

Smart contracts & the real world

Overview

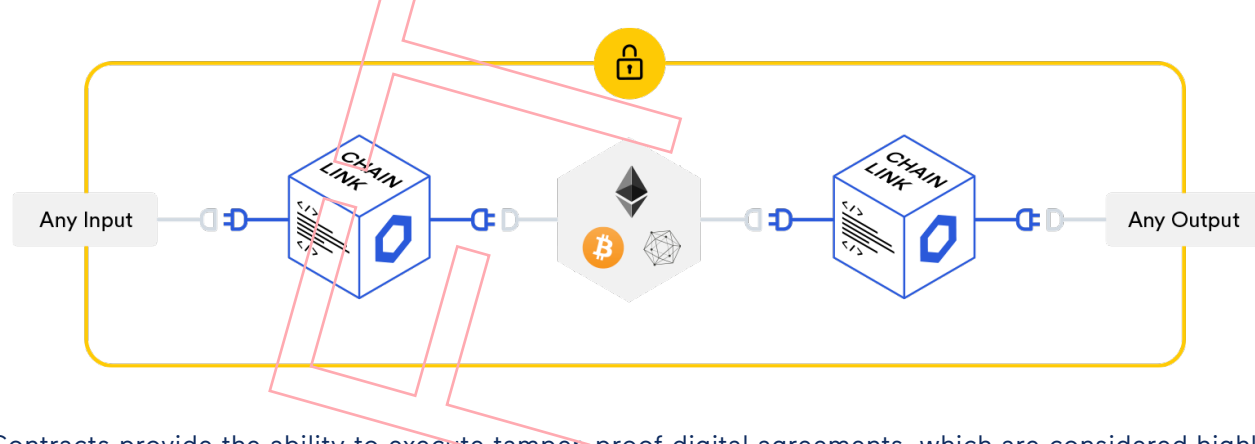


Historically, the blockchains on which smart contracts run cannot support native communication with external systems, and the potential that smart contracts provide have been throttled by their inability to connect off-chain.

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.

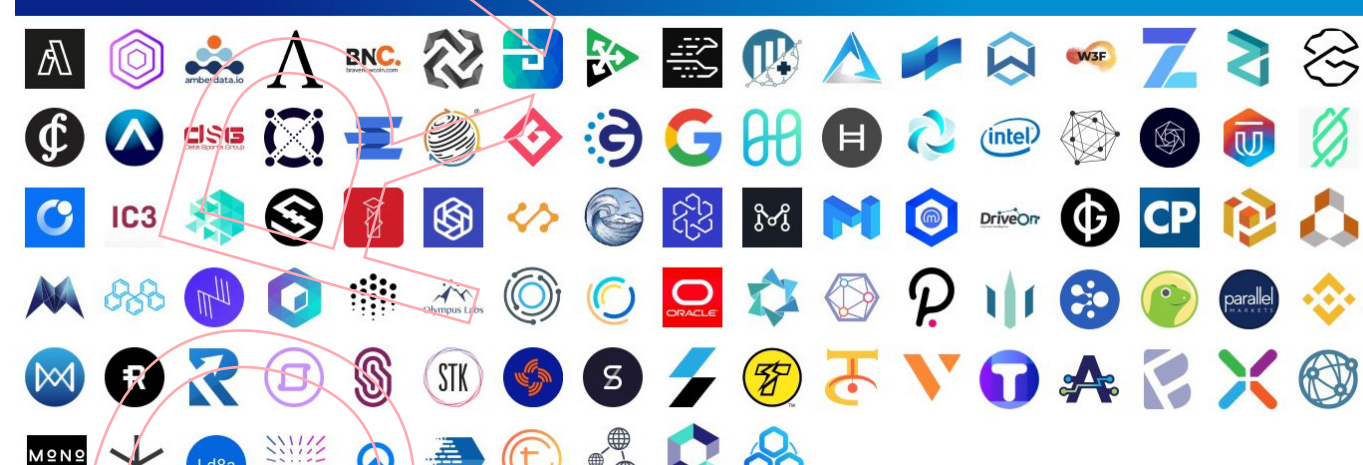
To fill this gap, Chainlink was developed as the first decentralized oracle that can provide external data to smart contracts. As a result, the security and determinism of smart contracts can be combined with the knowledge and breadth of real-world external events. Chainlink will provide your smart contract 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://chainlink> & <http://smartcontract.com>.



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 connection to external data that is provably secure end-to-end.

Partners & clients



- 17 Platform integrations. Amongst them [Google](#), [Hedera](#), [Harmony](#), [Web3](#), [Kaleido](#).
- 78 Smart Contract integrations. Amongst them [Oracle](#), [Synthetix](#), [V Systems](#), [OpenLaw](#), [OpenZeppelin](#)
- Available in 8 of most used frameworks, specially Truffle which is the most popular by far.
- Chainlink alongside with [Intel](#), [Microsoft](#), [IBM](#) and [others](#) are developing the "Trusted Computation Framework" allowing secure off-chain computations using TEE's like Intel SGX. (* What a TEE is?)

FULL LIST (updated until August) of platforms, integrations, frameworks, clients & partnerships: [Here](#)

Having decentralized blockchains & feed with unsecure data is pointless. Chainlink provides reliable tamper-proof I/O on ANY blockchain.

How Chainlink achieves decentralization?

Is it really possible to achieve truth in a world where you can't trust your sources? Chainlink achieves this by being a NETWORK of oracles. Data requested is served by multiple oracles ran by different node operators that are incentivized to provide proper data. By selecting enough data sources (nodes) you get the truth in a provable way. Furthermore Chainlink nodes have a reputation, hence you can get more security not only by selecting more nodes that aggregate their response and reach to an agreement but also by selecting high reputable nodes. See [chainlink market](#).

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 retrieving data for smart contracts.
2. Node operators place deposits (collateral or stake) as required by contract creators. In order to ensure they will behave correctly.

The LINK token is an ERC677 and was 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.

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 chainlink team (for continued development so they don't have to take fees).

Why not just use ETH instead of LINK?

- There are a limited number of LINK: inelastic supply.
- The bigger the network is, the more LINK tokens will be locked as collateral. Hence LINK will be scarce.
- Node operators need to stake LINK tokens.
- Node operators are always paid in LINK tokens.

If LINK is an ethereum token, it only works with Ethereum?

No, Chainlink is blockchain agnostic. ANY blockchain can easily write an external adapter so they can call chainlink. LINK is just a medium to pay / cut stakes to node operators in order to incentivize the good responses from the network.

Blockchain agnostic

Chainlink can serve data to ANY blockchain. The fact that LINK token is an Ethereum token doesn't mean the Chainlink network cannot 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](#) for their platform with very LOW EFFORT to access Chainlink network data. [See here an example](#).

- Deploying the 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 that already have adapters to chainlink are:

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

Customizing data & security

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

Customization of a wide range of parameters:

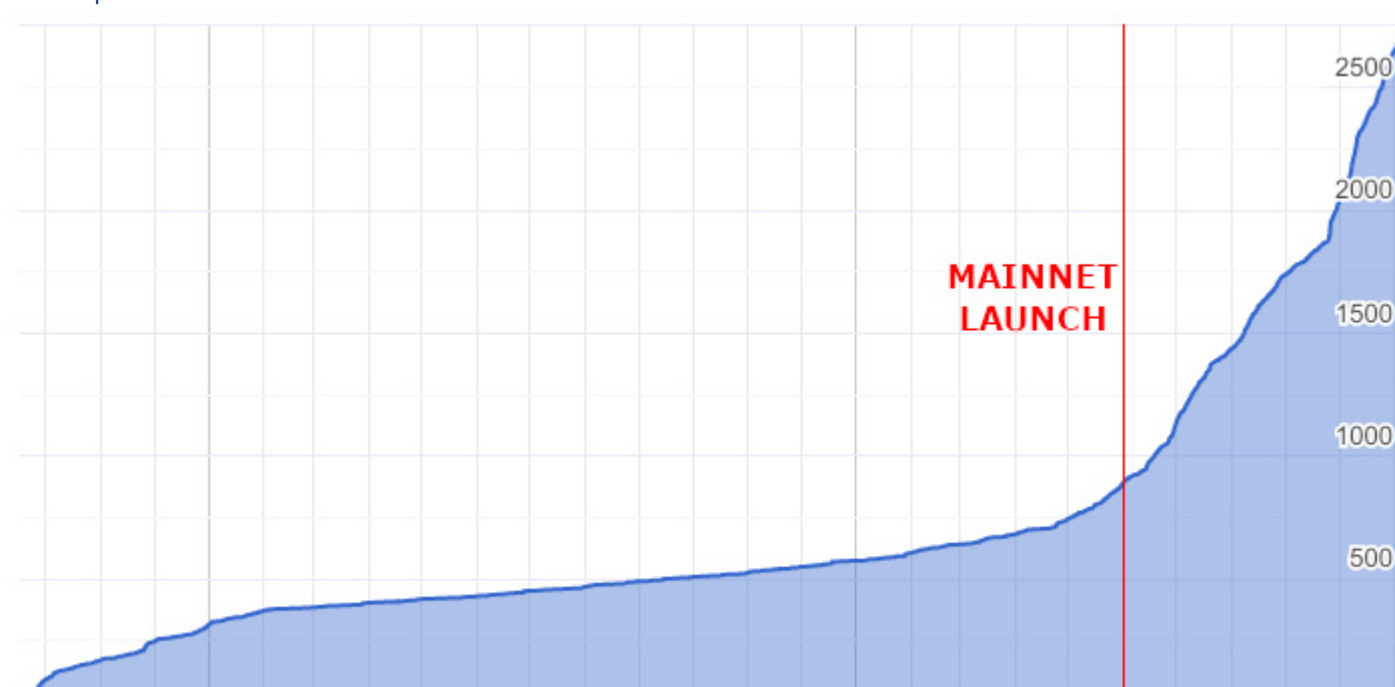
- Which /# of nodes
- Which /# of data sources
- Node Payments
- Collateral requirements
- Reputation requirements
- Slashing conditions
- Node certification
- Crypto/fiat settlement
- TEEs (What is a TEE?)
- Mixicles

Open source & audited

- Code is open source ([here](#)).
- Development publicly traceable ([here](#)).
- 4 independent audits:
 - 3 on main contracts [here](#).
 - 1 on Aggregator contract audit here.

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 received LINK for the first time.

First mover advantage

- 1st decentralized oracle.
- Early connections to industry leaders (swift & oracle) & leading research companies like [gartner](#) & [capgemini](#).
- Network effects: Great number of clients attract future ones.

Competitors

- **Direct:** Decentralized oracles which have not yet reached critical mass. Doracle, [band protocol](#).
- **Indirect:** Centralized oracles like [provable](#).

New competitors will appear, they will struggle with having level of security of such a big and heterogeneous network as Chainlink's one. Difficult to achieve Network effects as they won't have the 1st mover advantage.



Strong community

- Chainlink community is one of the biggest & well educated communities in the DLT space while at the same time enjoying fun art.
- Official [discord](#) & [gitter](#) to reach the team.
- No hype from the team.

Team

- 18 people [team](#) | Careers [here](#)
- Amongst team and advisors:
 - Tom Gonser (exCEO docusign). [Article](#)
 - Ari Juels ([co-creator](#) Proof of Work)
 - Evan Cheng ([Facebook](#) R&D Dir & LLVM co-creator at Apple)
 - Hudson Jameson ([Ethereum](#))

Use cases

Access to external data opens up a whole new wave of functionality for smart contracts.

Limitless potential of connected smart contracts, ranging a wide variety of sectors like:

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

Chainlink allows companies:

- Selling their API data to Smart Contracts through Chainlink nodes while they can still sell their API through their usual interface business as usual. Important note: Companies do NOT have run their own nodes for this.
- Companies can automate their contracts with clients/business partners using chainlinked smart contracts.

Insurance sector, derivatives & banks, are already investigating the application of blockchain technology through considerable investments. This is the case of [SWIFT](#) or insurance companies created the first [blockchain-centered insurance consortium](#).

Those sectors seek different goals: from revolutionizing auditing to to reducing costs of 3rd party trust providers or increasing transparency.

A HIGHLY RECOMMENDED READ: [44 ways to improve your smart contract](#)

Feature Needs by Customer Segment

Business Process Systems	Financial Institutions
- CRM Providers - HCM Providers - SaaS vendors - Payment Service Providers	- Insurance - Financial Derivatives - Banking - Credit/Lending
Today's Blockchain dApps	Scaled Blockchain dApps
- Synthetix - Compound - Maker	- Decentralized consumer applications - Decentralized finance - Decentralized Autonomous Organisations (DAOs)

↑
TEE
Integration
Threshold
Signatures
Aggregation
contract(s)
Initial
Implementation
Chainlink
Protocol
Development

Node Incentive Program → Data/node Marketplace → Professional Validators → Base Layer Scaling → Ecosystem Development

Selecting a phrase from community external reviewers. Something like "Chainlink does not compete with other bchain platforms, it boosts them."

A glance to the tech behind

1. Privacy & auditable: 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, see pic related.
3. Mixicles will be the genesis for the creation of confidentiality preserving DeFi instruments.

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. One possible use case with this is a random number generator that produces truly random numbers in an easily accessible fashion, thereby creating a virtually viable one-time pad. [Intel P.R](#) & [Article](#)

2. Low costs & scalable: Threshold signatures

Threshold signatures (TS) are being implemented in Chainlink which allows batching requests reducing costs + not clogging the network. How? TS pave the way for the oracle dilemma: One wants thousands of witnesses to each datum, but that costs a lot of gas.

So, TS, lot oracles talk to each other Offchain, to agree on an observation and aggregate & respond to the request using only one on-chain transaction.

4. Staking (aka: incentive good data)

Staking is amount of LINK as collateral in case they fail to deliver reliable data. If they provide reliable data, they are paid in LINK fees. [Article](#)

Interesting Highlights

- Chainlink was selected by the World Economic Forum's [Tipping point report](#) as the "Shift in action" for Smart Contracts.

- Chainlink has long been member of [IC3](#), the leading academic research initiative for DLT. Members of IC3 along with Chainlink are JPMorgan, Microsoft, Cisco, Siemens, Intel.

- Chainlink is member of the [Enterprise Ethereum Alliance](#), alongside with banks, tech companies and others.

- Chainlink is currently [working with SWIFT](#), which allows interbank messages. As of 2015, SWIFT linked more than 11,000 financial institutions in more than 200 countries and territories, who were exchanging an average of over 32 million messages per day.

- Sunny King is the inventor of Proof of Stake and currently CEO of VSYSCoin. Read [Here](#) what he says about their collaboration with Chainlink.

- If you are a developer, consider taking a look to the [Chainlink's documentation](#).

- Chainlink protocol natively supports ENS domains which abstracts away hexadecimal addresses into short simple domains like [oracle.linknode.eth](#)

- 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 writes about the potential of chainlink (See [Here](#))

- 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 able to expand the possibilities of their Oracles network with TEE's natively. ([Forbes article](#) | [More info](#) | * What a TEE is?)

- Chainlink is not a blockchain. It does not compete with blockchains. It seeks allowing trusted data and interoperability amongst blockchains.

- Chainlink has 2 market places:

1. [market.link](#), a marketplace allowing anyone to offer their nodes, adapters and the works they offer. Anyone can see the list of nodes and filter by different criteria.

2. [honeycomb.market](#) 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 CertusOne, LinkForest & Cosmostation. All testnet APIs are free.

- Even centralized oracles like 'provable' can keep their business of selling their data as usual and create and adapter to sell it also as another available source in the chainlink's network. Hence earn money from the centralized way and chainlink's network.

- This is the only thing talking about chainlink as an investment: It has been the BEST ROI asset in top100 for the whole last 12 months. (See [Here](#)).

* **What a TEE is?** It's a highly secure environment in modern CPUs to securely execute computation where not even the owner of the machine would see the data/results from these computations

RESOURCES

- White paper
- Community: 'The god protocol'
- Community: 'An In-depth look at LINK token'
- Community: 'Add extra by community'
- Devs: Chainlink technical documentation

CHAINLINK
SMART CONTRACTS & REAL WORLD

<http://smartcontract.com> <http://chainlink>

COORDINATED BY:
- @CryptoDavid_

SPECIAL THANKS TO:
- \$DAG community for providing us the template for this fact sheet.

- @ChainLinkP
- @ChainLinkGod
- @DLTPandu
- @Kwsantiago
- @TheLinkMarine1
- @CryptoSponge
- @Kyleodesign
- @Crypto__Oracle