# CLEARS

## BLOCKCHAIN IDENTITY CLEARING

## WHITE PAPER

MARCH 28TH, 2018

VERSION 1.0.5

CLEARS
BLOCKCHAIN IDENTITY CLEARING

## Contents

# Legal Disclaimer

The purpose of this document is to present the Clears project to potential CLRS token holders. The CLRS token will be issued by the company through a token sale. Further details will be available on https://clea.rs.

This whitepaper may be outdated and has no contractual value. Its only purpose is to provide information and explain the project to potential CLRS token holders.

This is not a secure nor a guaranteed investment. This whitepaper is not written in accordance to any law or jurisdiction protecting future token holders.

Token holders are by no means investors.

Financial forecasts and estimates appearing in this whitepaper constitute forward-looking statements and are for educational purposes only.

All future token holders must keep in mind that buying or holding ETH, CLRS, or any other cryptocurrency (or token) presents the possibility of losing 100% of their value over time.  Cryptocurrencies are not insured by any government or bank.

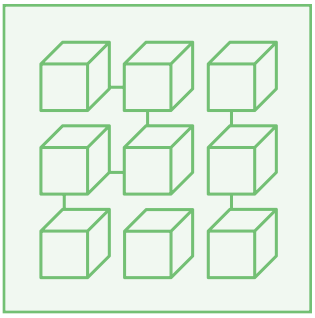
CLRS token is currently not tradable online and may never be. It is not guaranteed that the token will ever be available through online exchanges.

CLRS token is a utility token, not a security.

The information contained below may have been translated from another language, or may not be completely accurate. In the event of discrepancy, please refer to the English version.

## Abstract

KYC—or Know Your Customer—is a critical process for all financial companies dealing with international investors, shareholders and customers. Clears is a technology based on the Ethereum blockchain offering a scalable and personalized KYC process. It aims to expedite the acquisition and delivery of required information to companies and regulators around the world, simultaneously improving the user experience by increasing security of sensitive personal data while lowering the cost.



Today, most companies use proprietary and standardized KYC processes, requesting every new customer to submit an ID and a document certifying their current address. Only after a successful customer authentication has occurred are companies allowed to do business with a user. The data being used in a standard KYC process is often extremely fragmented, and there is no guarantee that the user completing the KYC is the legitimate ID holder. Additionally, many KYCs processes are unnecessarily complex in that the amount of documentation needed exceeds legal requirements for a given operation.

Ironically, the same crypto-technology companies at the forefront of blockchain innovation are using archaic and unsecured KYC processes.

## Market Size

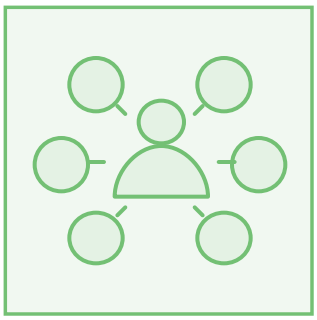
The global banking industry combined with the top five Asian markets constitute a 1.5 billion dollar yearly market, according to LexisNexis risk solutions.[1] But the KYC market goes far beyond the banking industry and is so large it's difficult to estimate the market size using publicly accessible data.

In the immediate future, Clears will focus its efforts of serving rapidly growing ICOs, Fintech and Cryptocurrency marketplaces.

Currently, there are more than a thousand ICOs yearly. Every ICO requires anywhere from 1000 to 50000 KYCs. This tiny fraction of the market represents $50M in potential revenue, a number that is expected to rise exponentially as cryptocurrencies gain mainstream popularity.

There are also more than 10,000 crypto related marketplaces and exchanges on-boarding thousand of new users daily. Each new user requires a KYC.

1 "Uncover the true cost of anti money laundering & KYC compliance (Rep.). (n.d.). Lexis Nexis."



Clears aims to be the standard KYC in the rapidly growing ICO market, expanding to serve all industries that require identity checks and KYC processing. We are confident that users will specifically request that Clears processes their KYCs due to its convenience and enhanced security.

## Problems

KYC costs and delays are notorious for crippling the crypto industry. The cost of providing such a service for 20,000 customers starts at ~$800K. During an ICO, when time is of the essence, ICO participants can be frustrated by the time it takes for the traditional KYC process to be completed. Even minor setbacks can prevent a user from purchasing tokens before the price goes up or cause them to miss the token sale altogether.

Players in the cryptocurrency market understand the importance of a legitimate KYC process. Because new regulation could change at any moment, the industry is cautious and needs a KYC process that is:

- Customizable, giving companies the ability to define what information to require based on current legislation
- Flexible, allowing users to amend and update their information in real time
- Accessible, allowing regulators and law enforcement agencies to be part of the process, if regulation becomes standard

### Pain Points for Organizations

ICOs websites and exchanges currently processing their own KYCs must hire a dedicated team, which is time-consuming and expensive. There are major risks with being responsible for this essential piece in the user acquisition puzzle--namely the responsibility to keep users' sensitive personal data private and the necessity of keeping up ever-evolving regulations that may vary from country to country. In an industry still in its infancy where exponential change is the norm, keeping up with shifting governance is a monumental challenge facing companies in the crypto space.

### Pain Points for Users

For users the primary concerns are convenience and security. Considering the extreme market fluctuations commonplace in cryptocurrency, time is of the essence. Users want to be able to buy or sell instantly. Delays in the KYC process can cause both fear and frustration. Users may be required to submit redundant documentation in order to create new accounts on different sites. Both the security of a user's sensitive personal documents and the security of the wallet itself can be called into question. Exchanges and ICOs websites are rarely based into the same country as the user and sending into valuable personal data, without adequate proof of security can leave a user vulnerable to identity theft. Recently, Japan's Coincheck's database was hacked resulting in the loss of some user's wallets,[2] highlighting the question of overall security in the crypto space.

## Why KYC is Critical and the Problem Clears Solves

Clears product solution has been designed to specifically address the concerns of companies, users and regulators.

Our one touch process ensures the proper identification of each customer and completes a sanity check (AML and criminal databases) and due diligence while continually monitoring regulations to ensure compliance. As a trusted third party, Clears guarantees the integrity of the process for both the end user and the company completing the process.

For companies, Clears provides a turnkey solution to the complex KYC problem. The process allows for each organization to customize the process to accommodate their needs while meeting regulation requirements. Extended database access allows Clears to utilize pre-existing data to crosscheck against information provided by the user.

2 The Coincheck hack and the issue with crypto assets on centralized... (2018, January 29). Retrieved March 19, 2018, from https://www.reuters.com/article/us-japan-cryptocurrency-q-a/the-coincheck-hack-and-the-issue-with-crypto-assets-on-centralized-exchanges-idUSKBN1FI0K4

The Clears process is certified and audited by several independent organizations. If a KYC is audited, Clears takes responsibility for working with the authorities. Companies can rely on Clears to pass any audit regarding the KYC process. If needed, Clears' worldwide network of attorneys and auditors can be leveraged to prove the integrity of a KYC completed with Clears.

For auditors, Clears is a simple and predicable access point when information needs to be checked. The Clears process is certified and audited by several independent organizations, ensuring the process is reliable from start to finish.

Clears offers a KYC solution that is:

- Fast: no longer than 30 minutes after the documents are submitted; when a user has already completed a KYC with Clears, the process is instant
- Convenient: once a user completes a KYC, the data remains valid for additional KYCs
- Cost-effective: by using the same data repeatedly, the average cost of a KYC decreases substantially
- Legitimate: Clears can process KYCs around the globe in accordance to local or international regulation
- Secure: all data is processed and stored using the most advanced technology available; and Clears never shares its data outside of official auditing
- Simple to integrate: adding a KYC process to any website will eventually be as simple as implementing Google Analytics. A single line of code will be enough to indicate where the process starts

All of the above shows that Clears can quickly become the easiest and most effective way to complete the KYC process (on any website relying on user registration).

# Clears Connect Product Solution

Clears can be seen as an escrow for personal data based on the blockchain. Clears will use top-tier processes for identity verification and background checks. It will leverage the power of a decentralized blockchain to simplify and reduce the cost of a traditional KYC process.

For every new user signing up to Clears, Clears creates a unique, unalterable blockchain ID, known as a Clears ID. This ID will be used to identify each user during all KYC processes they will ever be required to complete.

Using private and highly-secure databases, including Anti Money Laundering - AML databases, Clears will then perform a complete background check for every new user. Registrations and KYCs are always free for the user.

Clears will then be able to provide the following for every user:

A thorough identity check and proof that the KYC has been completed, with Clears acting as a third party

The ability for any company doing a KYC to validate their data by comparing it with the certified data only available through Clears

A complete data hash, hosted inside the Ethereum blockchain, complete with a timestamp

Additional background-checks, as needed

The Clears ID will never change for a given user; its integrity is guaranteed by the Ethereum blockchain, one of the most secure blockchains in existence.

When a user is asked to complete a new KYC via Clears on a given application, by providing their email or Clears ID, Clears will complete an identification check by asking random questions regarding the user and upon satisfaction will immediately certify that the KYC has been completed.

An additional transaction, called KYC hash is stored inside the blockchain to confirm the completion of a KYC between a company and a user.

For users, Clears provides peace of mind by limiting access to their private data by third parties.

From an organizational standpoint, Clears provides a quick and easy solution to gathering and storing sensitive data.

KYCs can be used for a variety of purposes. For example, Jane is a Canadian resident who wants to invest in the ABC Company's ICO. To invest, she must complete a KYC, managed by Clears.

Jane clicks on the "Clears CONNECT" button on ABC Company's website to do the KYC procedure.

- First, Clears asks Jane for her email or a CLEAR ID. Assuming she doesn't have an ID; Clears creates the ID **0xdceed1e982adcf0f57501b34dcfc36d6fcbfe8a4** for her. This hash is hosted on the Ethereum blockchain and can be checked on etherscan.io. For example, here is a real KYC ID: https://etherscan.io/address/0xdceed1e982adcf0f57501b34dcfc36d6fcbfe8a4.

- The row at the bottom is the smart contract creation, when Clears attributed this ID specifically to Jane. The middle row reveals the date of the KYC's first completion, and, when decoded to ASCII, contains the hash representation of Jane's KYC (**f194e6dd13e431112076b14267659bee4ed2564d5587b85d31e3accded1e133b**)

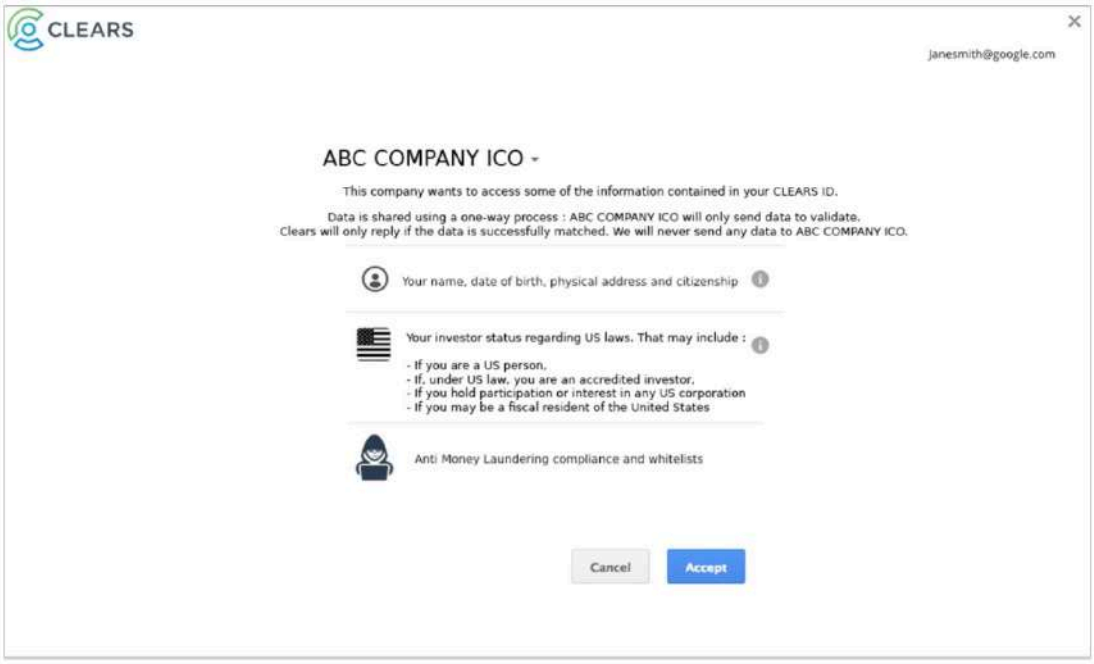
- This information can be added to or modified later in the process (an address was updated and resulted in a new hash representation of Jane's KYC)

- There is no other public information available for a specific hash. However, if the hash is modified, revoked or additional information is added, another row will be written by Clears under this specific contract

- While anyone with the Clears ID can verify its existence and legitimacy, the Clears ID is not linked to any personal information or account

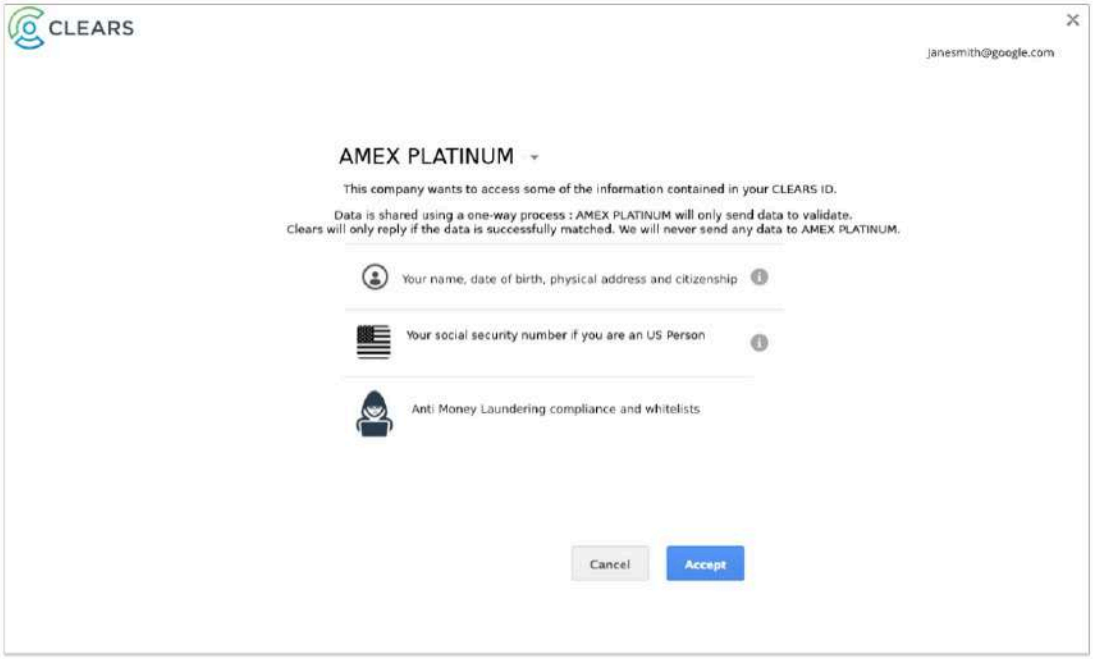
Once Jane has completed the KYC process, Clears asks her permission to complete the KYC on behalf of ABC Company.

The information Clears collects during the KYC process will never be shared. Clears certifies the KYC from data collection to completion.




Two days later, Jane submits an application for an American Express Platinum account. Let's assume, AMEX uses Clears KYC for their Canadian customers. To be compliant with the ALENA jurisdiction between the USA and Canada, AMEX must also verify that Jane is not a US citizen before issuing her a credit card.

During the application, there is a screen where Jane is prompted to complete a Clears KYC for AMEX. Since Jane has already completed a Clears KYC, she can use her credentials to log into her account and add any information needed to complete this particular KYC.




To use the service, ABC Company and AMEX have both paid several CLRS tokens, depending of the amount of data requested for their respective KYC. Clears allows companies to complete thorough KYCs customized to their needs via a simple dashboard. Companies can define their own KYC requirements, which the user must meet before their KYC can be validated. Clears will certify that all requirements have been met for a specific KYC by issuing a KYC hash.

This specific smart contract, called a KYC HASH, is populated inside the blockchain to irrevocably prove the completion of the KYC. It guarantees a users KYC based on requirements defined by the company.

Technically, Clears front-end service consists of a collection of webpages used to obtain a specific consent from a user to start a KYC process with a specific company. If the user has not completed a Clears profile, he/she will be asked to do so; if he/she has, Clears will process the necessary security checks and complete the KYC.

A KYC hash uses the same technology as a Clears ID, while storing a different type of data. While a Clears ID uniquely identifies a specific user, a KYC hash provides proof that a KYC has been completed for a specific company by a specific user: “On Friday, 22nd February 2018 at 3:20PM EST, a KYC has been completed for ABC Company by a specific user. “

For example, check out: https://etherscan.io/address/0xf97ef8a413bf425a1f826f3ced6485576bc583bf.

## Here are some of the rules that can be defined for a KYC process:

| |
|---|
| The user identity must be verified |
| The user identity must be verified using 2 pieces of ID |
| The user's age must be above XXX years (ie majority age in specific country) |
| The user must NOT be a US person |
| The user must BE a US person |
| The user must BE a US person AND an accredited investor |
| If the user is a US person, he also MUST be an accredited investor |
| The address of the user must have been verified within the last 6 months |
| The address of the user must have been verified within the last 12 months |
| The address of the user must have been verified within the last 24 months |
| The country of citizenship of an user must NOT be XXXXX |
| The country of citizenship of an user MUST be XXXXX |
| The user must be married |
| The user must not be married |
| The user must pass AML/CTF sanction databases checks |
| The user must pass CRS Criminal Records Checks |
| The user must NOT be an executive of a US company |
| The user country of birth must NOT be XXXXX |
| The user country of birth MUST be XXXXX |
| The user current zipcode MUST be XXXX |
| The user current zipcode must NOT be XXXX |
| User must have at least one ERC20 wallet verified by Clears |

## Clears Wallet Certification

Verifying the ownership and the integrity of a wallet can be a critical for ICO websites that wish to pre-screen potential token holders to ensure they have active wallets. Clears will have an optional flow that will allow a user verify the ownership of an ERC20 compatible wallet during the KYC Process.

Clears will initiate the procedure by sending a small amount of CLRS tokens and ETH coins. Using his/her private key the user must send back the same amount of CLRS tokens to a wallet generated by Clears. The user will pay the transaction fee using the ETH sent by Clears during the initial transaction.

## KYC Data Cross-Matching

The Clears goal is to provide a complete decentralized KYC solution, where companies can rely on Clears for the complete KYC process. When a KYC is audited or the authorities need additional information, companies can direct request to Clears.

In some instances such as common first and last names, it may be necessary for the company to maintain a record of the KYC, in addition to the KYC Hash provided by Clears, in order to properly identify an individual. These records can consist of users first and last name and the US or Canadian social security number to prove that the user is the same person as validated by the documented KYC.

To do so, Clears will create a collection of REST APIs to cross-match data.

It is important to note that Clears will never share, sell or send any data but will only provide a technical solution to verify the data entered by a specific user against the data collected and verified during the KYC process.

Here's the data available through the Clears web services.

| Data | Data to send to Clears example | Answer from Clears |
|---|---|---|
| First name | JOHN | 1 or 0 |
| Last name | SMITH | 1 or 0 |
| Current address | 1000 Island boulevard, Miami, Florida, 33160 | 1 or 0 – This use a % match with the address on file under 85% match 0 is replied |
| Any previous address | 1887 Acme Road, Las Vegas, Nevada, 89147 | 1 or 0 – This use a % match with the address on file under 85% match 0 is replied |

| | | |
|---|---|---|
| Current Zipcode | 33160 | 1 or 0 |
| Any previous Zipcode | 89147 | 1 or 0 |
| Date of Birth | 1980/08/14 | 1 or 0 |
| Social Security Number (US and Canada only) | 839123482 | 1 or 0 |
| Place of Birth (city) | Manilla | 1 or 0 |
| Country or Birth | Philippines | 1 or 0 |
| Citizenship | France | 1 or 0 |
| Is a US person | YES or NO | 1 or 0 |
| Is an executive of any US person | YES or NO | 1 or 0 |
| Is a US accredited investor | YES or NO | 1 or 0 |
| Country of residence | USA | 1 or 0 |
| Year of birth | 1980 | 1 or 0 |
| Legal status | Married | 1 or 0 |
| Passport number | 05AW82248 | 1 or 0 |
| Driver licence number | 1980-6658-585525 | 1 or 0 |
| Local ID number | 5526822458274 | 1 or 0 |
| Passport expiration date | 2022/04/01 | 1 or 0 |
| Passport issuing date | 2017/10/21 | 1 or 0 |
| Passport issuing country | France | 1 or 0 |
| Passport place of issuance | Paris | 1 or 0 |
| Driver licence issuing date | 2017/11/01 | 1 or 0 |

| | | |
|---|---|---|
| Driver licence issuing country | USA | 1 or 0 |
| Driver licence place of issuance | Las Vegas, Nevada | 1 or 0 |
| Local ID type | Health Card<br>Social Security Card<br>Credit Card<br>Other | 1 or 0 |
| Local ID authority issuance type | Government | 1 or 0 |
| Local ID expiration date | 2022/10/01 | 1 or 0 |
| Local ID issuance date | 2018/01/01 | 1 or 0 |
| AML/CTF sanction databases checks | PASSED | 1 or 0 |
| CRS – Criminal records checks | PASSED | 1 or 0 |
| ERC20 Wallet address | 0x91c66C538fa8496420DfcA6B6aD745a022C3c59e | 1 or 0 |

## Extended Usage for Bank-Level KYC Compliance

Companies launching ICOs and credit card issuers can use online KYC solutions, despite being less secure than physically validating documents. Some transactions—including opening a bank account, larger withdrawals requests on crypto exchanges—require a more robust KYC, where physically validating documents is mandatory.

To achieve this level of document authentication, Clears will build a worldwide network of professionals—notaries, CPAs, attorneys, etc.—legally eligible to certify documents.

Certification professionals will be able to join the Clears network after a thorough analysis of their credentials. They will be paid for their services in CLRS tokens. This is advantageous because payments can be made worldwide, nearly instantly and without the hassle or cost of international money transfers.

Our goal is to offer physical certification for any kind of document in less than 30 minutes in every major city[3] by the end of 2019.

3 Major city defined as a metropolitan area with a population greater than 1 million people

### The Procedure for Physically Checking Documents:

The user completes a standard (i.e. online) Clears KYC

At the end of this process, the user will be provided with a list of documents that need to be verified in person. Common documents include passport, driver license, proof of citizenship

Clears will use geolocation to match the user with a certification professional in their area. To avoid collusion, the user cannot choose the professional

The user has five days to have their documents verified by the selected certification professional. In the meantime, the certification professional will receive a digital copy of the documents to be certified, via the web or mobile app

When the user appears in person, the certification professional compares the physical document brought by the user to the digital version, certifying that the two documents are identical

A specific KYC hash of this transaction is issued to the blockchain

The professional is paid in CLRS tokens

## Data-Less Solution: Data Security and Integrity

The Clears cloud solution is based on a technical solution called data-less storage. Clears developed its own solution that consists of several libraries to clean, standardize and remove any personal information from it's database.

## The Clears Solution

- Data submitted by the user is processed using Amazon Kinesis Data Firehose and streamed directly inside others Amazon Services without storing it publicly
- All data submitted by the user is standardized after verification and converted using a HMAC-SHA-256 hash method. All hashs are then hashed together again and stored inside the Ethereum blockchain
- The Specific HMA-SHA-256 method provides a consistent method of hashing and a secret key to add another layer of entropy
- Documents uploaded by the user are natively encrypted and stored securely inside Amazon Glacier (https://aws.amazon.com/glacier/). Access to this data is only possible during the KYC verification process using a specific Amazon IAM Identity secured inside a closed Virtual Private Network (https://aws.amazon.com/iam/)
- The Clears Virtual Private Network utilizes security strategies to gain external access to data stored inside Clears cloud as the first layer of security. Access to this Private Network requires the usage of an IP address from the Clears network and a specific IAM key issued by Amazon
- The second layer of security is provided by Amazon Glacier itself and another IAM key used to access specific documents inside Glacier
- A third layer of security is added by using a 256-bit Advanced Encryption Standard (AES-256) tied to a specific key for each individual resource (passport, proofs of address etc...)


The data-less solution used by Clears, hash and secure the data provided by the user before storing it inside the DynamoDB Database using HMAC-SHA-256 protocol, the highest standard of cryptographic solution— the same protocol used to mine bitcoins.

The global representation of all the data is then hashed a second time before being published inside the Ethereum blockchain, serving as proof of collected data.

If, for any legal reason, it is necessary to verify the data collected and verified by Clears about a specific user, the Clears library can retrieve the hash of any data point based on the hash stored inside the blockchain and compare any external data to the appropriate datapoint by hashing the data again to compare it using the same SHA-256 protocol.

Data stored securely inside the DynamoDB databases can never be decrypted as they are hashed using a one-way process. In the improbable event of a data breach, any stolen data will be completely useless and can never be linked to a specific user.

Here's what an email address looks like inside Clears cloud766667766:

1cef6683953db966eec49a988cfd0fcf93f7008f8e25255f82c300fa5b976696

That is the SHA-256 representation of ico@clea.rs.

Note that this data is HASHED, not encrypted. The main difference between hashing and encrypting is that hashing is a one-way process and the data can never be decrypted. Rehashing specific data using SHA-256 protocol will always return the same result, allowing for comparison if the hashed data is known.

A hash does not contain any actual data that has been hashed. As a result, it's impossible to decrypt simply because the data in question isn't there to be decrypted. The hash is only a representation of the data, not the data itself. On the other hand, data strings containing encrypted data can be accessed using a private key, which creates the possibility for decryption.

### The Clears KYC Process Ensures That:

No data can be stolen or tampered with since there is no humanly readable data stored by Clears

Data hashes for users can be securely stored inside the blockchain, even publicly, since there is no possibility of decryption

Clears will provide authorities with the necessary tools to facilitate comparison and validation of the data

Because hashes are stored within the Ethereum blockchain there can be no question of the integrity of the data. By nature, once data has been populated into the blockchain, it cannot be modified

## GDPR and Privacy

Clears has been built with the GDPR policy compliance in mind.

The KYC process will outline how and why the data is collected, as well as data processing and storage procedures.

Clears keeps all user data private. Organizations using Clears' KYC can send data for matching or validation—Clears will only send a binary answer indicating whether the data sent is correct. Clears will never send raw data about its users.

Clears manages and controls how the data is stored

Consent boxes are never pre-filled nor pre-checked

Clears replies to any customer request in less than a month

Inquiries regarding personal information and information removal is free of charge

A disclaimer is available on our website defining how Clears uses cookies for the KYC process and how to opt-out

Clears has also set up protocols to guarantee a high degree of privacy. Clears uses cold storage to store the documentation sent by users. These data-vaults are regularly audited and are not accessible online

## CLRS Token Value Proposition

CLRS token is an ERC20 token relies on the Ethereum blockchain. Companies wishing to use the Clears KYC technology will be required to pay for services using the CLRS token.

### The following services will be paid for by the company requesting the KYC:

- Completed KYCs
- The physical validation of a document, via a Clears network certification professional
- Additional services

Companies that are not holding CLRS tokens but that wish to use Clears services will be able to buy tokens on the Clears website, using fiat currency. Clears will introduce a buy back program to create more token velocity and liquidity. This will allow companies to simply buy Clears tokens on the Clears website.

### Users asked by a company to complete a Clears KYC will never be asked to pay.

# CLRS Token Creation

| | |
|---|---|
| Private Sale | Starts on February 22nd 05h00 GMT<br>Ends on April 9th 05h00 GMT<br>Ends early when 5 000 ETH cap is reached<br>Bonus 55%<br>Available only to friends and family |
| Pre- Sale | Starts on April 9th 05h01 GMT<br>Ends on May 21st 05h00 GMT<br>Ends early when 25 000 ETH total cap is reached<br>Bonus 40% during the first week then 25%<br>Available only to pre-selected people |
| Public Sale | Starts on May 21st 05h01 GMT<br>Ends on July 9th 05h00 GMT<br>Ends early when 50 000 ETH total cap is reached<br>Bonus 20% during the first week then 0%<br>Available to everyone |
| Bonus fine-print | Bonus are paid in CLRS tokens |
| Tokens for 1 ETH | 1000 CLRS FOR 1 ETH / 1 CLRS = 0.001 ETH |
| Token creation policy | No additional coin will ever be created |
| Total token supply | 86,374,977 CLRS |
| Steps caps | Private sale: 5,000 ETH<br>Pre-sale: 20,000 ETH<br>Public sale: 25,000 ETH<br>TOTAL: 50,000 ETH |
| Minimum buy | 1 ETH |
| Maximum buy | 500 ETH |
| Team % | 9% -7,773,748 CLRS<br>Lockup: 12 months |
| Company % | 9% – 7,773,748 CLRS |
| Bounty Program % | 2% – 1,727,500 CLRS |
| Crowdsale (ICO, total cap) % | 56% – 48,369,987 CLRS |
| Bonus Program % | 19% - 16,411,245 CLRS |
| Advisors % | 5% – 4,318,749 CLRS<br>Lockup: 6 months |
| Digits after comma | 18 |
| Protocol | ERC20 Extended |
| Blockchain | Ethereum |