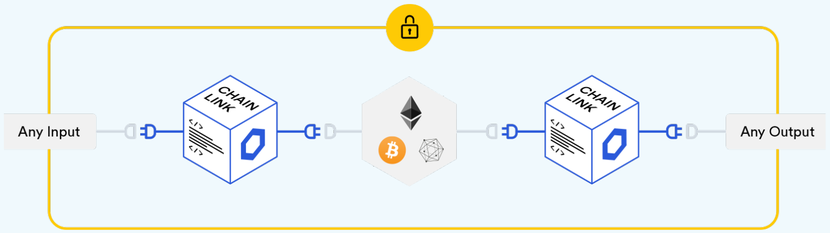
Smart contracts & the real world

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 the contract relies upon also need to be secure. Chainlink provides reliable and secure end-to-end connections to external data.



Overview

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

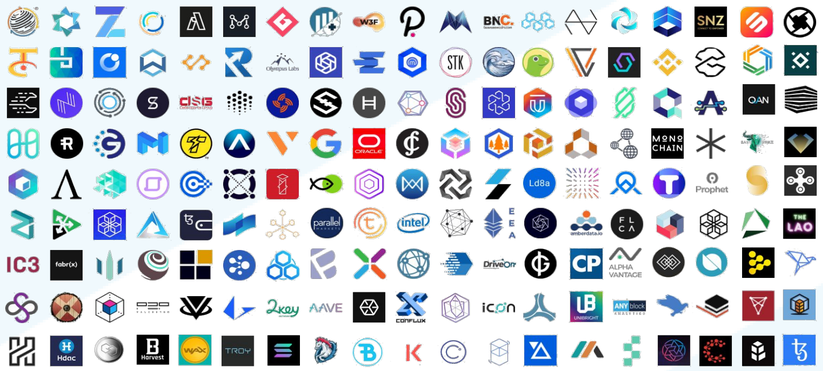
Today, the solution to this problem is to introduce a new functionality, called an **'ORACLE'**, that provides connectivity to the outside world. However, oracles to-date are centralized services, meaning any smart contract using such services has a single point of failure, which nullifies any benefits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

To fill this gap, Chainlink (token sale in '17, launched in '19) was developed by SmartContract.com (founded in '14) as the first decentralized oracle framework that can provide external data to smart contracts on any blockchain. As a result, the security and determinism of smart contracts can be combined with the knowledge and breadth of real-world external events. Chainlink provides your smart contract with access to any external data needed to connect your smart contract with.

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

Partners & clients

- 30+ Price Feeds on Ethereum Mainnet utilized by 14+ DeFi projects in production.
- 100+ integrations including Polkadot[3], Tezos[4], Synthetix[5], Aave[6], Openlaw[7], Web3[8] and more.
- Partnered with large enterprises such as Google[9], Oracle[10], SWIFT and more.
- Available in many development frameworks, specifically Truffle which is the most popular by far.
- Chainlink alongside with Intel, Microsoft, IBM and others[11] are developing "Hyperledger Avalon" allowing secure off-chain computations using TEE's like Intel SGX.



FULL LIST of platforms, integrations, frameworks, clients & partnerships https://chainlinkecosystem.com [12]

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 inputs with high reliability and accuracy.

No matter if you are a startup or a large enterprise, Chainlink as decentralized oracle middleware, can provide your smart contract with provably secure access to external data feeds, *APIs and payments.

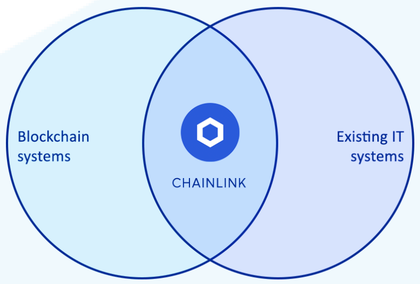
- **Any developer** can quickly build and launch their own Chainlink to sell any API to smart contracts while the data provider sells their API through their usual interface business as usual. By creating a new Chainlink as a developer, you'll be paid by making something thousands of smart contracts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

- **Larger enterprises** can partner with Chainlink to offer existing APIs for purchase by smart contracts. Quickly and easily sell your company's data and any of your other APIs using Chainlink. Provide countless smart contracts with 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 limitless potential covering a wide variety of industries:

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



Essentially, most of the visionary and useful use cases people came up with when being enthusiastic about Ethereum depend on data that is unavailable natively to blockchains. To name a few examples: derivatives based on real-world commodities and equities (Google prototype[13]), automatic insurance payout when a flight arrives late or when a flood occurs, triggering global banking fiat transfers based on the outcome of a trade finance smart contract, auto-rebalancing portfolios based on trading indicators such as RSI & EMA or transaction status, different types of lending products without middlemen based on over/undercollaterization or credit score, off-chain computation via cloud infrastructure and more.

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

*** I/O stands for Input/Output. In the blockchain context the inputs that will enter into the smart contracts and the outcomes from the execution of the smart contracts triggered by those inputs.**

*** An API allows programs communicate with another. TradingView uses a Binance API to fetch price/volume data to display it on their own site. Uber was built using payments, GPS, SMS and KYC APIs.**

Feeding decentralized blockchains with centralized data feeds is pointless

Chainlink provides decentralized, 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. Requested data is delivered by multiple oracles run by different independent node operators, using mutiple data source APIs, that are incentivized to provide proper data.

By selecting several nodes and data sources, you provably increase the chances of getting a highly probable truth. Using Threshold Signatures, nodes will aggregate their responses off-chain in order to reach an agreement before the final data point is sent to the smart contract on-chain. Furthermore, nodes are selected by reputation and previous performance. Hence, you ensure the smart contract's security not only by selecting a high number of nodes, but also by selecting highly reputable nodes to feed data. **You can see an step-by-step example on how Chainlink works in page 3.** See also Chainlink market[15].

LINK token utility

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

1. Paying node operators for delivering off-chain data to smart contracts.
2. Node operators use LINK as collateral (stake) when required by contract creators in order to ensure they will behave correctly. Malicious or non-responsive nodes will have their collateral slashed & reduced reputation as a punishment.

LINK is an ERC20 token with the ERC677 standard on top. ERC677 was developed specifically for Chainlink and integrated into Ethereum. It adds the TransferAndCall capability enabling payment & data retrieval within a single transaction.

LINK is an Ethereum token but in the worst case scenario, it can be transfered to any blockchain platform. Chainlink is not limited to just Ethereum.

Chainlink Token Distribution

There is a fixed quantity of LINK tokens: 1000M

- 350M were sold at token sale (fundrasing and initial distribution of tokens).
- 350M for incentivizing node operators through subsidies (solves chicken or egg problem of bootstrapping a new network).
- 300M to SmartContract Chainlink Ltd (for continued development so they don't take fees)

Why not just use ETH instead of LINK?

There are several reasons to use LINK over ETH:
- Ties the incentives of node operators together with the health of the overall Chainlink network.
- Isolates the security and economic bandwidth (staked LINK) from external factors outside the control of Chainlink stakeholders.
- If a major network attack occured, LINK collateral then becomes worthless hurting the attacker, this is not true with an unrelated asset (ETH).
- Stablecoins wouldn't work either as they are either backed by fiat & thus censorable or rely upon oracles to function.
- Growing demand for LINK combined with a shrinking supply (due to staking) creates a positive feedback loop where the increased adoption boosts the price of LINK, thus increasing economic bandwidth and enabling more adoption to be supported.
- Chainlink is blockchain agnostic & needs a token than can be easily bridged between blockchains.

If LINK is an ERC token, works only with Ethereum?

No, ANY blockchain can easily write an external adapter to call Chainlink. See next section.

Blockchain agnostic

Chainlink supports ANY blockchain. LINK was created as an Ethereum token but the Chainlink network can serve data to any platform.

There are two ways to integrate Chainlink:

1. Any developer can create a simple external adapter[16] enabling any blockchain to request and receive external data from Chainlink nodes. Through this, LINK payments and staking collateral is still performed on Ethereum.

2. The LINK token can be bridged to another blockchain through LockDeposit contract enabling native LINK payment and staking support on any blockchain enabling applications outside of Ethereum to request data without the need for routing through Ethereum.

Deploying Chainlink contracts in a new blockchain and bridging the token is a more complex process requiring cross-chain transaction support and therefore some simple data requests are likely still to be funneled through Ethereum for simplicity.

Blockchains supported by Chainlink:

- Ethereum
- Tezos
- Polkadot
- Hedera Hashgraph
- Any EVM-enabled blockchain
- Zilliqa
- Kava/Cosmos
- Bitcoin
- Many more

Customizing data & security

Chainlink's flexibility largely comes from the "Service Agreement" (SA) model: Any developer can connect to or build an oracle network that fits their exact needs.

Customization of a wide range of parameters:

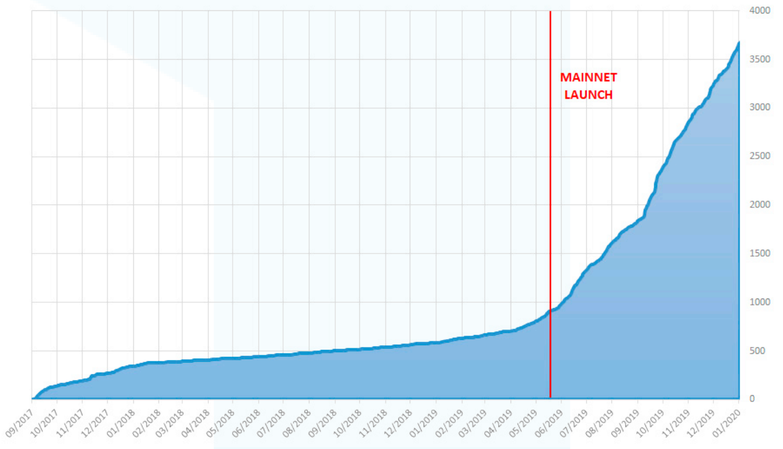
- Selection and number of nodes
- Selection and number of data sources
- LINK Node Payment amounts
- LINK Collateral requirements
- Minimum node reputation* requirements
- Slashing conditions
- Node certification
- Threshold signatures
- TEEs (See "*What is a TEE?")
- Mixicles

Node Reputation/Ranking*: Chainlink nodes have a 'reputation' factor. Chainlink clients will be able to require a minimum level of reputation for all the nodes. Node Reputation depends on these factors:

- Node availability (uptime)
- Correctness of responses
- Average time to respond
- Total number of assigned requests
- Total number of completed requests
- Total number of accepted requests
- Amount of penalty payments
- Amount of LINK held (staked)

Network usage

Growth of Chainlink related smart contracts is indicates increased network utility & 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 and DLT need a trustworthy oracle to be truly useful

First mover advantage

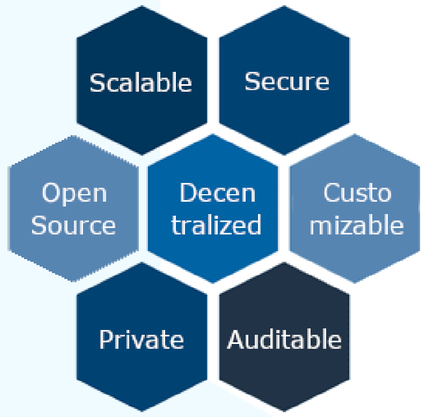
- First decentralized oracle framework.
- Long-standing connections to industry leaders (Swift, Google[17], & Oracle[18]), leading research consultants (Gartner[19] & Capgemini[20]) & enterprise consortiums (IC3[21], EEA[22], Baseline protocol[23] & Hyperledger[24]).
- Network effects: Chainlink's large number of clients, nodes & data sources attracts usage.

Competitors

- **Direct**: Alternative decentralized oracles which have little or no usage, inflexible and rigid customizability, have not yet reached critical mass, or is a homebrew and proprietary oracle solution. This includes Tellor[25], Witnet[26], Compound's OOS[27], Maker's OSM[28], Doracle[29] from iExec (integrated with Chainlink) & Band.

- **Indirect**: Centralized oracles like Provable[30] (partnered with Chainlink) and Rhombus[31].

New competitors will emerge and struggle to achieve marketshare since they will lack the large selection of nodes and data sources, subsidized oracle networks, time-tested security, first movers advantage and network effects.



Open source & audited

- Code is open source (here[32]).
- Development publicly traceable (here[33]).
- Bug bounty program (here[34])
- 4 independent audits:
  - 3 on main contracts (here[35]).
  - 1 on Aggregator contract (here[36]).
  - 1 on Mixicles (in progress).

Strong community

- The Chainlink community is one of the largest, best educated, most creative communities in the crypto space, renowned for its meme art and comradery.
- Official discord[37] & gitter[38] to reach the team.
- An official Chainlink community advocate program already exists in multiple cities and continents around the world. City list here[39].

Team

- 25+ people team[40]
- 6 advisors, amongst them:
  - Tom Gonser (Docusign founder). Article[41]
  - Ari Juels (formalized[42] Proof of Work; RSA chief scientist[43]; IC3 co-founder[44])
  - Evan Cheng (Facebook[45] R&D Dir & LLVM author at Apple)
  - Hudson Jameson (Ethereum Foundation[46])
  - Andrew Miller (Consensus researcher[47])

- Currently, 11 open positions. Careers here[48]
- No hype from the team, only professionalism.

*Note about competitors & 'Coinbase oracle': Although Coinbase being a big and reputable actor in this space, the service they provide is a price feed (not general oracle) and the results are not being written on chain. Therfore it cannot be considered a blockchain oracle nor competitor in the Oracle space.

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

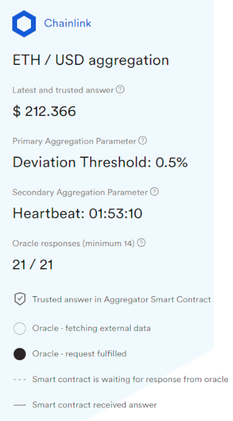
DeFi & Chainlink

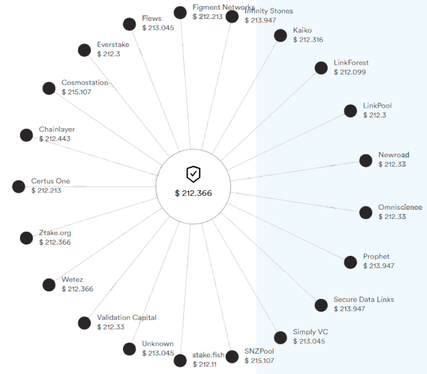
DeFi (Decentralized Finance) is currently one of the fastest growing sectors in the decentralized ecosystem. DeFi consists not only of decentralized exchanges but also lending platforms and derivatives that run in a fully decentralized and trustless manner.

Open finance is not about creating a new system from scratch, it's about democratizing the existing system[54] and making it more equitable using open protocols and transparent data. Traditional finance system has some drawbacks like slow cross-border remittances, high fees, censhorship/ discrimination ("you can't invest on unless you own 1M$), banks can freeze funds or even like in the financial crisis could crash banks.

The business model for the DeFi sector require 100% secure and accurate price feeds of all assets (90%+ of DeFi requires oracles). In DeFi, as in finance in general, security, reliability and reputability are all equally paramount for profitability. See this highly recommended article[55] 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[56] (top #2 locked USD value), Aave[57](top #5), Ampleforth[58] and under study by dy/dx[59] (top #7). Data from: defipulse.com[60], exploring.link[61] , reference ETH/USD[62], list of all feeds provided[63]





Live platforms using Chainlink

TOTAL VALUE SECURED
in 1st May 2020
158 M$

Synthetix
Synthetic assets
115 M$

Aave
Lend & Borrow
44 M$

DMM
DMM
Real World Assets
8 M$

Ampleforth
Commodity Money
5 M$

Loopring
DEX Protocol
5 M$

BZX
BZX
DEX Protocol
3 M$

A glance at the tech behind Chainlink

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

1. Privacy & auditability: Mixicles

Mixicles is essentially a mixer that uses external oracles to enable on-chain privacy for public blockchain smart contracts. The contract is split into two parts, where the sensitive data and business logic is kept off-chain with private settlement on-chain. Mixicles enable:

- Keeping private the contract business logic & the external oracle data & final payee result.
- Financial contracts are **private to the public but auditable to regulators**.
- Blockchain agnosticism & can be used in enterprise blockchains as well.
- A new generation of privacy preserving & scalable DeFi instruments.

Mixicles are currently under audit. Highly recommended article here[49].

2. Low cost & scalable: Threshold Signatures

Threshold signatures (TS) are being implemented in Chainlink which allows nodes to batch their responses off-chain substantially reducing transaction costs (gas) while minimizing the effects of blockchain network congestion.

How can this be achieved? Threshold Signatures pave the way to solving the oracle dilemma: One wants hundreds, thousands, even tens of thousands of witnesses to agree on a data point but that is expensive due to the growing amount of transactions needed.

TS enable oracles to talk to each other off-chain, agree on an observation, aggregate a single signature proving group observation and then respond to the original data request using only a single on-chain transaction. Article[52]

3. Trusted Computation Framework

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

Typically computation takes place on-chain and is very expensive. TCF instead allows contracts to shift complex computations from on-chain to off-chain systems (on-premise or in cloud VM's) and once finished post the results back on-chain all while keeping verification and attestation verification properties.

Chainlink is part of the "Hyperledger Avalon Trusted Compute Framework" amongst Intel, IBM, Microsoft, Alibaba Cloud and Banco Santander.
See Intel Press Release[50] & Article[51].

4. Staking Collateral (Direct skin in game)

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

- In the case nodes fail to deliver a reliable data point, provides it in an untimely manner, or doesn't deliver data at all, they are penalized by getting their LINK collateral slashed hurting nodes financially.

- When nodes instead provide a reliable, timely data point to an oracle assignment, they are paid a fee in LINK. They can withdraw the fees and keep their collateral or withdraw partially/totally their collateral too. Malicious or non-responsive nodes will have their collateral slashed & their reputation will be reduced as a punishment too. Article[53].

This is how the Chainlink network incentivizes honest behaviour and penalizes malicious behavior of nodes.

Chainlink and the standarization process

Chainlink is involved in several initiatives in order to harmonize and standarize blockchain technologies

1. Enterprise Ethereum Alliance & Chainlink

The Enterprise Ethereum Alliance (EEA)[64] 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 has been in the EEA since 2017 alongside with very well known enterprises. In January 2020, EEA created the Mainnet Integration for Enterprises 'EMINENT' taskforce, spearheaded by Chainlink and others[65].

The focus of this working 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 a 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

2. Baseline protocol & Chainlink

Baseline protocol, presented on March 2020 by big four Ernst & Young in collaboration with Microsoft, Consensys, AMD, Chainlink and others is an open source initiative that combines advances in cryptography, blockchain and open standards to deliver secure & private business processes at low cost via the public Ethereum Mainnet. The protocol will provide a common framework to enterprises that enable confidential and complex collaboration between them without leaving any sensitive data on-chain. See press release here[66].

EY · CONSENSYS · Microsoft · AMD

3. Hyperledger Avalon & Chainlink

In October 2019, Hyperledger introduced Hyperledger Avalon. It is a ledger independent implementation of the Trusted Compute Framework. It aims to shift in a secure manner the on-chain processing to off-chain (Cloud). Avalon is designed to mitigate the drawbacks of on-chain computation (scalability & confidentitality). It offloads the chain, increasing performance while still keeping integrity and attestation. Chainlink alongside with other partners such as IBM, Oracle, Microsoft and others is working on the Avalon specification.
Intel Press Release[67]

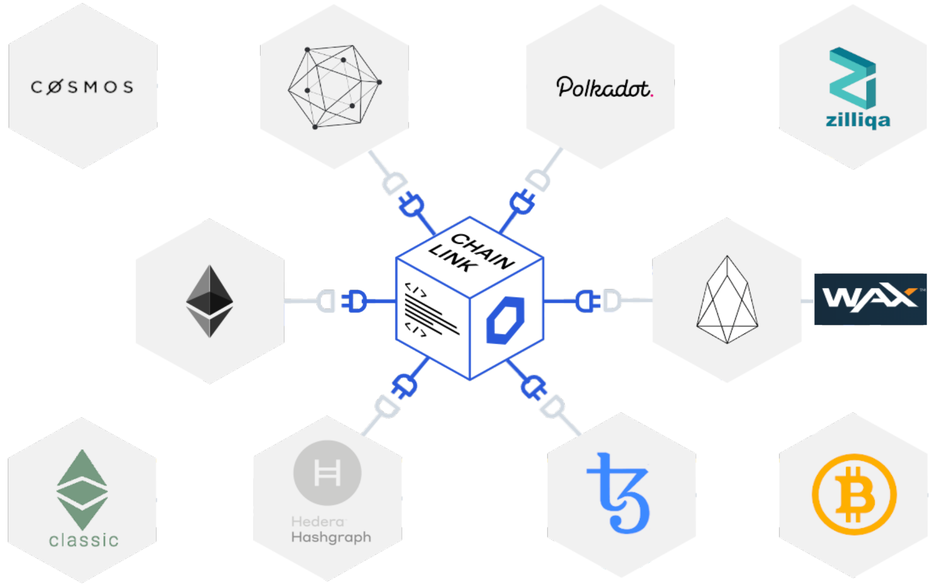
IBM · intel · Santander · Microsoft · ORACLE · Alibaba Cloud

*** What is TEE? A trusted execution environment (TEE) is a highly secure, hardware based isolated computational space in modern CPUs, allowing for the execution of private and attested computations, inaccessible to applications, the operating system, virtual machine manager, or even the computer's operator.**

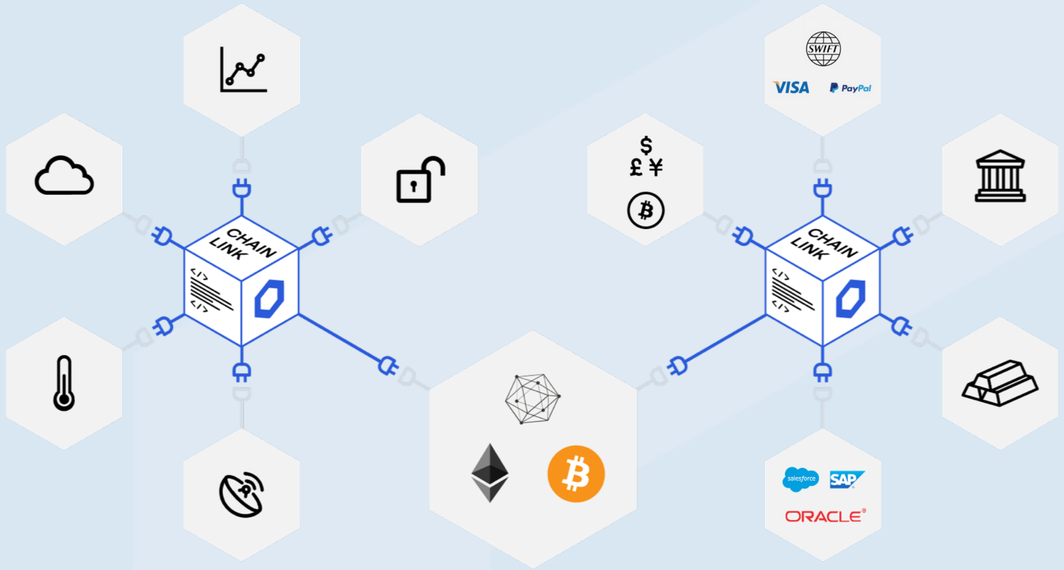
Some interesting highlights

- Oracle corp will be integrating Chainlink in Q3 2020 according to the Openworld 2020 conference by Oracle. Slides here[68].
- Chainlink was selected by the World Economic Forum's Tipping point report[69] as the "Shift in action" for smart contracts.
- Chainlink has long been member of IC3[70], the leading academic research initiative for DLT and cofounded by Ari Juels. IC3 Members alongside Chainlink are JPMorgan, Microsoft, Cisco, Siemens, Intel.
- About ISDA (International Swaps & Derivatives Association): On January 2020, BAPI[71] was announced, a bilateral smart derivatives platform using technology such as **a standard ISDA template**, Ethereum, OpenLaw, Chainlink and Kaleido. It was co-developed by Carlos Matilla, Executive Director at Santander Investment Bank.
- Chainlink is currently working with SWIFT[72], the global standard in interbank messaging. SWIFT is used by more than 11,000 financial institutions in more than 200 countries and territories, with over 32 million messages moving trillions of dollars each day.
- In January 2017, Professor Klaus Schwab, Founder & Chairman of the World Economic Forum, wrote a book called The Fourth Industrial Revolution. In this book, Schwab describes SmartContract.com as the tipping point for the "Shift in action" under "Bitcoin and the Blockchain." (See here[73]).
- There are 3 types of APIs: Private, partner or public. Two require passwords. Chainlink provides data from all three. Neither the direct competitors Tellor or Band can access data from private or partner APIs.
- Chainlink is listed US regulated exchanges Coinbase, Gemini and Kraken who offer LINK trading to New York investors. NYC financial security laws are some of the toughest in the world.
- Chainlink acquired IC3's "Town Crier" oracle in order to expand the possibilities of their decentralized oracle network with native TEEs support. (Forbes article[74] | More info[75] | * What is a TEE?)
- Chainlink has two major marketplaces:
  1. market.link[76], created by LinkPool, is a marketplace that allows anyone to list their nodes, adapters and the jobs they offer. Anyone can see this list of nodes and filter by different criteria.
  2. honeycomb.market[77], created by CLCG, allows developers to connect their smart contracts & decentralized apps to a wide variety of high quality paid APIs using multiple high-quality vetted Chainlink nodes from operators such as Certus.One, LinkForest & Cosmostation. Testnet APIs are offered free.
- Even centralized oracles like 'Provable' can keep their business of selling their data as usual by creating an external adapter and selling data as another available source in the Chainlink network. Hence, they both earn money selling data their regular centralized way as well as via the decentralized Chainlink network.
- This is the only remark regarding Chainlink as an investment: Chainlink has been the best performing cryptocurrency over the last 2.5 years. It's ROI is 1,700% higher than the average performing altcoin and +900% better than Bitcoin. (See here[78]).

Blockchains already supported by Chainlink



Any input. Any output. Any blockchain



Connect to any source of data feed / API

Public/private blockchains can support Chainlink

Send payments anywhere Connect to backend systems

Chainlink by examples & FAQ

An example of chainlink working (with Staking)

1. Bob wants trustless data for his smart contract, so he queries Chainlink.
2. Bob then requests a certain number of Chainlink nodes using a contract that specifies that they must meet at least a certain number of previous transactions, % of accuracy and demand a certain amount of LINK to be staked as a penalty payment from each individual node as a guarantee that they will fulfill their end of the contract.
3. Bob also sets up how much LINK is willing to pay for the data retrieval.
4. All the Chainlink nodes which met Bob's specifications now bid to be an oracle of his contract. Bob will then select the oracles that ask for the lowest amount of LINK as a transaction fee.
5. Bob's selected nodes provide their data and their answers are aggregated by the aggregating contract Bob selected. Bob's smart contract now gets this data, each node gets paid in LINK, and the penalty payments are given to all the nodes whose data did not disagree with the consensus.
6. The honest and correct nodes now have more LINK, which they can keep for future penalty payments or they can sell it on the market.

Two important notes:

- Once Mixicles is live (currently in audit), all this process will keep private the contract business logic & the external oracle data & final payee result while still being **auditable to regulators**.
- Once Threshold signatures are live, instead of each node writing their response on-chain (high costs, clogging network), they will reach to consensus off-chain and write results in just one transaction.

Frequent Questions / Answers

1. Is node ranking and staking the same thing?
No, each node has a ranking (reputation) determined by their past performance. Staking is an additional metric ontop of this which is taken into account by users when choosing which nodes to request. Having more LINK available for staking increases the probability that a node will be honest, but a node's ranking is a factor in this as well.

2. Wouldn't holding tons of LINK automatically rank your node to the top?
No, node ranking considers multiple factors in reputation (see #3), staking LINK just one of the parameters considered alongside others.

3. What are the factors considered for node ranking?
This depends on a wide variety of cators: Uptime, correctness/accuracy of responses, total number of assigned/accepted/completed/rejected requests, average time to respond, slashing history and the amount of LINK staked.

4. Is staking live?
No, it is likely to arrive after other major features such as mixicles & threshold signatures. Networks today are secured by a node's reputation and the opportunity cost of losing future income if malicious. The Chainlink core team also subsidizes oracle networks with the funds raised from the token sale to ensure proper responses from nodes and ensures running a node is economically feasible in the early days of the network.

5. What are the returns on staking?
This will vary from node to node based on their node ranking (see #3), reputation, amount of staked LINK, and the volume of jobs received. The more reliable, accurate, and quick to respond a node is, the more likely they are to generate higher returns on their staked LINK due to the higher volume of jobs and higher fees that can be charged.

6. Will be there contracts that require Zero LINK to be staked?
Yes, contracts can require any amount of LINK (including zero) to be staked (see section 'Customizing data & security in page 1'). The amount staked is just a single factor the requester can require in their service agreement. It is up to the requesters how much LINK will need to be staked for a job and it is up to the node to choose which jobs they are willing to accept.

CHAINLINK

SMART CONTRACTS & REAL WORLD

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

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

Whitepaper[79]

Community: 'The missing piece to the god protocol'[80]

Community: 'An in-depth look at LINK token'[81]

Devs: Chainlink technical documentation[82]