Wecan Group

Whitepaper

The Web 3.0 Compliance Solution

wecan®

Version 1.2

Summary

Abstract

Wecan Chain is a distributed infrastructure to improve high throughput without sacrificing security.

Wecan Comply is a system which disrupts the way we secure and exchange structured data with real time and systematic audit cockpit on blockchain with cryptographic proofs.

In order to guarantee auditability, we assume that no one should be able to alter the data at any time. To achieve this, we use 2 layers of blockchain. The second layer, Wecan Chain, records all data hashes. At the end of a 24 hours period, the last hash is recorded on Ethereum public blockchain. The challenge is to guarantee that no one, in any context, can corrupt the data ex post.

We conservatively assume that all data exchanged and stored may eventually be compromised. Thus, Wecan Comply uses end-to-end encryption to ensure that plaintext data is never sent to the server. If a server only contains encrypted data, then the risks of a central server breach are mitigated.

Finally, to ensure data quality, we administer a data catalogue, forms and modules as required. Thus, regardless of language, context or user, the data remains structured. This makes it possible to have a compliance dashboard in real time. The challenge here is to enable a systematic real-time compliance audit and no longer a random audit ex post.

In order to boost an ecosystem that is already composed of recognised institutional players such as banks, asset managers, notaries and luxury groups, we are issuing the Wecan token.

This token has one purpose, to pay a fee for each transaction sent and recorded on Wecan Chain. This pure utility token will be issued at a price of 0.001 swiss francs. The aim is that the transaction cost will never be a barrier for the users. 100 billion tokens will be issued at once. Wecan will have a reserve of 28% of the tokens and after the private pre-sale, the remaining tokens will only be accessible from a marketplace.

The limited number of tokens issued will be coupled with a systematic burn of a percentage of tokens on each transaction, with the expectation that this will not hinder the widespread adoption and use around the world.

1 · Data Management Dilemma

In 2020, 2.5 trillion bytes were generated every day[1]. For information, a trillion is a number followed by eighteen zeros. Every second, a single internet user generates 1.7 MB of data. By way of comparison, the 100-page pdf of the Swiss Federal Constitution is 0.4 MB in size.

While this increase in data volume offers new opportunities, it also imposes increasingly time-consuming and intense regulatory obligations. Data management is becoming a necessity for many industries. However, several challenges are embedded in this data management.

Firstly, there is the problem of data completeness. Each system has its own set of data depending on the problem it is trying to solve. This data is often dispersed in a multitude of independent applications, which does not facilitate its global management.

For example, it becomes complicated to identify the most relevant data in a system where data exists in many places, duplicated in many different applications. Redundancy does not go well with data management. The acronym WET (Wasting Everyone's Time while you're Writing Everything Twice) has even been coined for this purpose.

Secondly, the standardisation of data is a challenge for management projects and initiatives. Each system or set of data can be managed by different teams, in different formats and in drastically different volumes and qualities. At the enterprise level, this lack of standardisation requires increased oversight for each data record or change. It also makes interactions with peers, or international exchanges, more complex.

Finally, the risks of hacking and cybersecurity are a corollary of limited data management, or of a growing number of data distributed in a multitude of different systems. The year 2021 has been historic in terms of hacking and ransomware and since December 2020, computer attacks have been carried out against AstraZeneca, Shirbit, the European Medicine Agency, Facebook, New Zealand's Central Bank, Pfizer, Oxford University, Poland's National Atomic Energy Agency, Nine Entertainment, New York City's Metropolitan Transportation Authority, Verizon, United Nations, Voicenter, etc[2].

All these challenges can be addressed by relying on a "golden copy" system, sometimes called a "golden record", which designates a version of the data that serves as an official and recognised reference. A single source of truth for all stakeholders in relation to that data. The term "truth" is understood here as a source of information whose veracity allows it to be used by the greatest number of people in a wide variety of tasks. Our solution aims to be used as a Golden Copy, a Web 3.0 smart storage & exchange of structured data.

1 https://techjury.net/blog/how-much-data-is-created-every-day/#gref

2 https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

2 • Wecan Group

Vision

The vision of Wecan Group is that one day, every organisation and individuals will manage "golden copy of data" to improve data auditability, privacy and quality and act as a single authoritative source of truth. On that day, all exchanges will be digitised and secured, thanks to end-to-end encryption, during storage and exchanges.

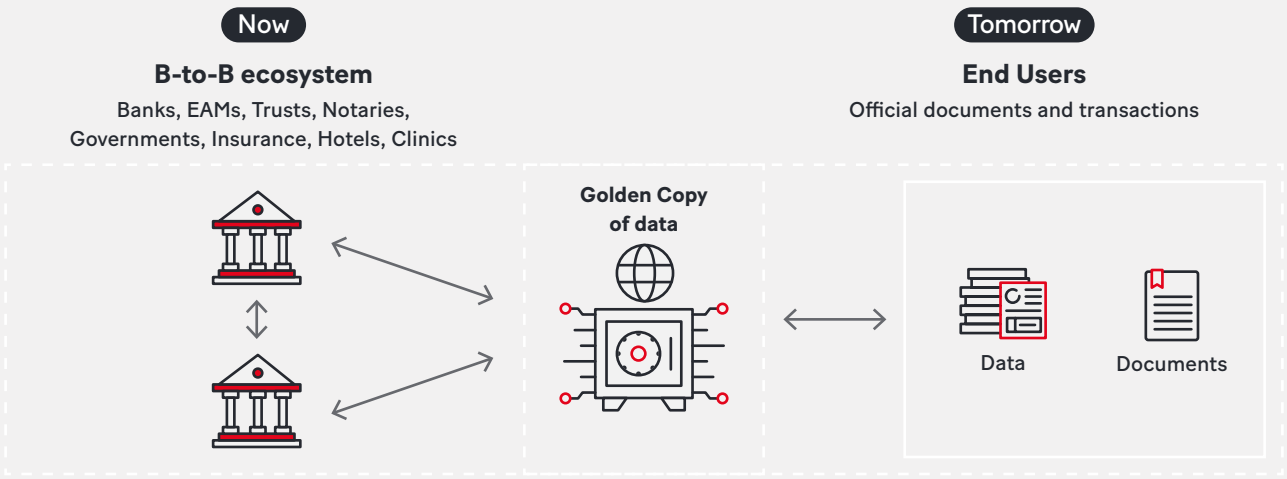
Timestamping, i.e. associating a date and time with a specific event, is central to the creation of golden copies that could serve as a reference source. One technology fits this criterion particularly well: blockchain.

This technology reinforces the notion of the veracity of data by allowing a group of participants to confirm it. The auditability will also be eased by blockchain's immutability and distributed storage.

After several years of research and development, we launched a first version of Wecan Comply in March 2021, which is used by 13 banks and 80 independent asset managers managing over 100 billion assets in 10 months to store and exchange compliance data. The implementation of Wecan Comply on a distributed and reliable blockchain solutions allowed us to create golden copy of transactions that can be accessible at any time.

Based on this first sectorial implementation and in order to accelerate the three pillars we are defending, auditability, privacy and data quality, we want to enable all organisations and individuals to secure data in a structured way and exchange it on a global scale on Wecan Comply.

• **Explanation of Wecan Group ecosystem**



Definition

Wecan Comply is a messaging system which provides smart storage and exchange of structured data with cryptographic proofs. The result is more secure data storage and sharing, enabling a wide range of automation possibilities.

Wecan Chain is a distributed infrastructure to improve auditability, privacy and data quality with blockchain. Wecan Comply is built on top of Wecan Chain.

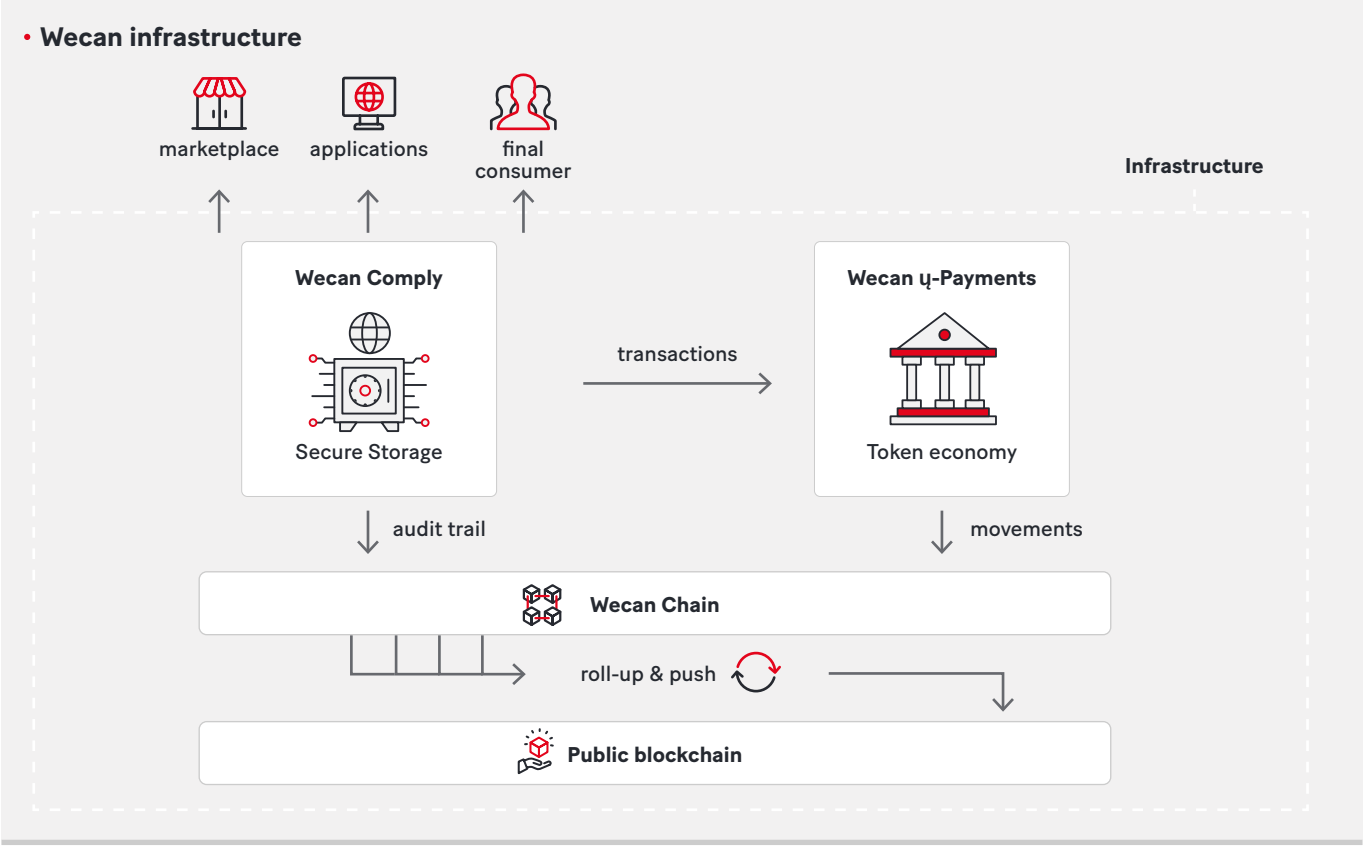
Data forms are sets of labelled and structured data/questions.

Modules are sets of forms bundled together.

Data catalogue is a dataset listing all the different data and questions available on Wecan Comply.

Wecan Token is a utility token used inside the Wecan ecosystem only.

Golden Copy is a version of the data used as an official trustworthy and recognized reference.



Any individual or organisation can create a golden copy to secure and share data. Access to this data is managed directly by the data owner. The exchange of information can be done with any third party using Wecan Comply solution.

To facilitate exchange, the use of Wecan Comply is based on the creation of data forms and modules. Wecan Comply will offer a marketplace, administered and managed by the community.

Independent modules that interact with Wecan Comply by offering specific functionality will be available in this marketplace. So will standardised data forms. Financial compliance was the first module built and used by leading players in their field of activity.

The cross-industry applications here are multiple, and the openness towards a multiple set of actors leaves the possibility for every participant to feed the marketplace.

Market Analysis

The corresponding market analysis must include three comparative segments. The first deals with traditional cloud storage solutions, which are the solutions that an individual may think of first. The second is about messaging solutions. And the last one is about Web 3.0 solutions.

Traditional Cloud Storage

The implementation of Wecan Comply should not be confused with traditional cloud solutions such as the hegemonic Google Drive, Dropbox, Microsoft OneDrive or Apple's iCloud, or lesser-known alternatives such as Nextcloud, pCloud, Box, SpiderOak One or MEGA.

The above-mentioned solutions deal exclusively with file storage (pdf, excel, png, word, pptx, etc.) and not with forms or data fields that are intended to be standardised in order to increase their usability in a third-party process (e.g. having to fill in similar forms each time with different players).

The infrastructure in question is also a key differentiator. The above solutions are built on centralised models which differ from the infrastructure approach of Wecan Comply built on Wecan Chain, a private and a public blockchain. The auditability offered by this system is a prerequisite in a number of business cases and industries we are targeting.

According to a Forrester report[3] from January 2016, between 60% and 73% of the data captured by enterprises remained unused for analytics. Qualified data structuring is the best way to avoid such problems. But the creation of standards cannot be done via traditional cloud storage.

Another key differentiating factor between Wecan Comply and traditional cloud storage like Dropbox is the auditability of the data made available via our blockchain based infrastructure. This is something traditional cloud storage solutions do not offer. The simple emailing interface is another key differentiator from Dropbox or Google Drive.

Messaging solutions

The exchange of information has undergone many changes over the years. In Web 1.0, exchanges were done by simple emails in the form of plain text. Messengers such as Gmail are still used today for information exchange. With Web 2.0 and the increasingly interactive and social exchanges, the amount of information has drastically increased. Yet mailboxes have remained. While they have more intelligent features than in the past, the data is still collected in plain text.

Using a messaging system 3.0, Wecan Comply intends to bring an intelligent structuring of data into data forms. By keeping the familiarity of a simple messaging system, Wecan Comply brings a smooth innovation. The pricing of Wecan Comply is also similar to Gmail's pricing, based on data volumes, storage and number of users. If email exchange will not disappear with Web 3.0, structured data exchange finds in Web 3.0 what it missed in Web 2.0.

3 Mordor Intelligence, Digital Vault Market -Growth, Trends, Covid-19 Impact, and Forecasts (2021-2026) https://www.mordorintelligence.com/industry-reports/digital-vault-market#

Web 3.0 solutions

According to a market study[4], the Web 3.0 Blockchain market is expected to grow exponentially by 2030. The dominant key players on this market are Helium System, Polkadot, Ocean Protocol and Decentraland.

Initiatives to give back control of data to users have emerged in the blockchain ecosystem in the previous years. Solutions such as Datum, Medicalchain or GeoDB offer solutions. However, these solutions are primarily based on the monetisation of personal data by offering third parties the opportunity to buy them in exchange for payment in cryptocurrency. This facet of Wecan Comply, while present, is not the USP of the value proposition. The adoption of Wecan Comply does not rely on this point, but rather in the Web 3.0 messaging system allowing to store and safely exchange structured data with internal and external stakeholders.

The main differences between our solution and current Web 3.0 projects, apart from the scope which is often not the same, consist of several points such as the structuring of data in universal forms, the data validation system and its automation for updates.

The user interface is also different. Our solution uses well known graphic systems, in this case a system visually close to the emailling, in order to offer a user experience close to the users habits.

- **Competitive analysis**

Actual solutions	Their challenges	Our solution
Traditional Cloud Storage (Dropbox, Google Drive, iCloud,etc.)	× No structured data × No auditability × No textual data (only files) × No data forms × No compliance check × No distributed infrastructure	• **Data Accuracy** ✓ Structured information ✓ Only up-to-date data ✓ Data validation system • **Time saving** ✓ Automated classification ✓ Pre-filled data ✓ Notifications • **Security** ✓ Secure data sharing ✓ Secure data storage ✓ Distributed infrastructure • **Compliance** ✓ General Dashboard ✓ Full auditability ✓ Certificate of completion
Messaging solutions (Gmail, Outlook, Hotmail, etc.)	× Security issues × Data in plain text × No updates × No structured data × No auditability × No data forms × No compliance check × No distributed infrastructure	
Web 3.0 solutions (Polkadot, Ocean Protocol, Datum, etc.)	× No structured data × No data forms × No compliance check × No updates × No universal use case	

4 https://www.globenewswire.com/news-release/2022/01/04/2360814/0/en/Web-3-0-Blockchain-Market-Projected-to-Grow-Exponentially-by-2030-Report-by-Market-Research-Future-MRFR.html

3 • An ecosystem of leading players

Actual Live Customers

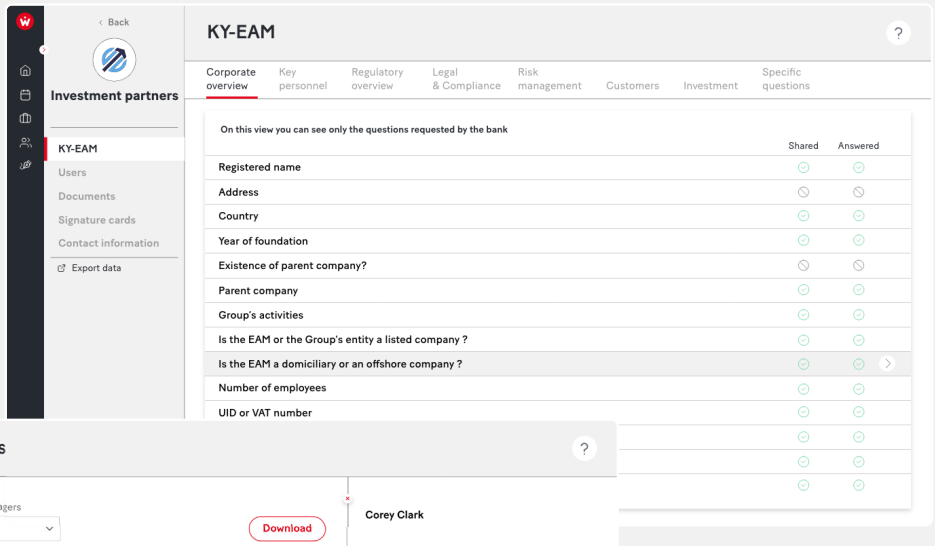
Wecan Comply for the financial industry

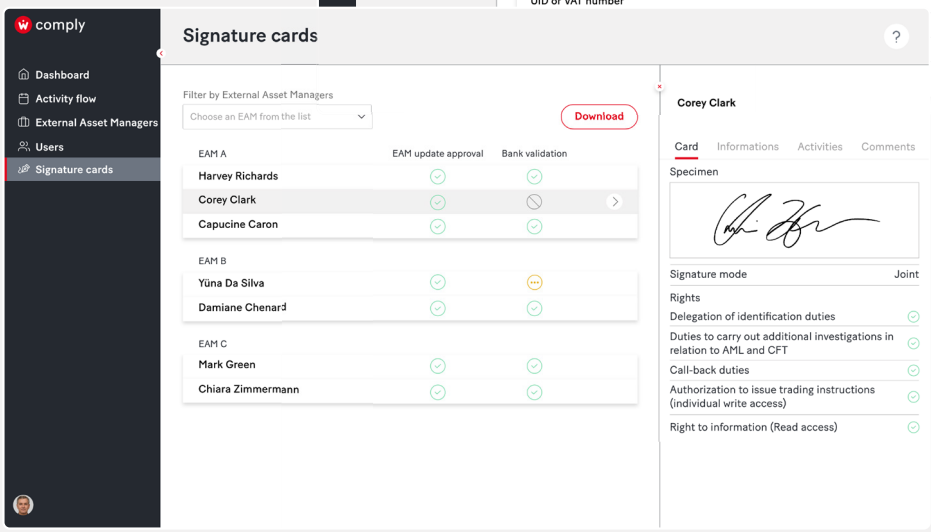
In just 10 months, Wecan Comply brings together 13 leading banks and more than 80 independent asset managers with over $100 billion in assets under management to drastically improve compliance processes linked to the onboarding and periodical review.

Wecan Comply facilitates communication between all financial actors, allowing faster onboarding, bringing systematic and real time compliance for the first time, improving data quality and lowering risk.

• **Wecan Comply platform**

KY-EAM management





Signature card management

Business Cases

Based on the experience acquired by working with banks, among the most demanding in terms of data security and privacy, we are extending the usage of Wecan Comply. Business cases are presented to illustrate how Wecan Comply is applied to various industries, at the organisation and private level.
Wecan does not aim at developing all the use cases by itself. By providing a software development kit (SDK), external contributors will be able to develop their own structured form based on a data catalogue

Human Resources:
Employee & Organisation Compliance
On the one hand, the employee needs to share data in order for the employer to process all the administrative paperwork such as proof of identity, diplomas, address, marital status, children etc. Wecan Comply could also facilitate recurring exchanges such as periodical evaluations, shared to one or several managers in the organisation.

On the other hand, the employer issues monthly or annual certificates such as salary slips, annual certificates, stock option contracts, reference letters etc. These documents are kept during the entire career of an employee, regardless of the employer. Moreover they might be requested by administrations upon retirement and therefore need to be kept securely. Third parties such as fiduciaries or pension funds could share documents to employees and employers, through this unique channel.

Wecan Comply helps employees to share necessary data to their employer in a structured way. The employee keeps a trace of all documents collected throughout their professional career, moreover the authenticity of documents is guaranteed.

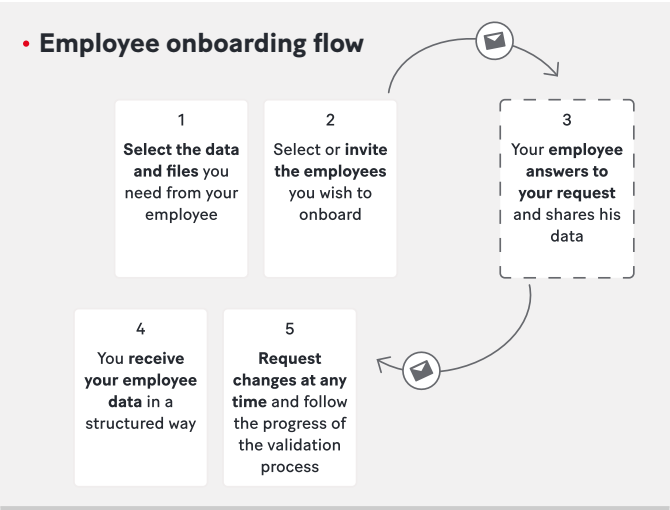
On the organisation side, Wecan Comply helps employers collect structured information from their employees and share certificates when needed.

Procurement:
Supplier & Organisation Compliance
Organisations such as companies, cities, governments are always required to carry out due diligence about a future supplier of goods or services and need further information when onboarded, for example to process a payment and avoid fraud.
On the other hand, suppliers systematically share the same data to potential customers in the case of a response to a call for tenders, or to future customers to be onboarded. For suppliers, maintaining and updating the shared data is difficult due to the exposure to a large number of counterparties. The risk of fraud is also important for payment processing.

The use of information coming directly from official registers, shared under the control of supplier to customer would be a key factor to speed up lengthy onboarding processes. The same principle applies to regulatory bodies emitting certificates for suppliers, with limited validity.

Agreement on contract and invoicing would be facilitated by the use of a centralised exchange place and would avoid exchange of mails or emails.
Wecan Comply is used to manage all data necessary to do a due diligence with a future customer and facilitate the update once onboarded.

Wecan Comply helps the customer to receive structured information about a supplier and working people, thus, facilitating the compliance review of data.



Sales:

Clients & Organisation Compliance

As private people we are consuming goods and services produced by companies, and thus are clients of many companies. Companies can also be clients of other organisations.

On one hand, companies want to access data of quality to better understand their market and their clients, to build efficient loyalty programs, and to anticipate future client needs.

On the other hand, clients are sometimes willing to share information to companies to obtain better services or to benefit from loyalty programs' advantages. Receipts and bills could also be stored centrally, emitted directly from the company and facilitating the management of warranty.

On the private user side, our solution is used to share requested information to companies in order to facilitate the onboarding as a new client and controlling the shared data over time. Moreover, token based loyalty programs can be centralised in our solution. Receipts and bills are also received by companies.

On the organisation side, our solution is used to access data of quality managed by clients directly. Consumption of goods and services are linked to Wecan and associated with token based loyalty programs.

Finance:

Shareholders & Organisation relationship

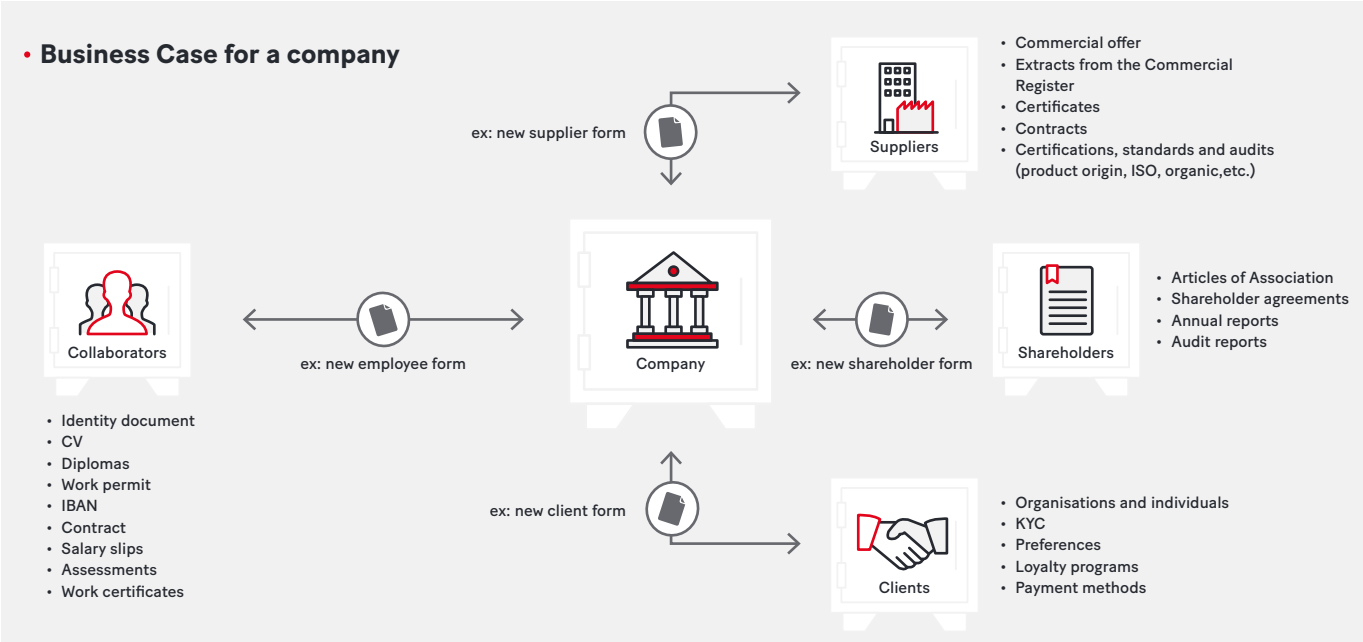
During a due diligence process, a company needs to share very sensitive data to potential investors. If the investors confirm their interest, many contractual agreements as well as reports are shared.

On one hand, the company wants to store all documents in one place and manage the sharing of data based on investor requests. Quarterly or annual reports need to be shared to all investors.

On the other hand, investors want to easily access data and be sure that the access of these documents are restricted only to the appropriate persons. Some documents may be shared to its organisation for further analysis.

On the organisation side, our solution is used to manage the sharing of documents during a due diligence process and central publishing of reports.

On the investor side, our solution is used to access documents of a company and share it to other persons of its organisation if necessary.



4 • Technology

Wecan Chain Design

At the heart of the our Infrastructure lies Wecan Chain, a technology which supports traceability and immutability requirements of the Wecan Comply Infrastructure. Wecan Chain is a type of distributed private blockchain optimized for storing and chaining events and transactions in near real-time.

Based upon Pulsar[5], a production proven Apache[6] top project, it can seamlessly expand to hundreds of nodes while maintaining low-latency (<5ms) and strong durability guarantees. Thanks to its built-in configurable geo-replication requirements Wecan Chain supports data partitioning and/or replication across different data centers and geographic regions.

Wecan Chain acts as the combination of message queuing and publish/subscribe mechanisms. Data publishers can push messages (events or transactions) on a shared distributed queue, participant nodes then agree on the publish order without harming correctness.

Once a total ordering of message has been defined, a built-in function chain messages via a double hashing mechanism:

1. The entire message content is hashed (sha-256) producing the 'content hash'
2. A second hash is then computed, the 'message hash' which is based out of the 'content hash' and the previous message's 'message hash'

Messages chaining ensures that events and transactions are immutable. Changing any past message would result in a broken chain, unless the entire chain of hashes is re-computed. Even though a full chain recompute is feasible in theory, it is practically made impossible by regularly anchoring Wecan Chain hashes on public blockchain.

Finally, when the chaining requirement is fulfilled, a notification system alerts subscribers with guaranteed messages delivery, allowing client modules to update state as per their own requirements.

A word on scalability

Wecan Chain is designed to handle thousands of concurrent reads and writes. It uses a system called BookKeeper for persistent storage. BookKeeper is a distributed write-ahead log (WAL) system that provides a number of crucial advantages for Wecan Chain: Multiple ledgers can be created for different topics over time, it offers very efficient storage for sequential data that handles entry real-time replication and distribution, it guarantees read consistency of ledgers in the presence of various system failures, it is capable of distributing I/Os across nodes, it's horizontally scalable in both capacity and throughput, and finally its capacity can scale horizontally over thousands of nodes in a hot manner and without rebalancing.

5 https://pulsar.apache.org/

6 https://blogs.apache.org/foundation/entry/the-apache-software-foundation-announces39

Layer Two

As demonstrated in specialised literature such as the Bitcoin white paper[7], public blockchains have long ago proven their capabilities in terms of resilience, security and immutability of information. Unfortunately, these benefits come at the cost of transactions' speed due to validation and distributed consensus requirements (Bitcoin blockchain can achieve about 4 transactions per second, Ethereum is about 15 tx/s, Ethereum 2 should be in a position to achieve 10k tx/s).

Public blockchain throughput improvement (Layer 1 scaling) is an on-going topic for research, but it is commonly admitted that they won't scale sufficiently to absorb heavy loads required by many real-world scenarii (eg: credit card transactions).

Layer 2 is a generic term which designates IT systems and protocols that are built upon public blockchain with the intent of addressing above limitations by improving transaction speed as well as cost. Participants on a layer 2 network can transact with high-throughput and only the result of their transactions is written to a public blockchain. This mechanism is particularly efficient when a set of participants are deemed to interact often.

Layer 2 solutions directly inherit from the security and decentralisation of Bitcoin. They increase throughput by taking heavy computation off-chain. They batch a large number of transactions together, generate a validity proof that is committed on-chain to update the state (who owns what).

Given Wecan's ecosystem, it makes total sense to transact on Layer 2 and bundle transactions (roll-up) on a regular basis, hence being scalable and realising huge savings on transaction costs (gas fees) at the same time.

7 https://bitcoin.org/bitcoin.pdf

Vaults

Our Infrastructure is aimed at a network of participants, whether physical persons or organisations, which have requirements around gathering or sharing of data.

From a technical standpoint, a Vault is a logical unit which holds structured (datasets) and unstructured (documents, pictures, etc...) data. At the lowest level, each Vault's content is fully encrypted with a different cryptographic key which makes the entire environment barely attractive to hackers.

Participants can establish secure channels with each others' vaults and organise seamless key exchanges securely and privately. This latest mechanism allows data exchange between participants with end-to-end encryption.

Finally, each participant owns one or many Vaults and has the ability to open/close channels on a fine grained basis ensuring that they can keep the highest level of control and confidentiality they deem necessary on their proprietary information.

End-to-end Encryption

All along the design process, choices made were following a Security First principle and the most secure cryptographic mechanisms have been implemented to meet this principle.

Every piece of information collected in Wecan Comply is fully encrypted (in flight and at rest) and a unique set of keys is used for each account. Wecan Group employees or providers have no ability at all to access personal or organisational information as keys are protected by the most secure cryptographic mechanisms through secret passphrase derivation.

To guarantee ease of use and conformity with classic enterprise processes, additional capabilities have been implemented to allow Organisations' administrators to benefit from keys' recovery capabilities as long as one administrator has access to his secret passphrase.

Encryption principles for information security
Each Organization is assigned a random pair of asymmetric keys (OK: Organization Key and OPK: Organization Private Key) which are stored on the platform, the private key is never stored in clear text but encrypted with Key Masters' public keys (see further below).

Each User is assigned a random pair of asymmetric keys (UK: User Key and UPK: User Private Key) which are stored on the platform, the UPK is itself never stored in clear text but is encrypted with a passphrase derived symmetric key (see further below). The first User of an Organization is given a Key Master role, this role is transmissible to other users allowing several Key Masters in each Organization. Each Key Master has access to a personal copy of his/her Organization Private Key (KMOPK: Key Master Organization Private Key) which is never stored in clear text on the platform but encrypted using key master's UK.

Each Vault belongs whether to a User or an Organization and is assigned a random symmetric key (VK: Vault Key) which is used to encrypt the vault's entire content (datasets and/or files). The VK is never stored in clear text but encrypted with its owner's UK (or OUK).

Whenever a user provides access to one of its vault to another user, a personal copy of the VK (UVKC: User Vault Key Copy) is created and asymmetrically encrypted using the UK. The UKVC is stored on the platform.

Users Private Keys are the only mean available to access Vaults' content. UPKs are very sensitive piece of information and are never stored in clear text. In order to avoid their loss, which could result in an ability to access one or many vault's content, UPKs are stored encrypted using 3 different methods allowing for different recovery mechanisms.

Method 1
UPK is protected using a first passphrase derived symmetric key. In this method, the passphrase is a NIST compliant password that the user only knows. Passwords (or their hashes) are never stored on the platform.

Method 2
UPK is protected using a second passphrase derived symmetric key. In this method, the passphrase is a combination of 12 random words that the user is given when he is on-boarded on the platform. The user is instructed (and should) keep these 12 words in a safe place and can re-use them as a recovery method in case he/she forgets his password. These 12 words combination are never stored on the platform.

Method 3
Finally each UPK is encrypted using the his organization public key, allowing Key Masters to reset a user password and re-encrypt the UPK via Method 1.
The above model ensures that no data, nor files are ever stored in clear text, that each vault has different encryption keys, that the system is extremely resilient to brute force and that, for as long as a user (or his organization's key master) remembers his/her password or has access to its 12words list then the entire dataset is safe against and attack as well as data loss.

Depending on needs, the following algorithms are used all across the platform:

- AES (Advanced Encryption Standard) for symmetric encryptions
- RSA (Rivest–Shamir–Adleman) for asymmetric encryptions and data signing
- SHA256 (Secure Hashing Function) for hashing
- PKDBF2 (Password-Based Key Derivation Function) for symmetric keys derivation

5 • Token Economics

The Wecan Token Description

The Wecan Token is a pure utility token inspired by a model that has been tried, tested and validated by the Blockchain community: the Request network[8], one of the Shareholders of Wecan Group. The Request token has indeed proven itself and has a tokenonomics model adapted to the very similar Wecan Token. Note that the Request token (REQ) is the 223rd largest crypto-currency on the market, and has a market cap of nearly US$300 million following a 10-fold increase in its value between August 2021 and December 2021[9].

Based on the Request model, the Wecan Token is a pure utility token which allows to finance each transaction / registration on Wecan Chain to guarantee security, auditability and decentralization with registration on a public blockchain.

The token system is implemented in Wecan Comply in such a way that the token component is most easily digestible for the user. To this end, the user might buy some fixed number of data exchanges (messages, file transfers and more) on the front-end side when buying tokens on the back-end side.

Wecan Group is following a community-based, co-creative and collaborative approach. Like collective platforms, Wecan Comply allows its community to create data forms specific to each profession, activity or information flow which can then be shared with the community.

The following flow illustrates the utility of the Wecan Token:

1. An organisation user, say a Bank, wishes to access the information of a person type user, say a customer wishing to open an account in the said bank.
2. The organisation user sends a data form to be filled in to the person user.
3. The person user validates the sharing of his data with the organisation user. In doing so, the exchange of data takes place for a **transaction fee** (*T*) (always equal to US$ 0.001 and paid for in WECAN tokens) charged to the organisation user and which will be sent to Wecan Group to feed the network.

The transaction fee *(T)* will be used to support the blockchain's **transaction costs** (*TC*) both on Wecan Chain and on the public blockchain . A small portion of each transaction will also be **burned** (*B*). This gives us $T = TC + B$. This burner feature will be explained in more detail in the next chapter Token structure. The above example is valid regardless of whether the user is an organisation or a person. All steps are documented and stored on the Wecan Chain.

Summary of the main utilities:

- Wecan Token is used inside the Wecan ecosystem in order to pay the **transaction costs** *(TC)* on the blockchain.
- Users can pay for their data exchanges with Wecan Tokens.
- For each data exchanges (messages, file transfers and more) a portion of the tokens is used to pay the transaction are burnt.

8 https://request.network/en/
9 https://www.coingecko.com/en/coins/request-network

Macro Model

Money needs to be a medium of exchange, a unit of account and a store of value. The velocity of the stock of Wecan Token is primordial. To enhance the velocity of exchanges we need a high number of Token.

One of the key drivers of Wecan Token price is the interaction between Wecan Token supply and demand on the market. We can use the quantity theory of money developed by Barro (1979) in its standard model of gold price formation to determine Wecan Token price formation. This approach was firstly done by Pavel Ciaian, Miroslava Rajcaniova and d'Artis Kancs in their 2014 paper on the Economics of BitCoin Price formation[10].

The Wecan Token money supply (*MS*) is calculated in Equation (1) by multiplying the **total stock of Wecan Token** (*W*) with the **exchange rate of Wecan Token** (P_W) (i.e. US$ per unit of Wecan Token).

$$(1)\ Ms = W * P_w$$

The **Wecan Token money demand** (*MD*) is set in Equation (2) by the general **price level of goods and services** (*P*), the **size of the Wecan Token economy** (*Y*) and its **velocity** (*V*). The velocity measures the frequency at which one unit of Wecan Token is used for purchase of goods and services, and it depends on the opportunity cost for holding it (inflation).

$$(2)\ Md = \frac{P * Y}{V}$$

The Equilibrium is calculated in Equations (3) and (4) to determine Equation (5) in which the price of Wecan Token decreases with the velocity (*V*) and the stock of Wecan Token (*W*) but increases with the size of Wecan Token economy (*Y*) and the general price level (*P*).

$$(3)\ Md = Ms$$

$$(4)\ W * P_w = \frac{P * Y}{V}$$

$$(5)\ P_w = \frac{P * Y}{V * W}$$

The size of the Wecan ecosystem (*Y*) is an important factor here. This is one of the strengths of the Wecan Token model. Indeed, the Wecan Comply solution (launched in 2021 and used by more than seventy external asset managers and thirteen Swiss custodian banks) guarantee from the outset a leading ecosystem for the Wecan Token.

As Pavel Ciaian, Miroslava Rajcaniova and d'Artis Kancs did, we can rewrite logarithmically Equation (5) into an empirically estimable model of Wecan Token price in Equation (6). In this equation t is the time subscript and ϵ_t is an error term.

$$(6)\ P_T^W = \beta_0 + \beta_1 P_T + \beta_2 Y_T + \beta_3 V_T + \beta_4 W_T + \epsilon_T$$

Wecan Token **attractiveness for investors** (*at*), and **global macroeconomic development** (*mt*) still need to be incorporated into the model in Equation (7). *ß5* and *ß6* can either be positive or negative.

$$(7)\ P_T^W = \beta_0 + \beta_1 P_T + \beta_2 Y_T + \beta_3 V_T + \beta_4 b_t + \beta_5 a_t + \beta_6 m_T + \epsilon_T$$

The **attractiveness of investors** (a_t) here is closely linked to the size of the **Wecan ecosystem** (*Y*). The announcements in relation to the ecosystem (increase in the number of stakeholders: banks, EAMs, trustees, notaries, lawyers) on Wecan Comply, as well as the announcements of new cross-industries leaders will, by increasing Y, directly stimulate the **valuation of the Token** (P_t^W), as will the attractiveness of investors which will also increase the value of the Token.

10 The Economics of bitcoin Price Formation, P.CIAIAN, M.RAJCNANIOVA, A.KANCS, 2014 https://arxiv.org/ftp/arxiv/papers/1405/1405.4498.pdf

Token Structure

Token Supply: 100’000’000’000
Token Ticker: WECAN
Token issuer: WeCanGroup SA
Initial token price: 0.001 US$

- **Total stock of Wecan Token (W)**