Getting started with Chainlink development

Chainlink

Maiko Trindade

June 2021 v1.0

Why

- Blockchain’s inability to fetch reliable information from the real world
- Huge vulnerability in decentralized applications when Blockchain wants to take advantage of **off-chain** data
- Origins of data are also the points where data can be manipulated, compromised, or simply falsified
- Chainlink started on **Ethereum** but it's also available on Polkadot, Hyperledger, etc...

Chainlink

Decentralized network of nodes that provide data and information from off-blockchain sources to on-blockchain smart contracts via **oracles**

LINK is built on Ethereum in accordance with the ERC-20 standard for tokens

- Sep 2017 – Chainlink raises $32 million in an ICO creating 1 billion LINK tokens
- Nov 2018 – Chainlink acquires TownCrier
- May 2019 – Chainlink is launched on Ethereum mainnet
- May 2021 – Chainlink 2.0 whitepaper

The Chainlink's oracle

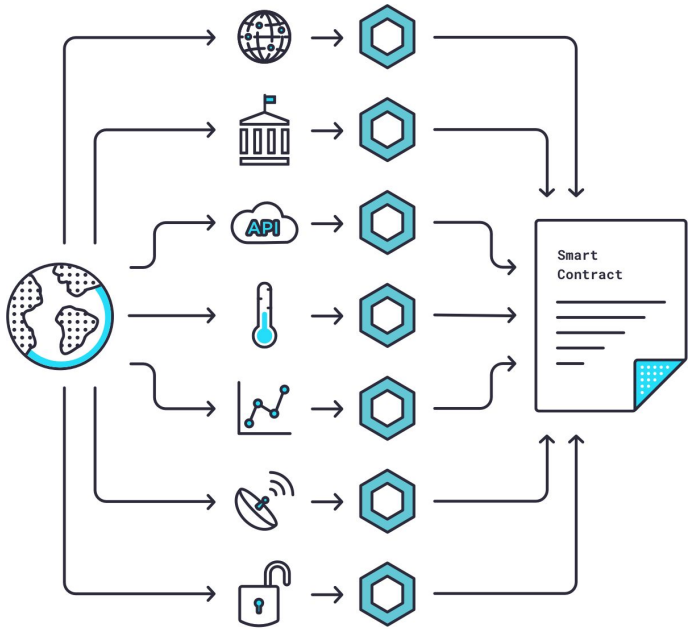
Oracle – Middleware that acts as an intermediary, translating data from the real world to smart contracts on the blockchain and back again

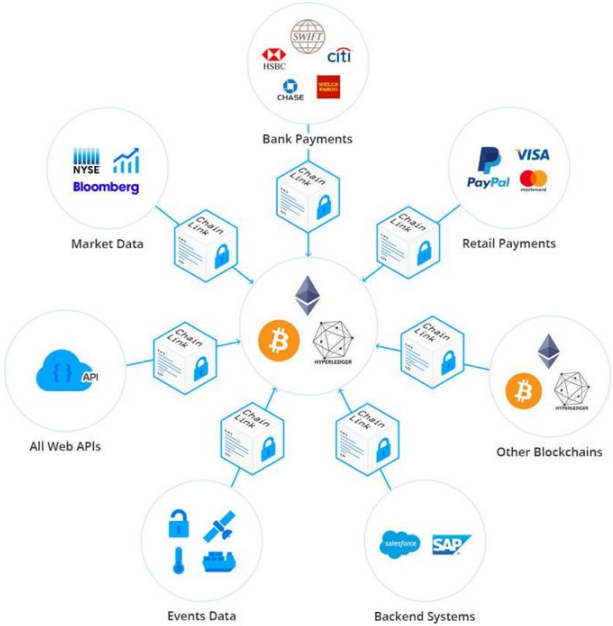
Chainlink – Decentralized network of nodes that provide data and information from off-blockchain sources to on-blockchain smart contracts via oracles

🥇 Market standard for decentralized oracles

Name	Market Cap
Chainlink LINK	$10,352,049,001
UMA UMA	$713,943,947
iExec RLC RLC	$342,090,181
Augur REP	$239,380,720
Band Protocol BAND	$131,486,201

The Chainlink's oracle





The Chainlink's oracle

✅ Enhance and extend the capabilities of smart contracts on a target blockchain through functions that are not available natively

✅ To minimize the potential failure of oracles: Distribution of data sources, Distribution of oracles and Use of trusted hardware

✅ *The Chainlink Reputation Contract*

Chainlink 2.0

Chainlink 2.0: Next Steps in the Evolution of Decentralized Oracle Networks

> *"Oracle networks go far beyond delivering highly validated data, they provide the various decentralized services that are combined with smart contracts to create real world outcomes. These hybrid smart contracts are already redefining our industry as DeFi."*

🔥 Hybrid Smart Contracts that are seamlessly connected to all necessary off-chain resources, while retaining increased levels of privacy and being secured

🔥 New "architecture" enables more advanced off-chain computation

🔥 Increase number of services since ecosystem is more flexible and enhance its capabilities. Chainlink is the future of DeFi

Hands on: Truffle + Chainlink

Prerequisite: Truffle/Ganache setup

Repository: https://github.com/smartcontractkit/truffle-starter-kit

```
npm install --global yarn

mkdir Chainlink

cd Chainlink

truffle unbox smartcontractkit/box

yarn
```

Running tests

Run Ganache or enable/integrate **Kovan** testnet

`npm test`

All tests of `/test` will be executed. There are tests about creating requests with and without Link tokens, sending these requests to oracle contract addresses, and testing contract ownership

```
only for Kovan right now!


  Contract: MyContract
    #createRequest
      without LINK
        ✓ reverts (681ms)
      with LINK
        sending a request to a specific oracle contract address
          ✓ triggers a log event in the new Oracle contract (104ms)
    #fulfill
      ✓ records the data given to it by the oracle
      when my contract does not recognize the request ID
        ✓ does not accept the data provided (64ms)
      when called by anyone other than the oracle contract
        ✓ does not accept the data provided (45ms)
    #cancelRequest
      before the expiration time
        ✓ cannot cancel a request (78ms)
      after the expiration time
        when called by a non-owner
          ✓ cannot cancel a request (40ms)
        when called by an owner
          ✓ can cancel a request (49ms)
    #withdrawLink
      when called by a non-owner
        ✓ cannot withdraw
      when called by the owner
        ✓ transfers LINK to the owner (97ms)

  Contract: PriceConsumerV3
    #getLatestPrice
      ✓ returns a price

  Contract: RandomNumberConsumer
    #request random number
      ✓ it revert without LINK (50ms)
      ✓ returns a random number with link (203ms)


  13 passing (8s)
```

Ganache deployment

Deploy

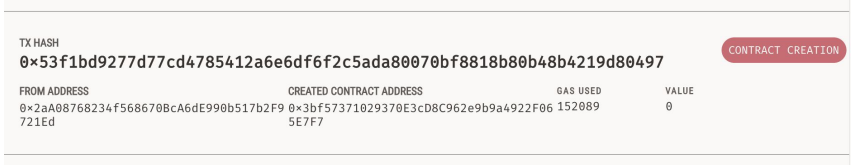
```
truffle migrate --network ganache
--reset
```

truffle-config.js

```
ganache: {
  host: '127.0.0.1',
  port: 7545,
  network_id: '*',
},
```

Gas – fee required to conduct a transaction or execute a contract on the Ethereum blockchain.

```
Summary
=======
> Total deployments:   5
> Final cost:          0.08533364 ETH
```



Kovan deployment

1. Setup Metamask and connect to Kovan network
2. Faucet: faucet.kovan.network
3. Create account and a project using Infura.io – step-by-step tutorial
4. Infura setup and "env.sample" file configuration

```
kovan: {
    provider: () =>
        new HDWalletProvider({
            mnemonic: {
                phrase: "[redacted]"
            },
            providerOrUrl: '[redacted]',
            numberOfAddresses: 1,
            shareNonce: true,
        }),
    network_id: '42',
}
```

truffle-config.js

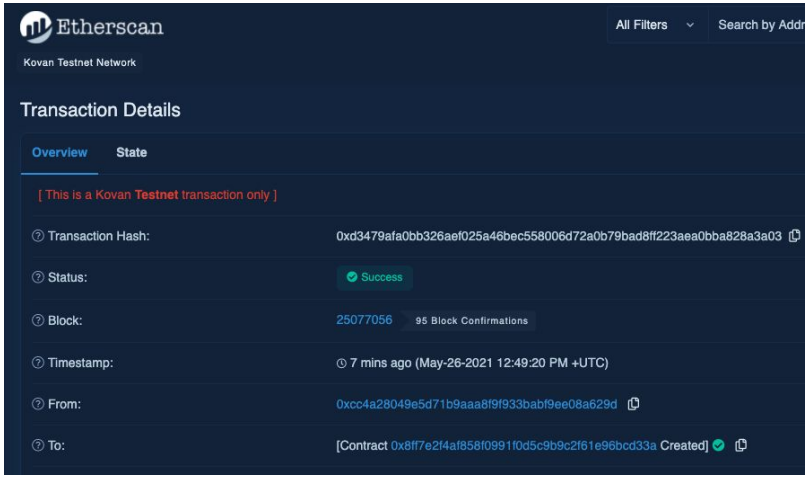
Migration

```
truffle migrate --network kovan --reset
```

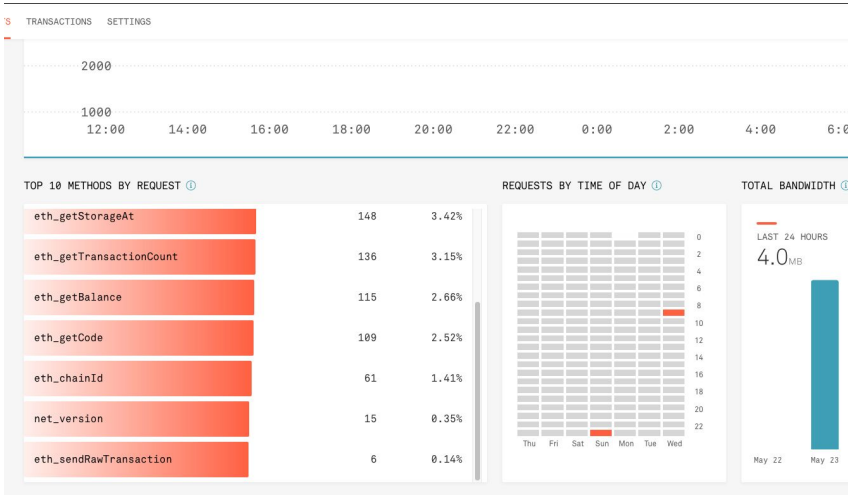
```
1_initial_migration.js
======================

   Deploying 'Migrations'
   ----------------------
   > transaction hash:    0x7d157b9cbc88160877d9c4b0c8b43813d2fcc8eb9a9dac811b9d6821aa2a02c2
   > Blocks: 2            Seconds: 9
   > contract address:    0x6546CF14DDB5DBe249ADA524d80644A1C57CDf3B
   > block number:        24880596
   > block timestamp:     1621212048
   > account:             0xCc4A28049E5D71B9AAa8f9F933bABf9eE08A629D
   > balance:             1.99540194
   > gas used:            226753 (0x375c1)
   > gas price:           20 gwei
   > value sent:          0 ETH
   > total cost:          0.00453506 ETH
```

```
Summary
========
> Total deployments:   4
> Final cost:          0.04958734 ETH
```

Migration



Etherscan / Kovan



Infura Project

Acquire testnet LINK

```
Funding contract: 0x1123c6967701ab4a86f7781Fa4E3091383314121
Transaction: 0x0e5447b9f367d76a0bc4c6b9683d4e8d8f7e49c28dc4aeac07ed2e11c0e80d91 exited with an error (status 0)
after consuming all gas.
     Please check that the transaction:
     - satisfies all conditions set by Solidity `assert` statements.
     - has enough gas to execute the full transaction.
        - does not trigger an invalid opcode by other means (ex: accessing an array out of bounds).
```

Required: Acquire LINK via Chainlink Kovan **Faucet** website 🤑 🤑 🤑

Optional: Add LINK token to Metamask - Chainlink docs

Helper scripts

Scripts to interact with deployed smart contract without any frontend implementation:

1. fund-contract.js

```
npx truffle exec scripts/fund-contract.js --network kovan
```

2. request-data.js

```
npx truffle exec scripts/request-data.js --network kovan
```

3. read-contract.js

```
npx truffle exec scripts/read-contract.js --network kovan
```

Helper scripts

- **fund-contract.js**
  - ➢ Send 1 LINK to requesting contract
- **request-data.js**
  - ➢ Chainlink request to be created from the requesting contract
- **read-contract.js**
  - ➢ Read the data variable of the requesting contract (current price of pair ETH/USD)

Additional Information

1. Top Oracles Tokens by Market Capitalization
2. Code a REAL WORLD dApp with Chainlink - Ethereum, Solidity, Web3.js
3. 77 Smart Contract Use Cases Enabled By Chainlink
4. Expanding Beyond Data Delivery With Chainlink 2.0 | Sergey Nazarov at Consensus 2021
5. Chainlink's Founder Says DeFi and Oracles Can Help Fight Climate Change
6. Reversing Climate Change: How Hybrid Smart Contracts Incentivize Regenerative Agriculture

Glossary

- ERC-20: technical standard used to issue and implement tokens on the Ethereum blockchain. It makes easier for developers to predict with more accuracy the interaction between different tokens and applications
- Faucet: website that distributes small amounts of crypto
- ICO: An Initial coin offering occurs when company looking to raise money to create a new coin, app, or service launches an ICO as a way to raise funds. Similar to an IPO
- Middleware: software that acts as a bridge between an operating system or database and applications, especially on a network
- Off-chain: Transactions which agree to happen outside the blockchain
- On-chain: normally refer to as blockchain transactions which happens inside the blockchain

References

- Chainlink docs - https://docs.chain.link/docs/tutorials
- Chainlink official website - https://chain.link
- How to use Chainlink with Truffle - https://blog.chain.link/how-to-use-chainlink-with-truffle-2/
- Truffle Starter kit - https://github.com/smartcontractkit/truffle-starter-kit
- Truffle Starter kit impl - https://github.com/CryptoDevBR/crypto-feed-chainlink-oracle
- What Is Chainlink in 5 Minutes - https://www.gemini.com/cryptopedia/what-is-chainlink-and-how-does-it-work