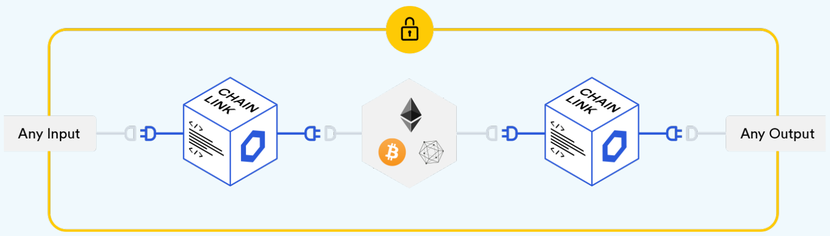
CHAINLINK

COMMUNITY FACT SHEET
January 2020.1

Smart contracts & the real world

Enabling secure I/O into smart contracts & interoperability between blockchains

Smart contracts provide the ability to execute tamper-proof digital agreements, which are considered highly secure and highly reliable. In order to maintain a contract's overall reliability, the inputs and outputs that the contract relies on also need to be secure. Chainlinks provide a reliable and secure end-to-end connection to external data.



Overview

Historically, the blockchains on which smart contracts run cannot support native communication with external systems, and the potential that smart contracts provide have been throttled by their inability to connect off-chain.

Today, the solution to this problem is to introduce a new functionality, called an **'ORACLE'**, that provides connectivity to the outside world. However, oracles to-date are centralized services, meaning any smart contract using such services has a single point of failure, which nullifies any benefits gained from the decentralized nature of smart contracts.

To fill this gap, Chainlink was developed as the first decentralized oracle that can provide external data to smart contracts. As a result, the security and determinism of smart contracts can be combined with the knowledge and breadth of real-world external events. Chainlink will provide your smart contract with access to any external data you want to connect your smart contract with, and all the information needed to do so are listed here.

You'll see Chainlink references in articles both as http://chain.link[1] & smartcontract.com[2].

Partners & clients

- 17 Platform integrations. Amongst them Google[3], Hedera[4], Harmony[5], Web3[6], Kaleido[7].
- 100+ Smart Contract integrations like Oracle[8], Synthetix[9], OpenLaw[10], OpenZeppelin[11].
- Available in 8 of most used frameworks, specially Truffle which is the most popular by far.
- Chainlink alongside with Intel, Microsoft, IBM and others[12] are developing the "Trusted Computation Framework" allowing secure off-chain computations using TEE's like Intel SGX.

FULL LIST (updated until August 2019) of platforms, integrations, frameworks, clients & partnerships here [13]

What Chainlink has to offer

Smart contracts require middleware to connect them to real-world data. Importantly, this data will trigger a contract's outcome, thus creating the need for data input with high reliability.

No matter if you are a startup or a big corporation, Chainlink, as decentralized, oracle middleware, will provide your smart contract with provably secure access to data feeds, APIs and payments.

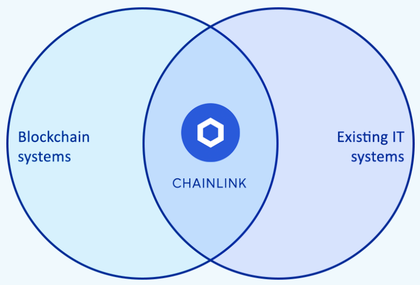
- **A developer** can quickly build and launch their own Chainlink to sell any API to smart contracts while the business can still sell their API through their usual interface business interface. By creating a new Chainlink as a developer, you'll be paid by making something thousands of smart contracts will rely on.

- **Larger enterprises** can partner with Chainlink to offer any existing APIs for purchase by smart contracts. Quickly and easily sell your company's data and any of your other APIs using Chainlink. Provide millions of smart contracts the ability to purchase your services directly.

Use cases

Access to external data enables an entirely new wave of functionality for smart contracts. Connected smart contracts have a limitless potential, covering a wide variety of sectors:

- Money and Finance
- Payments
- Insurance
- Supply chain
- Government
- Enterprise Systems
- Authorization and Identity
- Utilities
- Gambling



A HIGHLY RECOMMENDED READ ABOUT USE CASES: 44 ways to improve your smart contract[14]

Feeding decentralized blockchains with centralized data feeds is pointless. Chainlink provides reliable, tamper-proof I/O on ANY blockchain.

Achieving decentralization

Is it really possible to achieve truth in a world where you can't trust your souces? Chainlink achieves this by being a NETWORK of oracles. Data requested is served by multiple oracles run by different node operators that are incentivized to provide proper data.

By selecting several data sources (nodes) you provably increase the chances of getting a highly probable truth. Nodes aggregate their response to reach an agreement before data is sent to the smart contract (SC). Furthermore, nodes work by reputation. Hence, you ensure the SC's security not only by selecting a high number of nodes, but also by selecting highly reputable nodes to feed data. See Chainlink market[15].

LINK token utility

LINK is used as collateral to maintain the network security and maintain the incentives of the network. The token will be used for:

1. Paying node operators for serving data to SCs.
2. Node operators place deposits (collateral or stake) as required. by contract creators. In order to ensure they will behave correctly.

LINK is an ERC677-token developed specifically for Chainlink and integrated into Ethereum. An ERC677 is just an ERC20 token but adds the native capability so that payment and data retrieval is triggered with one transaction.

The LINK token is an Ethereum token but in case of need, it can be moved to any other blockchain platform. Chainlink is not tied to Ethereum.

Chainlink Token Distribution

There is a fixed quantity of LINK tokens: 1000M

- 350M were sold at token sale.
- 350M for incentivizing node operators (solves chicken or egg problem of bootstrapping a new network through subsidies).
- 300M to the project (for continued development so they don't have to take fees)

Why not just use ETH instead of LINK?

- Limited number of LINK: inelastic supply.
- The bigger the network, the more LINK tokens locked as collateral*. Hence LINK will be scarce. *Staking is not mandatory (see customization).
- Node operators need to stake LINK tokens.
- Node operators always paid in LINK tokens.

If LINK is an Ethereum token, does it only work with Ethereum?

No, Chainlink is blockchain agnostic. ANY blockchain can easily write an external adapter so they can call Chainlink. LINK token pays/cuts stakes to node operators in order to incentivize trustworthy responses from the network.

Blockchain agnostic

Chainlink can serve data to ANY blockchain. LINK token is an Ethereum token but the Chainlink network can serve data to any blockchain. The token is just the way to pay node operators to ensure reliable data delivered.

There are two ways to integrate Chainlink:

- Anyone can write an adapter[16] for any platform with very LOW EFFORT to access Chainlink network data. Example here[17].

- Deploying Chainlink contracts in the new blockchain: More complex as it requires some way to bridge to the token (likely what polkadot will be doing since polkadot will have an Ethereum mainnet bridge).

Blockchains with adapters to Chainlink already implemented:

- Hedera Hashgraph
- IOTA
- Zilliqa
- Polkadot (In progress)

Customizing data & security

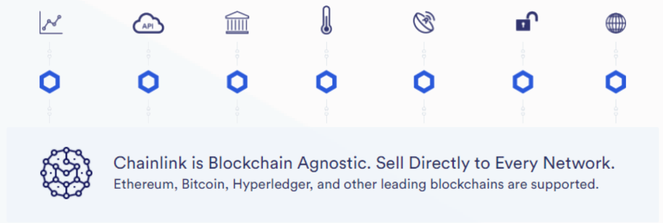
Flexibility largely comes from the "Service Agreement" (SA) model: Any developer can connect/build any oracle network that can fit their exact needs (Note: SA's are not live yet).

Customization of a wide range of parameters:

- Which /# of nodes
- Which /# of data sources
- Node Payments
- Collateral requirements
- Reputation requirements
- Slashing conditions
- Node certification
- Crypto/fiat settlement
- TEEs (See below "What is a TEE?")
- Mixicles

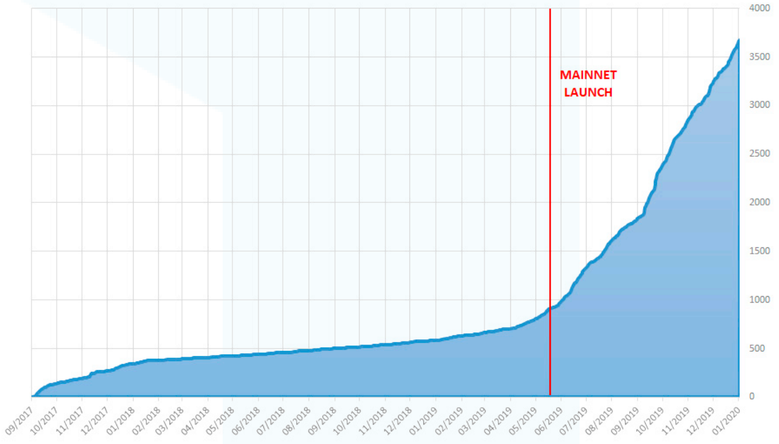
Open source & audited

- Code is open source (here[18]).
- Development publicly traceable (here[19]).
- 4 independent audits:
  - 3 on main contracts (here[20]).
  - 1 on Aggregator contract (here[21]).
  - 1 on Mixicles (in progress).



Network usage

Growth of Chainlink related smart contract addresses is an indication of increased network utility and developer interest.



Total number of smart contract addresses that have ever received LINK vs. Date each contract recevied LINK for the first time.

Permissioned or permissionless, public or private all blockchains need a trustworthy oracle to be truly useful

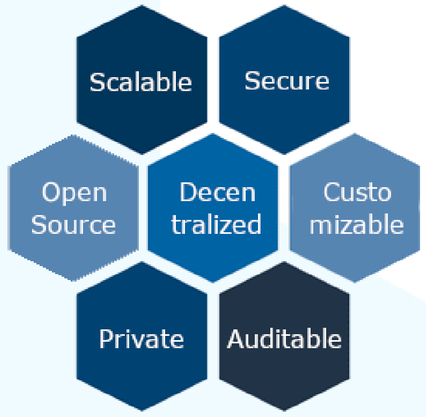
First mover advantage

- 1st decentralized oracle service.
- Long-standing connections to industry leaders (Swift & Oracle[22]) & leading research companies (Gartner[23] & Capgemini[24]).
- Network effects: Chainlink's large number of clients will attract future ones.

Competitors

- **Direct**: Decentralized oracles which have not yet reached critical mass. Band protocol[25], Tellor[26], Compound OOS (includes Chainlink as feed), Doracle from iExec (no clients) although iExec partnered with Chainlink[27] on Jan'20.
- **Indirect**: Centralized oracles like Provable[28](uses Chainlink as feed).

New competitors will emerge. They will struggle to achieve the same level of security as Chainlink's quickly growing, heterogeneous network. Competitors will also have a hard time achieving network effects without the 1st mover advantage.



Strong community

- The Chainlink community is one of the largest, best educated, most creative communities in the DLT space, renowned for its meme art.
- An official Chainlink community advocate program already exists in multiple cities acrossthe world. List of cities here[29].
- Official discord[30] & gitter[31] to reach the team.

Team

- 25 people team[32]
- 6 advisors, amongst them:
  - T. Gonser (ex-CEO Docusign). Article[33]
  - Ari Juels (co-creator[34] Proof of Work)
  - Evan Cheng (Facebook[35] R&D Dir & LLVM author at Apple)
  - Hudson Jameson (Ethereum[36])
  - Andrew Miller (consensus researcher[37])
- Currently, 13 open positions. Careers here[38]
- No hype from the team.

A glance at the tech behind Chainlink

1. Privacy & auditability: Mixicles

Mixicles is essentially a mixer that uses oracles to enable on-chain privacy to public blockchain smart contracts. The contract is split into two parts, where the sensitive data is computed off-chain, and the sensitive data is private on-chain. Mixicles offer:

1. Mixicles enable financial txns to be **private yet auditable to regulators**.
2. Mixicles are agnostic and will be used for Bitcoin as well.
3. Mixicles will be the genesis for the creation of confidentiality preserving DeFi instruments.

Mixicles is currently in audit phase. Highly recommended article here[39].

2. Low costs & scalable: Threshold signatures

Threshold signatures (TS) are being implemented in Chainlink which allows batching requests reducing costs (gas) while at the same time not clogging the network.

How can this be achieved? Threshold Signatures pave the way for the oracle dilemma: One wants thousands of witnesses to each datum, but that costs a lot of gas due lots of transactions.

Threshold signatures, let oracles talk to each other off-chain, to agree on an observation and aggregate & respond to the request using only one on-chain transaction. If you want to dig ore on TS, here is a nice article[42] .

3. Trusted Computing Framework

The Trusted Compute Framework (TCF) is way for enterprises to use trusted execution environments (TEEs) to secure off-chain computations. Chainlink ensures that the data being delivered from each end is encrypted and tamperproof.

Typically on-chain computation is reduced to very simple computations. TCF allows shifting complex computations from on-chain to off-chain (on-premise or in cloud VM's) and once finished post the results back on-chain while keeping verification, attestation verification.

Chainlink is part of the "Hyperledger Avalon Trusted Compute Framework" amongst Intel, IBM, Microsoft, Alibaba, and Banco Santander.
See Intel Press Release[40] & Article[41].

4. Staking (incentivizing good data)

In short, staking is when nodes collecting data for a smart contract stake a predetermined amount of LINK as collateral.

- In case nodes fail to deliver reliable data or provides it in an untimely manner, they are penalized by losing an amount of the staked LINK tokens.
- When nodes provide reliable, timely data to an oracle assignment, they are paid a fee in LINK. Article[43].

This is the way Chainlink network incentivizes the good and honest behaviour of nodes.

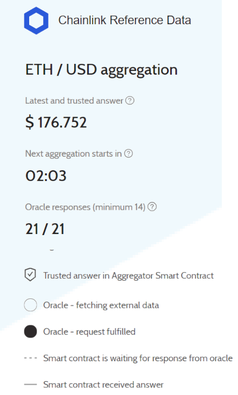
Together these innovative pieces of technology provide the most advanced oracle solution to date

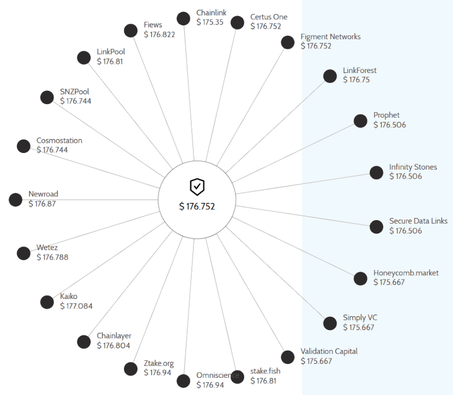
Chainlink does not compete with other blockchain platforms, it improves them

DeFi & Chainlink

DeFi (Decentralized Finance) is currently one of the fastest growing sectors in the decentralized ecosystem. DeFi consists not only of decentralized exchanges but also lending platforms and derivatives that run in a fully decentralized manner. The business model for the DeFi sector require 100% secure and accurate price feeds of all assets. In DeFi, as in finance in general, security, reliability and reputability are equally paramount for profitability. See this highly recommended article[44] from team about DEFI.

Chainlink is currently providing the reference data for 36 assets or pairs like EUR/USD. Those price feeds are already being used by Synthetix (top #2 locked USD value), Aave, Ampleforth and under study by dy/dx (top #6). Data from: defipulse.com[45] | exploring.link[46] | reference ETH/USD





Enterprise Ethereum Alliance & Chainlink

The Enterprise Ethereum Alliance (EEA)[47] is a member-driven standards organization whose charter is to develop open, blockchain specifications that drive harmonization and interoperability for businesses and consumers worldwide. Chainlink belongs to EEA since 2017 alongside with very well known enterprises. In January 2020, EEA creates the Mainnet Integration for Enterprises 'EMINENT' taskforce, spearheaded by Chainlink and others[48]. The focus of this work group is to build open source available reference implementations and guidelines for Ethereum mainnet integration with enterprise "systems of record". In other words, the goal is to achieve an standard which allows connecting business backends (CRMs & ERPs) to Ethereum mainnet.

ENTERPRISE ETHEREUM ALLIANCE · cisco · CREDIT SUISSE · BBVA · Deloitte. · THOMSON REUTERS · intel · bp · HYPERLEDGER · J.P.Morgan · ING · UBS · Santander · Microsoft · AMD · +178 more

Interesting Highlights

- Chainlink was selected by the World Economic Forum's Tipping point report[49] as the "Shift in action" for smart contracts.
- Chainlink has long been member of IC3[50], the leading academic research initiative for DLT. IC3 Members alongside Chainlink are JPMorgan, Microsoft, Cisco, Siemens, Intel.
- About ISDA (International Swaps & Derivatives Association) : On January 2020, BAPI[51] was announced, a bilateral smart derivatives platform using technology such as **a standard ISDA template**, Ethereum, OpenLaw, Chainlink and Kaleido_io. Co-developed by Carlos Matilla, Executive Director at Santander Investment Bank.
- Chainlink is currently working with SWIFT[52], which allows interbank messaging. As of 2015, SWIFT linked more than 11,000 financial institutions in more than 200 countries and territories, with over 32 million messages per day.
- Sunny King is the inventor of Proof of Stake and current CEO of VSYSCoin. Read here[53] what he says about Chainlink's collaboration.
- If you are a developer, consider looking at Chainlink's documentation[54].
- The Chainlink protocol natively supports ENS domains which abstracts away hexadecimal addresses into short, simple domains like oracle.linknode.eth
- In Jan 2017, Professor Klaus Schwab, Founder and Chairman of the World Economic Forum, wrote a book called The Fourth Industrial Revolution. In this book, Schwab describes the potential of Chainlink (See here[55])
- Chainlink is the only ICO funded Ethereum token available to New York investors (via Coinbase). NYC laws are one of the toughest for trading.
- Chainlink acquired "Town Crier" in order to be expand the possibilities of their Oracles network with TEEs natively embedded. (Forbes article[56] | More info[57]| * What is a TEE?)
- Chainlink is not a blockchain, nor does it compete with them. It seeks allowing trusted data and interoperatility amongst blockchains.
- Chainlink has two market places:
  1. market.link[58], a marketplace allowing anyone to offer their nodes, adapters and the jobs they offer. Anyone can see the list of nodes and filter by different criteria.
  2. honeycomb.market[59] allows devs to connect their smart contracts & decentralized apps to a wide variety of paid APIs using multiple high-quality Chainlink nodes from operators such as Certus.One, LinkForest & Cosmostation. Testnet APIs free.
- Even centralized oracles like 'Provable' can keep their business of selling their data as usual and create an adapter and still sell it as another available source in the Chainlink network. Hence, they both earn money selling data the centralized way as well as via the Chainlink network.
- This is the only remark regarding Chainlink as an investment: The Chainlink token LINK has been the BEST ROI investment asset in the top 100 of 2019, outperforming ALL other crypto assets, including Bitcoin. (See here[60]).

* **What is TEE?** A trusted execution environment (TEE) is a highly secure, boxed-in computational space in modern CPUs, allowing for the execution of computations, inaccessible even to the computer's owner.

CHAINLINK
SMART CONTRACTS & REAL WORLD

http://chain.link | http://smartcontract.com

COORDINATED BY: @CRYPTODAVID_ SPECIAL THANKS TO: @HAHUS | @CHAINLINKP | @CHAINLINKGOD | @DLTPANDU | @CRYPTOSPONGE3 | @CRYPTO___ORACLE | @KWSANTIAGO | @THELINKMARINE1 | @DAGCHADHEADROOM | THE INVISIBLE DESIGNER

Whitepaper[36]
Community: 'The missing piece to the god protocol'[37]
Community: 'An in-depth look at LINK token'[38]
Devs: Chainlink technical documentation[39]