LGO Group

Building Trust

White Paper part 2 - November 2018

Summary

In the part 1 of our White Paper , we described the architecture of a "*fair by design*" platform using a protocol that rendered market manipulation impossible. However, a robust platform can only reach its full potential in a healthy environment.

For that reason, and thanks to the success of our ICO, LGO Group is creating a healthy environment for the entire cryptocurrency ecosystem. Specifically, LGO Group has set a goal of building trust during every stage of the life of a crypto-asset, including its creation, its promotion, its purchase, its storage, and, of course, its use.

In this second version of our White Paper, we will begin by presenting LGO Group's plan, and the fundamental principles we abide by as part of our approach. We will then present the organizational structure of our teams, and expand on the role of each department in detail. To conclude, we will present LGO Group's technical innovations and major research topics.

1. An ecosystem that still frightens people

1.1 Lack of trust

Satoshi Nakamoto proposed *"a system for electronic transactions without relying on trust"* on 31 October, 2008. However, since the creation of Bitcoin, the main scandals that have rocked the community have been caused by the abuse of trust committed by certain operators. This may appear paradoxical at first glance, although it becomes obvious when we understand that "*without relying on trust*" actually means "*without relying on trusted authority*".

Not relying on trusted authority, which limits the recourse for victims of fraud, has often been interpreted by unscrupulous individuals as a way to circumvent the fundamental principles which enable a secure marketplace. The Bitcoin community quickly realized that a "*trustless system*" was an ideal environment for the acts of *"trustless people"*. Potential solutions such as the "web of trust" have emerged, but this type of system based on reputation has struggled due to the difficulty of consistent implementation.

1.2 Lack of security

Over US$1 billion in crypto-assets were stolen between January and June 2018 (1), and the list of hacking attacks grows longer every day. The popularity of crypto-assets among "cyber-criminals" is explained by their intrinsic attributes, i.e. anonymity and non-reversibility. In fact, unlike a bank account, anyone can create a Bitcoin address in just a few minutes and perform transactions without any central authority in place to cancel them. We believe that this explanation is wrong, since most of the known hacking attacks are a direct consequence of a lack of professionalism among operators who are not sufficiently informed of the associated risks (2).

1.3 Lack of regulation

The U.S. Securities and Exchange Commission (SEC) describes the existing platforms for crypto-assets as an "unregulated mess" (3), and requests that professionals who wish to invest in ICOs exercise extreme caution (4). Most regulatory agencies throughout the world have reviewed the case of crypto-assets, although most have not issued clear and detailed legislation regarding them. Many people have taken advantage of this legal void to create platforms or launch ICOs outside any legal framework, and without any means of recourse. While some individuals may have a greater risk tolerance, several institutions will not take these types of risks without defined regulation (5).

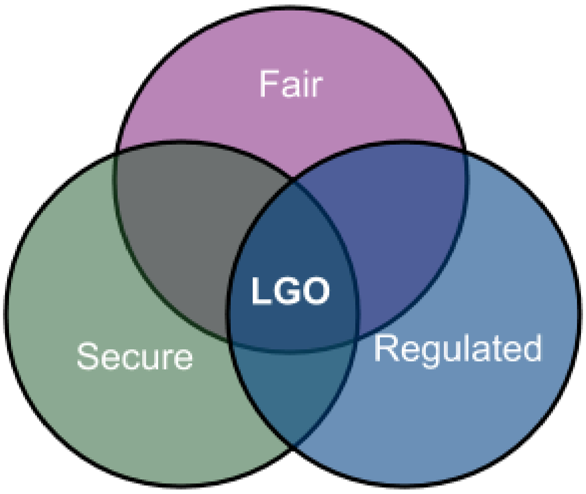
2. Solutions are within our reach

In order to mitigate the problems mentioned previously, LGO is proposing a comprehensive and consistent environment that systematically leverages components and ensures each action can be independently verified by its users. Accordingly, none of the components of the system require blind trust, which is precisely what enables people to use it with complete confidence: *"trustless therefore trustworthy"*.

The lack of security in the ecosystem can be addressed. The tools and methods that secure digital assets are well-known, such as using a *"hardware wallet"* or *multisig* addresses. The design of our platform has been governed by strict security rules since its inception: it is a *"secure by design"* platform.

Meanwhile, where the regulation of the market is concerned, it is now possible to establish a legal framework with processes that enables institutions to invest in crypto-assets and ICOs with the assistance of international experts and the collaboration of regulatory authorities. Our teams are establishing this framework, which is described later on in this document, and all of our activities are *"regulated by default"*.

Accordingly, LGO's approach is to build a trustworthy environment for all of the operators: A trustworthy, secure, and regulated environment.



3. LGO’s golden rules for building trust

3.1 Hybrid architecture

LGO’s goal is to build a “fair by design” platform, and not a completely decentralized platform. To ensure that a system cannot be manipulated by those who maintain it, that system must have two attributes:

- Verifiable,
- Multilateralism.

Verifiable implies logging all of the actions performed by the system on an immutable medium. The Bitcoin blockchain is the best technical tool for this function, because immutability can only be promoted by a medium free of any central control.

Once the actions have been logged, it is not necessary for the system’s actions to be systematically executed in a decentralized manner. Conversely, it becomes necessary for some information not to be revealed before a certain event. For instance, the content of a trader’s order must not be revealed before its place in the order book has been determined. This is the point when **multilateralism** becomes relevant. By allocating the information among various operators with different interests, we can ensure that none of them are in possession of all of the information. Therefore, no single entity will be able to use the data for their own interests.

This is what we call **hybrid architecture** at LGO, i.e. using decentralisation to ensure verifiability and multilateralism in order to promote the protection of sensitive information. This type of architecture avoids the constraints of completely decentralized systems, while achieving the same functionality, performance, and security of a fully centralized system.

3.2 The two-man rule

The two-man rule mandates dividing the power of performing important tasks between multiple people. It adds a layer of control and security by the fact that actions must be performed jointly.

In the LGO environment, all of the operations which enable individuals to take control of funds, either directly or indirectly, require verification and authorization by more than one person. This applies to the monitoring and approval of transactions in crypto-assets, as well as for publishing an update to the platform online.

3.3 End-to-end security

End-to-end security involves the systematic implementation of security mechanisms at the connection points. In the case of LGO, this primarily means that we supply our users with the software and hardware tools required to comply with the best security practices for the storage of crypto-assets and the signing of transactions.

3.4 Error-prevention system

The LGO environment is designed in such a way that any errors are immediately identified and corrected. This is particularly important given the non-reversible nature of crypto-asset transactions.

The four main error-prevention mechanisms that LGO uses are:

- Multilateralism, which provides effective protection against theft, or the loss of one of the three keys;
- Manual controls on all critical operations by several people (see the two-man rule);
- A "machine learning" system to identify and flag unusual behaviours such as ”fat-finger” errors;
- The implementation of holding periods before the execution of non-reversible transactions such as withdrawals, in order to give the user an opportunity to cancel or modify them.

3.5 No unilateral controls on our customers' funds

Given the lack of a central authority, one of the main challenges for scaling in the crypto-asset environment is building effective mechanisms to protect against counterparty risk.

To solve this problem, LGO has elected to never have total control over its users' funds, but instead shares that control between:

- the users;
- regulated partners such as custodians, clearing houses and banks;
- LGO.

Sharing responsibilities among multiple entities enables the highest level of security and aligns with the best practices of the traditional financial sector.

3.6 Legal compliance as the foremost prerequisite

The technical architecture and the processes of the LGO environment have been designed in collaboration with our legal and regulatory partners. Therefore, the current regulatory framework is taken into account by the technical and product teams. This is the reason why we are able to have partners and customers among regulated financial institutions.

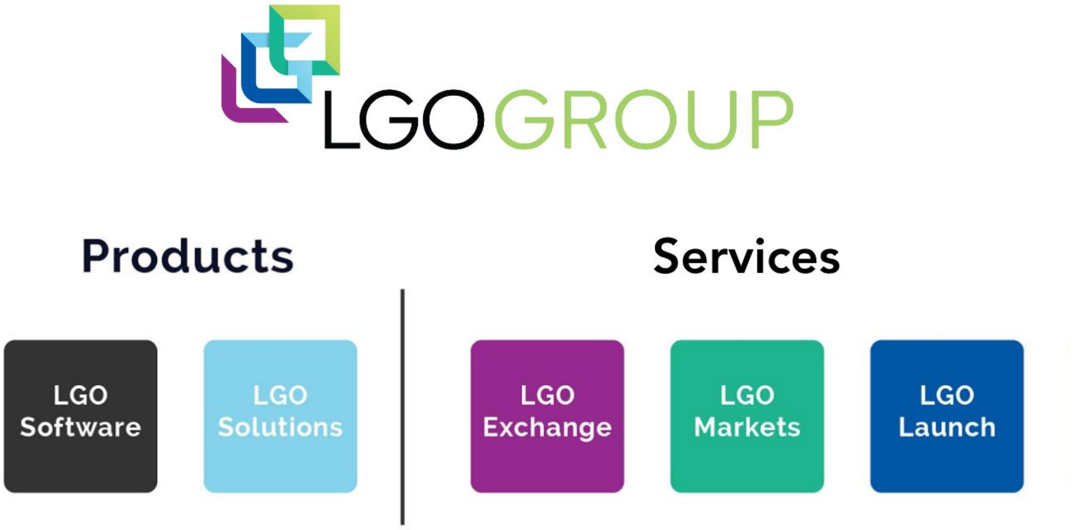
Furthermore, our teams maintain regular communications with the regulatory authorities, which allows us to be accurately informed, as well as to help those authorities understand the specific features of the crypto-asset ecosystem.

4. LGO Group, an organization that lives up to our goals

LGO's aim is to build trust in the entire crypto-asset ecosystem. Accordingly, the scope of our remit covers a wide range of technical and legal issues, and therefore requires a thorough organizational process. The challenge posed by this organizational process consists of pooling expertise, to the extent possible, while allowing every team a maximum amount of independence and flexibility. This means that every team is in a position to take advantage of its own potential to the maximum possible extent, as well as to benefit from the other teams' expertise in an optimal manner.

LGO is divided into two types of departments: the "product" teams and the "service" teams. The responsibility of the service teams is to design out-of-the-box services based on the product teams' innovative developments.

In fact, it is crucial for the crypto-assets used, which circulate between our various services, to be fully legal and compliant with the laws in effect, as well as with our values. We will refrain from working with digital assets issued via suspicious ICOs or traded for market manipulation purposes.



4.1 Team

Our main goal is to create a trusted cryptocurrency platform. This is why, since day one, we have been striving to put together an unbeatable team with a surplus of talent.

The LGO team is composed of entrepreneurs, investors and software engineers who have worked, co-founded and exited companies in the past.

As of September 2018, our recruitment efforts have certainly paid off and we are proud to have welcomed more than 30 people to the LGO family in New York (US) and Bordeaux (France), working everyday to bring the project one step closer to launch. Our goal is to offer the best product and level of service to our clients. We believe this is possible with our great team.

4.2 Products

LGO Software and LGO Solutions develop the software applications and the hardware tools used by the teams responsible for the LGO services. The main LGO products are:

- A "fair by design" hybrid platform
- A platform for ICOs
- An HSM (Hardware Secure Module)
- A hardware wallet

4.3 Services

LGO Markets operates a trading platform for institutional investors.

LGO Exchange is a trading platform for retail investors.

LGO Launch provides services to clients that function to expand their reach to the widespread crypto-community.

5. LGO Exchange & LGO Markets

We aim to bring to both retail and institutional investors the same level of security and fairness. Our approach is to provide two separate trading platforms, leveraging the same technological stack. This is why, in order to accommodate the needs and requirements of each type of client, we will launch two adapted platforms: LGO Markets for institutions and LGO Exchange for retail investors.

5.1 Fair by design

LGO promotes fairness and transparency by utilizing an innovative anti-front running solution and a novel blockchain-based technology. Blockchain technology is the main mechanism that makes it possible to reintroduce trust in an industry that lacks transparency. Our trading platform is built on a semi-decentralized protocol, in which the orderbooks and the trades are saved on a blockchain.

5.1.1 Anti-front running protocol

The main characteristic of our trading platform is the Anti-Front Running module, which belongs at the center of the LGO protocol. It is designed to meet our values by matching the requirements of traditional stock platforms both in terms of security and transparency.

The LGO protocol requires the user's order to be confidential before reaching the platform and nobody can know the client's order content. Moreover, the protocol protects the trading flow from any malicious treatment or market manipulation. We use the blockchain as proof of the orders' placement on the platform. Anyone will be able to verify the trades which were executed and the orders that were placed beforehand are logically and transparently linked. The trade records are publicly available and can be audited.

5.1.2 Traceable and auditable

LGO believes that the only efficient means of reporting rests with technologies making every platform operation traceable in a public blockchain.

The essence of blockchains is to be immutable. Once a block is written onto a blockchain, data is legitimized and becomes very difficult to change. The Bitcoin blockchain is a publicly distributed decentralized network, meaning nobody "owns" it. As LGO will batch all orders placed on our platform and engrave a footprint in the blockchain, this will make our trading activity fully traceable and auditable. Most of the current platforms today define transparency as delivering log files generated under their sole control and not in real time.

5.1.3 Matching Engine

The Matching Engine takes orders as an input, matches them and produces trades as an output.

The behaviour of the matching engine is absolutely deterministic. Given a starting snapshot and given the same sequence of events, the business logic ends up in exactly the same state and produces exactly the same output. This is beneficial for testing, recovery, diagnostics, analytics and auditability. The matching engine will use algorithms designed to handle high volume trading and large orders.

In order to deliver a fair platform, we need to find the best balance for all investor types and order sizes issued. We don't want to set up priority rules that will create disadvantages and frustration. An optimal trading platform is built with matching engine algorithms that avoid phantom orders and striking an equitable balance that rewards both liquidity providers and market participants.

The matching engine algorithm needs to create a balanced environment by leveraging various criteria such as time, price and volume. We believe it is crucial in order to build a framework that will attract investors with rational behaviors who want to trade efficiently.

5.2 Secure by design

5.2.1 Secure onboarding and authentication

The objective of the LGO onboarding and authentication process is to identify our clients and to create a trusted environment for them.

As several exchanges have been the victim of hacks throughout the years, the LGO team wants to bring a high level of authentication security to this marketplace. We will utilize a strong authentication mechanism in order to access our platform.

For each connection, we actively monitor who tries to access the platform. We require users to verify their identity; all institutions and traders must successfully complete LGO's onboarding process. This includes Know Your Customer ("KYC") and Anti Money Laundering ("AML") reviews. The connection to the platform is then initiated via a hardware wallet.

KYC is the process of obtaining information about a client's identity, assessing potential risks of illegal intentions and ensuring full compliance of the source of funds. AML checks are done to ensure that institutions and individuals are not on any sanction lists in the United States or other countries. These requirements are in line with traditionally regulated entities.

5.2.2 Hardware wallet

We have opted to use a hardware wallet to:

- Verify a user's identity;
- Secure movements of funds.

The hardware wallet is highly recommended for substantial holdings. Moreover, it will significantly increase safeness and trustworthiness of the transactions happening through LGO.

5.2.3 Multisig wallet

In order to promote the protection of orders and the signing of transactions, LGO utilizes the "two-man rule". This requires the consent of two parties to authorize access to sensitive information or any transfer of funds.

Accordingly, we will exclusively offer a 2-of-3 multi-signature wallet that will de facto comply with our two-man rule, in order to avoid unilateral control over the funds, and enable shared management.

All of these arrangements provide a high degree of protection for the data and enable the full safeguarding of funds in the event that a key is stolen or lost.

Traders will find an environment that ensures the integrity of their funds on the LGO platform thanks to a portfolio dedicated to trading activities.

5.3 Regulated by design

5.3.1 Clearing Firm

In the traditional financial industry, clearing firms are responsible for components of the post-trade processes. They are highly regulated and are used to routinely process millions of transactions, ensuring the accuracy of the trade details and seamless settlement.

At LGO, the Clearing firm's role is to::

- Maintain custody of one key for the trading wallet;

- Handle the confirmation, settlement and delivery of the transactions.

This setup is a complete innovation in the cryptocurrency space: LGO is not claiming custody of any assets, and thanks to the 2-of-3 multi-signature feature of our clients' wallets, their funds are at no time at risk of being lost or stolen. This is a unique and secure transaction management system that we are deploying on the platform.

As a result, clients will be able to focus on buying and selling cryptocurrencies without worrying about the safety of their funds.

Through strong partnerships with clearing firms, LGO Markets clients will have accounts at established fiat custodians in which they'll be able to deposit fiat currency. This is a differentiator in the cryptocurrency platform industry. On several platforms, fiat money is usually deposited in an account controlled by the platform operator. This makes deposits (especially large ones) slow and difficult to complete.

In this configuration, our clients will have a segregated account in which their funds are held separate from the funds of LGO and other clients.

The account is under the client's name and LGO Markets has no right over it.

When a client makes a fiat deposit, the clearing firm notifies LGO. The client's balance is then updated to reflect the deposit and funds are made available for trading.

At LGO Markets, we make a clear separation between clients' funds. The main reason is to help ensure that the money can be easily identified as belonging to customers, which lowers their risks. In a traditionally regulated marketplace, there are stringent rules governing the separation of customer funds and securities (7).

5.3.2 Settlement

Each LGO client has its own segregated account and its own wallet. Because of this setup, we have to introduce a concept that is key in the traditional financial space: the settlement of trades.

The clearing firms will receive all executed trades at LGO and proceed to clearing and settlement of these trades accordingly.

Settlement in a multi-signature wallet environment will require the clearing firm to countersign any transaction using their key before broadcasting to the blockchain. Every movement of funds will be verified by both LGO and the clearing firm.

5.3.3 Transparency

All order data will be stored in our internal databases (off-chain) and a footprint on the blockchain (on-chain). Blockchain storage means that this data will be publicly accessible at any time for traceability and auditing purposes. It won't contain any Personally Identifiable Information ("PII") as this information is stored off-chain and encrypted in our databases. In addition, we will have technical logs for all the flows on the platform (deposits, withdrawals, orders, trades, etc) for audit purposes. This is in line with recordkeeping requirements at traditionally regulated firms.

5.3.4 Compliant tokens

LGO Markets, through its affiliate LGO Securities, is applying for a FINRA membership and as an Alternative Trading System ("ATS") with the SEC. Once we are approved, it will permit LGO to list tokens (which are considered as securities by the SEC) and be compliant with the United States securities laws.

As such, we will follow strict internal and external guidelines when listing new tokens on our trading platforms (8).

Wash trading and price manipulation have been common in the cryptocurrency market. LGO will establish rules regarding any asset listed (9) on our platform. The goal is to create a sound regulatory framework.

We will continuously monitor the trading on our platform in order to identify and remediate any manipulative activity. When listing new tokens, we will comply with all rules from the applicable regulators within the United States.

5.4 Performance by design

5.4.1 Scalability

The LGO platform is designed to support any digital asset. Listing new products will possible as our components (API, Matching Engine, ...) are agnostic to the asset being traded. When necessary, our back-office processes will be adapted for accounting purposes.

5.4.2 High Throughput

Each block on a blockchain contains a limited amount of information. This creates limitations when the activity on the platform grows beyond network capacity. This low throughput is a major obstacle for trading, as delaying a client's order due to technological limitations is unacceptable.

Our trading platform is designed to maintain industry-level trade execution time while leveraging the blockchain technology with our anti front-running protocol. By processing multiple orders per batch, we are able to reach a high volume of transactions issued per second.

5.5 Standard Interfaces for all usage

5.5.1 API (Rest, FIX, websocket)

LGO will propose different ways to access the trading platform, according to our customers' needs and size. A Websocket API will be implemented to reach our platform functionalities and retrieve the latest trades and orders in real time.

In future release, we will also be compatible with the Financial Information eXchange (FIX) protocol, the most efficient standard of the industry, to receive market quotes and place orders.

5.5.2 User Interface

Most of the interfaces proposed by our competitors appear in the form of web interfaces. Web apps have many advantages:

- there is no installation (the application runs on the browser);
- the ecosystem has been tried and tested by a large number of developers;
- the application does not depend on the OS.

Considering the significant amounts of money that could be transacted by our customers on the platform, the security is a strong aspect of our application; we cannot rely on a browser that could be compromised.

The Electron framework enables us to create an application based on web technologies. By using this framework, we will retain the advantages of web-based technology, while gaining greater control over the environment in which our application will run. The use of Electron enables us to gain access to the machines' hardware (USB ports) in a straightforward manner.

We have made the decision to use the React and Redux stacks in combination with Electron.

This stack has already proven its ability to support a large number of simultaneous connections. A vibrant community and ecosystem ensure the sustainability of this powerful stack.

TypeScript is the language used the Electron developments, it has been created by Microsoft and it enables a type system to be added to JavaScript.

The typing introduced by TypeScript has several advantages:

- a stronger code
- simplified re-factoring
- natural documentation

6. LGO Launch

LGO's mission is to create a fully regulated platform to buy and sell crypto-assets. In order to scale this platform effectively, we must be able to accommodate and service external clients on a global scale through a structured process. Therefore, we established LGO Launch - an agency to provide services to external clients which function to extend their reach to the wider crypto-community.

Furthermore, LGO's knowledge of the crypto-community is unmatched and backed by experience. The LGO Launch team utilizes a content creation, diffusion, and traction approach that is unmatched in the industry.

6.1 New Markets, New Economy

The scale of LGO's global impact, the size of the community we built, and the level of success of our ICO attracted interest from other entrepreneurs in the blockchain space. As they were conducting their own token sales, they approached us seeking strategies, knowledge, and guidance. Because we wanted to promote the opportunities presented by distributed ledger technologies, we decided to help them in a very informal manner. In addition, a number of existing companies that have implemented blockchain solutions into their existing processes approached us, looking to strengthen their community outreach regarding their developments and product releases.

We quickly came to understand how valuable our strategies were for these projects, and realized that **a structured system needed to be created to provide these services in a more formal manner.**

As we need to grow our network ahead of the platform's launch, we believe that providing our services and support for external clients will bring both a new community and a wealth of knowledge onto our platform.

6.2 LGO Launch Services

It is important for LGO Launch to follow the high-quality standards set by LGO Markets & Exchange, which is why each potential client will be thoroughly reviewed and vetted by our team and advisors before any onboarding discussions are considered. This pre-onboarding stage is essential to making sure all interests are aligned.

LGO Launch offers the following services:

- International Marketing: raising awareness all around the globe
- Content and Multimedia Production

- Ad Campaign Management
- Social Media and Community Management
- Public Relations

7. LGO Solutions

End-to-end security is clearly not a respected practice by most of the existing crypto platforms. It is never a good practice for users to keep cryptocurrencies in unprotected distant wallets on unregulated and uninsured platforms or in unsecured local software wallets. If crypto-assets are required to be stored online, even for a short period of time, it should be done inside a dedicated secure hardware called an HSM (Hardware Security Module) and they should have local control of private keys, one would rather use Hardware wallets. Both solutions are separately safe and highly recommended but can even be combined through multi-signature to obtain the highest level of security. LGO Solutions will bring innovative products with built-in smart card based security as a new high security standard in the crypto space.

7.1 Full security for crypto asset management

The main goal of our strong authentication control is to strictly identify, for each connection, who tries to access the platform. LGO has learned from the mistakes made by hacked crypto platforms and wants to bring a high level of authentication security.

We believe an optimal security level can only be ensured by a secure electronic solution based on "smart card" components (Secure Elements) that embed software adapted to the storage and use of private keys for sensitive digital assets.

After a long string of failures that hit "crypto-assets" owners, it is time to introduce a new framework to protect cryptocurrency wallets.

LGO Solutions will develop and offer security products through:

- Smart card based hardware wallets for crypto-asset owners
- Hardware Security Module (HSM) for service providers (platform, vendors, neo-banks)

In addition to our "turnkey" offerings, we will integrate our solutions into the infrastructure, products and services (OEM, white label, custom) of our customers and partners.

7.2 Hardware wallet

Hardware wallets are highly recommended for substantial holdings. Moreover, it will significantly increase the safety and trust of the transactions happening through LGO services. Our team will provide hardware wallets to all of our institutional investors.

Hardware wallets are required for authentication and as well for transactions validation.

Private keys are generated, stored and used inside the secure element of the hardware wallet, and are never exposed to unsecure operating systems and applications.

Hardware wallets are used on offline air-gap machines for special cold wallet storage.

7.3 HSM

When partially automated signature for the custody wallets are required, some private keys must be live, and may be at risk. An HSM is a physical computing device that safeguards and manages cryptographic keys, providing secure execution of critical code: in our case, the transaction signing.

HSMs have built-in anti-tampering technology that wipes secrets in case of a physical breach. They are architectured around secure cryptoprocessor chips and active physical security measures. These devices are heavily used in the financial industry, particularly when critical secrets must be protected.

As a hardware wallet, private keys can't be extracted from an HSM. Initialization and backups are done on "m of n" secure backups. Restoration of private keys can't be done with one person or one access and requires a complex procedure involving the gathering of several members and securely stored partial secrets, rendering physical attacks (on servers or on people) useless.

8. Annexes

1. Clearing & Settlement processes

LGO Markets will provide a platform to institutional investors. As a result, clearing and settlement are fundamental processes of the platform. After a trade is executed, the record is submitted to a clearing firm, which confirms that the counterparts agree to the trade.

The settlement firm receives securities from the seller and cash from the buyer and gives securities to the buyer and cash to the seller.

This process is made to reduce risk: it provides trust between two traders by checking that both sides are trustworthy and creditworthy. In addition, it makes trade possible between two parties that do not necessarily need to trust one another.

1.1 Domain context

A trade lifecycle is divided into three parts:

- Execution, when the trade is created by matching orders
- Clearing, with two sub process: reconciliation in which the trade validity is checked, and netting to produce newer balances
- Settlement when assets are actually exchanged

This lifecycle is why banks manage their trading activities into three entities: the front, middle and back offices.

In our case, the Clearing and Settlement processes will be processed by the same entity described in the following document as a « clearing Firm ».

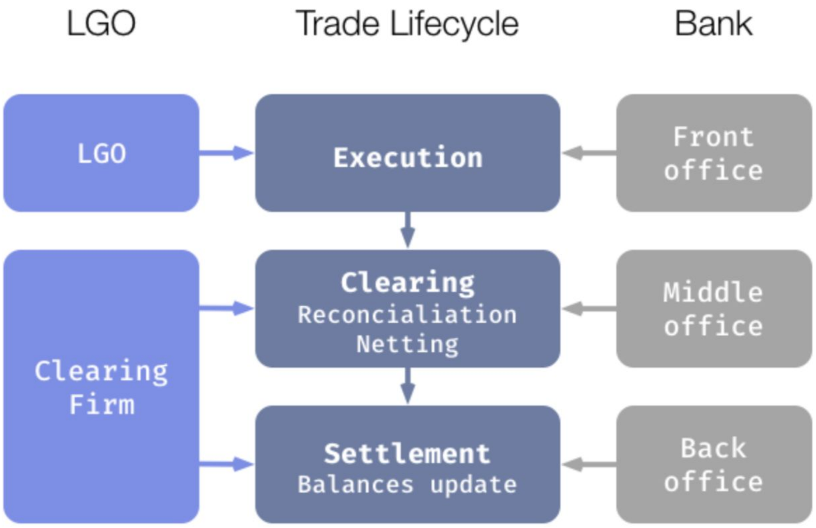


fig 1.1: Overview of a trade lifecycle

Ultimately, the clearing and settlement mechanisms could be decoupled and operated by separates legal entities.

1.2 Temporal context

In order to avoid a continuous flow of cash between the trading actors' bank accounts, the clearing and settlement process will be triggered with a specific time interval between two runs.

The process will be triggered as a specific « cut off » event in the orders' flow to avoid any race condition.

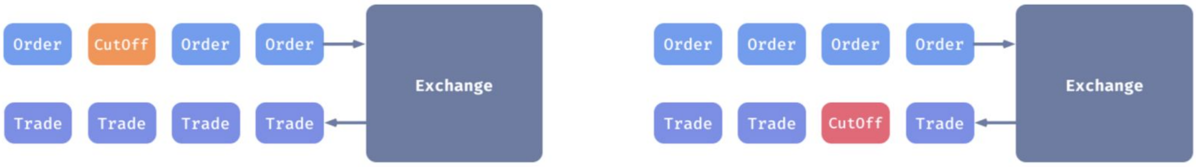


fig 1.2: Cut-off event inserted in the platform flow

Of course, this event handling will be designed to have a minimum impact on the platform 's operations and should allow us to launch the clearing process while allowing the platform to continue processing orders.

1.3. Temporal context, cashflow consideration

Thanks to the delay between two settlement processes, we will be able to aggregate transactions into a multilateral netting operation.

We can use multiple input with multiple output transaction to mimic a multilateral netting on the bitcoin network.

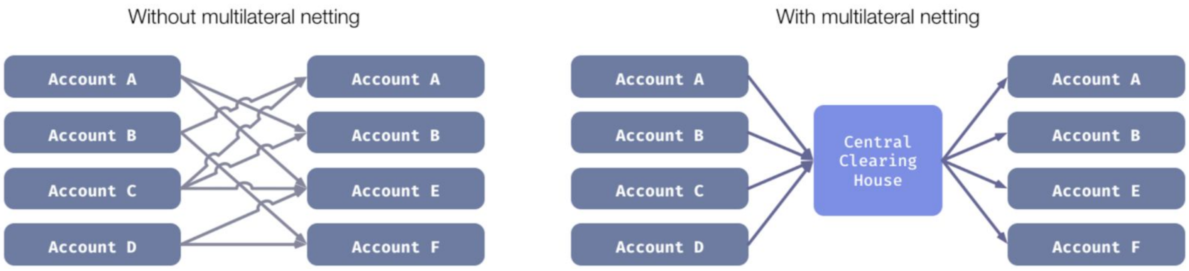


fig. 1.3 : Multilateral netting

2. Architecture

To ensure the lowest latency possible in the processing of a batch and to promote the valence of operations, in particular the balances' updates and the platform's critical processes, some strong architecture principles must be established and respected.

2.1. Low latency

Critical platform components (management of balances, matching engine) perform all business processes on a single thread, having access to all the data needed to do the job in memory.

Waiting for a database query to execute can be slow; the same statement is true for in-memory caching because disk access or network access involves too much latency and risk of IO errors.

The price to pay for distributing business processes over multiple threads is also too high in terms of primitives synchronization, even using green threads.

To ensure that as much work as possible is provided to the business thread, other threads are busy listening to the network to retrieve or send messages, save them, and deserialise/serialise them.

To synchronize work on all threads, a competition pattern, the disruptor, is used to succeed in doing so as quickly as possible (10).

By optimizing the business code and taking care of memory consumption, this approach can reach several million operations per second.

To recover the memory state, all the input messages are saved on disk quickly, thanks to memory mapping and writing in append only. They are simply replayed at the start of the application. This requires our systems to be perfectly deterministic, therefore banning edge effects.

To eventually go back up to this state more quickly, snapshots are produced at regular time intervals.

To track the production rate of critical component messages, LGO relies more on natural network capabilities rather than using a broker (RabbitMQ, Redis, or pub/sub). The use of reliable multicast protocols covers this need without involving a broker.

Since everything runs in RAM, and must run as quickly as possible, there is a strict minimum required for critical services (for example, updating balances after order execution). Projections are made by other components by subscribing to the events produced by these systems.

2.2. High availability

Since there is no traditional database behind critical services, the high availability of the data state must be ensured by other processes.

The adopted solution is to use a network consensus algorithm, RAFT, slightly adapted to the context of high frequency. RAFT ensures that in a cluster, a majority of members have received and written the message to apply (11).

Thus, all the members of our cluster receive all the messages and process them, but only the outputs of the leader are taken into account.

In the case of losing the leader, a member is always ready to take over.

2.3. Throughput

The different components which produce projections are more sensitive to volume than latency. Batch manufacturing by our anti-front running component optimizes writing in these systems.

Depending on the type of projection, a database built for this use can then be used. The price history is stored in a time series database which is very suitable for storing quantized data sorted by date. A time series database can then also easily produce aggregations in a given time period (e.g.: prices aggregated by hour in a period of a week).

The platform's activity history (completed orders, old trades), can easily be inserted into a traditional relational database.

Finally, market data are broadcasted to subscribers over FIX or websocket when execution engine events occur.

The scaling of these projections goes through the sharding in a fairly traditional way (e.g. launching as many processes, generating market data as there are products). The use of multicast for the propagation of events makes this approach work without slowing down critical services.

References

(1) $1.1 billion in cryptocurrency stolen in 2018

June 2018,
https://www.carbonblack.com/wp-content/uploads/2018/06/Cryptocurrency_Gold_Rush_on_the_Dark_Web_Carbon_Black_Report_June_2018.pdf

(2) New Study Says 80 Percent of ICOs Conducted in 2017 Were Scams

July 2018,
https://research.bloomberg.com/pub/res/d28giW28tf6G7T_Wr77aU0gDgFQ

(3) SEC says cryptocurrency exchanges are an unregulated mess

March 2018,
https://techcrunch.com/2018/03/07/sec-says-cryptocurrency-exchanges-are-an-unregulated-mess/

(4) Hackers steal almost $400M from cryptocurrency ICOs

https://www.ey.com/Publication/vwLUAssets/ey-research-initial-coin-offerings-icos/%24File/ey-research-initial-coin-offerings-icos.pdf

(5) Is 2018 the Year Institutional Investors Belly Up to ICOs?

https://thirtyk.com/2018/03/27/institutional-investors-icos/

(6) LGO Smart contract available on github

https://github.com/LegolasExchange/LegolasToken

(7) Customer Protection Rule Initiative

https://www.sec.gov/divisions/enforce/customer-protection-rule-initiative.shtml

(8) Opening Remarks at the Securities Regulation Institute, SEC Chairman Jay Clayton

https://www.sec.gov/news/speech/speech-clayton-012218

(9) Statement on Potentially Unlawful Online Platforms for Trading Digital Assets

March 2018,
https://www.sec.gov/news/public-statement/enforcement-tm-statement-potentially-unlawful-online-platforms-trading

(10) High performance alternative to bounded queues for exchanging data between concurrent threads

http://lmax-exchange.github.io/disruptor/files/Disruptor-1.0.pdf

(11) The Raft Consensus Algorithm

https://raft.github.io