema al que pertenece

- Electrónica
- App (SesNe)
- Blockchain

Lenguaje de programación empleado

- C++
- Java
- Python
- Solidity

Funcionamiento



Arduino + SesNe + ethereum

Red de sensores

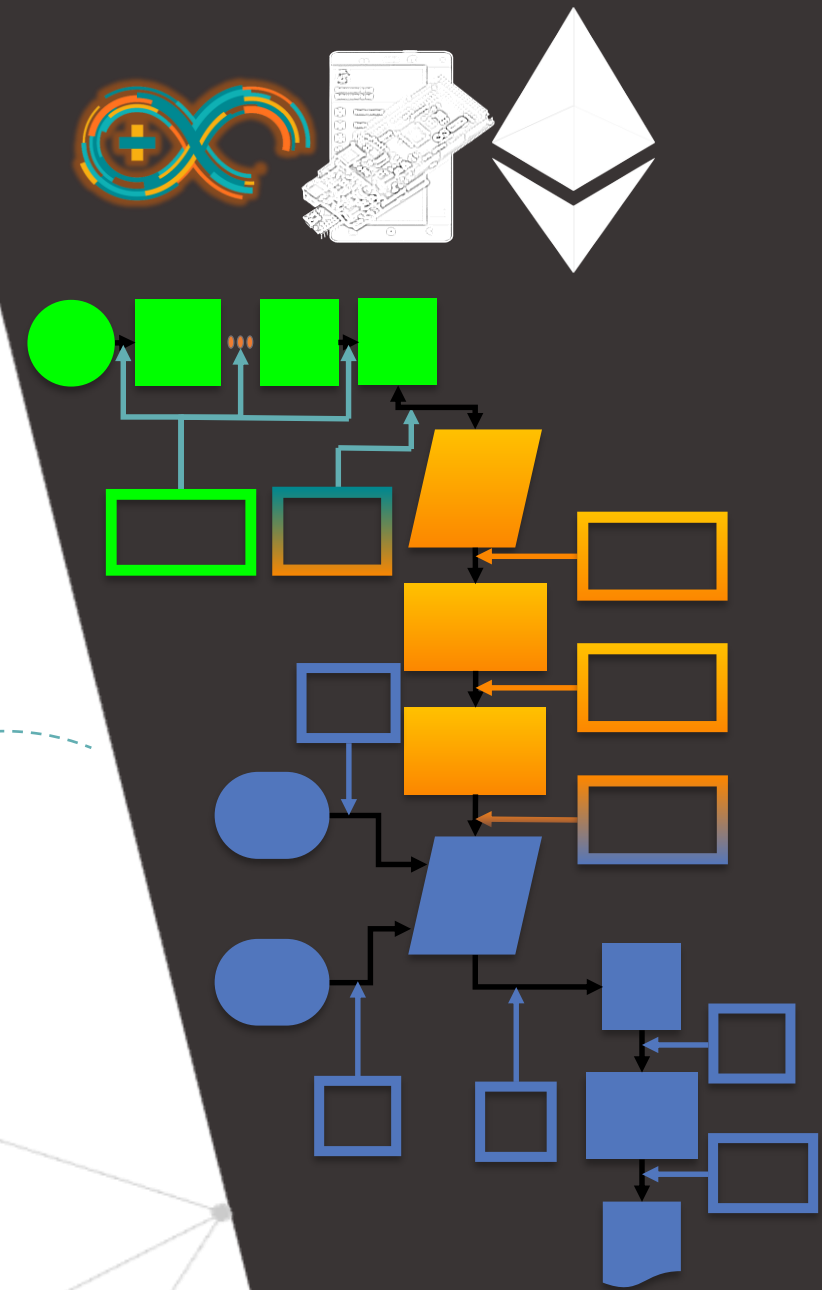
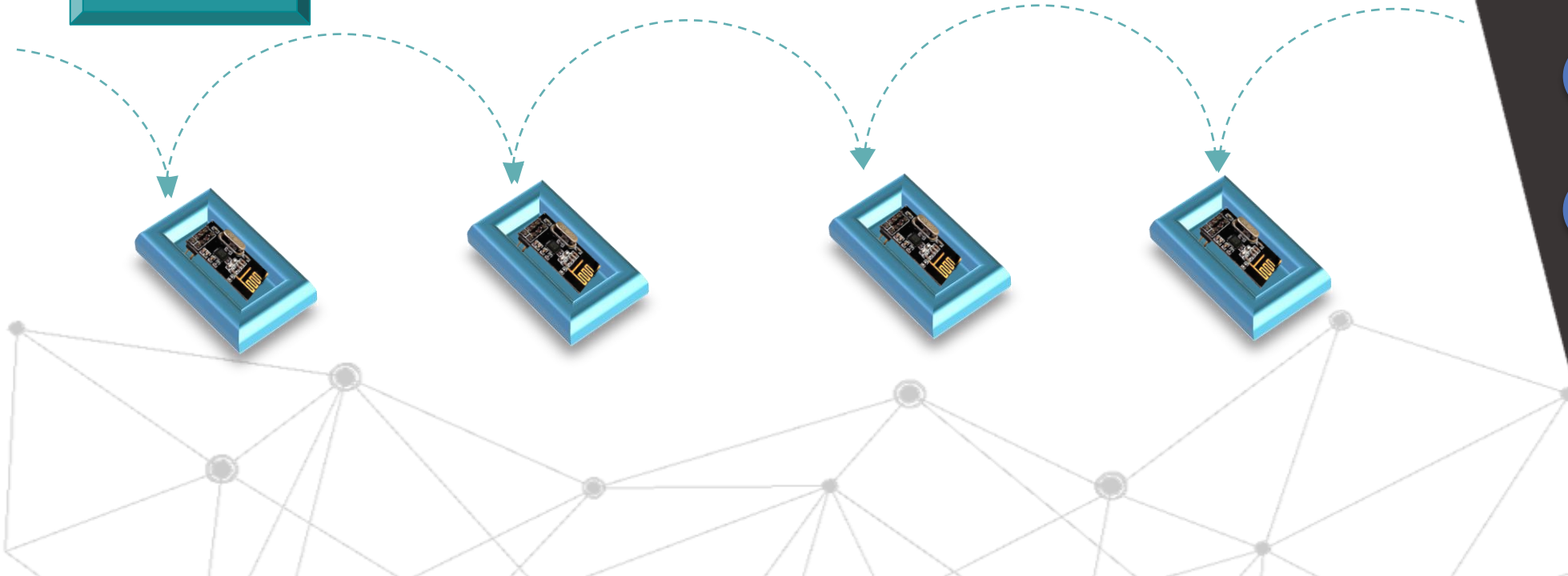
Comunicación Nodo - Nodo

Diseño Multi-Hop

Protocolo propio

Nrf24l01

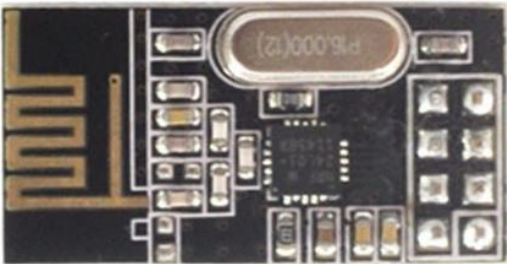
Nodo Seleccionado	Valor activación enviado
Nodo 1	10
Nodo 2	20
...	...
Nodo X	$X \cdot 10$



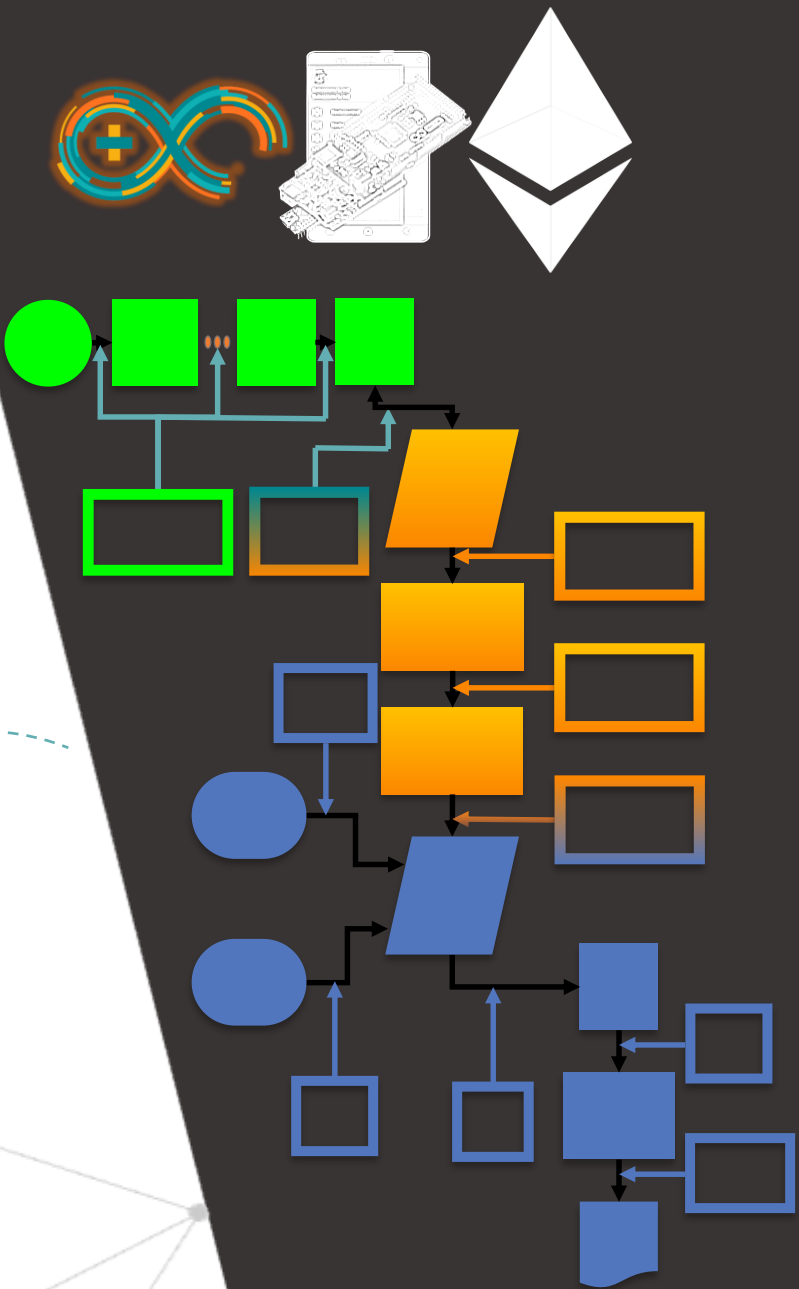
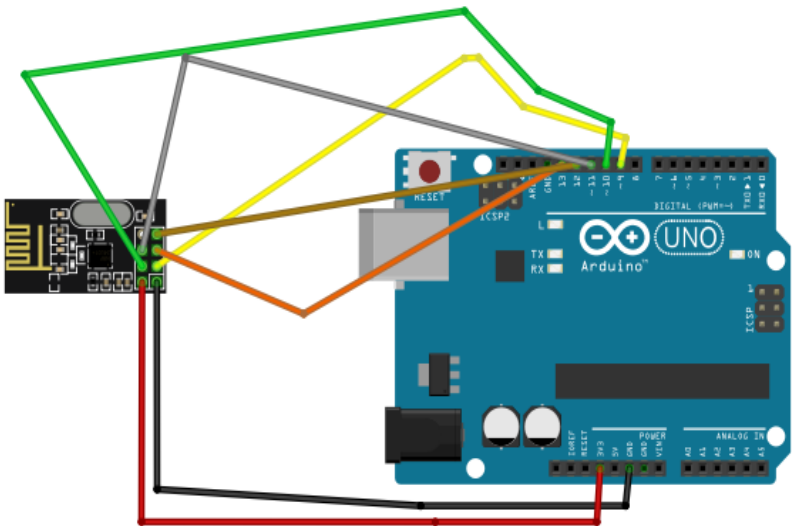
Nodo N – Nodo 0
Comunicación entre nodos

Red de sensores

Comunicación Nodo - Nodo



- | | | |
|---|---|---------|
| 8 | 7 | 1: GND |
| 6 | 5 | 2: VCC |
| 4 | 3 | 3: CE |
| 2 | 1 | 4: CS |
| | | 5: SCK |
| | | 6: MOSI |
| | | 7: MISO |
| | | 8: IRQ |



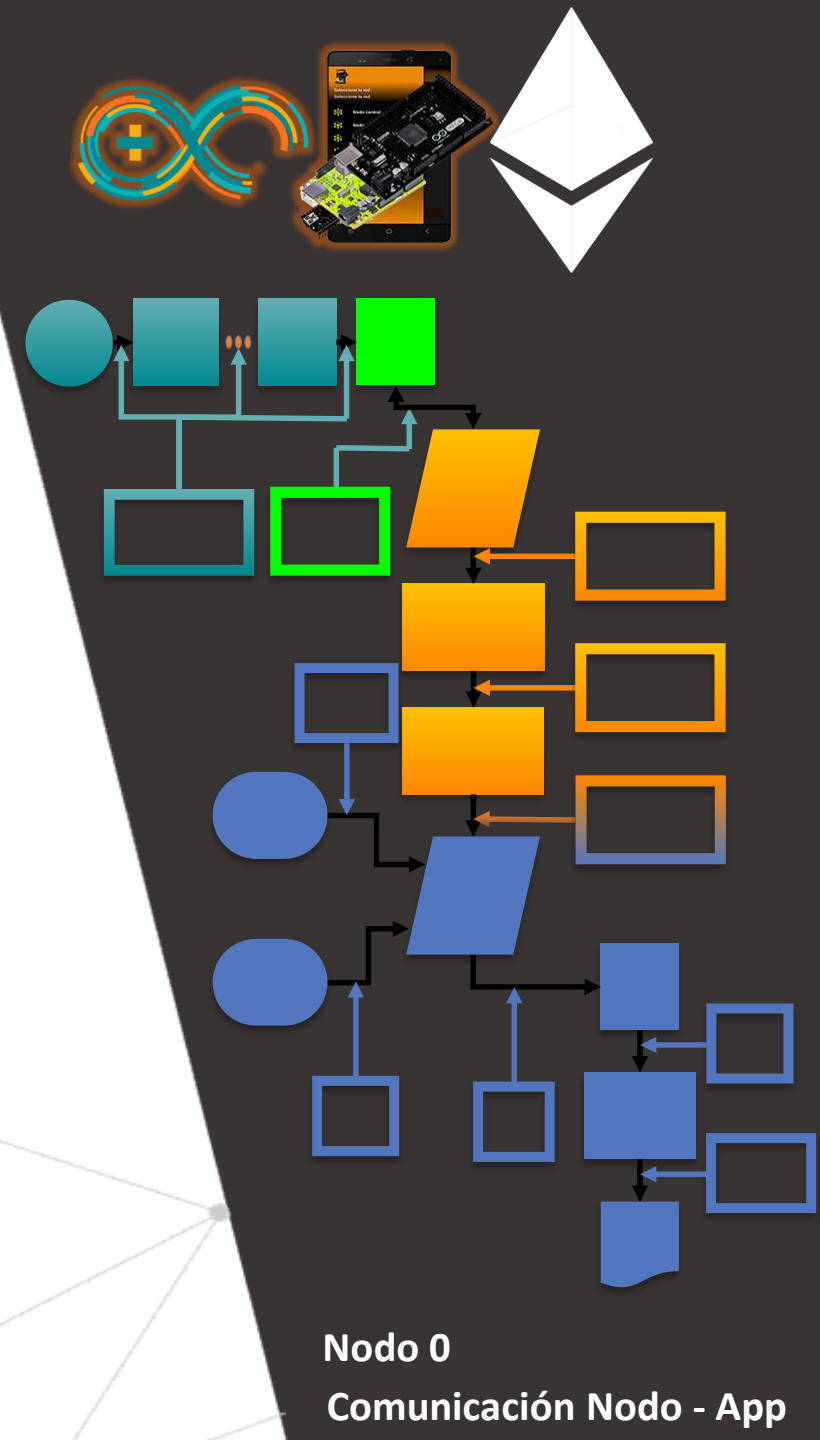
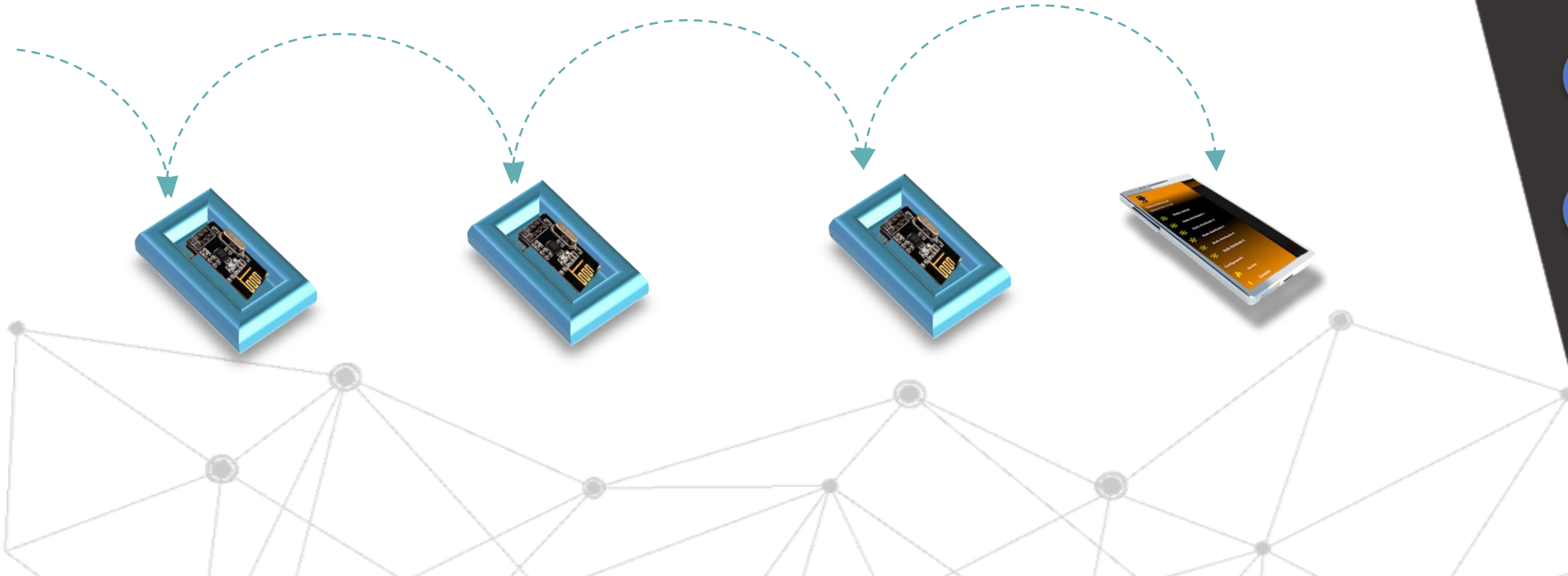
Nodo N – Nodo 0
Comunicación entre nodos

Red de sensores

Comunicación Nodo - Red

Trama elementos de la Red

Trama lectura sensores



Nodo 0

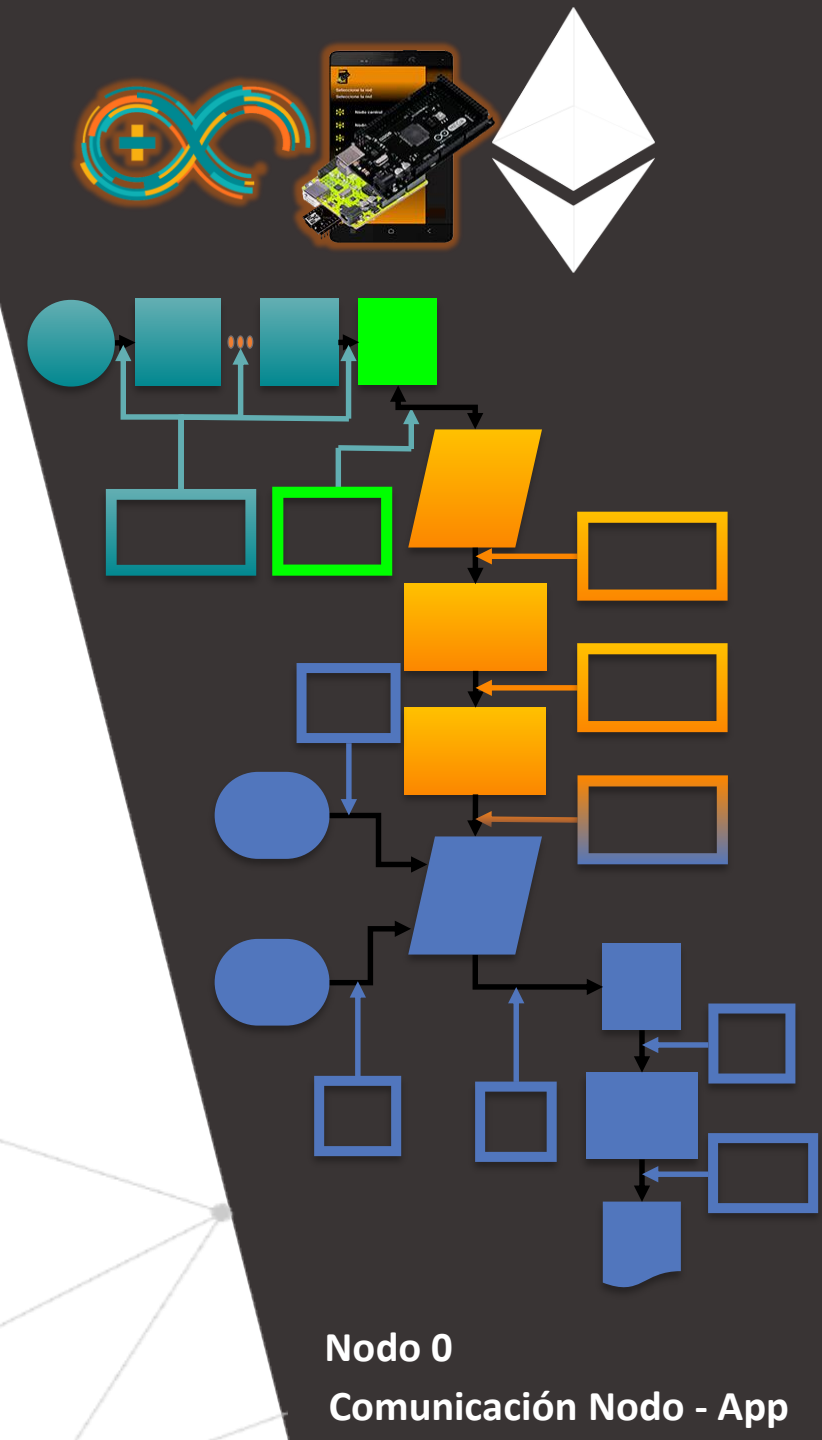
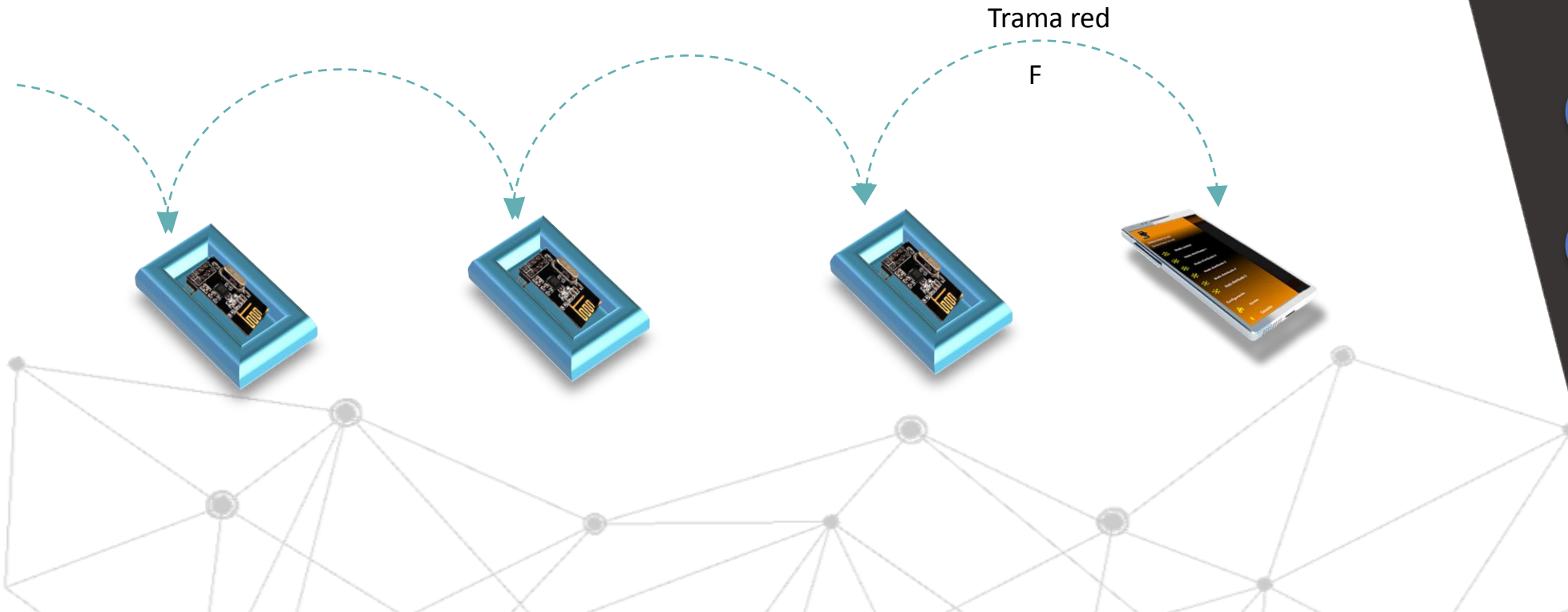
Comunicación Nodo - App

Red de sensores

Comunicación Nodo - Red

Trama elementos de la Red

"%%" + Numero_Nodos + "/" + Nombre_Red + "%" + Nombre_Nodo_0 + "%" +
Nombre_Nodo_1 + "%" + Nombre_Nodo_2 + "%"+ ...



Red de sensores

Comunicación Nodo - Red

Trama lectura sensores

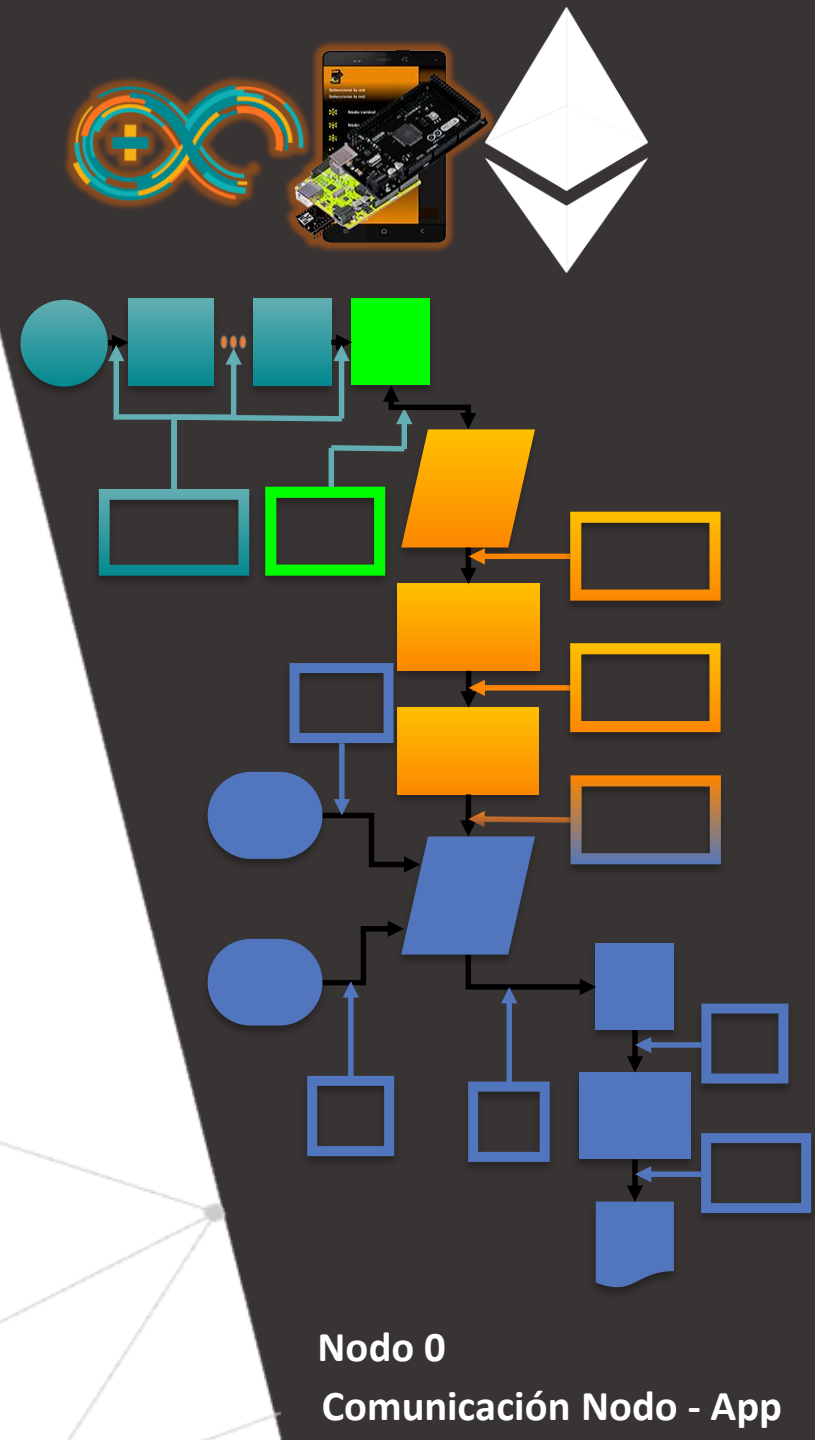
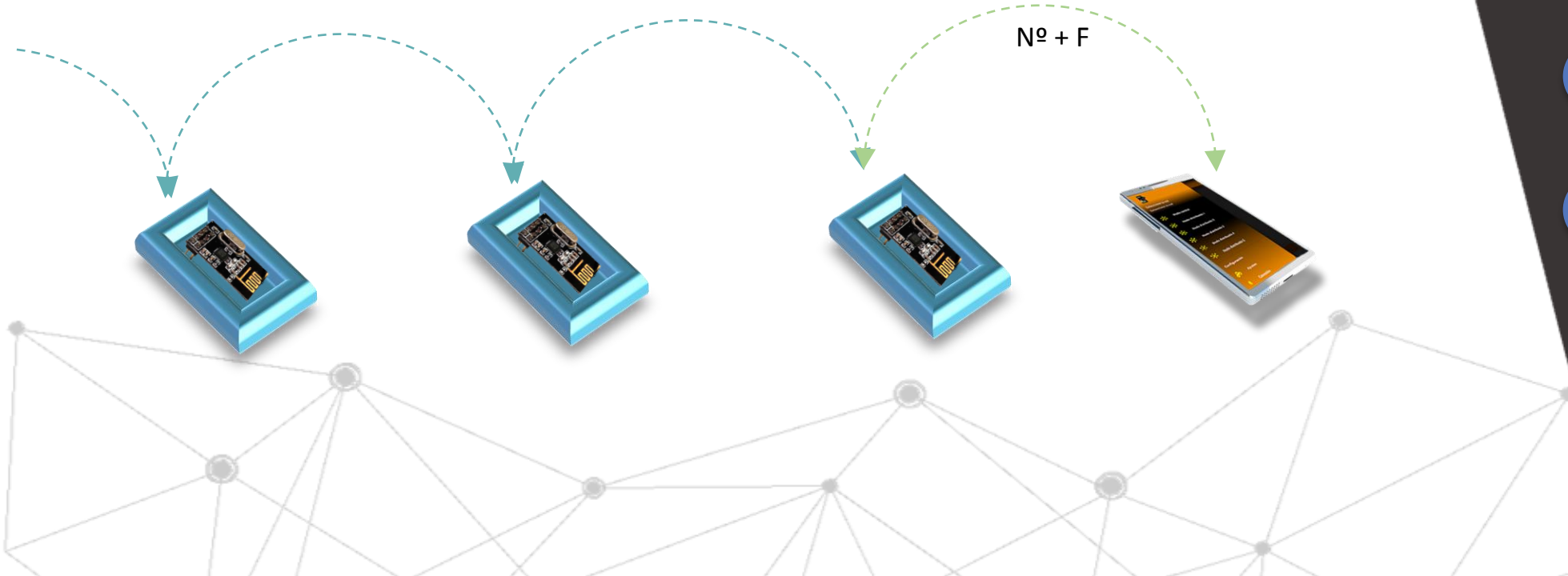
ID_Sensor1 + "|" + Valor_Sensor1 + "/" + Unidades_Sensor1 + "!"

ID_Sensor2 + "|" + Valor_Sensor2 + "/" + Unidades_Sensor2 + "!"

"#"

Trama lectura

Nº + F



Red de sensores

Comunicación Nodo - Red

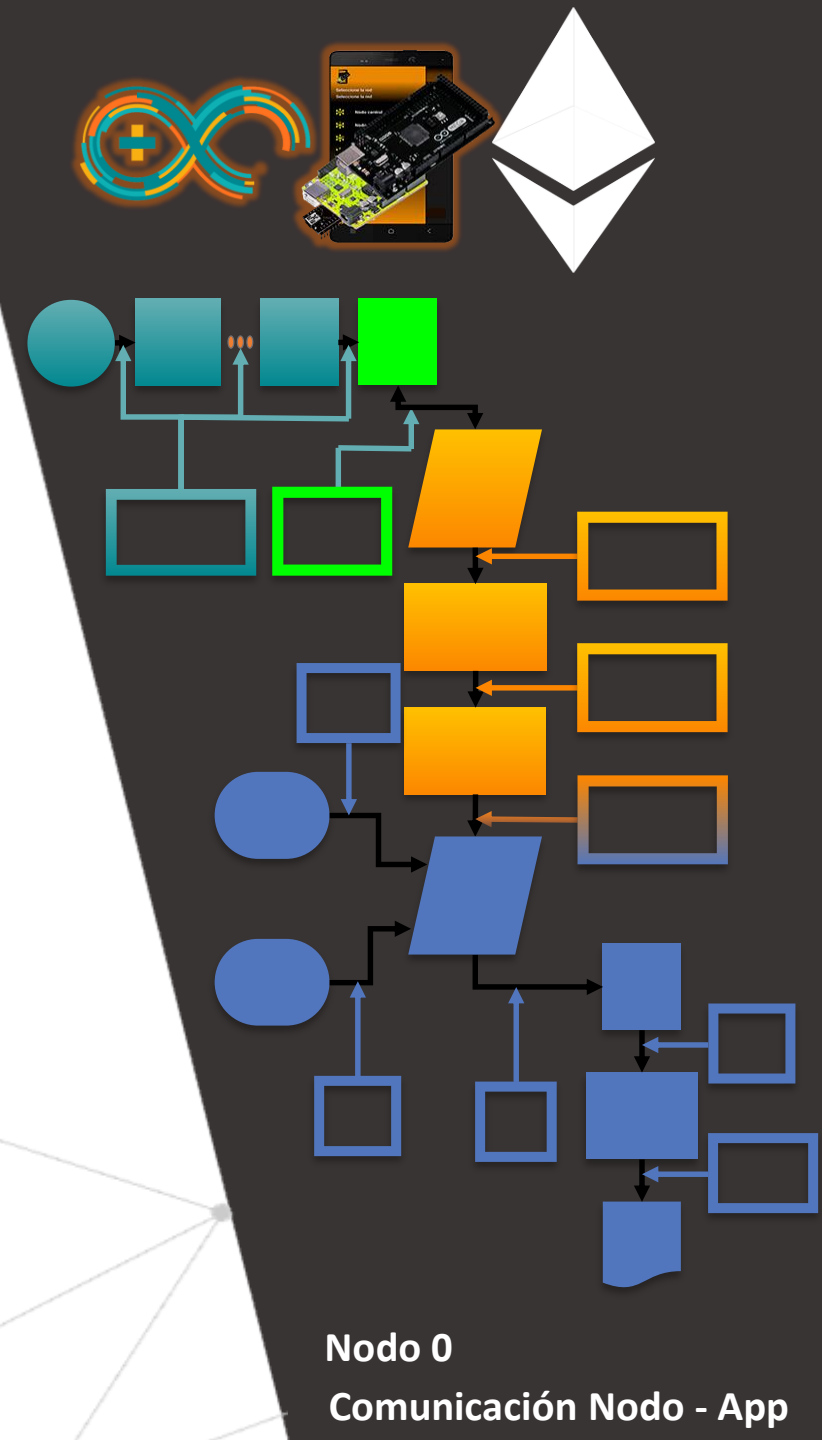
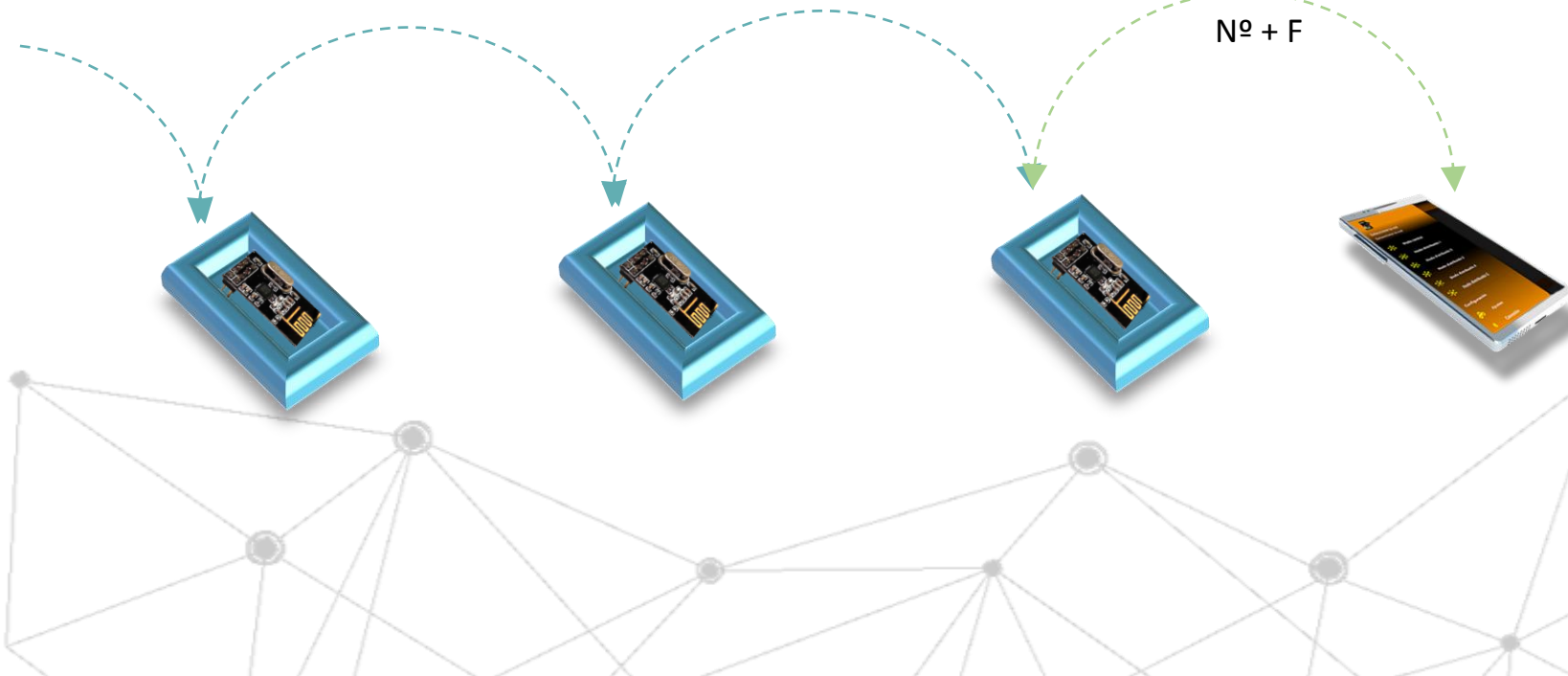
Trama lectura sensores

ID_Sensor1 + "|" + Valor_Sensor1 + "/" +
Unidades_Sensor1 + "!"

Valor recibido	Unidades
0	C
1	m
2	cm
3	bar
4	mL
5	Lm (lumen)
...	...


Trama lectura

Nº + F



App (SesNe)

Conexión - Configuración

 SesNe

Dispositivos conocidos

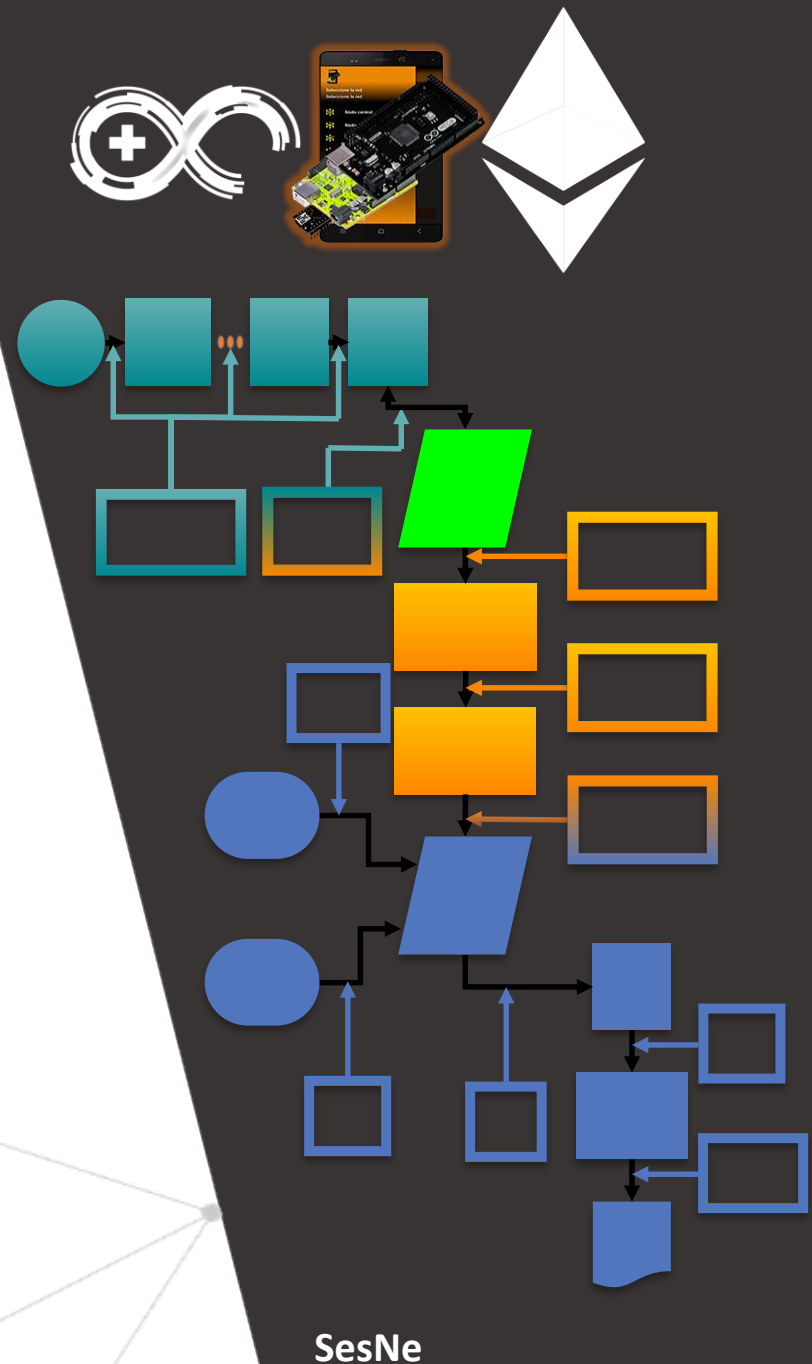
2131558417

Dispositivos nuevos

DTVBluetooth

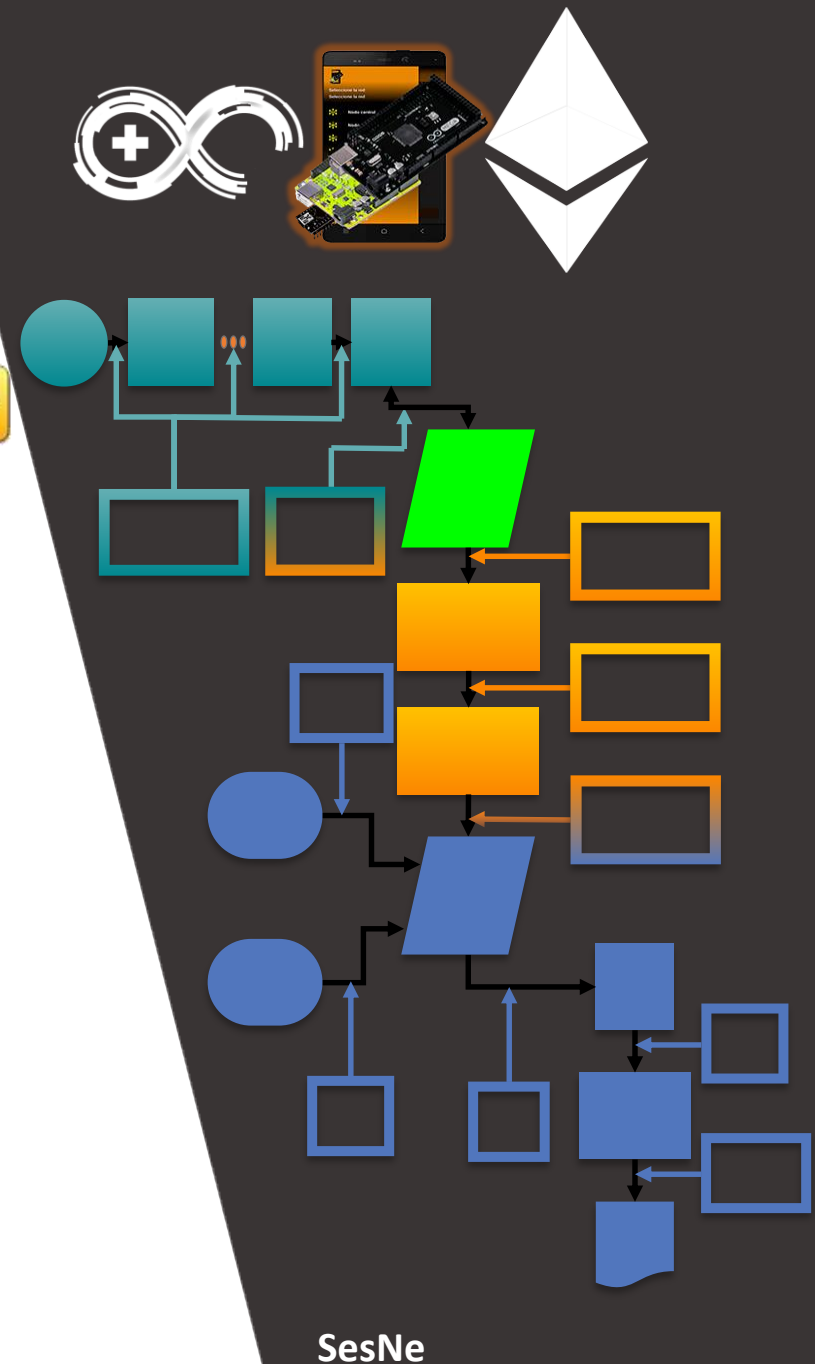
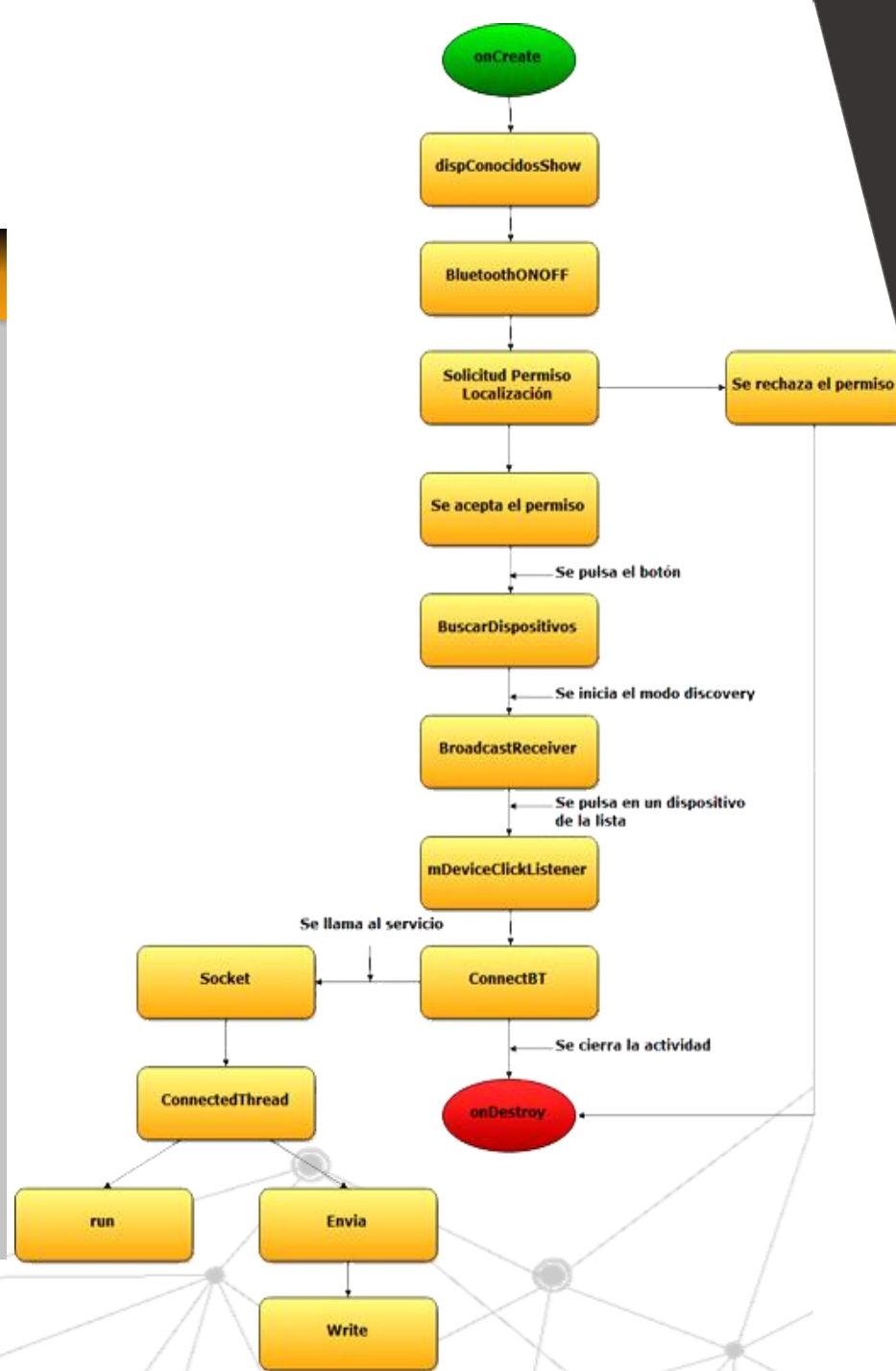
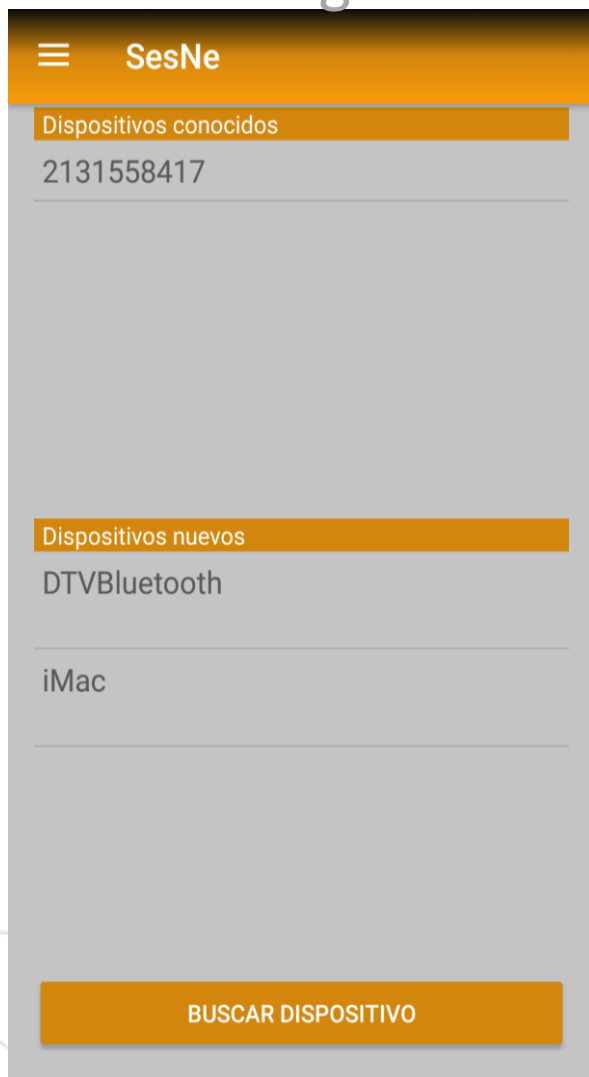
iMac

BUSCAR DISPOSITIVO



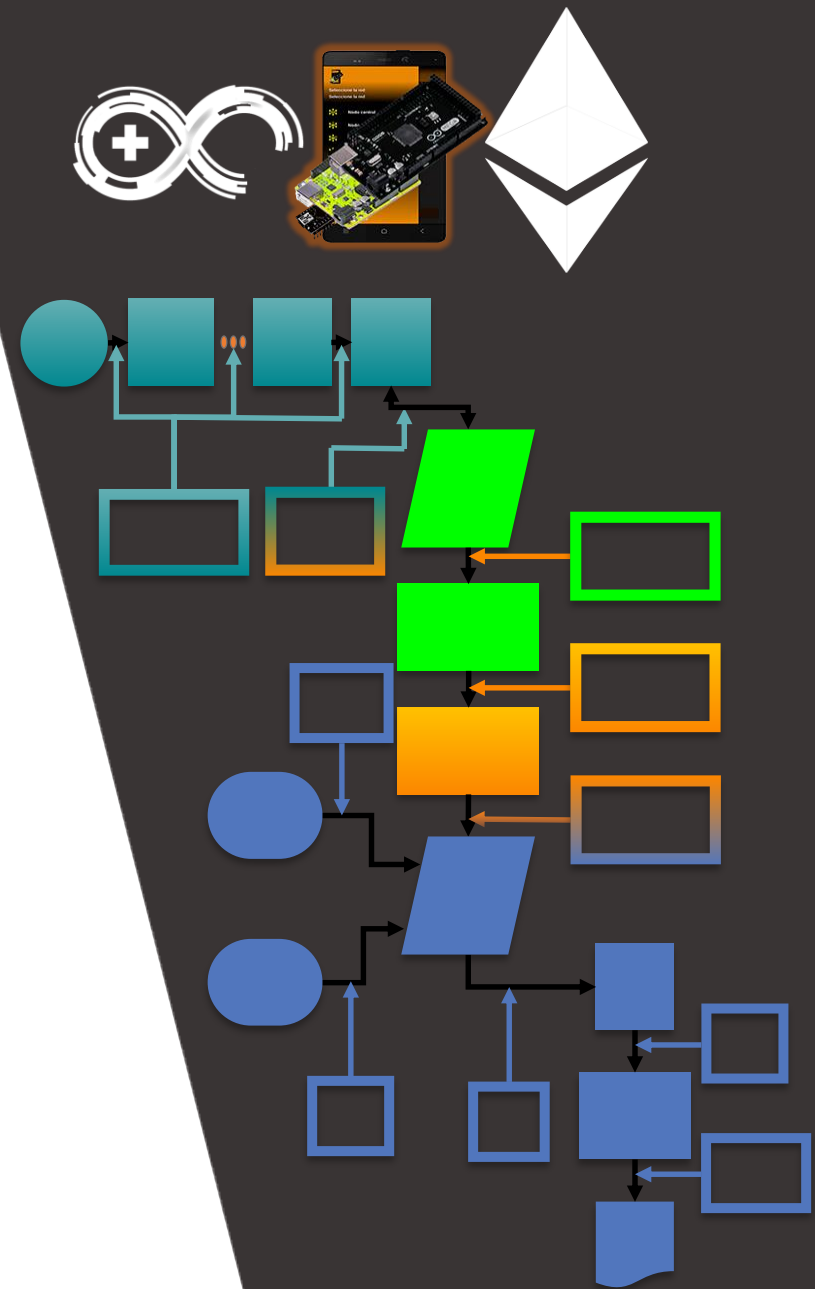
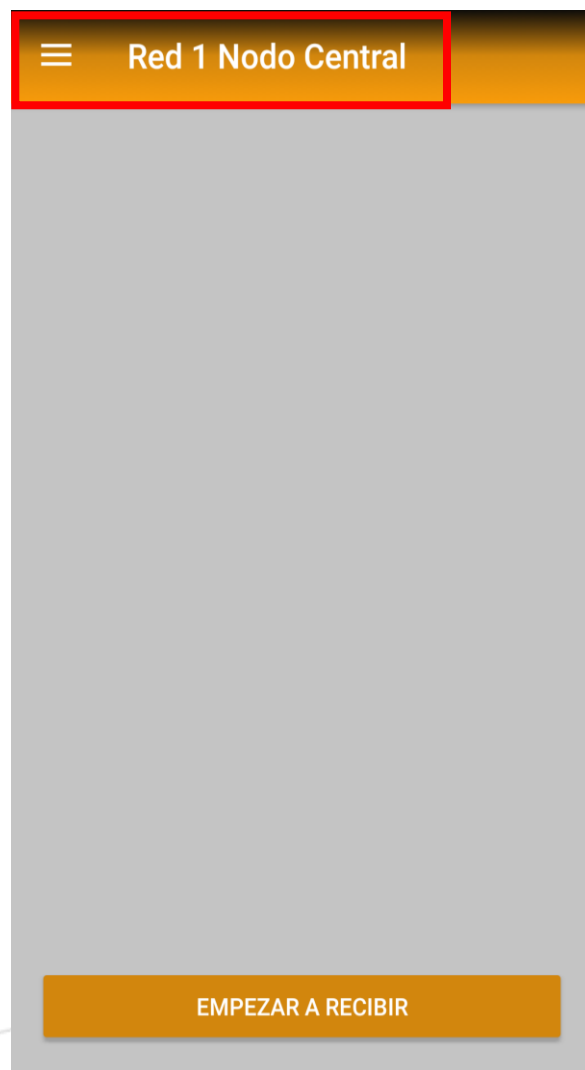
App (SesNe)

Conexión - Configuración



App (SesNe)

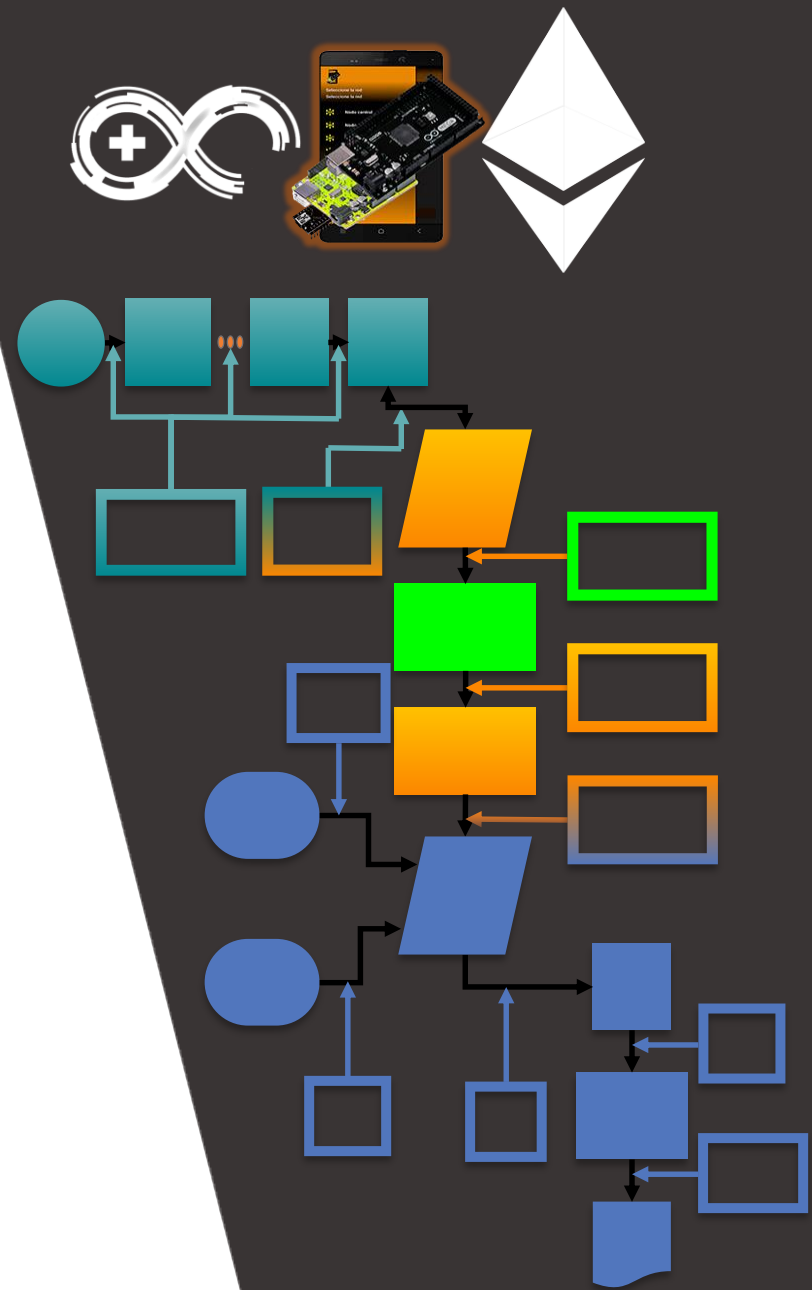
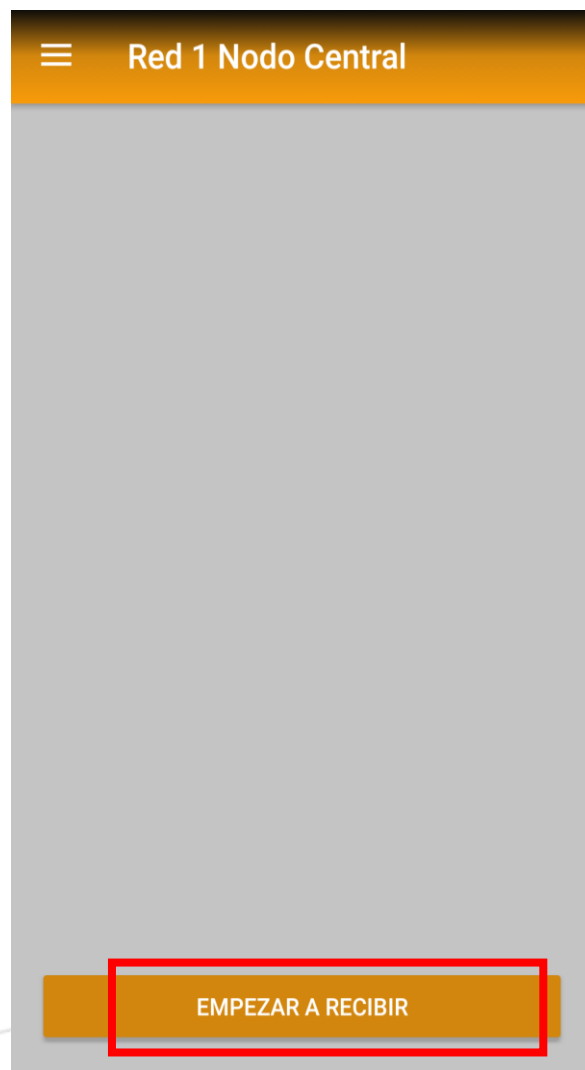
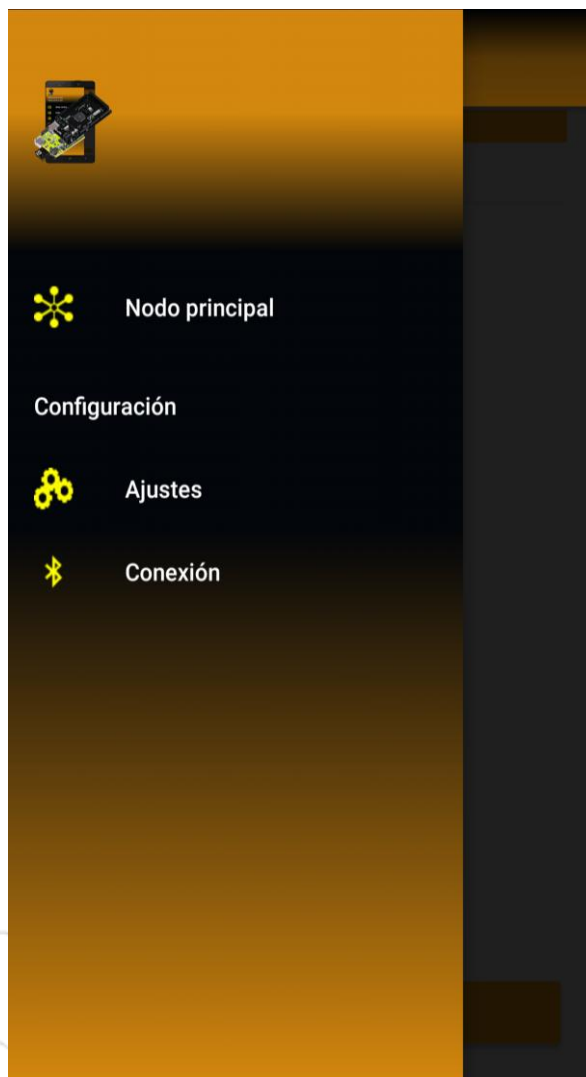
Buenas prácticas



Adaptación datos
Visualización

App (SesNe)

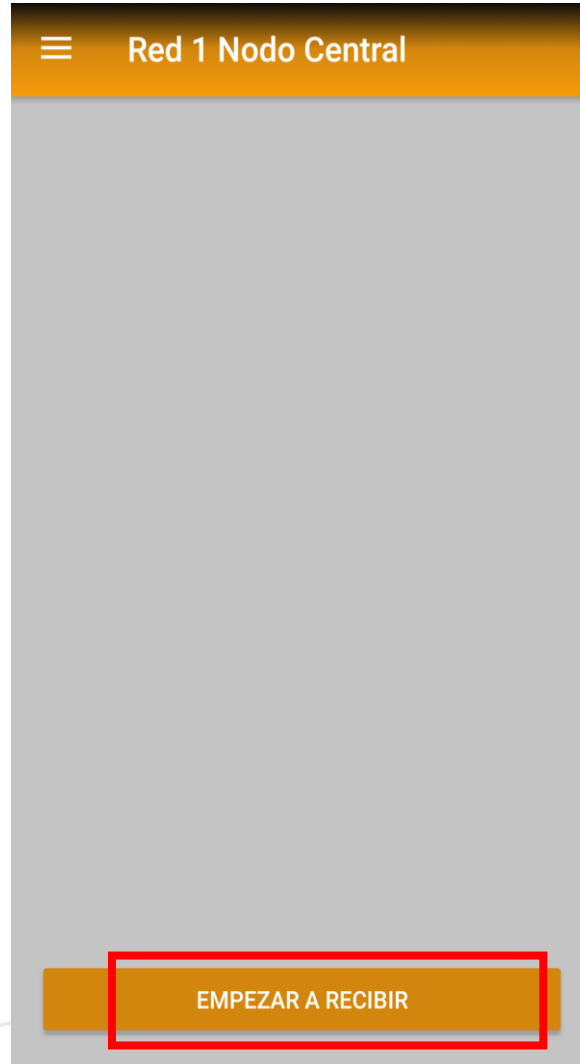
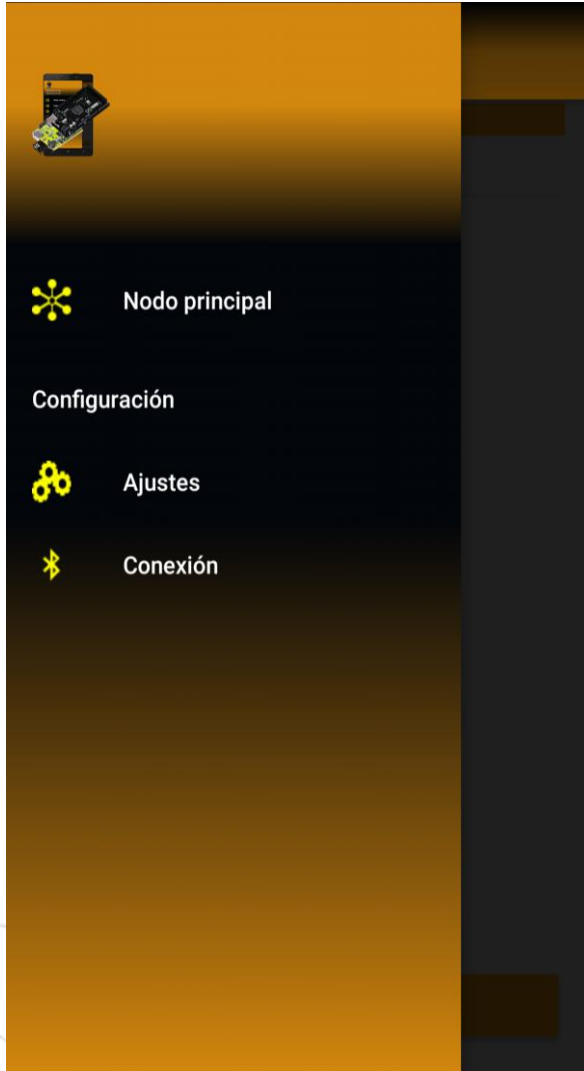
Visualización



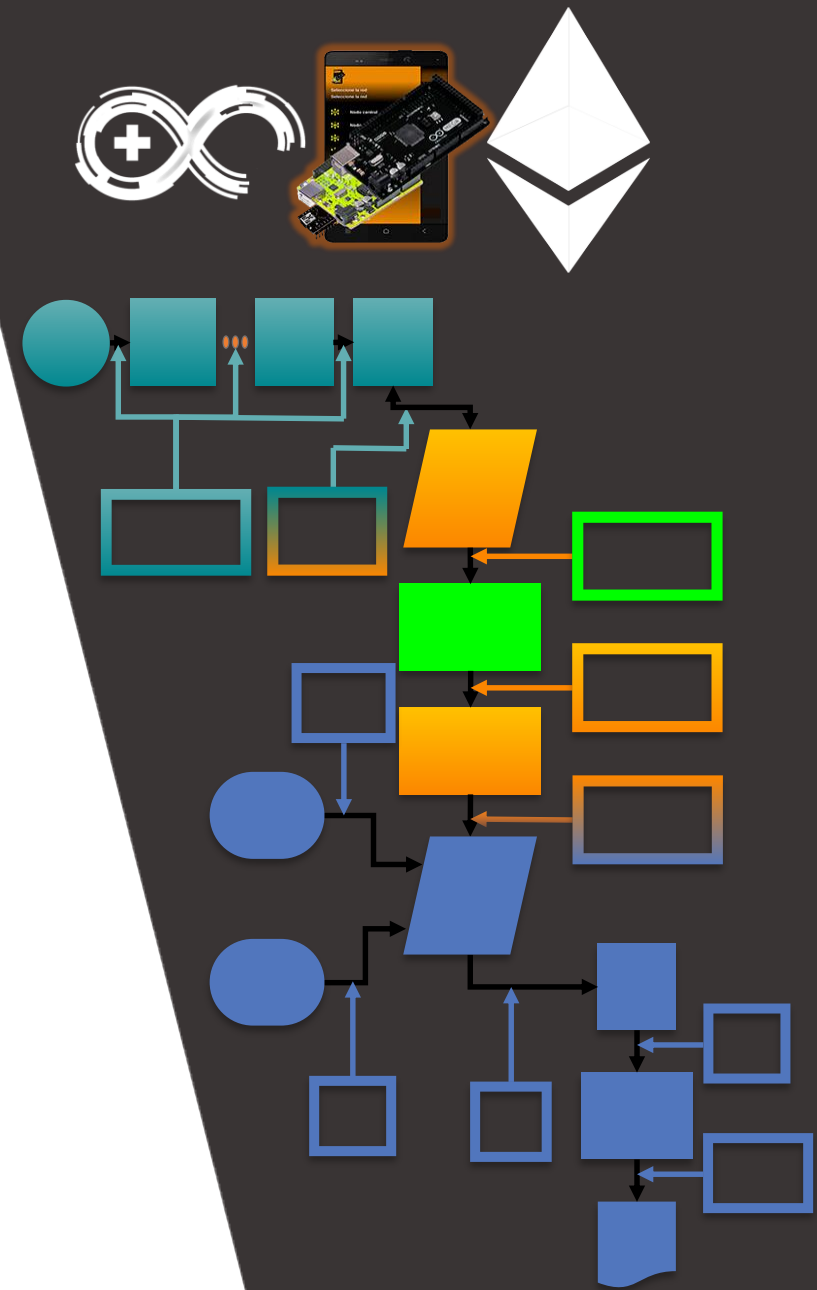
Adaptación datos
Visualización

App (SesNe)

Visualización



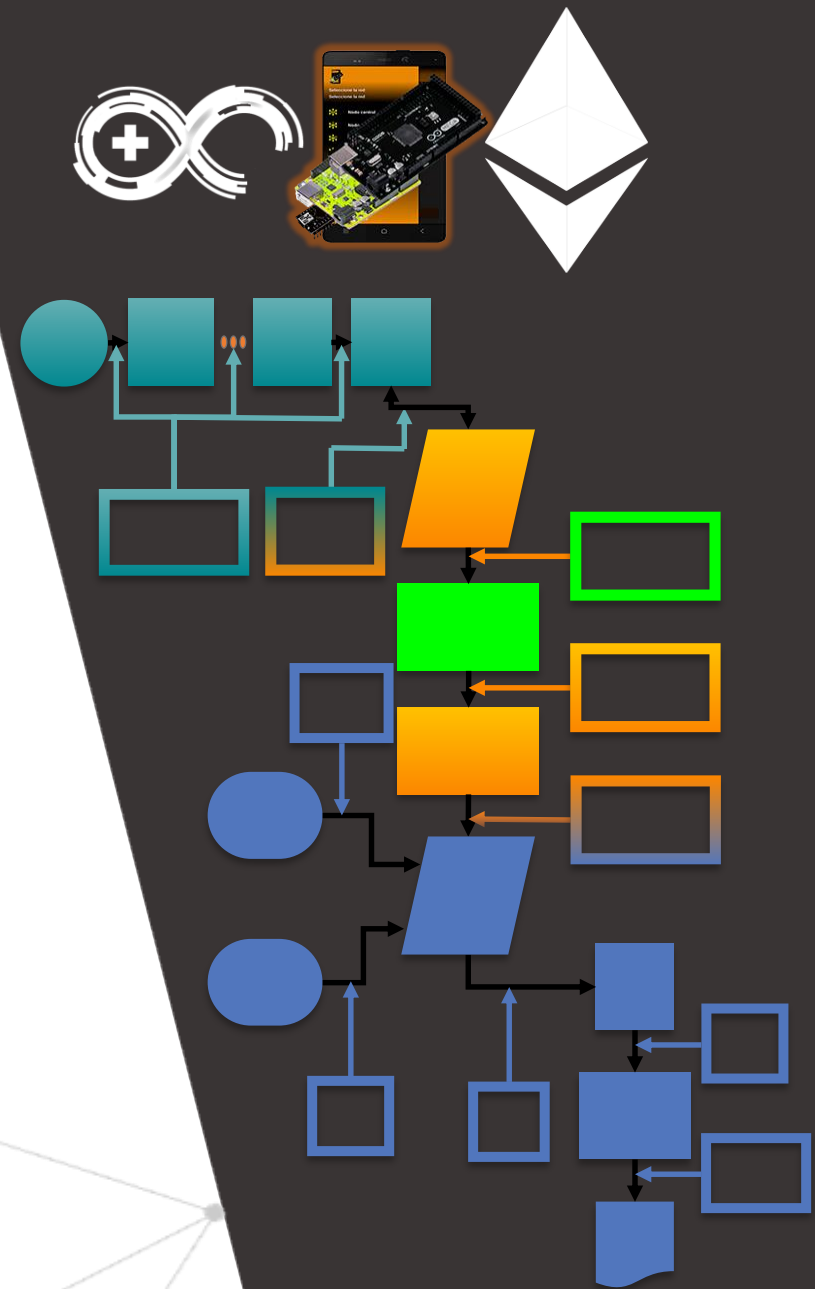
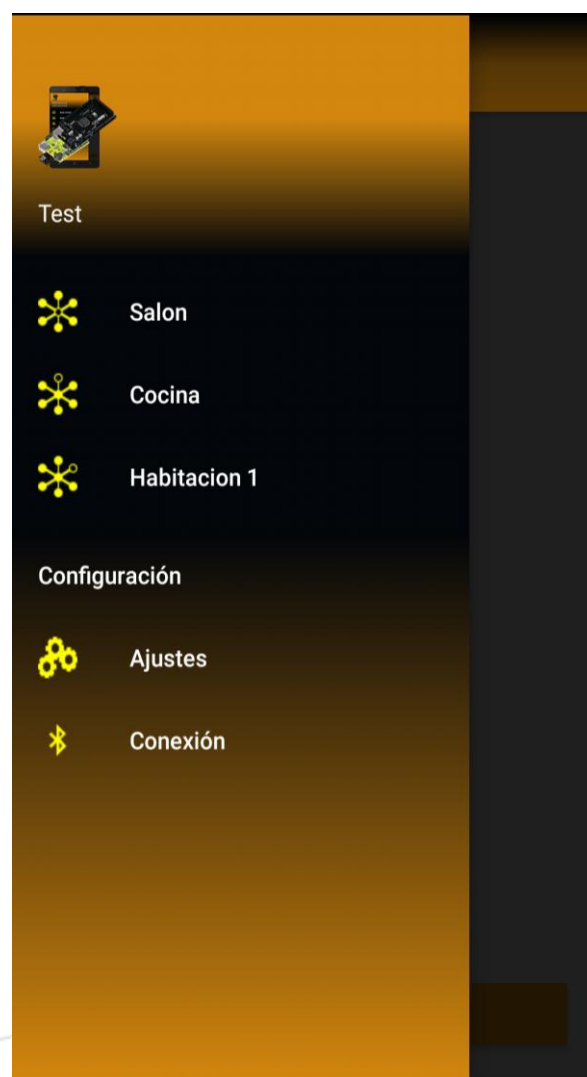
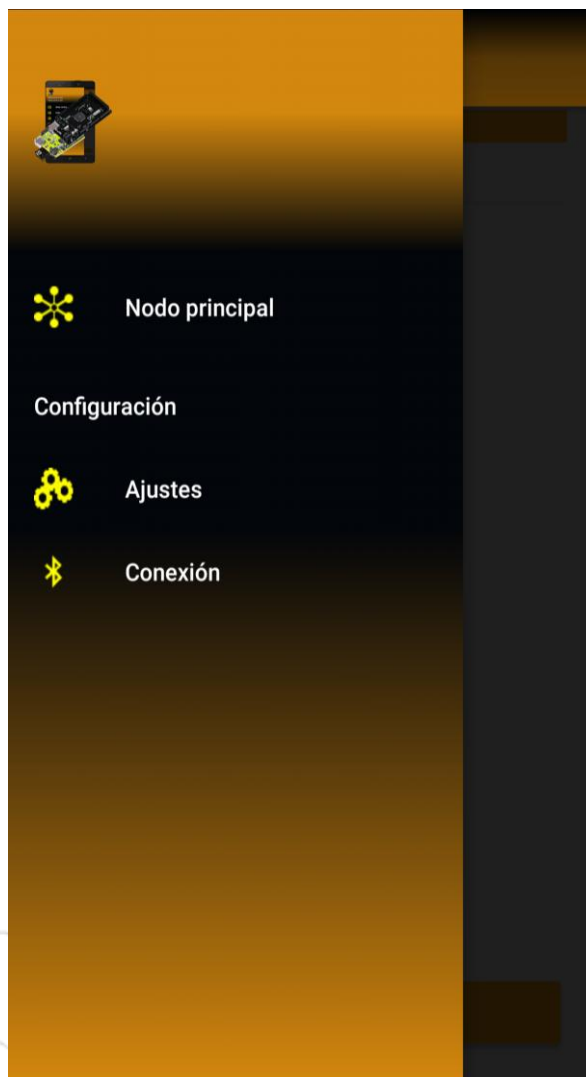
"%%" + "3" + "/" + "Test" + "%" + "Salon" + "%" + "Cocina" + "%" + "Habitación_1" + "%"



Adaptación datos
Visualización

App (SesNe)

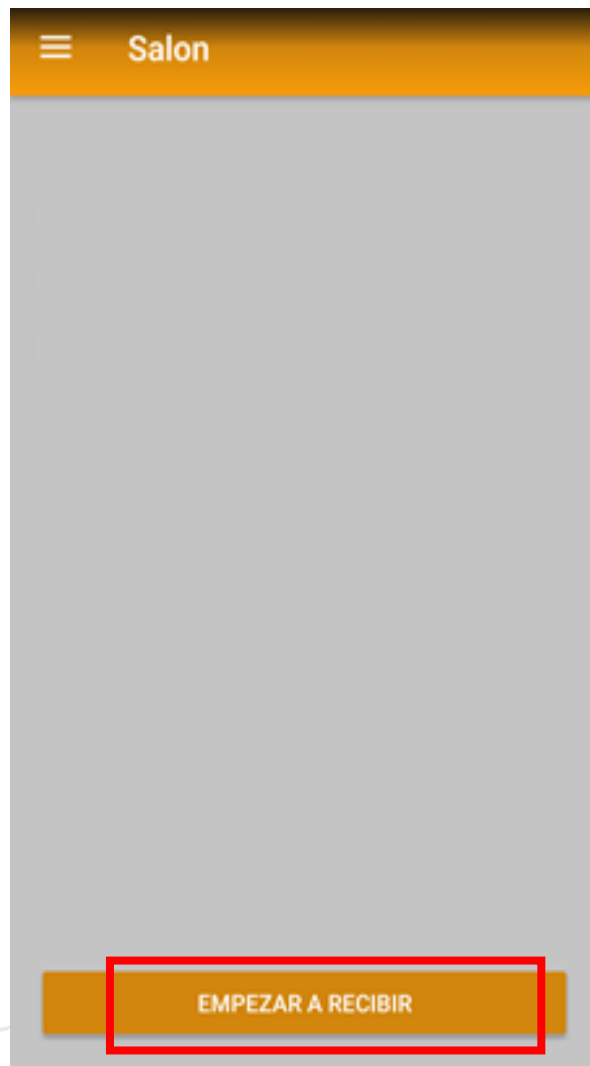
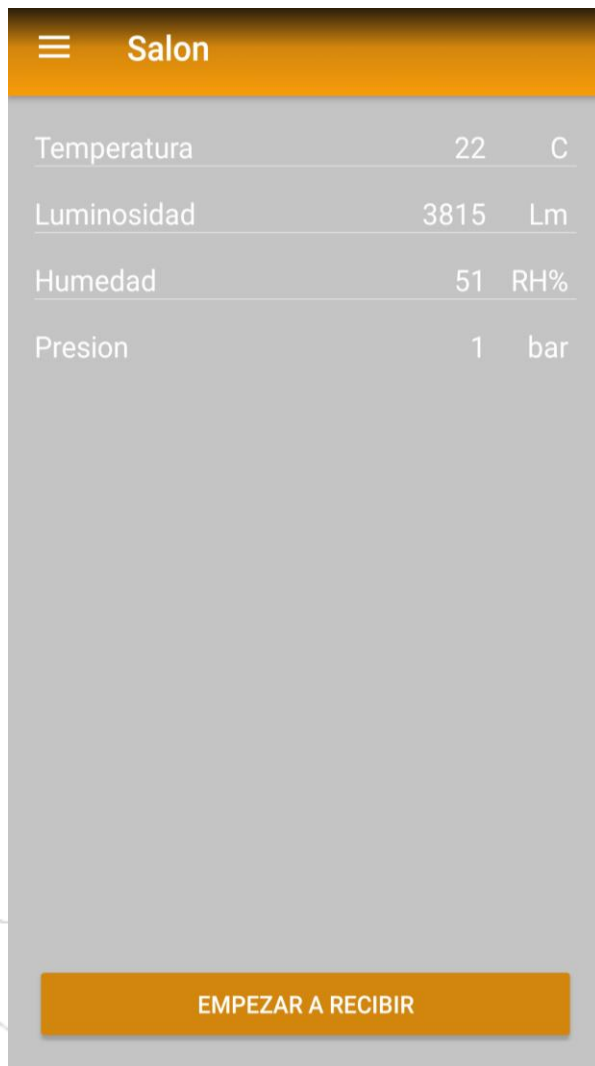
Visualización



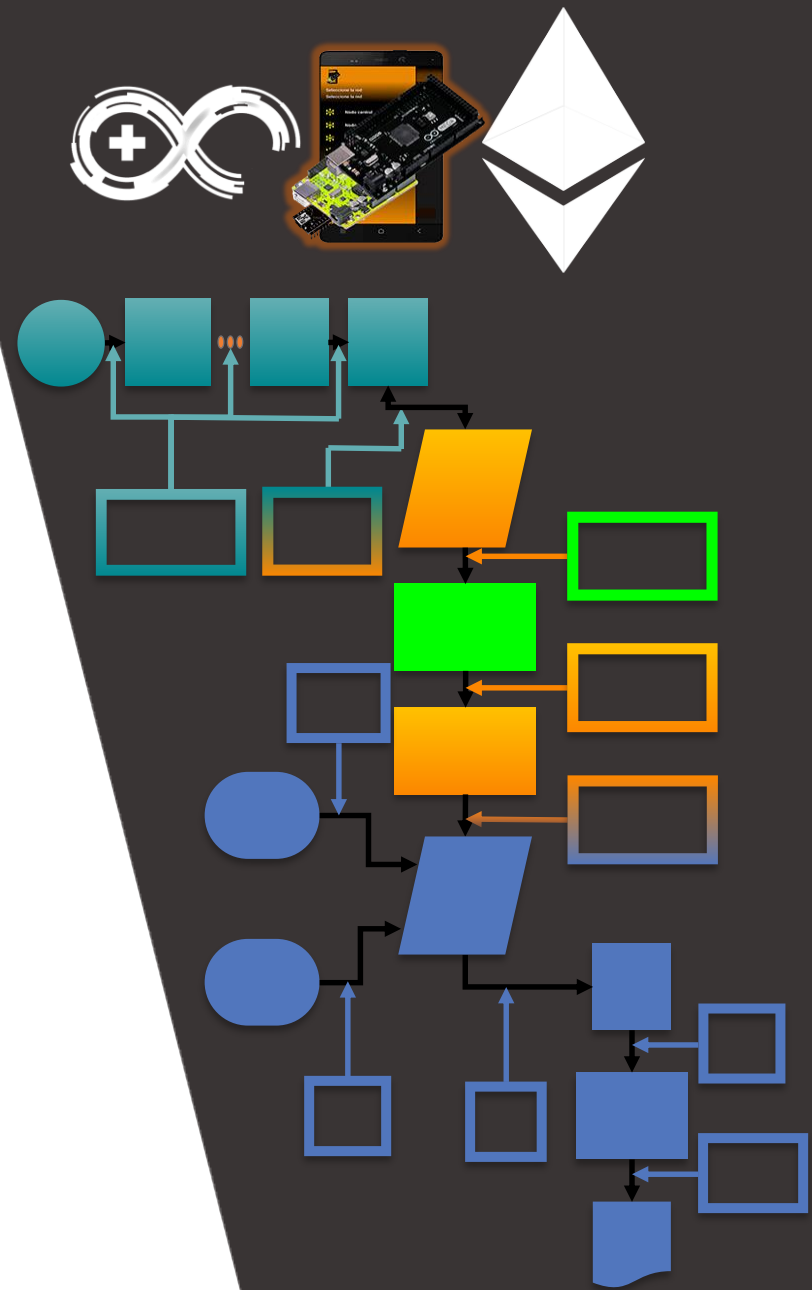
Adaptación datos
Visualización

App (SesNe)

Visualización



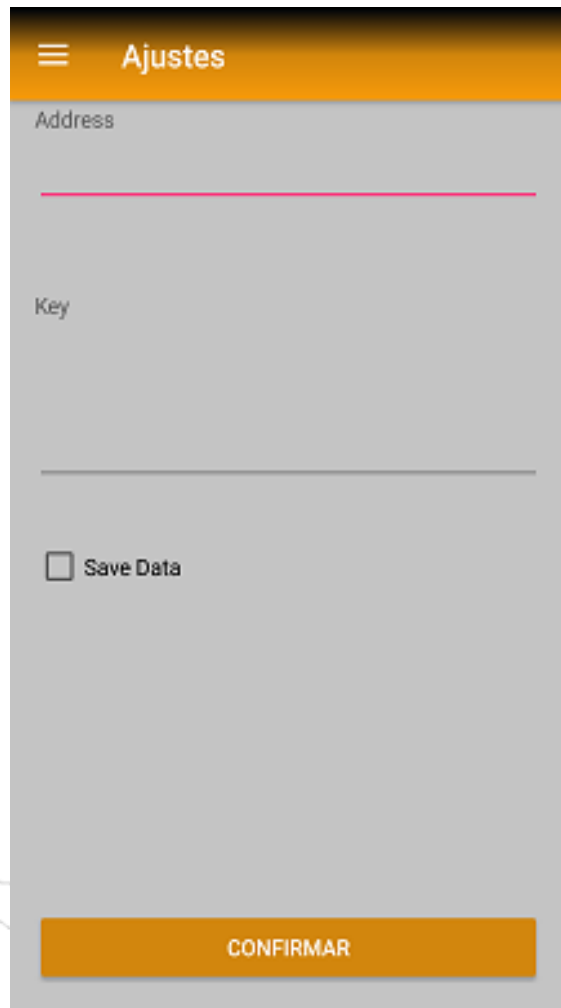
"0"+"Temperatura" + "|" + "22" + "/" + "0" + "!"+"Luminosidad"+"|"+"3815"+...+"#"



Adaptación datos
Visualización

App (SesNe)

Almacenamiento en blockchain



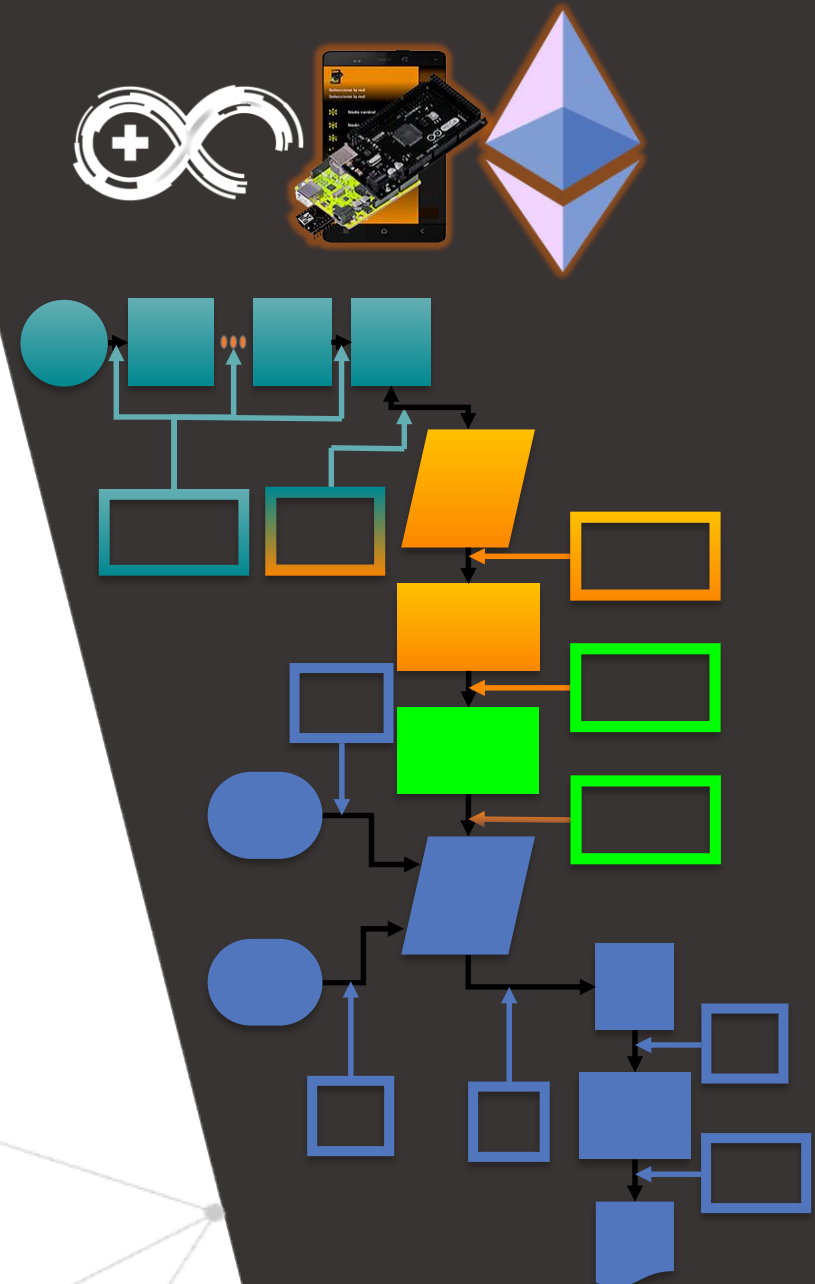
≡ Ajustes

Address

Key

☐ Save Data

CONFIRMAR



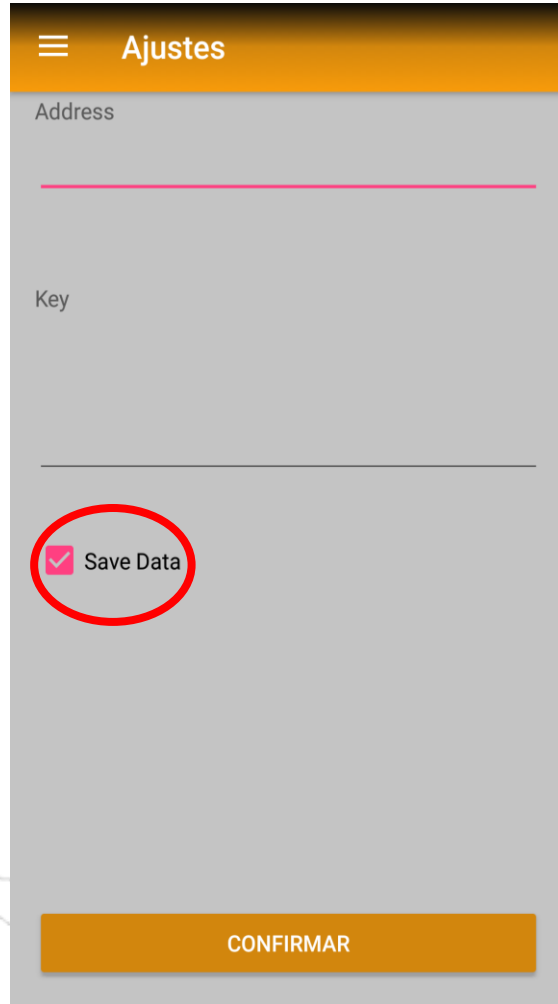
Comprobación Ajustes

Api blockchain

Encriptar y almacenar en contrato

App (SesNe)

Almacenamiento en blockchain



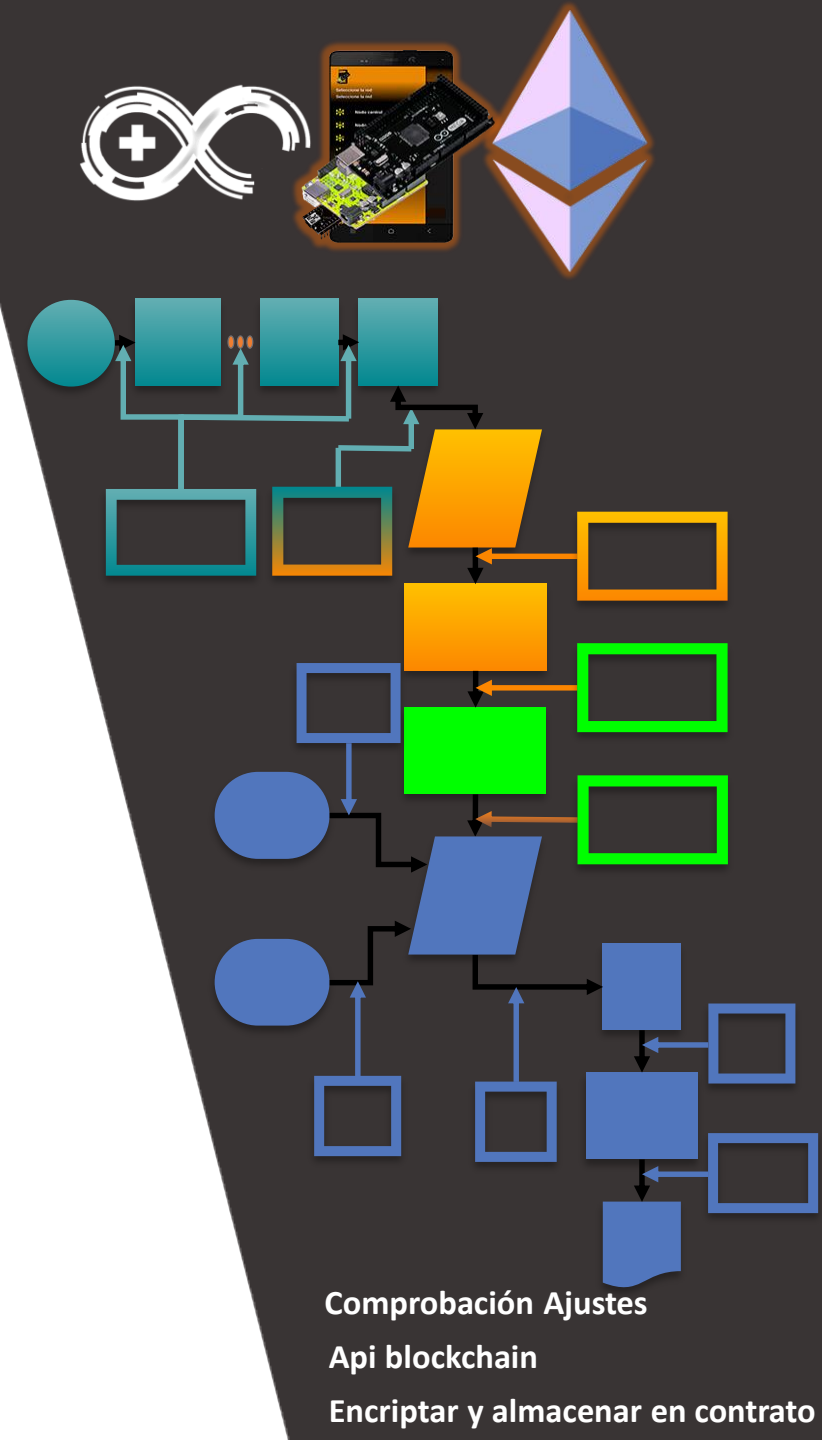
≡ Ajustes

Address

Key

☒ Save Data

CONFIRMAR



App (SesNe)

Almacenamiento en blockchain

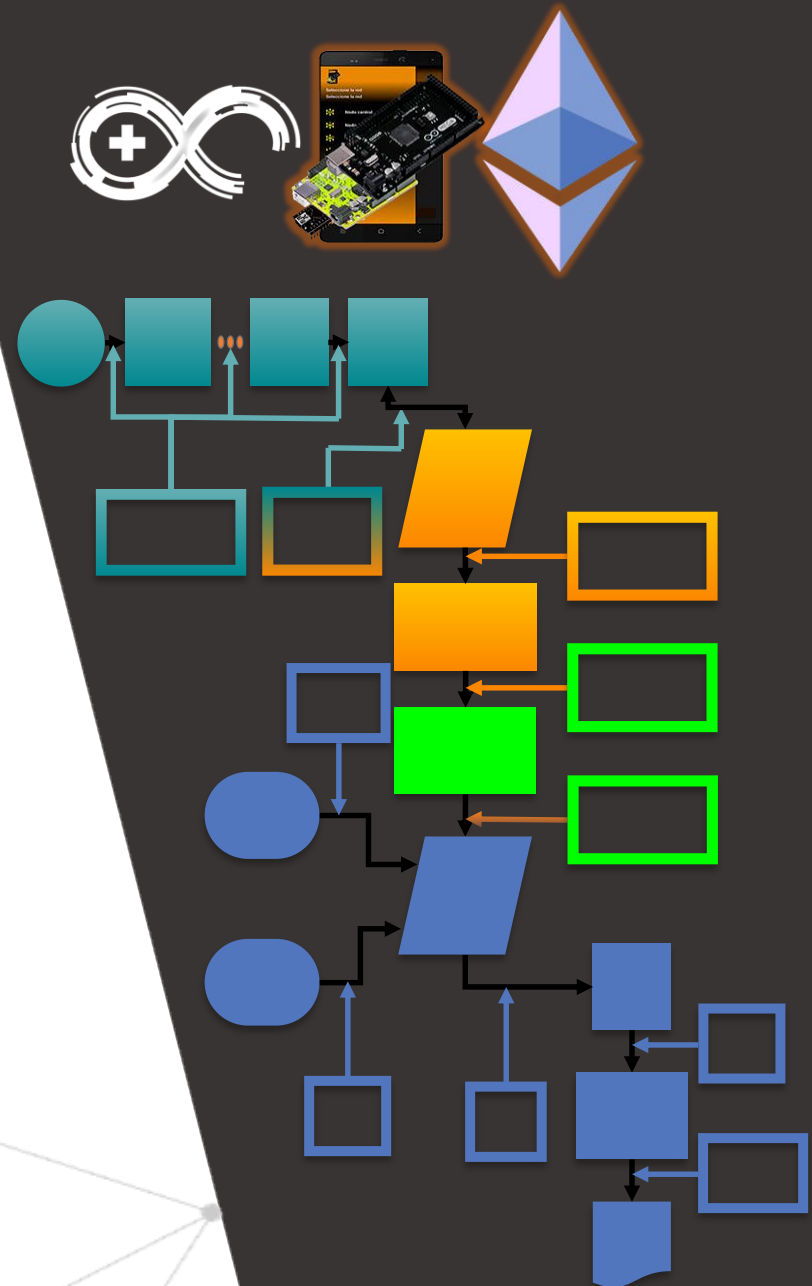
Ajustes

Address

Key

☒ Save Data

CONFIRMAR



Comprobación Ajustes

Api blockchain

Encriptar y almacenar en contrato

Almacenamiento en blockchain

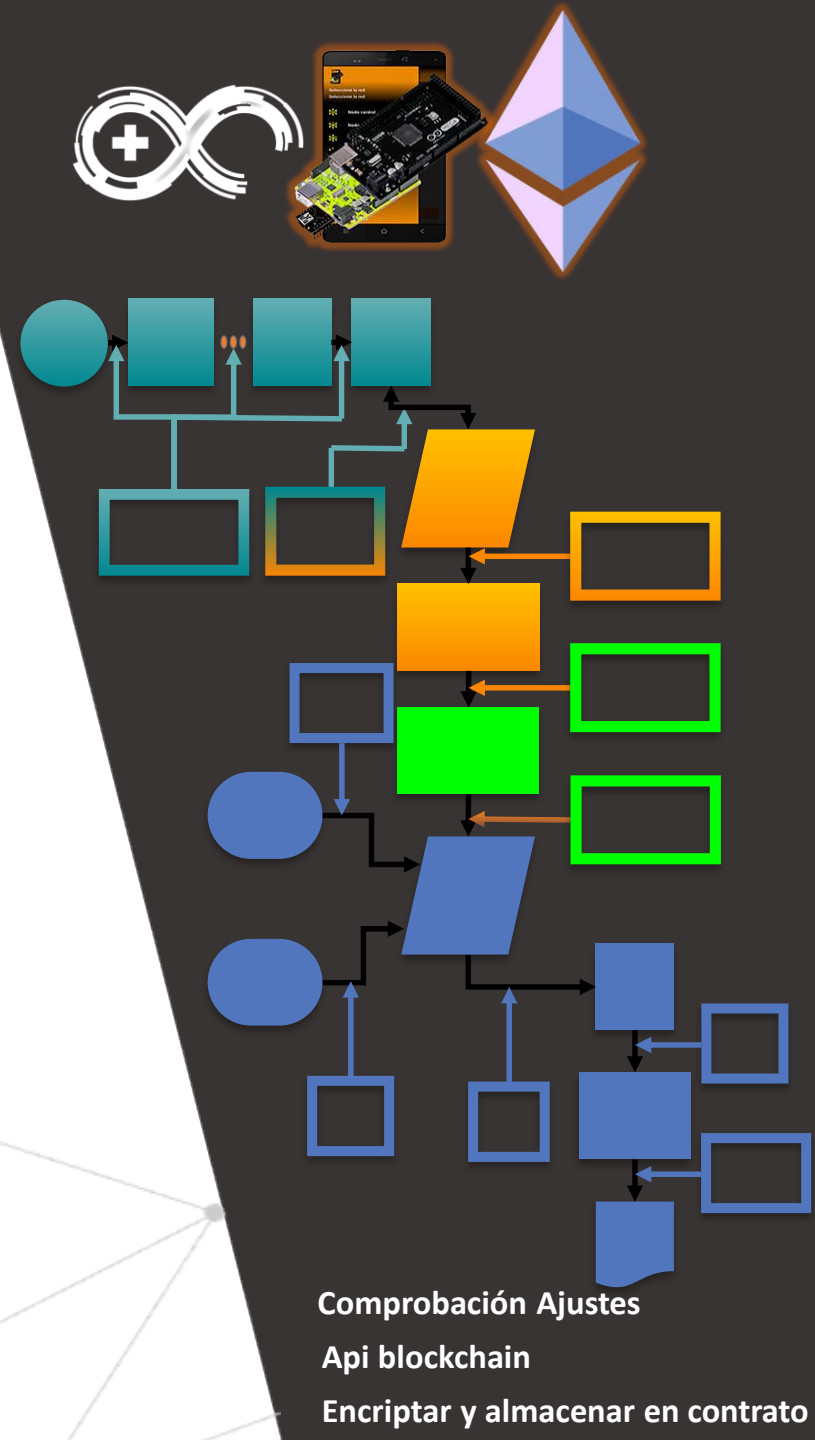
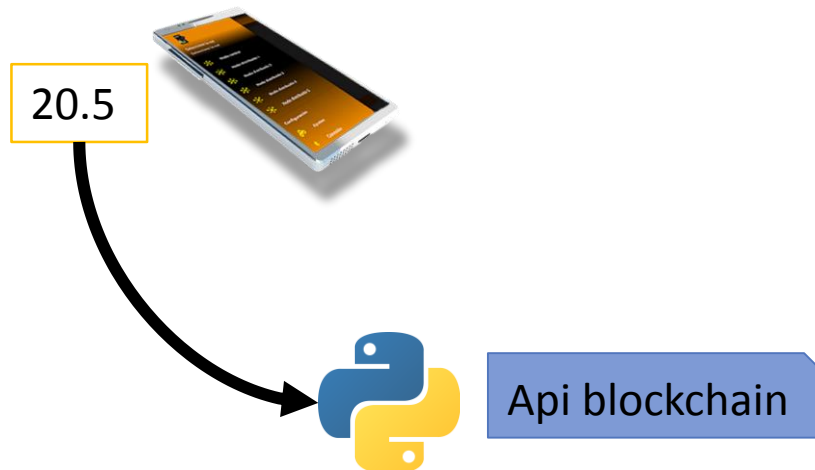
A network diagram with a central button. The background is a light gray network of nodes and edges. In the center, there is a gray rectangular box. Inside this box is a smaller orange rectangular button with the word "CONFIRMAR" in white capital letters. The orange button is highlighted with a thick red border.

Api blockchain

Encriptar y almacenar en contrato

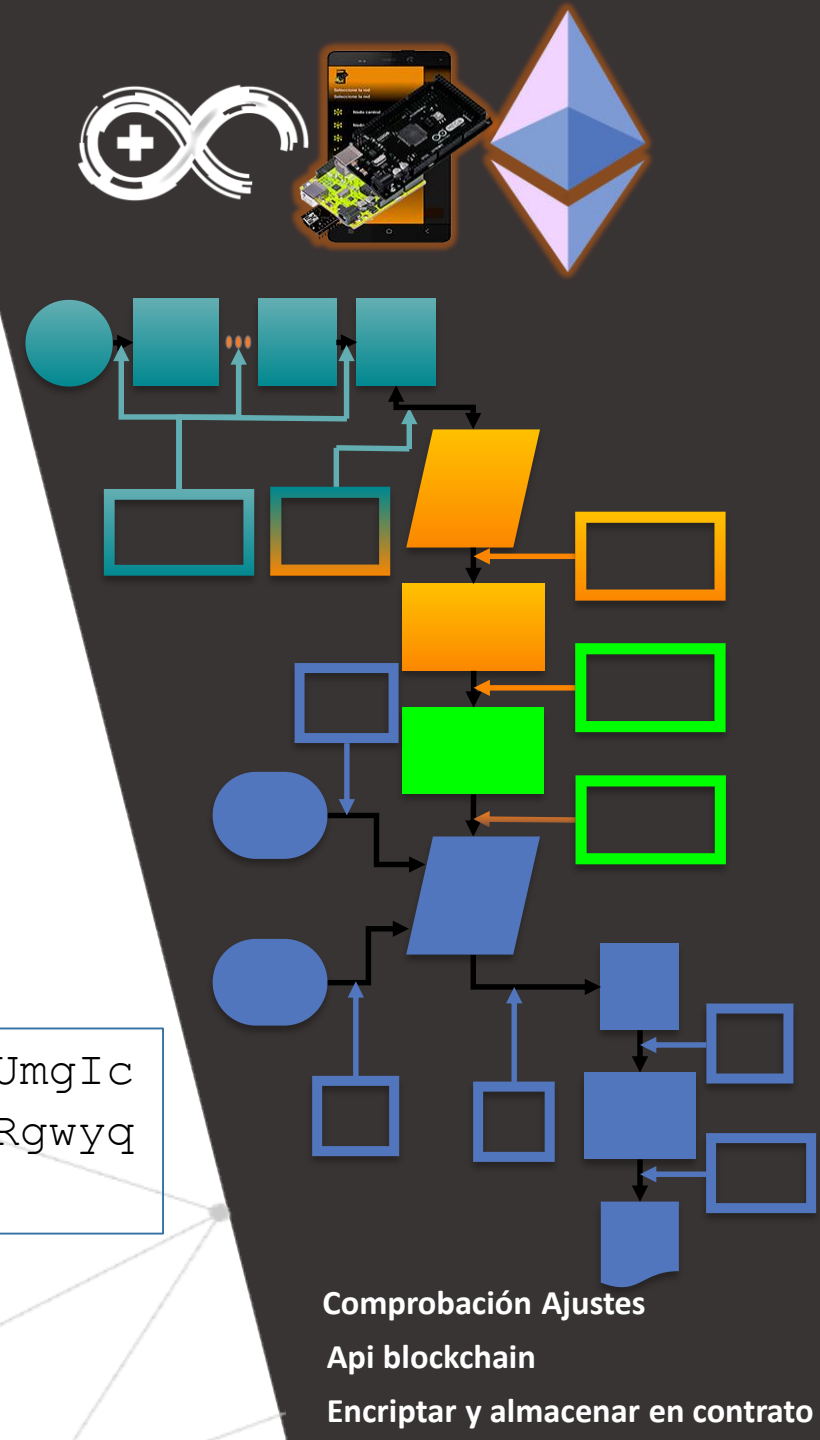
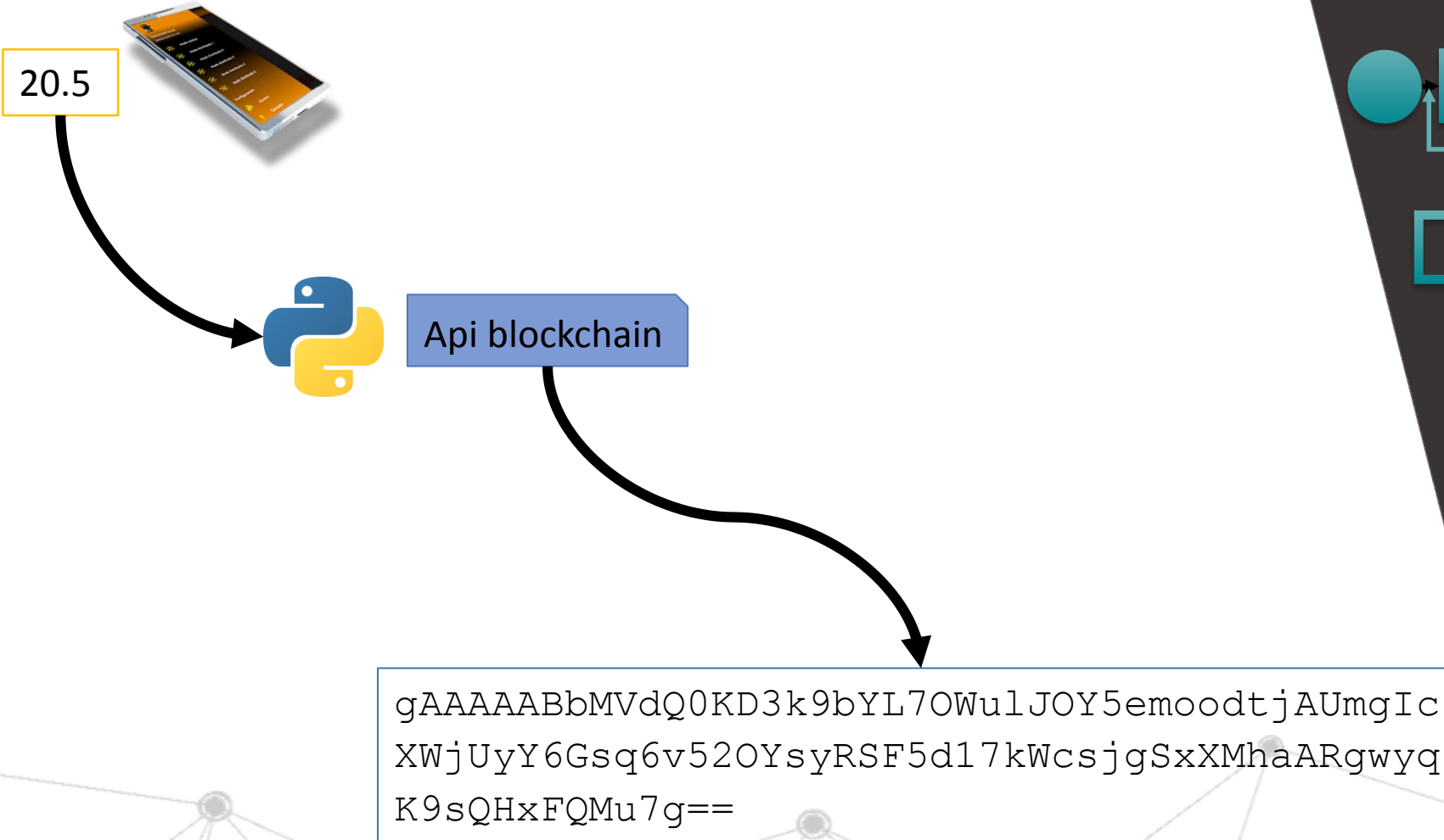
App (SesNe)

Almacenamiento en blockchain



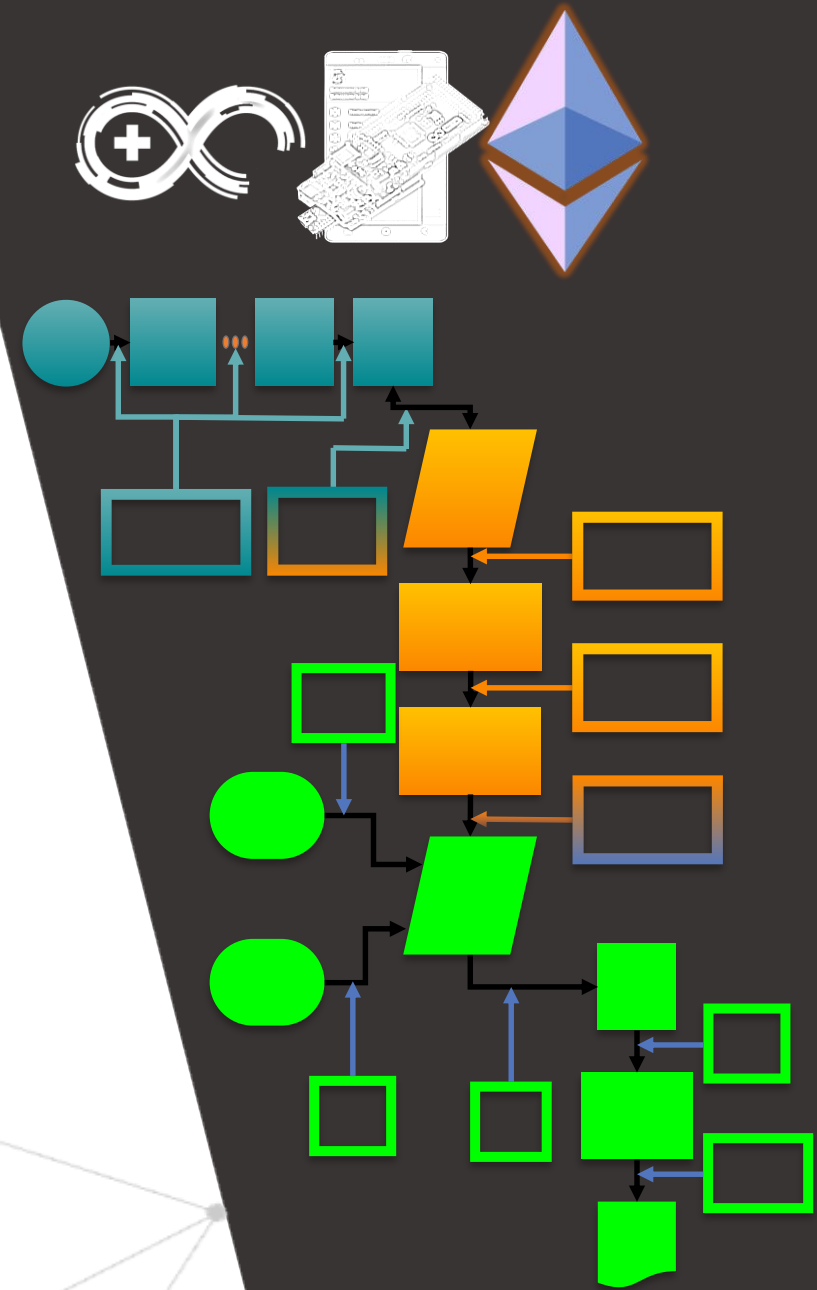
App (SesNe)

Almacenamiento en blockchain



Blockchain

Tecnología



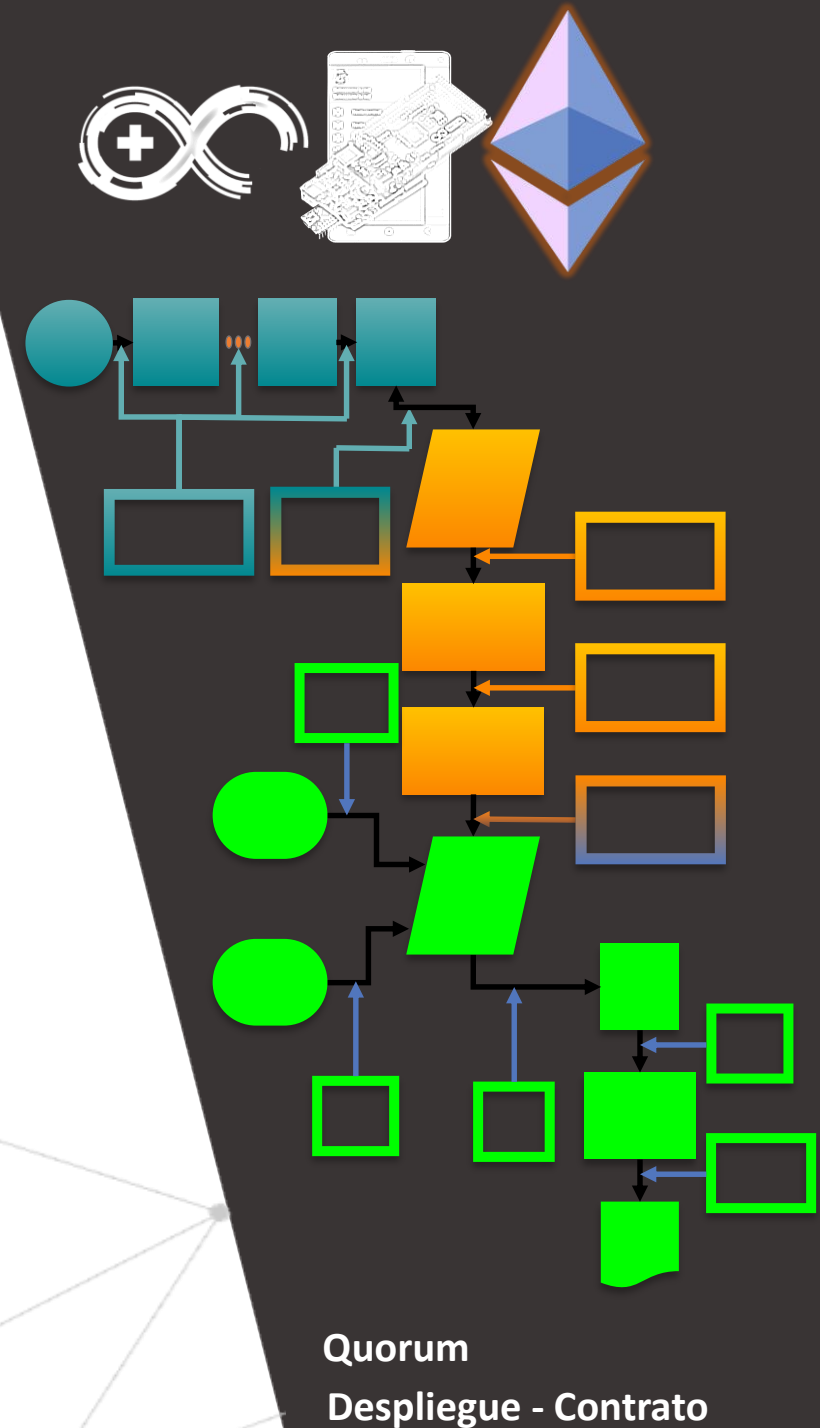
Quorum

Despliegue - Contrato

Blockchain

Tecnología

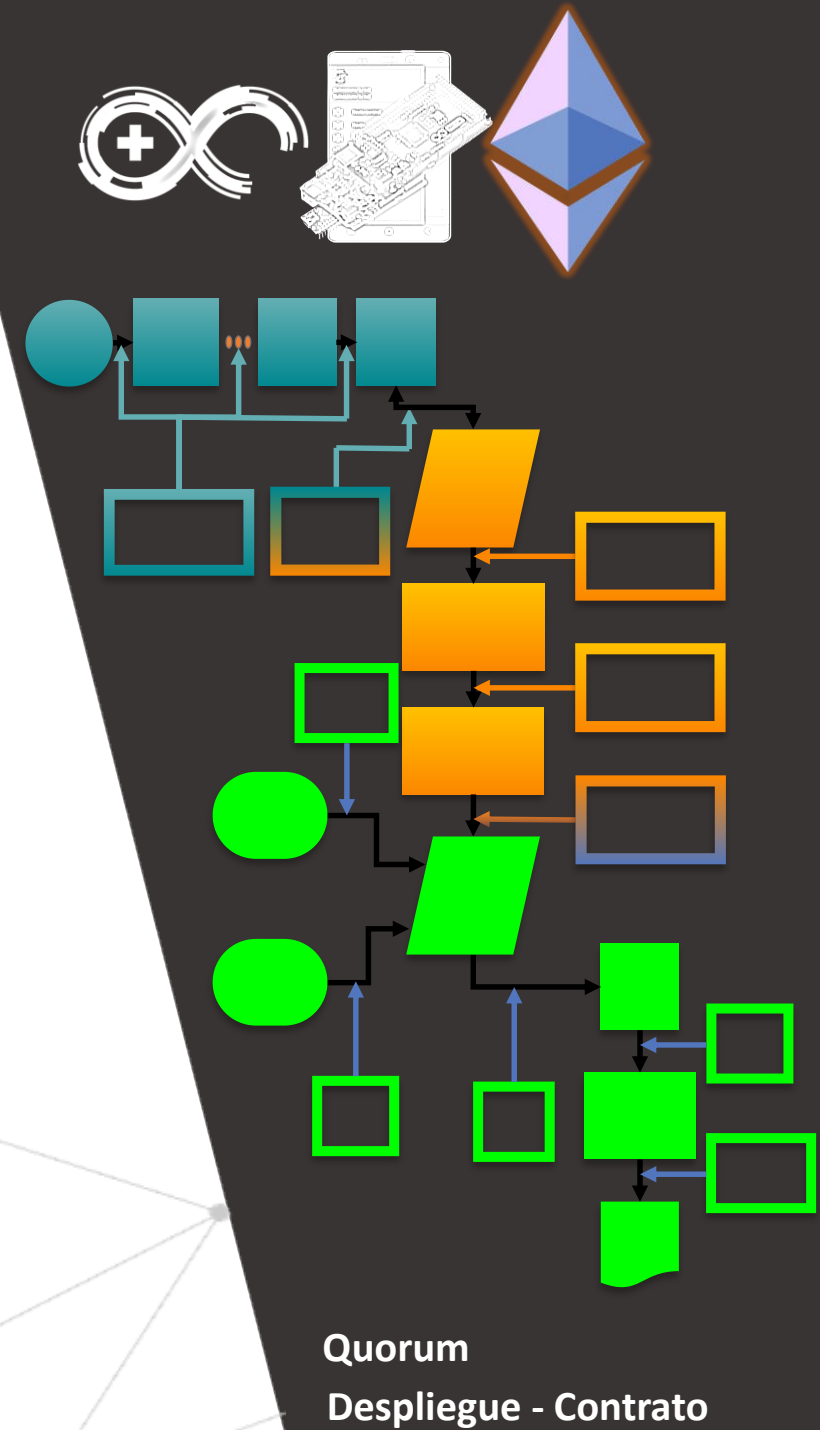
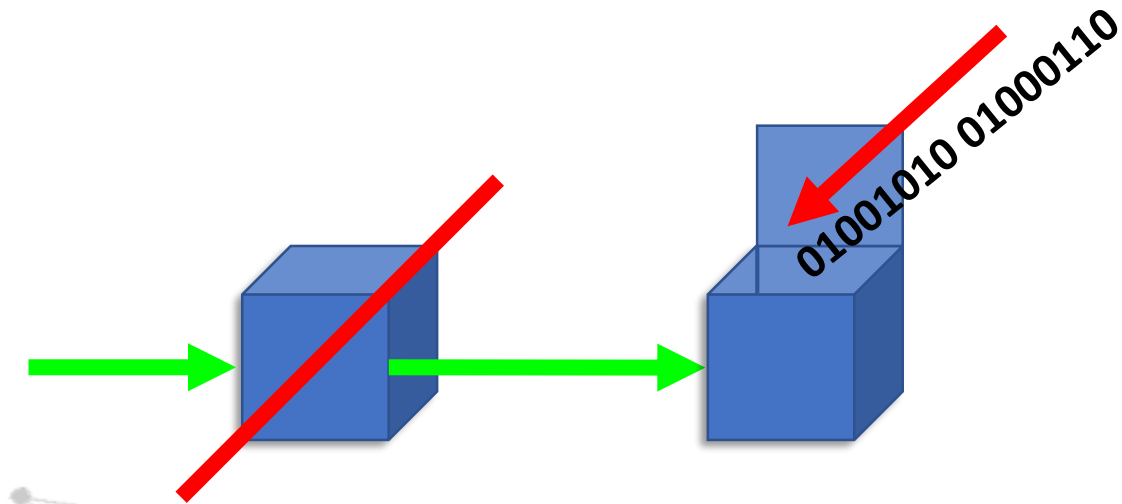
¿Qué es y por qué se ha usado en este proyecto?



Blockchain

Tecnología

Permite almacenar información inmutable

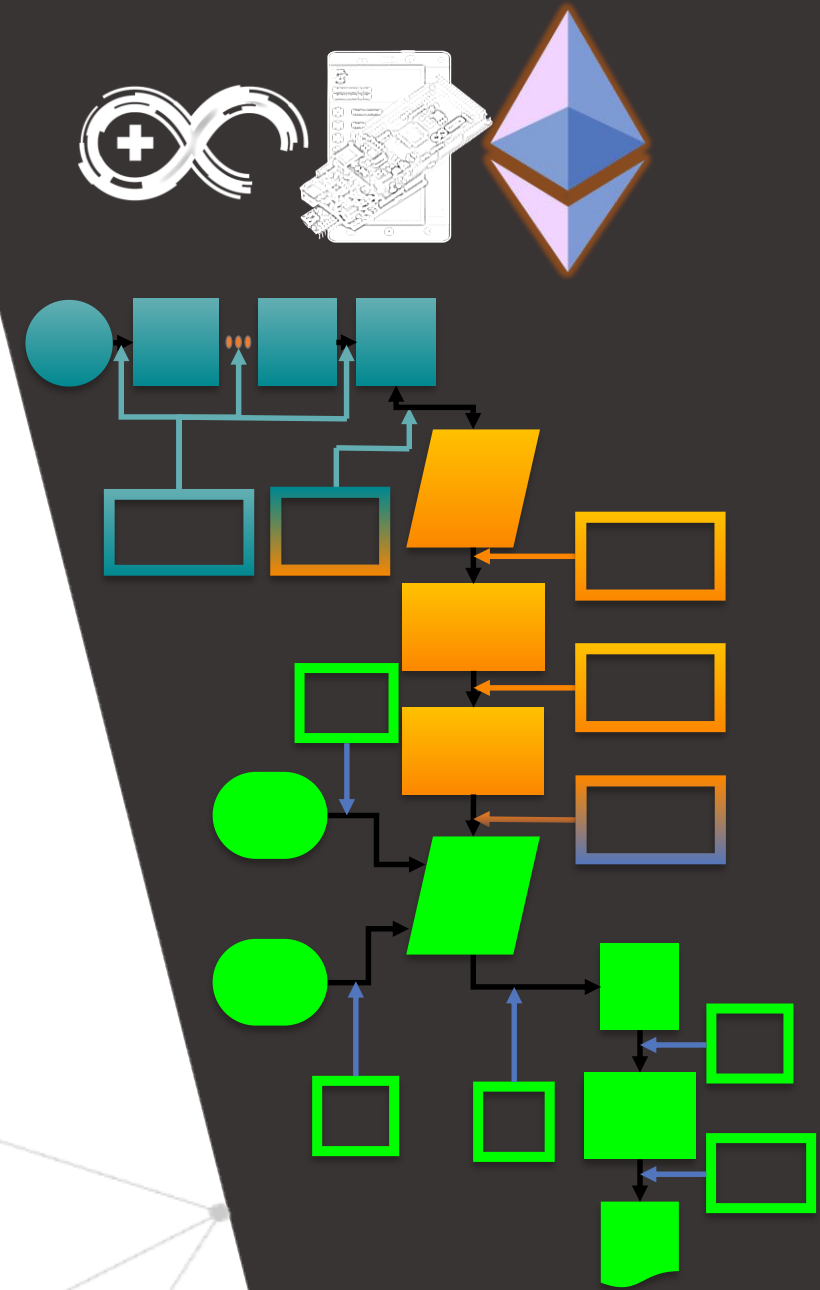
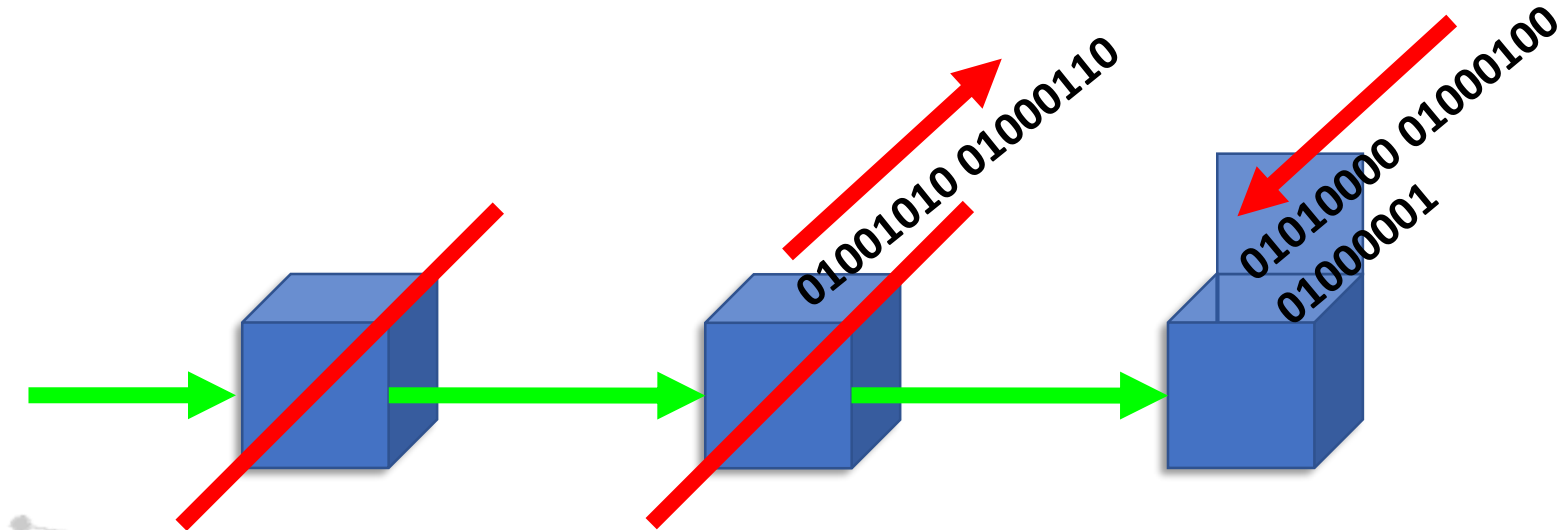


Blockchain

Tecnología

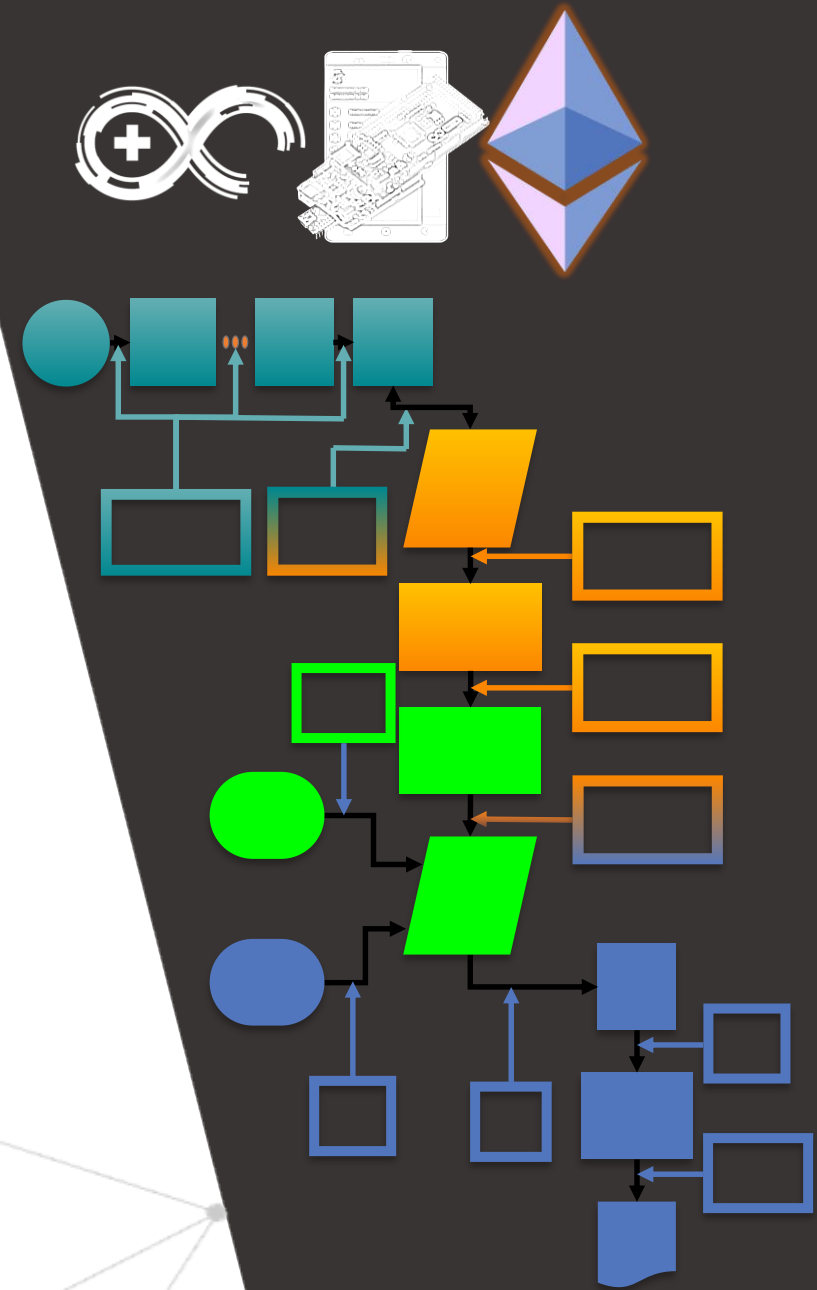
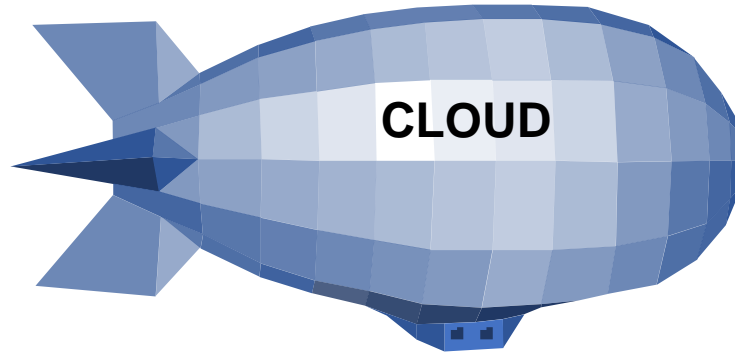
Permite almacenar información inmutable

Realizar transacciones de forma automática



Blockchain

Red + Contrato

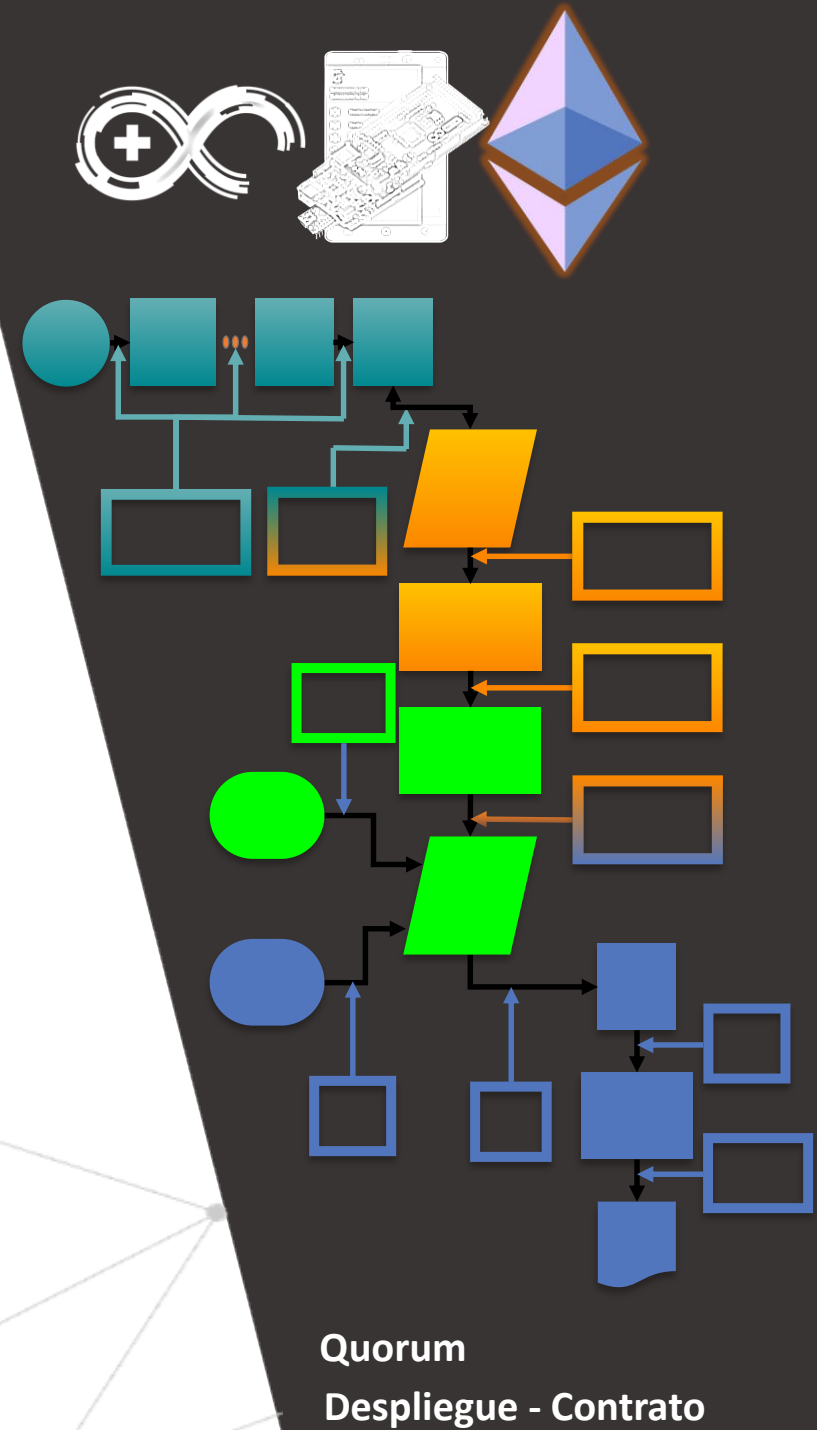
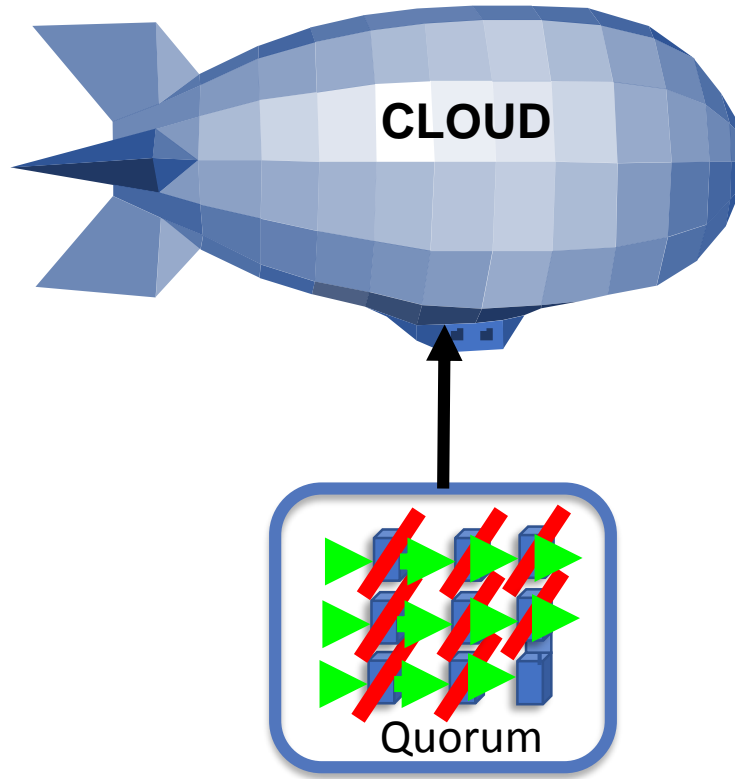


Quorum

Despliegue - Contrato

Blockchain

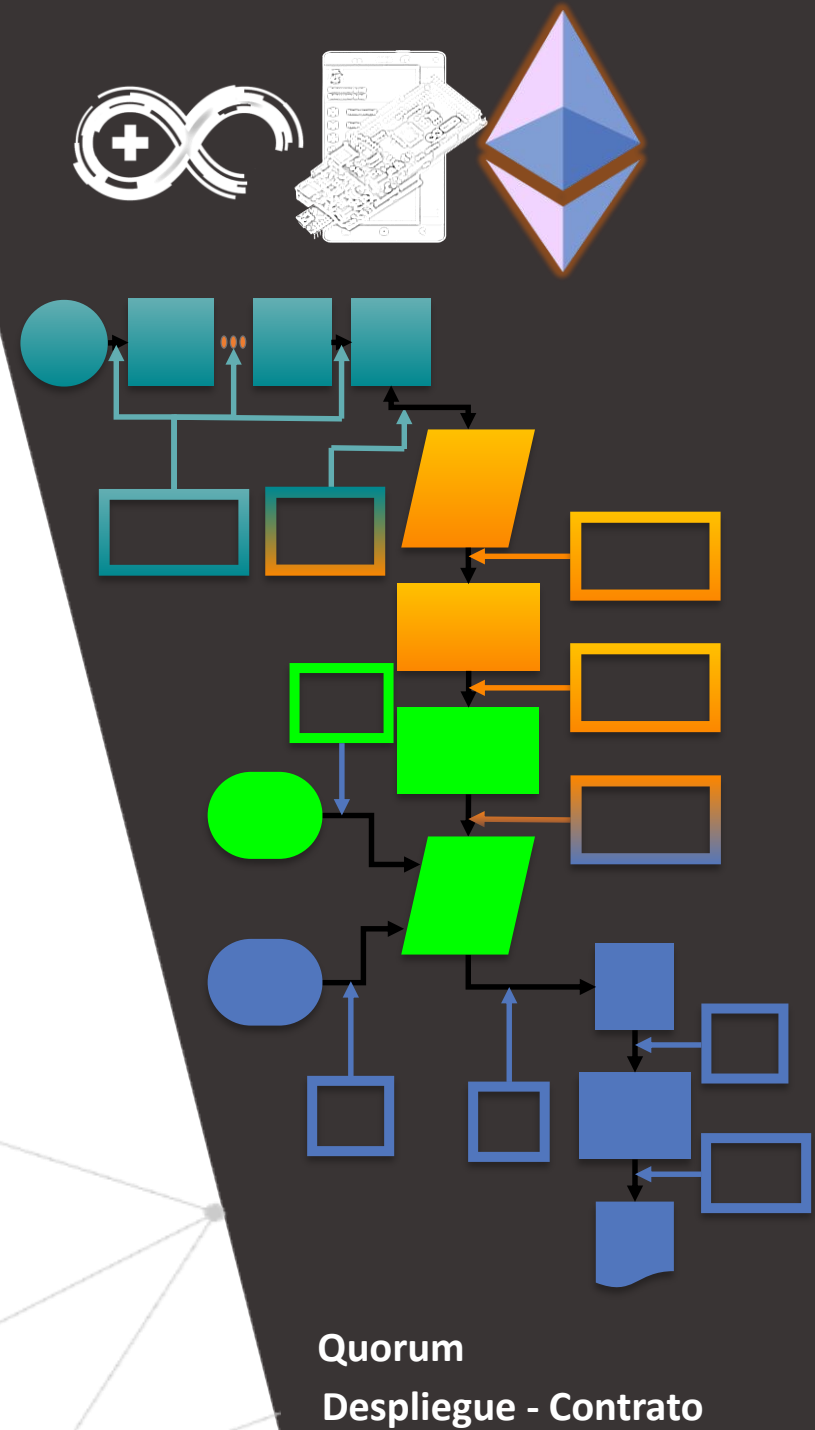
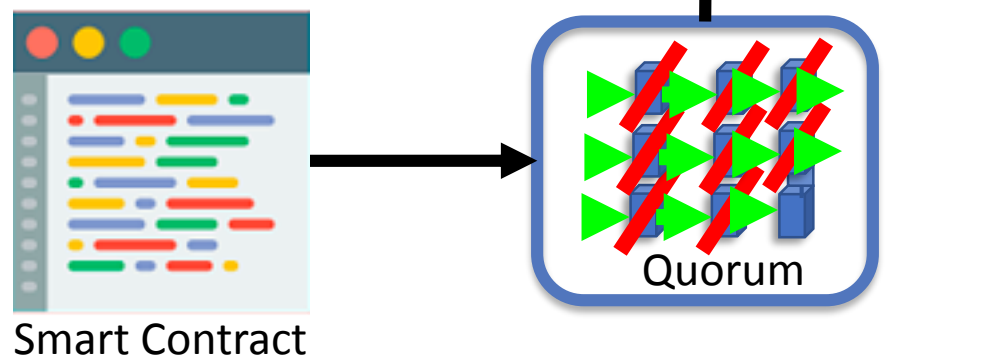
Red + Contrato



Quorum
Despliegue - Contrato

Blockchain

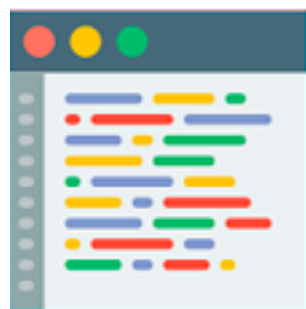
Red + Contrato



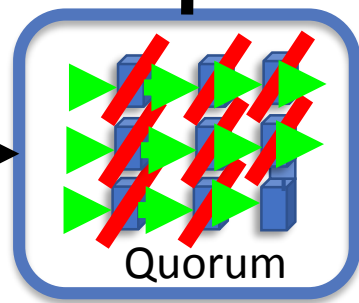
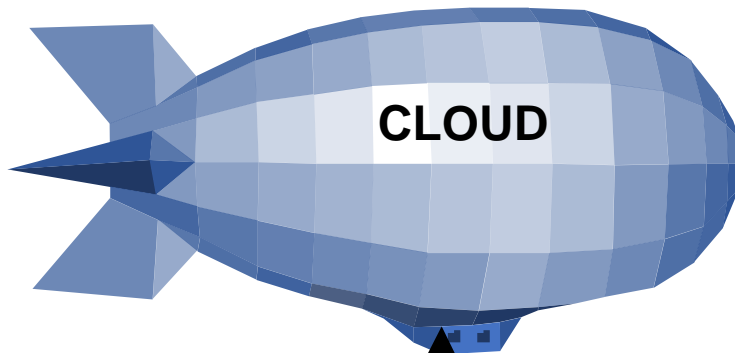
Quorum
Despliegue - Contrato

Blockchain

Red + Contrato

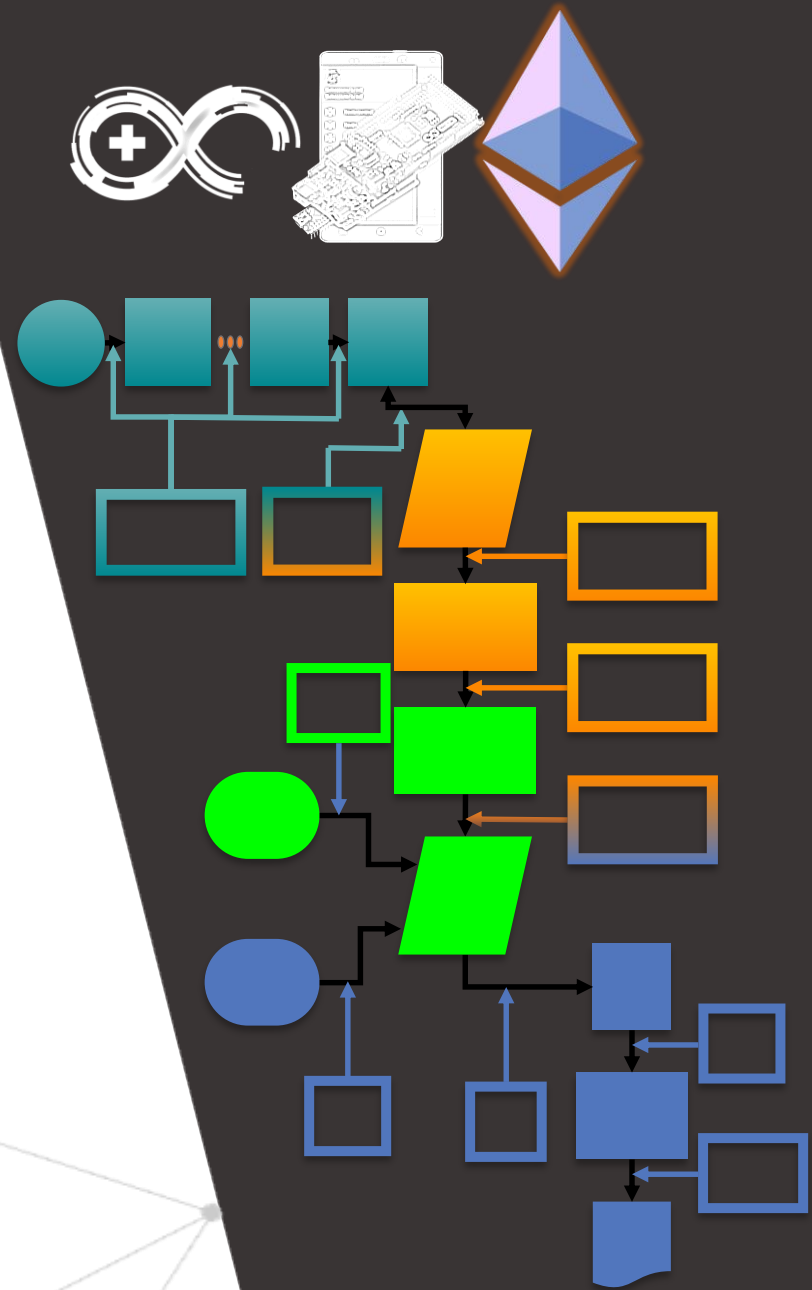


Smart Contract



CLOUD

Quorum



Quorum

Despliegue - Contrato

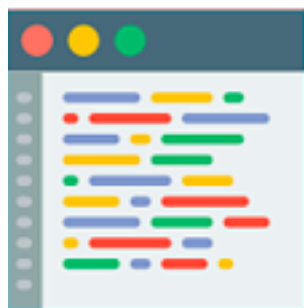
Blockchain

Red + Contrato

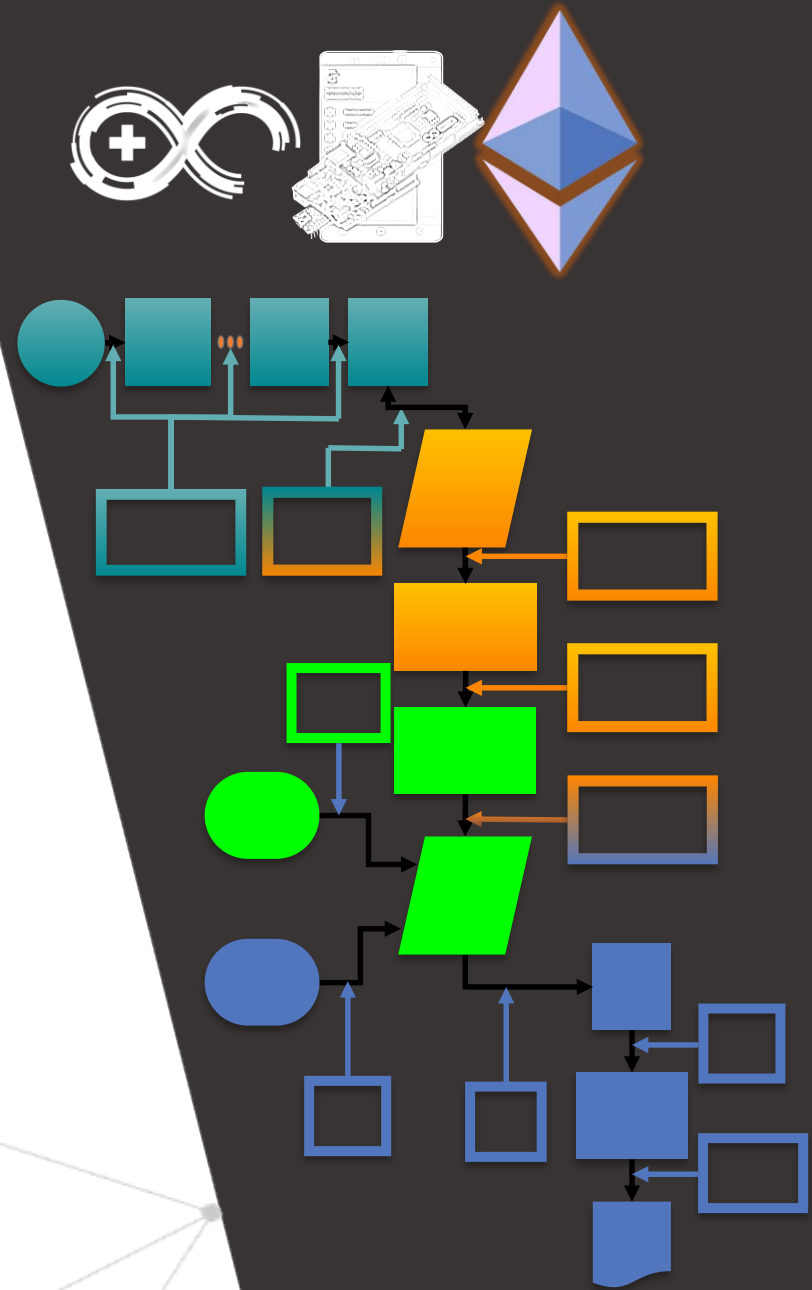
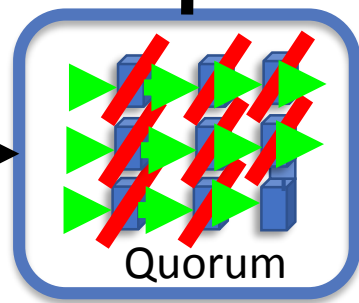
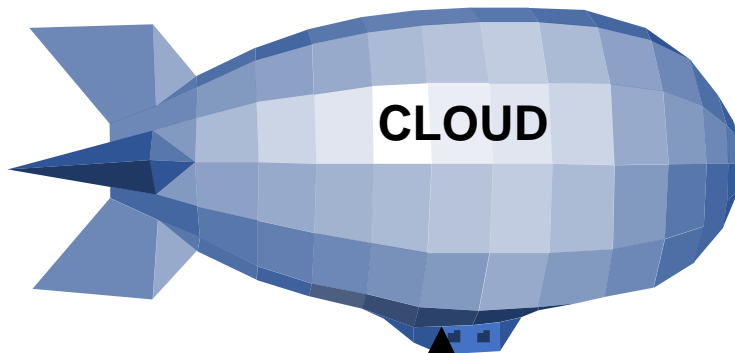


solidity

10 de julio de 2015



Smart Contract



Quorum

Despliegue - Contrato

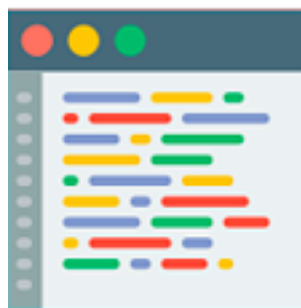
Blockchain

Red + Contrato

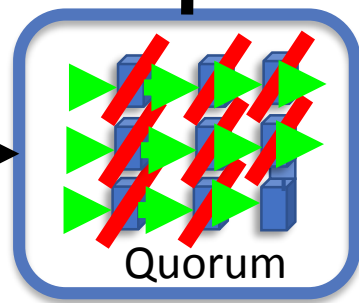
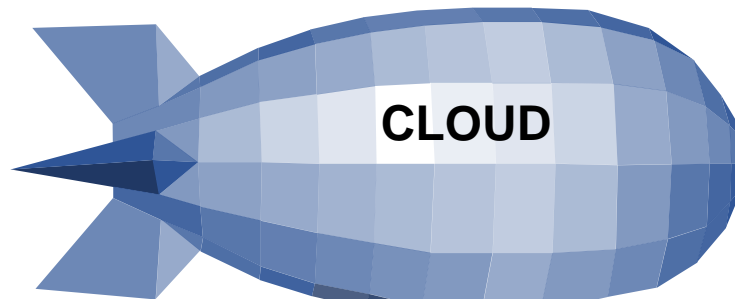


solidity

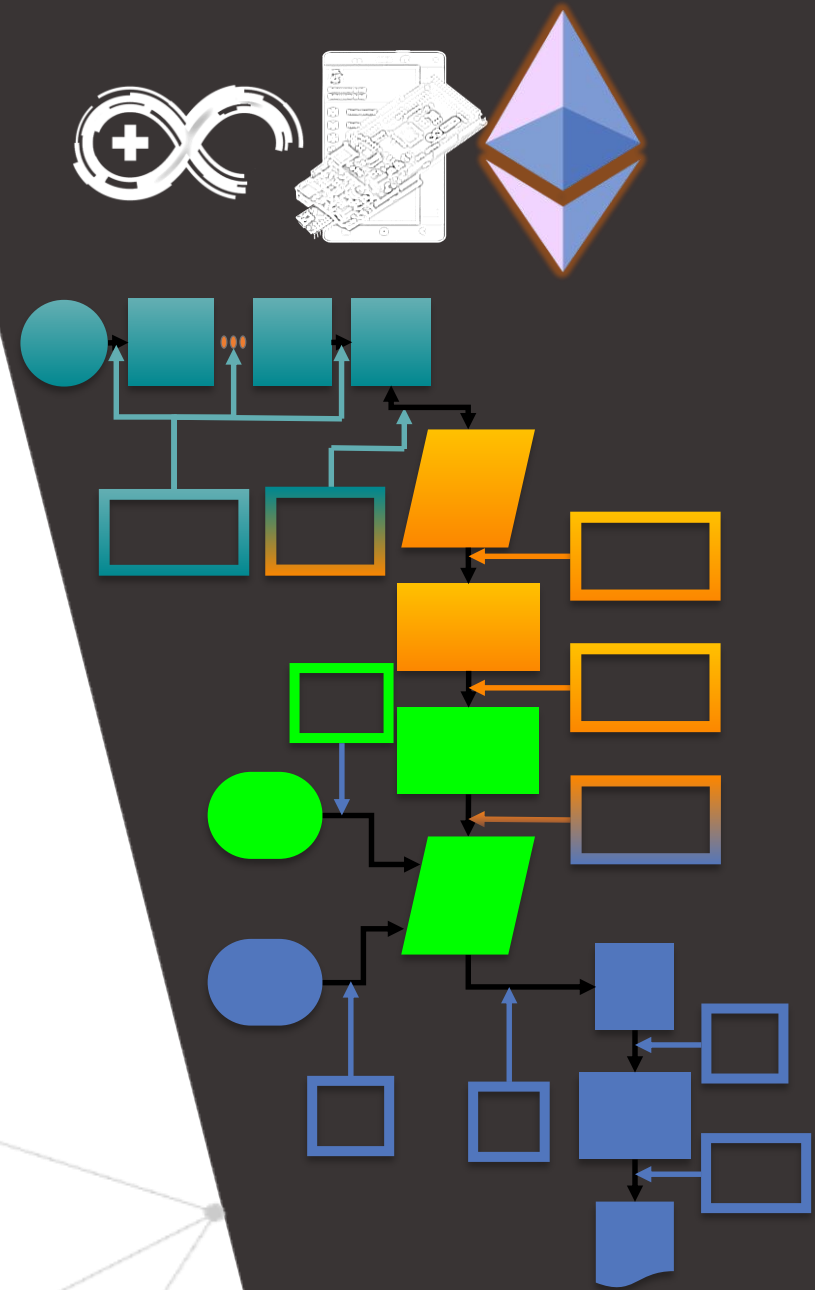
10 de julio de 2015



Smart Contract



APIs - Bot



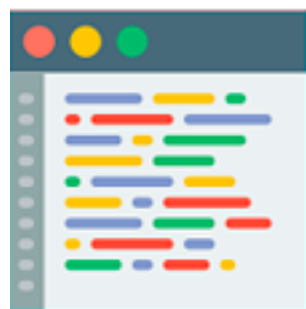
Quorum

Despliegue - Contrato

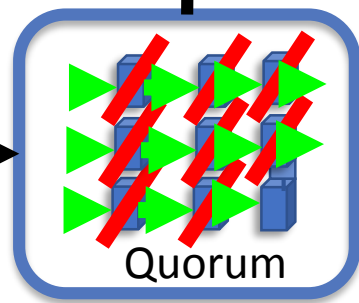
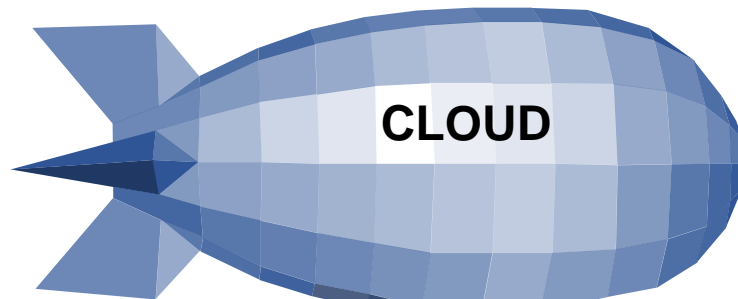
Blockchain

Red + Contrato


solidity
10 de julio de 2015



Smart Contract

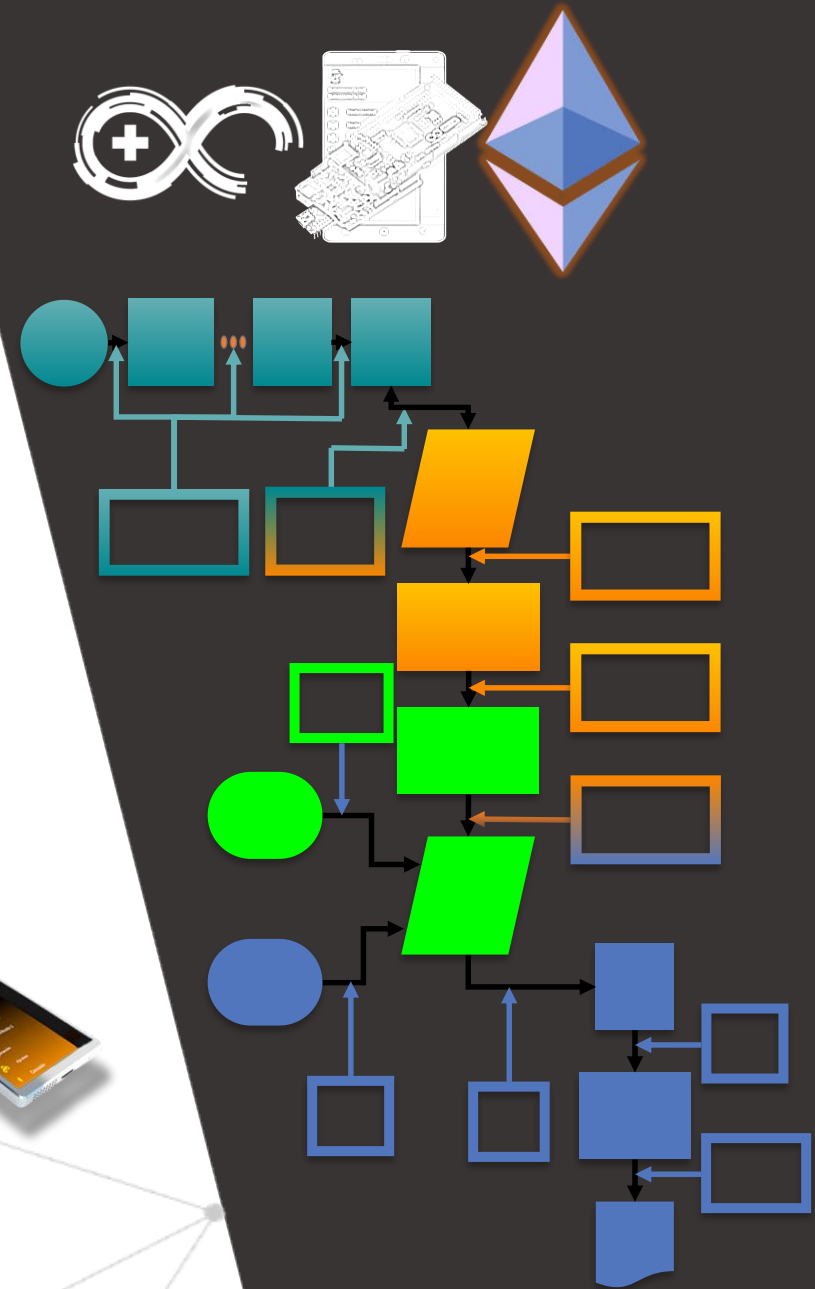


CLOUD

Quorum



APIs - Bot

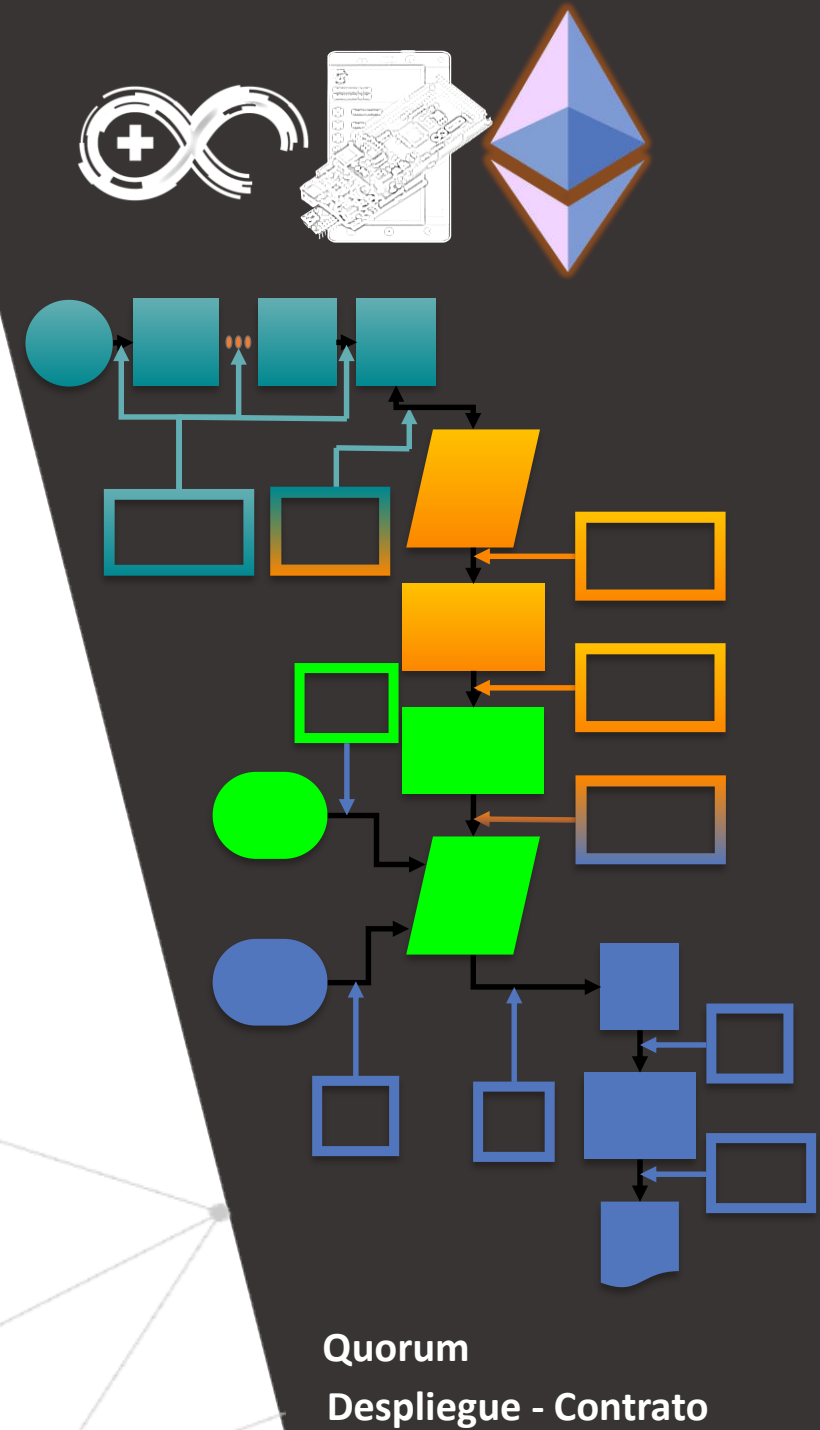
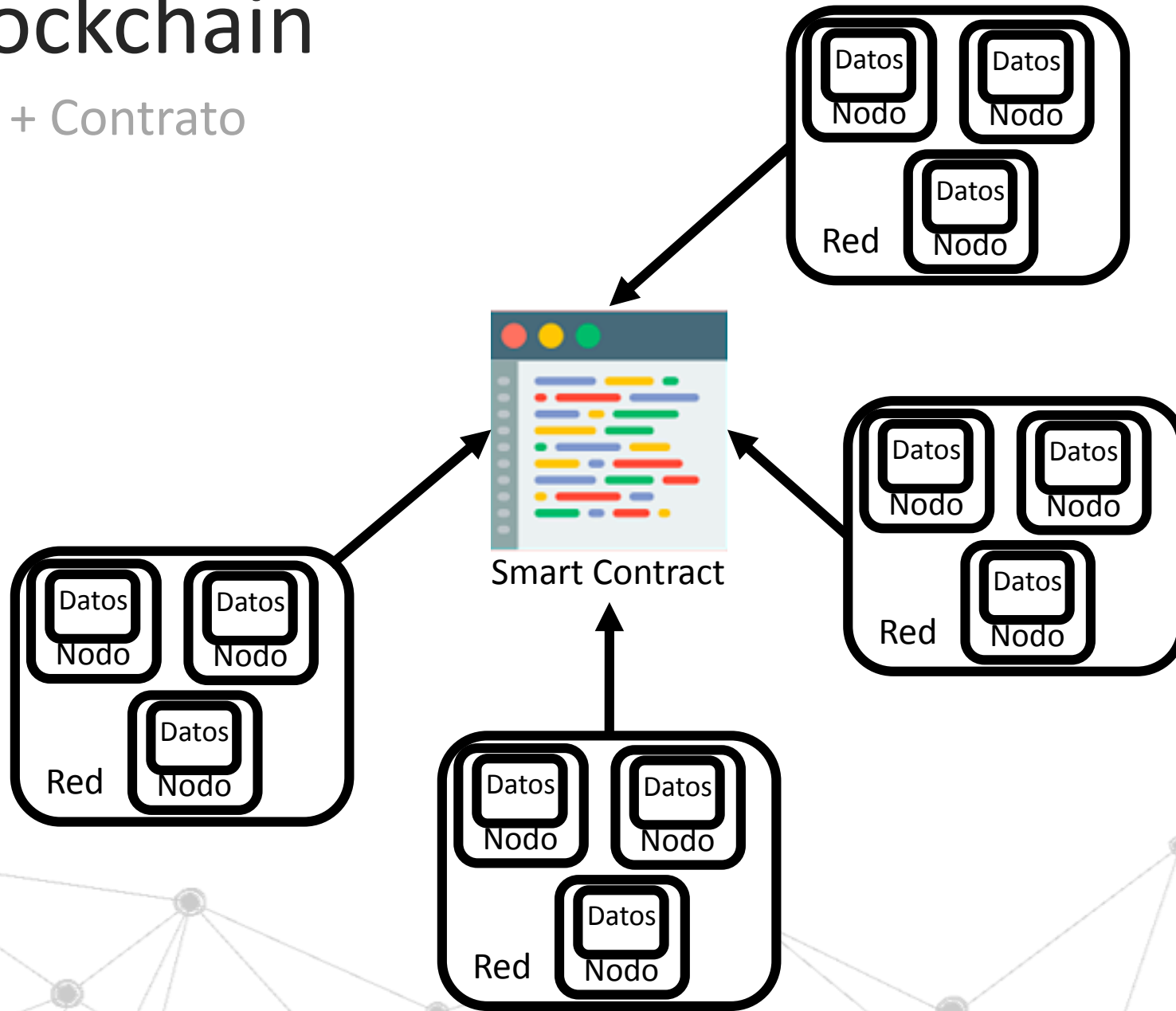


Quorum

Despliegue - Contrato

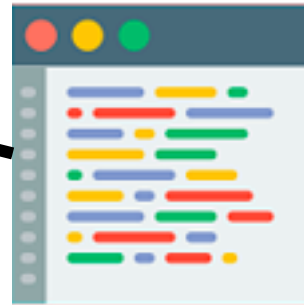
Blockchain

Red + Contrato

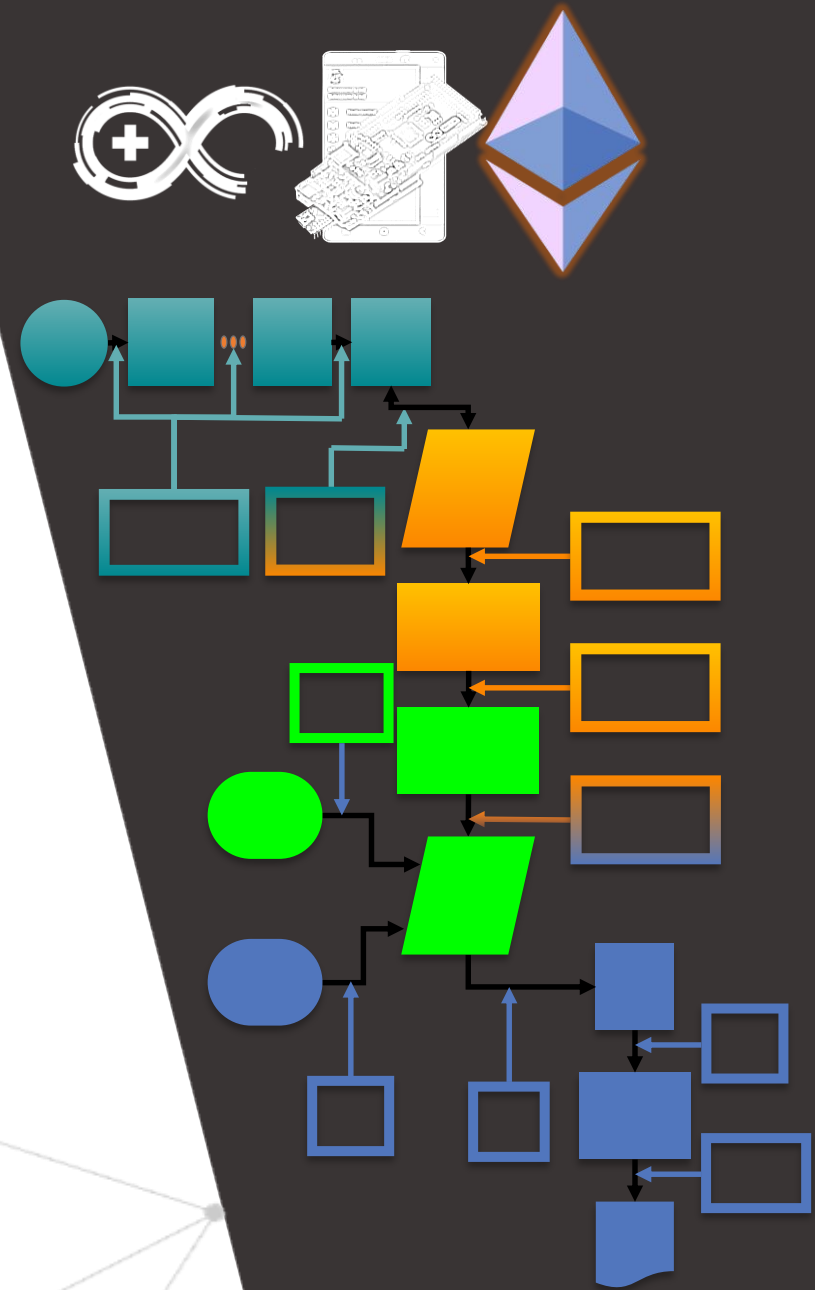


Blockchain

Red + Contrato



Smart Contract



Quorum

Despliegue - Contrato

Blockchain

Compra de datos

Ofrece

Compra de datos

Balance de la dirección

Lista de redes almacenadas

Compra de datos

Dirección
0x794cf499E37B14B5413Ad7042ced7B3f09168CB3

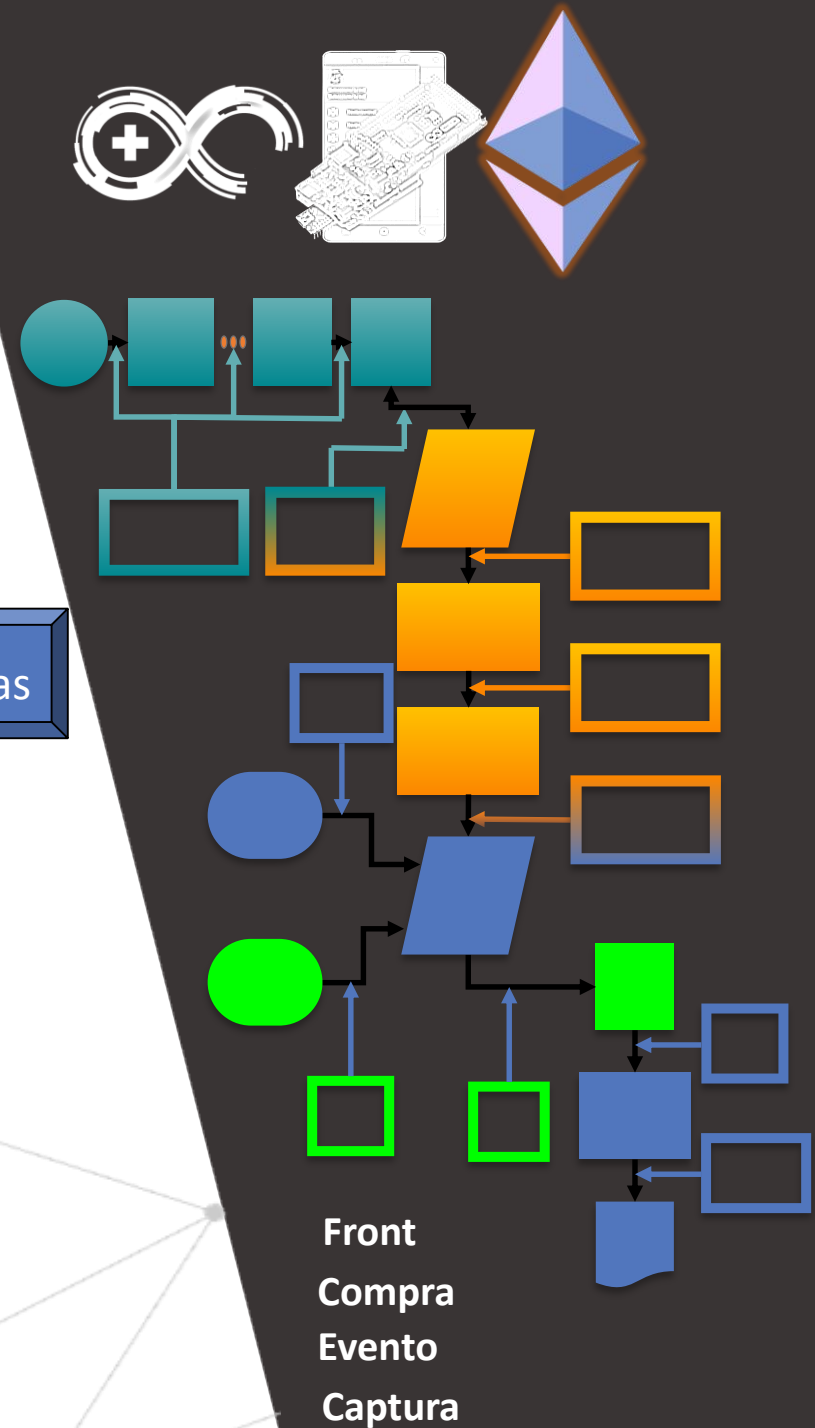
Clave
[]

Balance []

Comprar Datos []

Casa [v]

El coste total sera de: 40 Arken

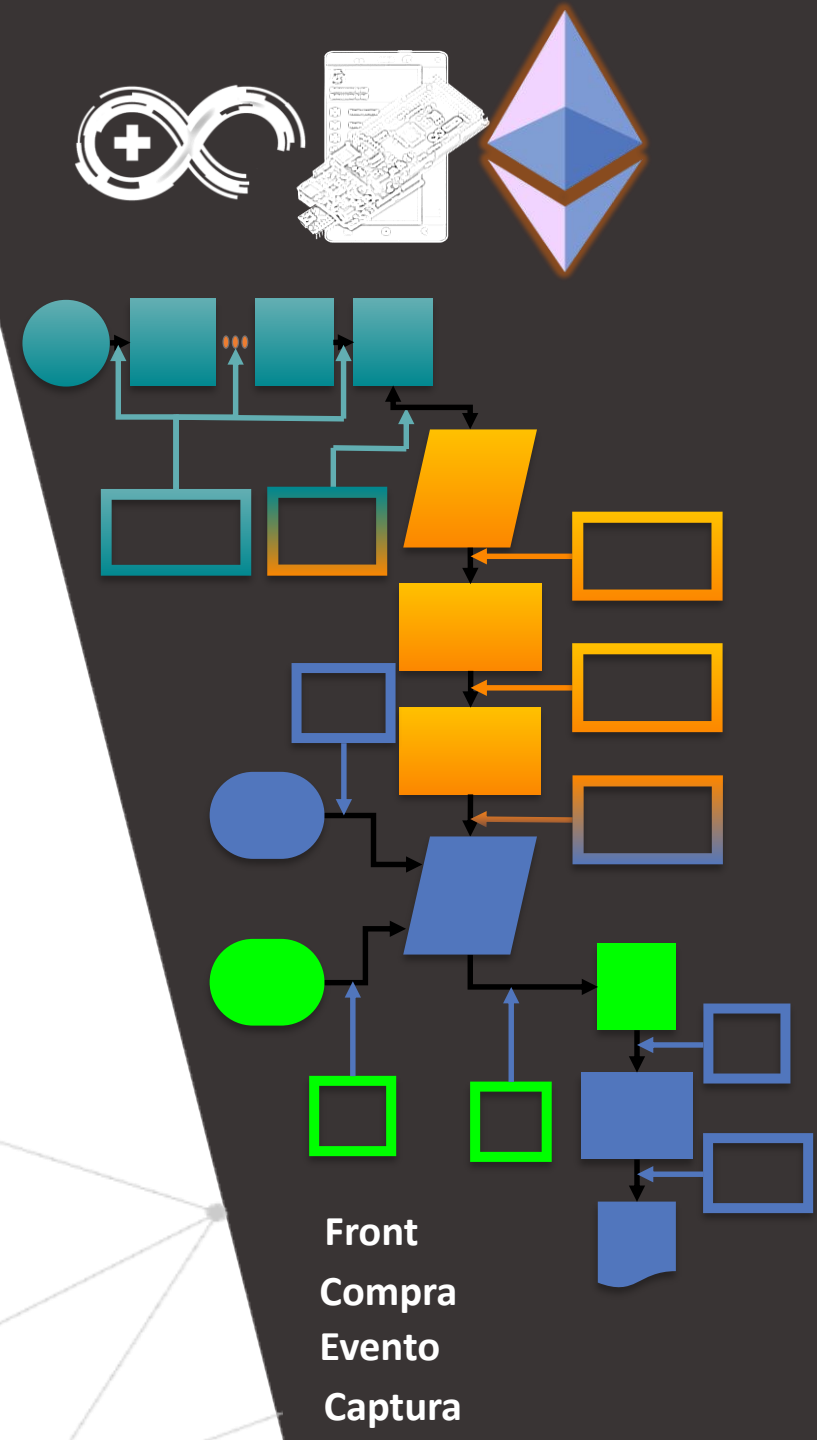


Blockchain

Compra de datos

Compra

Comprar Datos



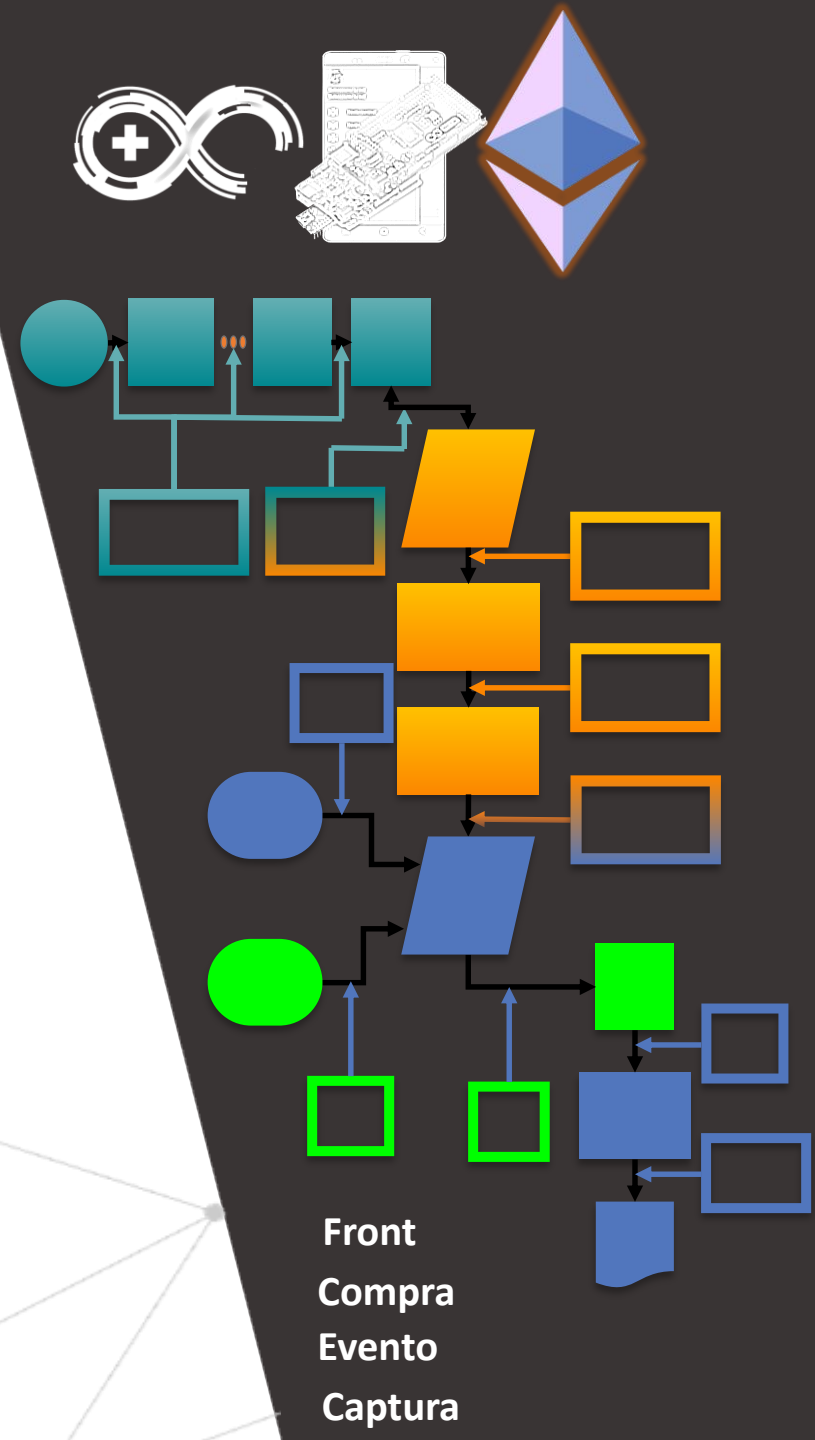
Blockchain

Compra de datos

Compra

Pago

Evento Deposit



Blockchain

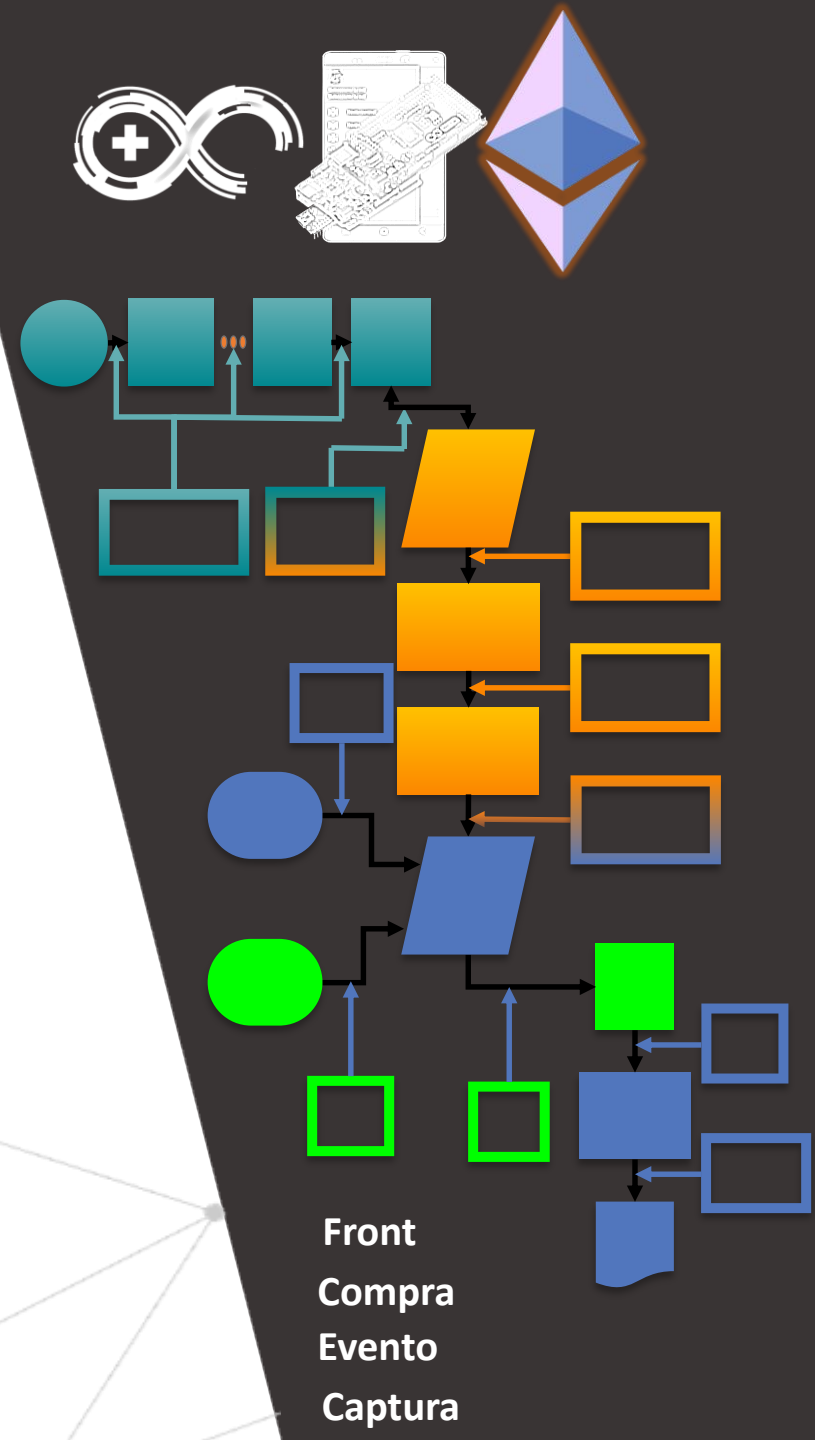
Compra de datos

Compra

Pago

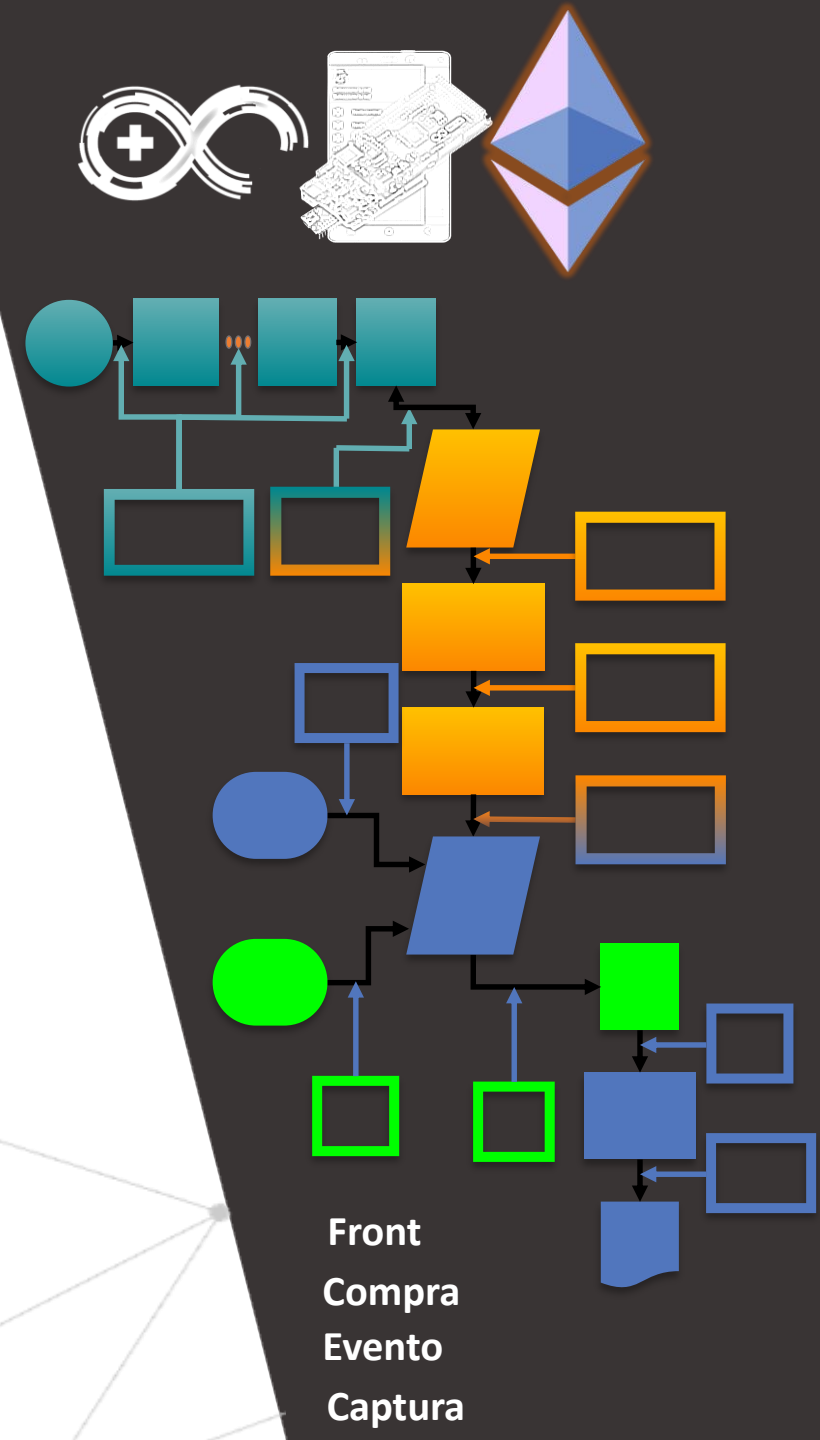
Evento Deposit

Red, Nodo, timestamp,
nombre Sensor, unidades,
medida



Compra de datos

Evento Deposit

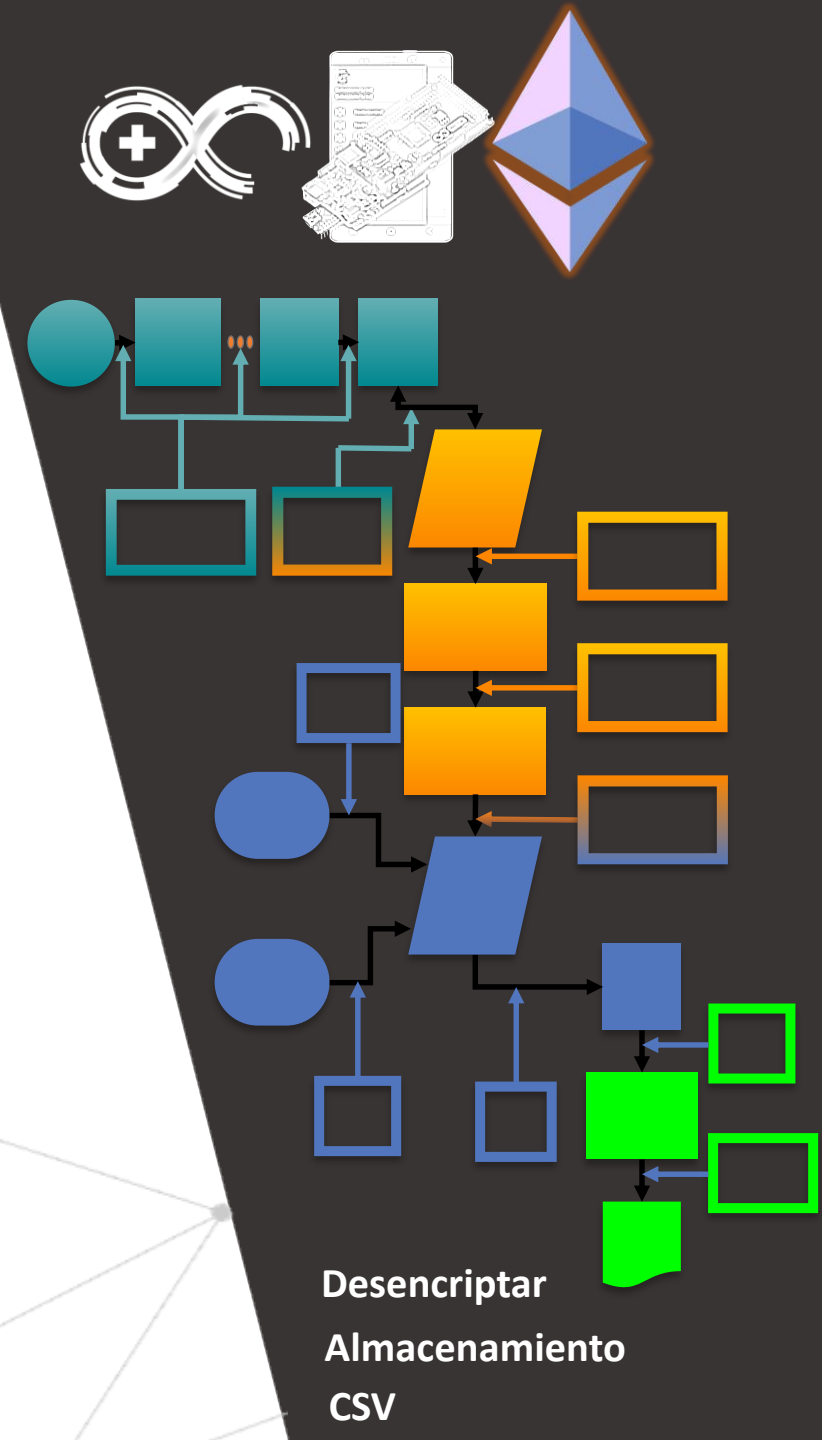
[illegible]

Blockchain

Resultado

Paso 1

```
['00000153695d7a77ddf49', '000443617361', '000000000c48616269746163696f6e5f3',  
'00064674141414141426248432d755474716d4a7068515f664d416e7554774c542d777a6e6147314831776f4e346b6a76424c4f7a685f35346a6e3564687979613  
36a4a4c4d4b33634a6769335931536b3678552d43563679413172472d4e45354f6276413d3d',  
'0000000064674141414141426248432d7549583144496e586659714b6866584476397444516333317a496e61664c5458754e77437653474950657a65486f665948  
513079734773726d4e354f6f495f3035566e484c343139507034794835616d686c6650584a413d3d',  
'0000000064674141414141426248432d75542d56576545446773596a33344176314258436243465239336432724b54334f5755624e675451626e5a647347797a39  
564d63766b3936774c6a4d7744564d585052326e4a47646a3431357438464f79626e69614d513d3d', '000000']
```



Blockchain

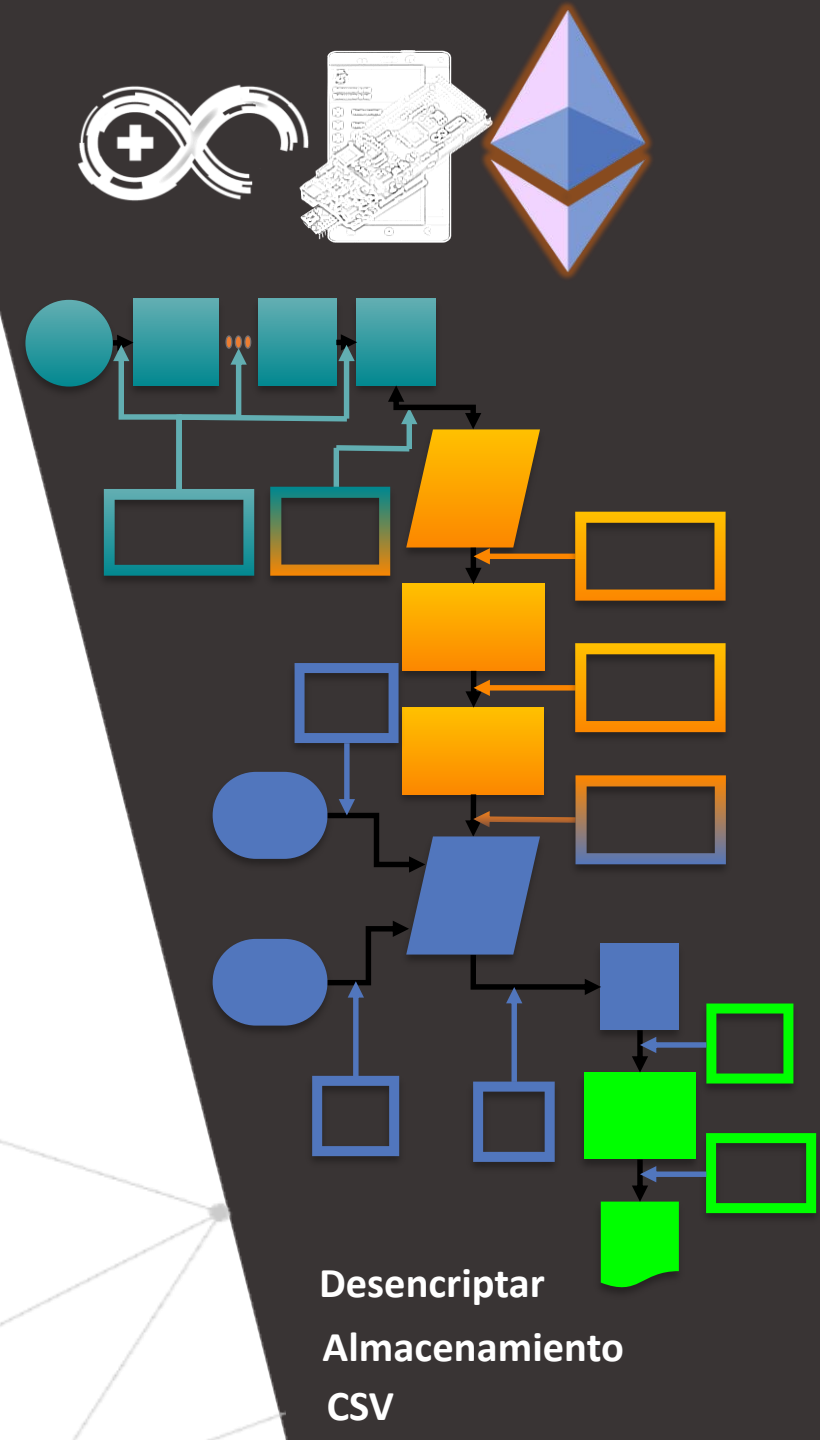
Resultado

Paso 1

```
['00000153695d7a77ddf49', '000443617361', '000000000c48616269746163696f6e5f3',  
'00064674141414141426248432d755474716d4a7068515f664d416e7554774c542d777a6e6147314831776f4e346b6a76424c4f7a685f35346a6e3564687979613  
36a4a4c4d4b33634a6769335931536b3678552d43563679413172472d4e45354f6276413d3d',  
'0000000064674141414141426248432d7549583144496e586659714b6866584476397444516333317a496e61664c5458754e77437653474950657a65486f665948  
513079734773726d4e354f6f495f3035566e484c343139507034794835616d686c6650584a413d3d',  
'0000000064674141414141426248432d75542d56576545446773596a33344176314258436243465239336432724b54334f5755624e675451626e5a647347797a39  
564d63766b3936774c6a4d7744564d585052326e4a47646a3431357438464f79626e69614d513d3d', '000000']
```

Paso 2

```
153695d7a77ddf49  
443617361  
c48616269746163696f6e5f3  
64674141414141426248432d755474716d4a7068515f664d416e7554774c542d777a6e6147314831776f4e346b6a76424c4f7a685f35346a6e356  
468797961336a4a4c4d4b33634a6769335931536b3678552d43563679413172472d4e45354f6276413d3d  
64674141414141426248432d7549583144496e586659714b6866584476397444516333317a496e61664c5458754e77437653474950657a65486f6  
65948513079734773726d4e354f6f495f3035566e484c343139507034794835616d686c6650584a413d3d  
64674141414141426248432d75542d56576545446773596a33344176314258436243465239336432724b54334f5755624e675451626e5a6473477  
97a39564d63766b3936774c6a4d7744564d585052326e4a47646a3431357438464f79626e69614d513d3d
```



Blockchain

Resultado

Paso 1

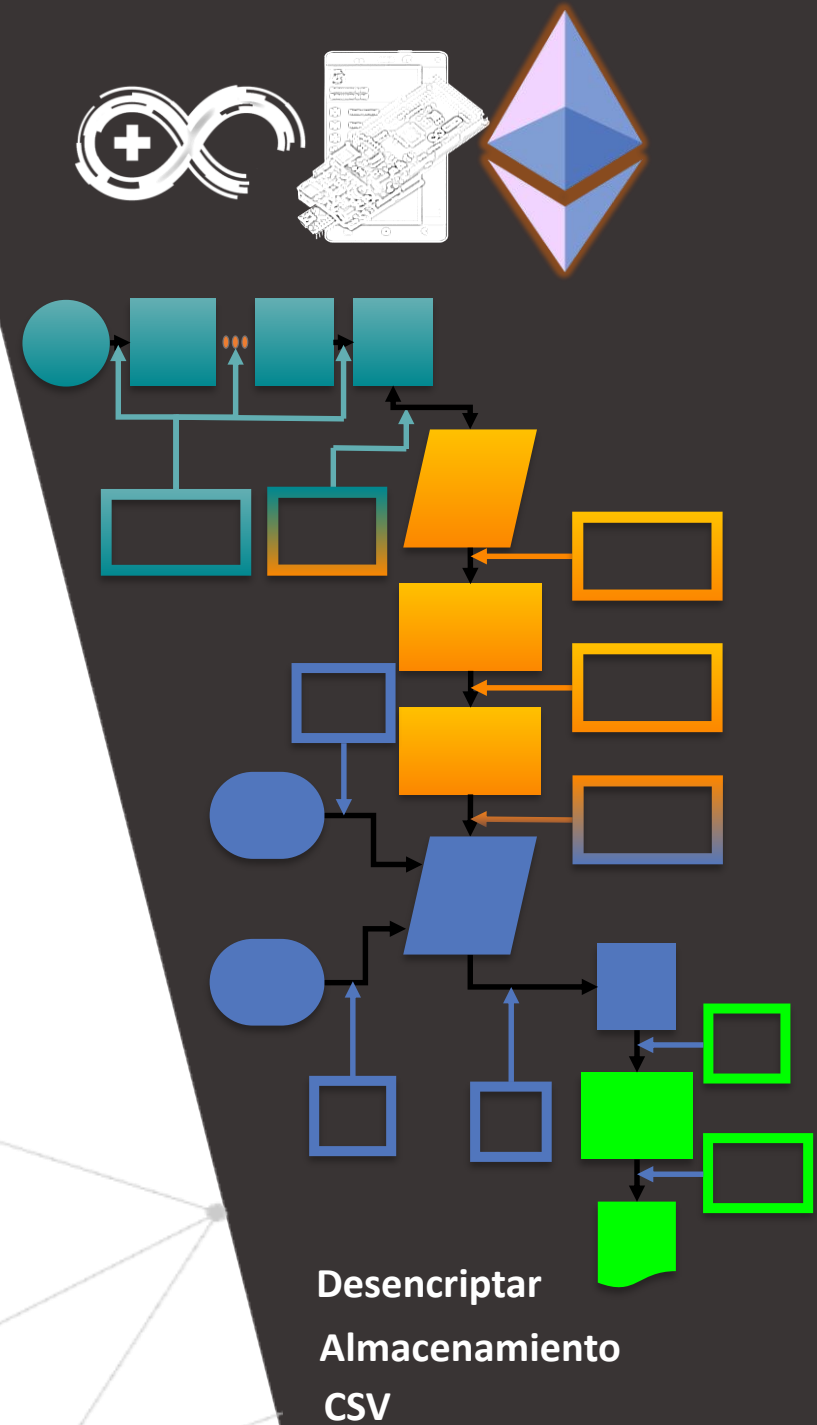
```
['00000153695d7a77ddf49', '000443617361', '000000000c48616269746163696f6e5f3',  
'00064674141414141426248432d755474716d4a7068515f664d416e7554774c542d777a6e6147314831776f4e346b6a76424c4f7a685f35346a6e3564687979613  
36a4a4c4d4b33634a6769335931536b3678552d43563679413172472d4e45354f6276413d3d',  
'0000000064674141414141426248432d7549583144496e586659714b6866584476397444516333317a496e61664c5458754e77437653474950657a65486f665948  
513079734773726d4e354f6f495f3035566e484c343139507034794835616d686c6650584a413d3d',  
'0000000064674141414141426248432d75542d56576545446773596a33344176314258436243465239336432724b54334f5755624e675451626e5a647347797a39  
564d63766b3936774c6a4d7744564d585052326e4a47646a3431357438464f79626e69614d513d3d', '000000']
```

Paso 2

```
153695d7a77ddf49  
443617361  
c48616269746163696f6e5f3  
64674141414141426248432d755474716d4a7068515f664d416e7554774c542d777a6e6147314831776f4e346b6a76424c4f7a685f35346a6e356  
468797961336a4a4c4d4b33634a6769335931536b3678552d43563679413172472d4e45354f6276413d3d  
64674141414141426248432d7549583144496e586659714b6866584476397444516333317a496e61664c5458754e77437653474950657a65486f6  
65948513079734773726d4e354f6f495f3035566e484c343139507034794835616d686c6650584a413d3d  
64674141414141426248432d75542d56576545446773596a33344176314258436243465239336432724b54334f5755624e675451626e5a6473477  
97a39564d63766b3936774c6a4d7744564d585052326e4a47646a3431357438464f79626e69614d513d3d
```



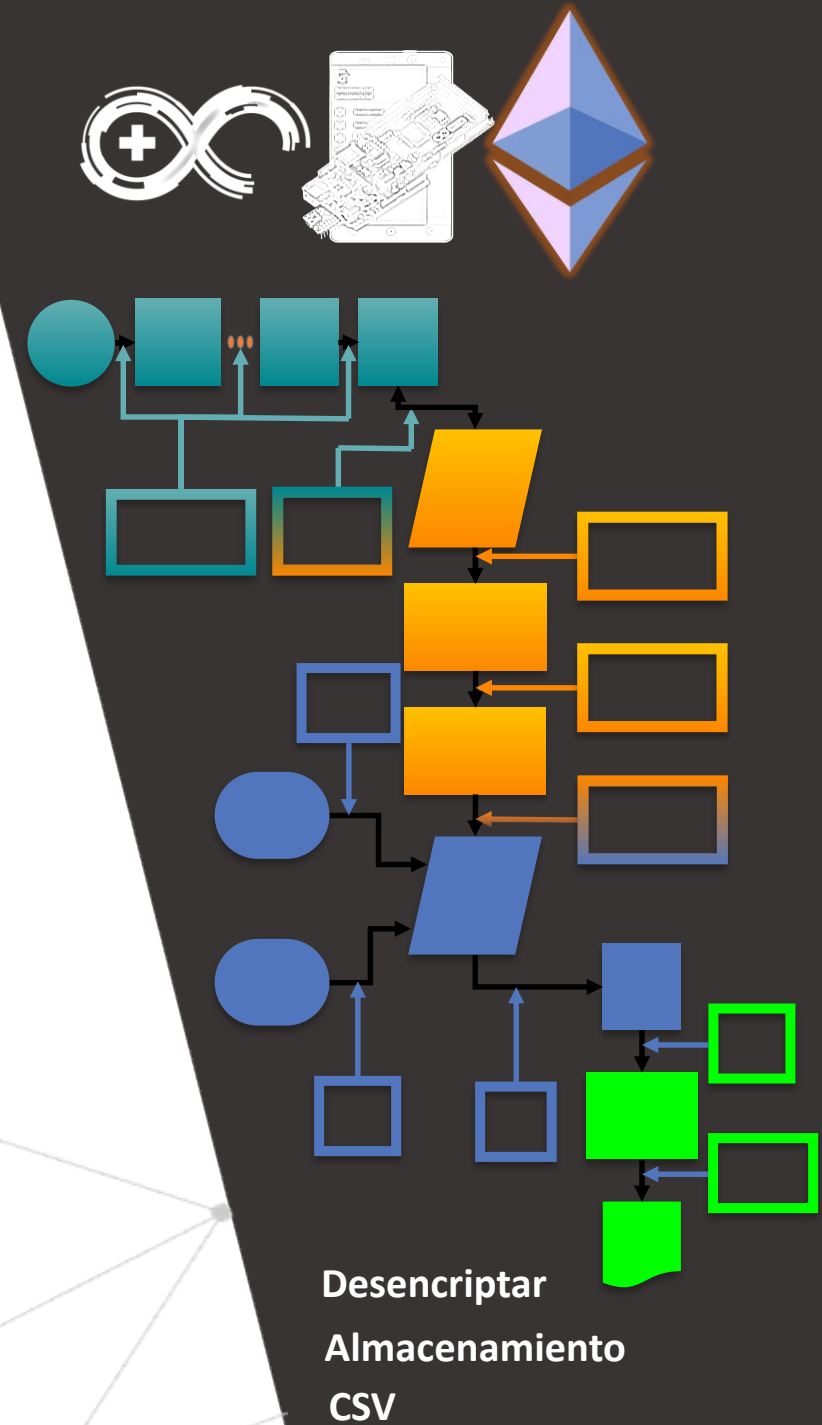
Api desencriptar



Resultado

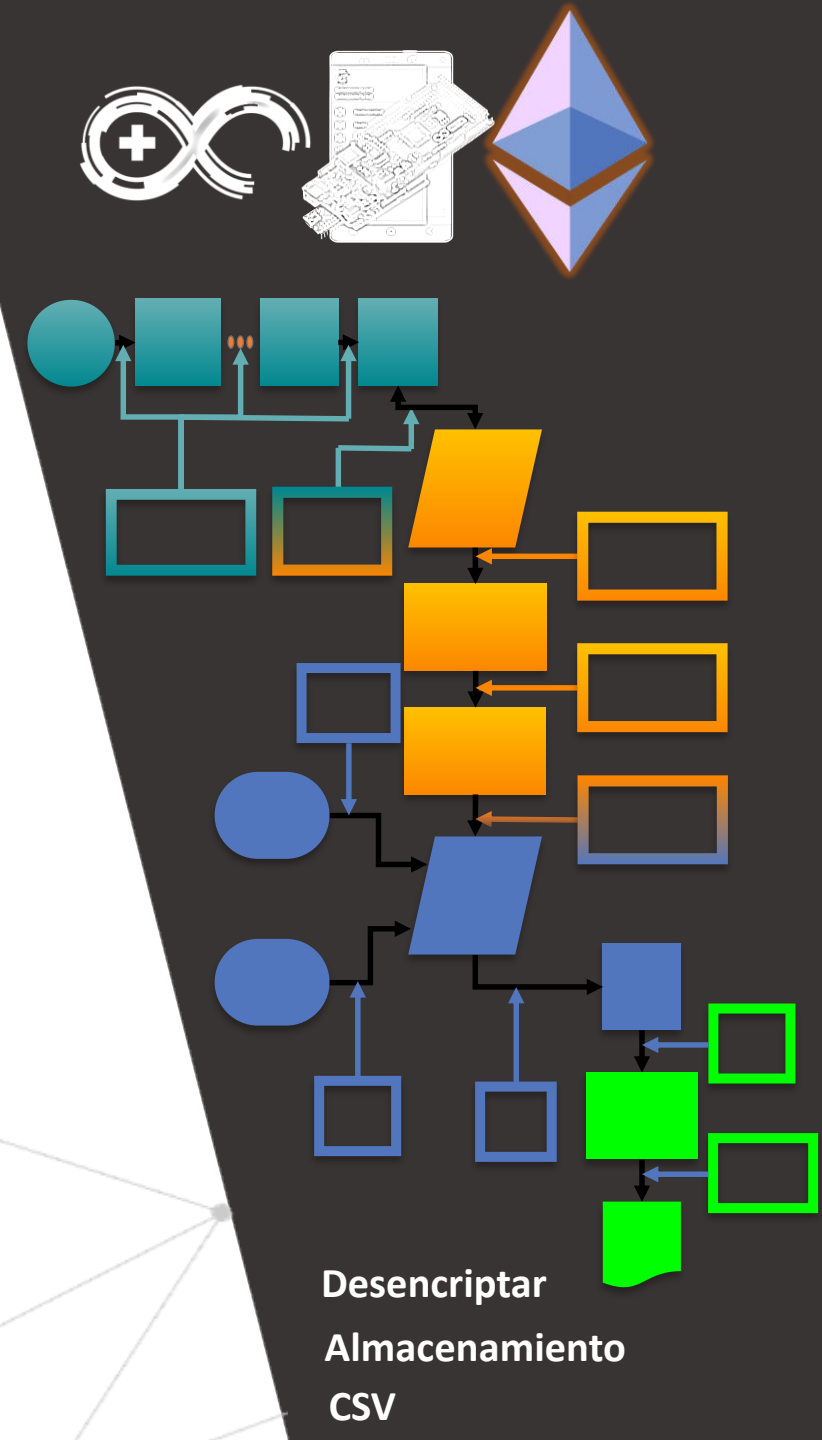
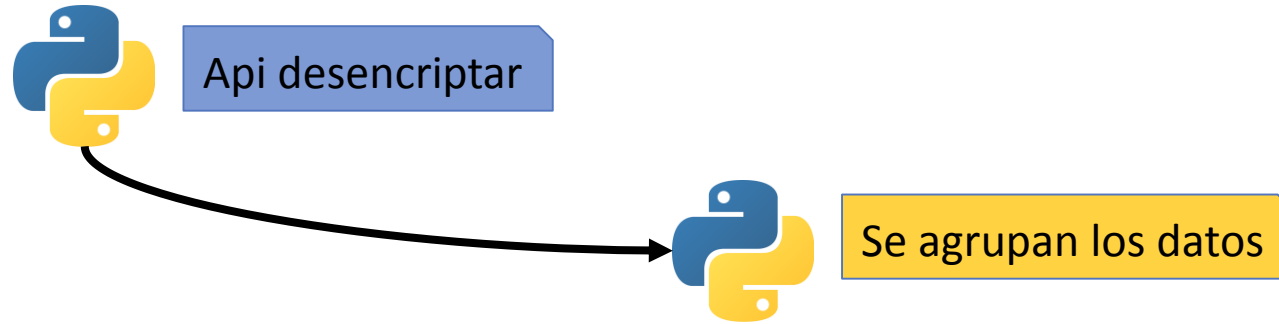


```
['2018-06-09 19:51:16', 'Casa', 'Habitacion_0', '0', 'SensorPresion_1', 'Bar']
```

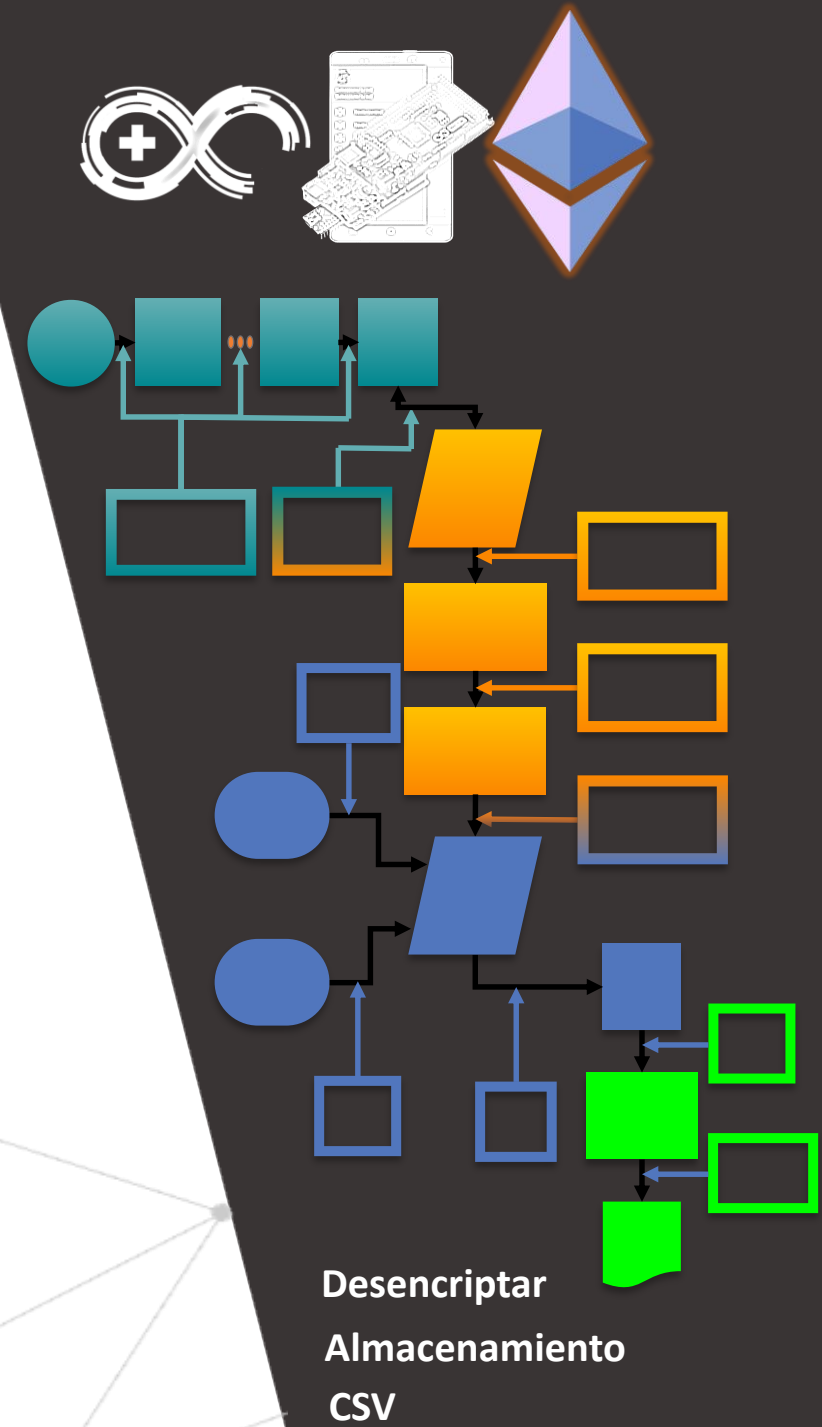


Blockchain

Resultado



Resultado



Fin



Arduino + SesNe + ethereum