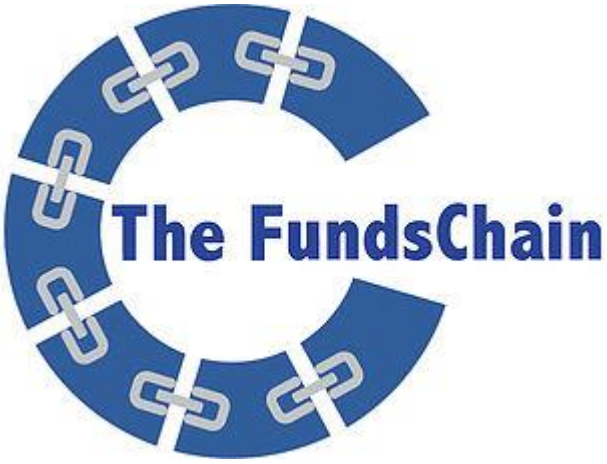


TheFundsChain

Distributed Ledger Technology for the Asset Management Industry

White Paper

November 2016

FIVE TAKEAWAYS FROM THIS PAPER

1. DLT has a strong potential to drive the asset management industry toward greater efficiency levels.
2. It is time for buy-side actors to thoroughly assess how their core business may be impacted.
3. Best use-cases lay at the upper end of the value chain, toward clients: appropriation of the investors' registry.
4. We advocate for an incremental scenario to gradually deploy a new mutualized infrastructure for funds.
5. *TheFundsChain* initiative strives to promote and coordinate the path toward such a future platform.

EXECUTIVE SUMMARY

Distributed Ledger Technology (DLT) has a tremendous potential for financial services. Its core feature, a distributed ledger, along with its indispensable companion, smart contracts, could address existing inefficiencies due to the need to reconcile heterogeneous data among participants.

The Asset Management industry will certainly benefit from DLT, notably by streamlining trade confirmation and settlement processes. As a long-term investor, Fund Managers hold and trade sizeable volumes of all kinds of financial instruments (shares, bonds, derivative contracts) that will be impacted by DLT. But innovation will be driven by other actors. At the vanguard of this revolution to come will be sell-side actors, as trading and settling financial instruments is their core business. How then would Asset Managers' core business, mutual funds, be impacted?

Designing, registering and selling funds is a unique business. In most cases, except notably for ETFs, there is no secondary markets for mutual funds' units (or shares). Mutual funds' units are created and cancelled on a primary market only. DLT could well be used for issuing securities, but managing a fund (i.e. dealing with subscription/redemption orders and keeping the record of ownership) is quite different from issuing other kinds of securities.

This paper argues that the most significant application of DLT to the Asset Management industry would be to develop a distributed registry of funds' units. Numerous processes could be leveraged from this foundation, from KYC to trailer fees calculation. In addition, keeping track of orders and investors' holdings on such a distributed ledger would make the whole distribution process more transparent and ultimately allow fund managers to get a much better knowledge of their clients. The re-appropriation of the investor's registry by fund managers is a key benefit developed in this paper.

Other DLT applications are also possible regarding the assets held by fund managers, covering a wide range of business processes, from Net Asset Value (NAV) to compliance and risk management. A distributed ledger keeping track of assets could be developed and integrated with the one keeping track of funds' units, in effect producing a real-time view of a fund's balance sheet. However valuable, such a development would prove more complex to build than the above mentioned registry of investors. Ultimately, a full-fledged DLT applied to funds would indeed yield a distributed balance sheet of funds. This paper suggests to focus on the liabilities side of funds as a first objective.

Eventually, such specific Asset Management ledger would be interconnected to other specialized financial ledgers (e.g. cash ledger, collateral ledger). Given the complexity and diversity of financial instruments, bespoke ledgers will be developed to specifically address the requirements from each segment of the industry. The resulting potential fragmentation issues are discussed in this paper.

To which extent will the Asset Management industry be affected by DLT?

As noted above, a new ecosystem of interconnected ledgers covering most industry's processes is a long-term scenario, say a decade or so. Indeed, given the existing infrastructure and the number of players involved, an incremental scenario is much more likely.

Still, there are more benefits to be gained from DLT adoption than plain disintermediation and the obvious cost savings generated by reconciliation-free processes. Analyzing different scenarios, this paper attempts to identify more subtle challenges. We contend that the most prominent, long-term benefit lays with the emergence of an efficient "distributed back-office", powered by DLT. In essence, such a distributed back-office platform would allow all participants to validate and share information, in a collaborative way. At present, information is fragmented along the distribution chain and controlled at various degrees by the actors of that chain. Some key participants are able to extract rents from data they manage but do not, fundamentally, own. The simple and most powerful idea behind DLT is to grant access to reliable information - confirmed and up to date - to every relevant actor. Perhaps more than the "immutable" DLT feature, the ability to efficiently share information constitutes a powerful leverage toward a brand new ecosystem of services. Indeed, exchanging certified and standardized data between service providers and consumers generates a formidable incentive for innovation and competition by ensuring a level playing field. As a result, Fund Managers would not be bound any longer to service providers controlling their data.

We reckon that the total costs savings generated could reach EUR 10bn annually and we expect final investors to benefit from this new paradigm promoting competition as well as investor protection.

Will this new ecosystem be completely deregulated?

On the contrary, a platform where certified data is shared among participants (obviously, with different access privileges) is the best way to promote transparency and investor protection. Regulators could be onboarded as active platform participants, either as proactive observers or, in some cases, as transaction validators. Compliance processes carried on by fund managers and distributors would therefore be vastly simplified, another important source of cost savings. We believe that DLT delivers its best value precisely in the context of highly regulated markets.

What are the regulatory impacts of such a technology?

DLT affects the way the ownership of assets is managed. Therefore, it potentially conflicts with existing regulatory frameworks. Process automation leveraging smart contracts may also raises some legal questions. In this paper, we argue that this is not a necessary outcome. On the contrary, we advocate for a transition path which would minimize legal issues, while keeping most of the technology's value.

What is missing to get there?

The final section of this white paper proposes a thorough assessment of the technology needed to make this vision possible. Clearly, the original blockchain was not supposed to support complex financial services beyond securely exchanging a digital currency without a trusted party. Hence the emergence of more general DLTs, powered by smart contracts, and the intuition that there will not be a one size fits all DLT. Some important characteristics of original blockchains are not required, and even defeat the purpose of certain financial applications. Open network, anonymity of participants and full disclosure of all transactions in particular are not desirable features, whereas some mandatory ones are missing, such as data privacy and granular access rights, or flexible consensus protocol according to the type of transaction to be validated. Besides, early blockchain technology lacked the scalability to support high volumes and throughput, as well as basic database features. The technology field is moving rapidly, though, and some solutions are now available. This paper takes the view to assess the technological features needed to match the business requirements from the asset management industry, and not the other way around.

The analysis developed in this paper has led to the conclusion that a joint effort from the Asset Management industry is necessary to design such a much needed dedicated DLT serving its needs.

WHAT IS *THEFUNDSCHAIN*?

TheFundsChain initiative is based on our assessment of the impact of Distributed Ledger Technology (DLT) on the Asset Management industry. As noted in the executive summary, we strongly believe in DLT potential to address the major challenges the industry is facing, notably but not only, regarding fund administration and regulatory compliance. As a first significant objective, setting up a dedicated distributed ledger to record transactions in funds' units would indeed be a real game changer for the industry. Managing funds' assets inventories would further reinforce this potential, in effect covering all processes. *TheFundsChain* is intended to serve buy-side actors in order to study and promote DLT applied to funds. It is technology agnostic.

We firmly advocate for the buy-side to develop its own DLT.

A passive attitude towards this forthcoming revolution would result in dictated technological choices and a limited share of the overall cost savings achieved. Most likely, business opportunities would be missed. Given the specificities of the Asset Management industry, it is very unlikely that ledgers developed without its active participation would meet its requirements and aspirations, especially given its different focus from the sell-side. To build the distributed back-office envisioned in this paper, the buy-side needs to pool its resources as this is not a turf on which fund managers are fiercely competing. As a first key deliverable, *TheFundsChain* initiative shall assess the most promising use cases for the industry, and identify some "quick wins", delivering actual incremental benefits.

We also advocate for the buy-side to develop its DLT in close cooperation with its partners.

Notably asset servicers, distributors and regulators. As our analysis shows, an incremental approach is much more likely to take place, since multiple parties are involved in this infrastructure build-up. Moreover, it is quite doubtful that a single actor, be it a software vendor or an asset servicer could achieve a monopolistic situation thanks to DLT and would be able to extract subsequent rents. In our view, a consortium-based approach potentially leading to a new utility, is much more plausible – and desirable. DLT has the potential to unlock tremendous innovation and foster competition among service providers in this industry. As *the main beneficiary* of such innovation, alongside investors, it is up to the buy-side to take the lead and initiate this new paradigm. *TheFundsChain* aims at helping the buy-side to become such a driving force, globally, with its business partners.

We finally advocate for the buy-side to become DLT savvy.

Although we expect to see the first concrete applications of DLT in a near future (i.e. new services or products running in production with a profitable business model), its full potential remains largely theoretical at this stage. Our analysis shows that DLT core functions (distributed ledger, smart contracts) could address existing business issues, but also that some **key requirements** (scalability, confidentiality, flexibility) remain largely under development: most required bricks are indeed available, but the integration effort is far from being completed. This is a technological revolution in the making: there will neither be a one size fits all DLT for financial services nor a winner takes all outcome. DLT is above all a technology, a nascent one. As such, it needs to be further developed and tested: specific use cases will define bespoke DLTs. It is thus critical for the industry to define its own business scenario and experiment about it. Eventually, **standards** will emerge, and fund managers should have a say in their definition. Although not a solution vendor, *TheFundsChain* aims at mutualizing buy-side resources to achieve this goal and to monitor and further spur innovation in that field.

TheFundsChain ambition is to serve the asset management industry in designing a dedicated DLT - "*TheFundsChain* platform" - and will take a number of initiatives to achieve this aim. We recently contributed to the ESMA consultation[1] on DLT.

[1] https://www.esma.europa.eu/file/19557/download?token=1oGKSa7O

On the Agenda

PART ONE DISTRIBUTED LEDGERS

WHAT THEY ARE

WHAT THEY ARE GOOD FOR

DISTRIBUTED LEDGER TECHNOLOGY

Main features of DLT

When first introduced in 2008, Bitcoin aimed to be a "purely peer-to-peer version of electronic cash". This simple statement was actually extremely ambitious as all previous attempts failed, typically by overlooking the "double spending" issue. Indeed, the key when operating a digital currency without any central authority is to make sure that a user cannot spend twice the same coins.

Whether Bitcoin as a currency will prevail remains to be seen. In the meantime, blockchain, the underlying technology powering Bitcoin, has generated tremendous interest from the financial industry, with a much wider scope of applications than digital currencies alone.

This interest mostly focuses on one of the core features of the blockchain: the distributed ledger, leaving aside other aspects deemed specific to crypto-currency applications. Hence the shift from "blockchains" to the more general term DLT (Distributed Ledger Technology).

The main features of any DLT are thus the following:

- **a distributed database**, that is the ability given to participants to share the same information;
- **a consensus protocol** allowing the participants to agree on legitimate transactions;
- **a stamping mechanism** for transactions: once validated, transactions become immutable;
- **secure authentication** of participants and of their holdings;
- a **real-time** settlement mechanism, which is a direct consequence of properly applying the consensus protocol.

DLT is based on various technologies, most notably:

- peer to peer networks;
- fault-tolerance protocols;
- cryptography (hash functions, public-key cryptography);
- distributed databases.

Although none of these technologies, considered separately, is truly innovating, DLT astutely interleaves previously independent technological streams in order to produce a "new alloy", with outstanding features of its own.

The original blockchain has proven its resilience over time as it has been working as planned since inception. Now envisioning an extended scope for new applications, it proves to be limited, as it was designed to be a peer-to-peer digital cash, and only that.

A QUESTION OF TRUST

In its October 2015 issue, *The Economist* famously coined the term "Trust Machine" to refer to DLT, together with a clever analysis of the promises behind blockchain technologies. A perfect vision. But does such a machine, or rather, the cryptographic algorithms it runs, really create trust out of vacuum?

Observing some public initiatives, such as Bitcoin or Ethereum, might be worth a comparison. Such platforms allow participants to exchange tokens as payment for some form of asset or service. And it works: such payments have indeed been secure so far. However, the promise of delivering the asset, or service paid for, is far from being guaranteed, as no rule-enforcing authority is entitled to provide such a guarantee. In lieu of such authority, buyers have to contend with a "seller's reputation", an external trust indicator which isn't part of the blockchain. To put it differently, **DLTs have a weak point: their relationship with the real world**.

Coming back to the business of exchanging securities, and especially mutual funds, which are a highly regulated form of securities for the sake of protecting investors' interests, our conclusion is that algorithms alone do not create trust by themselves. Instead, they would rather foster trust between participants, which already trust each other to a certain extent.

An all-round DLT platform would simply require too many links to the real world to eliminate the need for trusted participants. Such analysis naturally advocates the choice of a permissioned ledger run by responsible caretakers, which role is to feed "the machine" with trustworthy input from the outer world.

Even within the Bitcoin universe, Bitcoin wallet providers and marketplaces must also be trusted parties (to exchange BTC for USD or EUR…).

To take a comparison with the futuristic "Ethereum DAO fund", assessing the value of invested money (converted into "DAO tokens") also requires somehow a trusted party.

This observation corroborates our deep belief that DLT merely foster trust between parties but does not create it ex-nihilo. Or to put it shortly: **trusted, reputable, parties remain a key requirement to move around investments in financial assets.**

As such, its elegant design includes various features which do not quite fit with financial industry reality and requirements:

- open network: anyone can join as there is no need to trust the participants. The system was indeed designed to allow secure transactions in such a trustless environment;
- anonymity of participants;
- full transparency of all transactions recorded on the blockchain;
- complex and computationally intensive process to validate transactions ("proof-of-work"), which is somewhat a consequence of the platform's openness;
- internal economy relying on a built-in system of rewards paid to active participants.

As a result, the financial industry is embracing private (or permissioned) blockchains, aiming basically at keeping the desired features while fixing the controversial ones.

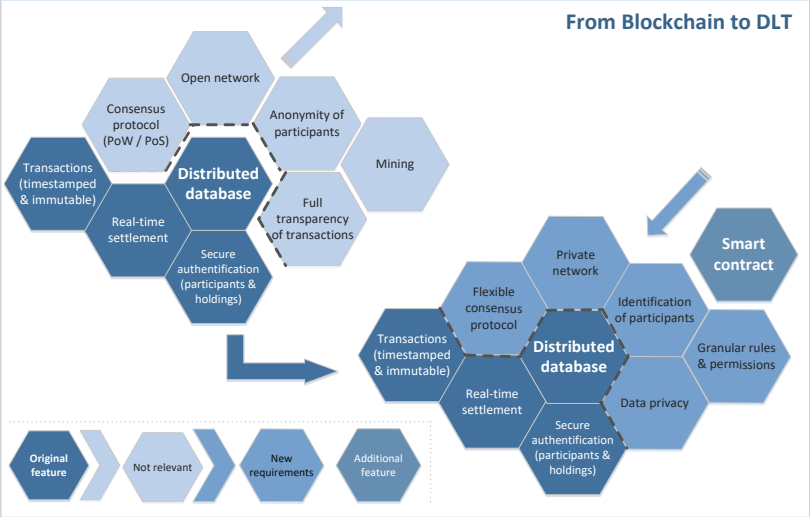
Those new blockchains, from now on called DLTs, are currently under development and require features which are not found in Bitcoin-inspired platforms (we develop further on these in the third part of this document):

- identification of all participants;
- granular roles and permissions attributed to participants;
- support for complex data structures;
- data privacy;
- flexible consensus protocol;
- scalable architecture (see box).

This list of additional requirements so deeply challenged the original developments that brand new platforms have had to be developed and experimented, retaining only the broad concepts from the original blockchain.

A number of platforms have thus spawned from the early pioneers, some publicly available, some proprietary. Each one comes along with original solutions to the many challenges ahead of a truly workable DLT for the financial industry.

Therefore, DLT is often to be used as a plural noun...



HIGHLY SCALABLE DLTs

The Bitcoin blockchain stores a very limited amount of information: this ledger is no more than a journal of debit/credit transactions. This ever-growing journal now amounts for about 75 GB, or almost 150 million of transactions.

All voting participants (or "miners") store a full copy of this database. Such amount of replication across the network of participants also generates network bandwidth issues and results in an inherent limit to the scale the system may reach.

In the context of a DLT adapted to fund management, a much larger scope of data is most certainly needed: in order to be able to handle transactions on fund products and to keep track of all investors and distribution channels, *TheFundsChain* platform should handle a much greater quantity as well as variety of data.

Fortunately, DLTs have now largely overcome the initial limitations of the early pioneer platforms. It is nowadays possible **to deploy DLT platforms capable of handling petabytes of data** (thousands of terabytes, or more than 10 000 times larger than the current Bitcoin platform), while maintaining excellent processing performances.

Meanwhile, excruciating bandwidth limitations are also solved thanks to a better engineering trade-off between system resilience and redundancy.

Our own research on technology revealed that the original, intricate, design could be simplified in many ways. Together with some other protocol optimizations, such new designs could prove to be real game-changers in terms of transaction handling capabilities, allowing some platforms **to deliver thousands of transactions per seconds** instead of a thousand or so per 10 minutes (Bitcoin's average settlement delay).

Using such advanced DLTs ("grown-up" but not yet mature), which depart significantly from Bitcoin-inspired platforms, we believe that several the original technical challenges may now be considered solved, or at least **close enough to our target to start a serious prototyping effort**.

We refer to *TheFundsChain* platform as the codename for the bespoke DLT to be developed for the asset management industry.

Toward specialized DLTs

Know your business

The relative success of the Bitcoin platform may be in part explained by this platform's deep understanding of what digital cash and cash transactions really are. Indeed, the system fully captured the fundamentals of two parties exchanging virtual coins. It is also worth noting that the design of the platform has been specially tailored to address this need with a rather compact architecture. Likewise, the promises of DLT applied to the financial industry may only be fulfilled **if and only if the economics and inner workings of financial instruments are accurately and extensively modeled** by such a platform.

Another key to this initial success was the design of a **closed economy**, without much need to interact with the outside world. As a result, Bitcoin-like technologies fall wide of the mark when it comes to generalize to other real-world applications.

To put it differently, any given DLT platform shall offer a narrow field of applications for which it has been specifically tailored to. Conversely, finance is a wide and complex field, with many different actors, asset classes, instruments and a vast array of regulatory constraints.

MYTH BUSTER #1
ONE SIZE FITS ALL

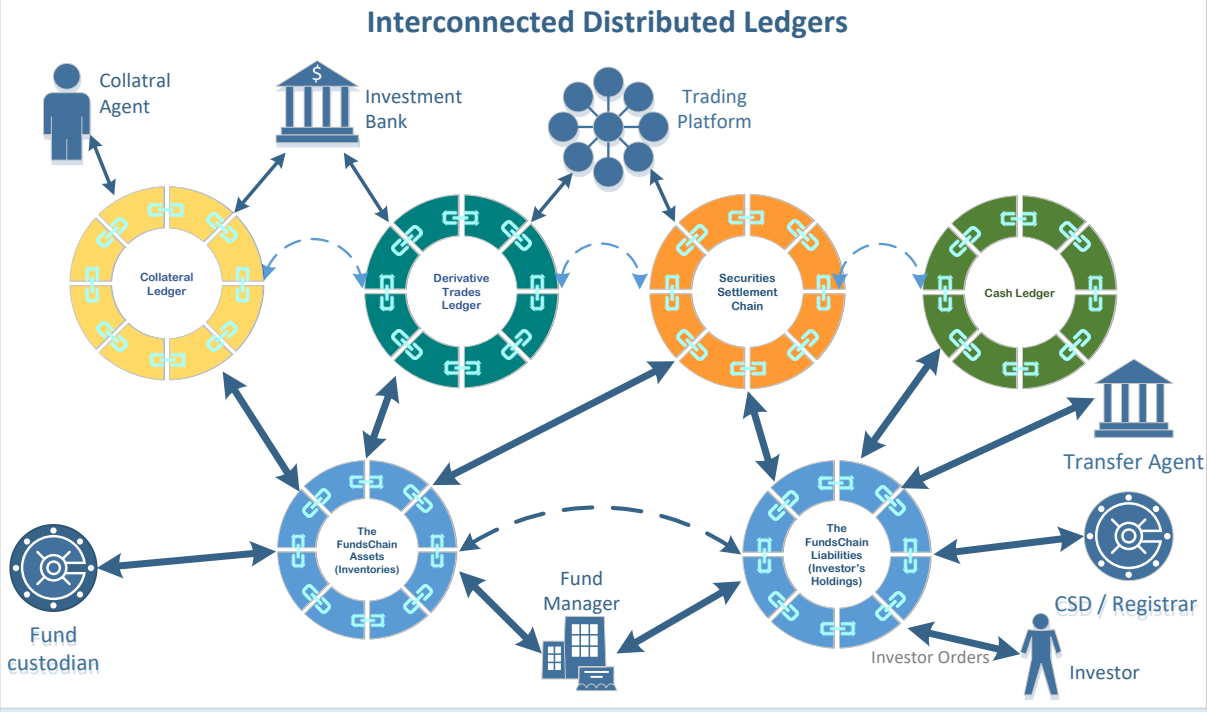
Definitely no. **The DLT promise is to deliver highly capable solutions to specific business issues**. Because of the inherent complexity of its underlying mechanics (distributed database, consensus protocol, proof of ownership, …), a single DLT setup is likely to address a narrow range of businesses only. *TheFundsChain* initiative focuses for its part on the asset management industry.

As a matter of fact, we feel that much work and thinking has already been spent on the sell-side of business – settling trades on securities or derivatives, while the buy-side – channelling public savings to investment vehicles – remains to date relatively unexplored.

We strive to fill this gap and expose in the following a genuine ambition for buy-side actors, leading to creation of a dedicated DLT: *TheFundsChain* platform.

Flexible, up to a point

It is true that the concept of "smart contracts" provides a flexible way to extend a DLT platform with new business rules and workflows. But then how about defining the thousands of specific data structures required to run a single "universe of finance", which would seamlessly interconnect every business to one another? In our opinion such an undertaking is not workable. Therefore, we believe that several initiatives shall be conducted in parallel.



A world of interconnected DLT platforms

A generic one-size-fits-all DLT designed for the financial industry will thus probably not meet the different requirements originating with various financial businesses. For instance, B-to-B activities would set different requirements than B-to-C ones. We may also expect that prominent B-to-B platforms would likely rapidly emerge as single, global, cross-jurisdictional exchanges for securities markets or derivatives markets, but securities lending activities would probably require some platform of their own. Eventually, cash being the *lingua franca* of finance could be handled as one single ledger accessible to all parties.

We expect therefore that the standardization of cross-DLT protocols will soon become a key industry-wide issue. Existing standard-setting organizations, such as ISDA or SWIFT will remain important players in this field.

The warden at the crossroads

The future is thus likely to be populated by several such interoperating distributed ledgers. Interconnected platforms would require some trusted parties to exchange reliable events and data, or "oracles". This defines a new "oracle gatekeeper" role for a number of industry actors, positioned at the crossroads of these systems. This approach allows for a realistic path to a full DLT implementation, since every specialized subpart does not require it counterparts to be implemented with DLTs.

Diversity versus Fragmentation

Most obviously, such an approach favors innovation and local, fragmented, efficiencies over global coordination, which would curb DLT adoption. Our view is that, provided platform promoters abide by some baseline business standards, such platforms would operate at similar levels of technology, and could merge later, thus reducing market fragmentation. National or regional platforms may coexist for some time, but market pressures would soon reduce such undue fragmentation. Such industry standardization initiatives have already started, for instance to define "templates" for smart contracts. Our intent with *TheFundsChain* is to develop similar standards for asset management. As an example, the industry could adopt a common definition for investor suitability, to be shared between distributors and fund managers.

Funds management: at the cross of finance

Funds being vehicles used to channel investment to other specialized assets, they essentially provide a connection to other areas of finance, such as equities, bonds or derivative contracts. At the heart of this flurry of products lies cash. A DLT platform dedicated to funds would naturally be positioned as a central hub connected to such an array of dedicated ledgers.

Our vision is that funds constitute a large, yet sufficiently homogenous business to be handled by one single, global platform. Funds are subject to many local jurisdictions, each providing in turn its own source of complexity. However, deploying DLT at a national scale would produce way too fragmented a landscape.

We believe that technology under proper governance is now sufficiently flexible to overcome the challenges of local peculiarities in the fund management industry. For instance, we do not think that the coexistence of a "CSD model" and a "Registrar & Transfer Agent model" would pose much of a problem with the unified approach we are promoting.

On the other hand, we argue that the specifics of the fund management business would make it difficult to fit as a sub-part of, say, a general-purpose system designed to trade securities. Our ambition is thus to focus on funds as a single asset class and gradually expand the coverage to all business processes related to funds, in effect contributing to the emergence of a "buy-side platform".

Smart contracts

An extremely attracting feature introduced by DLT is the concept of "smart contract". This concept is actually not new and may be tracked back some 20 years ago. However, the idea of being able to execute smart contracts on a blockchain has given renewed momentum to the concept.

Blockchains were originally created to store simple data (e.g. bitcoin transaction data). As such, they present themselves as a distributed database storing a complete transaction log, in a way much similar to an accounting journal. This simple, perhaps even simplistic, design unfortunately does not allow for operations more complex than the elementary "A pays B" type.

The idea behind smart contracts is that, in addition to manipulating data, the distributed ledger could also contain code that would autonomously perform certain actions under certain pre-defined conditions, called oracles or triggers (when the conditions are events). Putting it another way, smart contracts allow to share behaviors over the distributed ledger, not only data.

Such behaviors, that is processes or workflows, are not always particularly smarts. And they do not necessarily relate to a contractual relationship in the legal sense. Therefore, we find it best to think of smart contracts as business rules which participants agree upon and are carried on automatically[2].

Here comes into play another fundamental aspect of smart contracts: their immutability. The code implementing a business rule is sealed, much like a real contract signed by parties, notwithstanding legal issues such as: is a smart contract legally binding (see also box).

Smart contracts bring additional potential to DLT: complex transactions become possible and we are no more limited to simple debit/credit transactions. It becomes possible to define financial instruments as smart contracts and accurately specify their behavior.

Example: a bond paying interest and principal according to a predefined schedule could be specified as a smart contract, in effect triggering a payment transaction according to its schedule.

Another example: an investor subscribing to a mutual fund would trigger several predefined rules to compute the price of the transaction, ascertain the payment and issue the corresponding units for this fund.

MYTH BUSTER #2
DLT & LEGAL ISSUES

It is often argued that DLT create a juridical no man's land, a belief supported by crypto-currency platforms and Distributed Autonomous Organizations (DAOs), a series of initiatives which indeed, overcome traditional jurisdictional boundaries. This is clearly a threat to highly regulated industries such as finance.

In this paper, not only do we argue that DLT do not necessarily part away from regulator's oversight, but on the contrary, that regulatory bodies get a unique opportunity to leverage on such technology and gain comprehensive and accurate oversighting capabilities. All the while, other industry actors would be able to keep compliance costs from rising.

DLT is seen as raising potential legal show stoppers, especially in its most disruptive implementation scenarios. Indeed, with such scenarios, existing infrastructures would be wiped off and so would traditional legal frameworks.

Taking the opposite approach, this paper pushes forward for an incremental scenario. Our approach considers DLT as an enabler technology, used to reshape existing infrastructures without raising major legal concerns.

The term *smart contract*, indeed describing enforceable business logics, is confusing, as it suggests a legally fully self-sustained entity, that is, defined "by the four corners of the document", as lawyers put it. Interacting with the real world is usually more complicated than that.

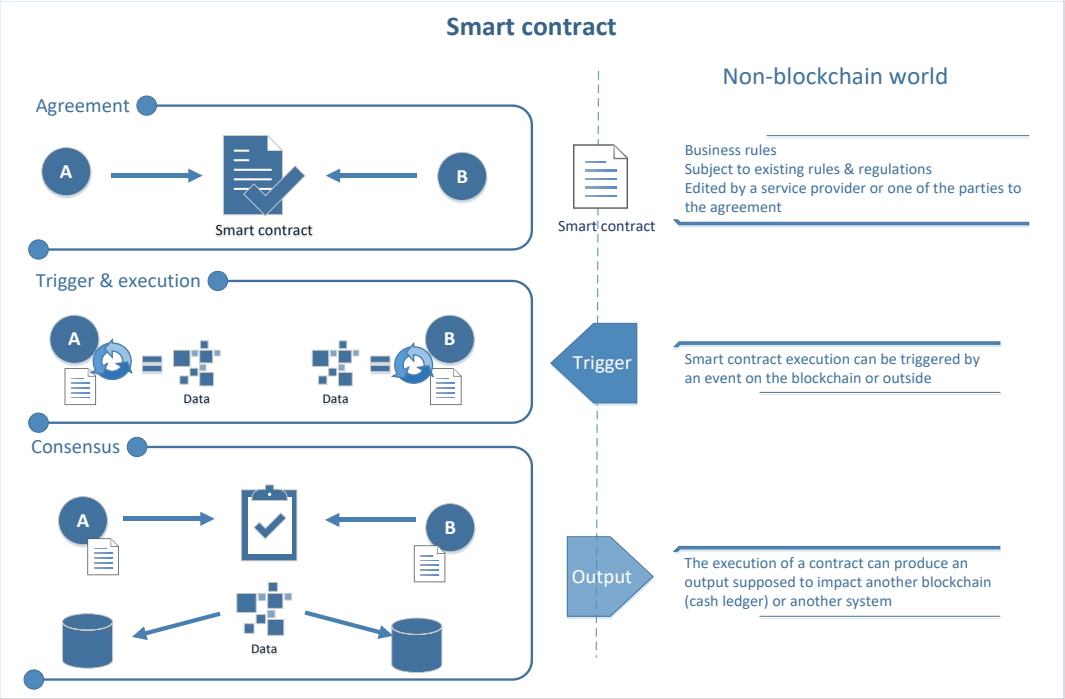
The implementation of smart contracts we envision in this paper thus **keeps an operational focus and shall not change the legal responsibilities of the involved parties**.

As a matter of fact, and contrary to some futuristic visions, we do not see smart contracts as totally autonomous objects in which every single outcome of the business relationship would have been encoded beforehand.

Therefore, in our view, smart contracts remain subject to the relevant legal framework and should merely act as business processes facilitators between participants.

Should a dispute occur, participants would still able to call on an arbitration process or a court.

[2] Additional details are presented in part III



More generally, it is possible this way to bind a predefined workflow of actions to any external event, and not necessarily limit ourselves to contracts that model an instantaneous purchase or sale of assets on the ledger. Example: the registration of a new fund could be specified as a sequence of verifiable actions and events. Such a workflow would obviously be dependent on the country of registration.

Last but not least, smart contracts could also provide a convenient way to enforce market rules and regulations. Example: an investor may subscribe to a given fund only if previously checked with a valid KYC status and risk profile adequacy.

Oracles establish the link with the real world

Regular smart contracts are limited to interacting with objects living on the distributed ledger: they cannot access by themselves the world outside the chain they live on. For real world applications, "oracles" are thus needed. Oracles represent external information provided to the DLT by trusted participants, or "gatekeepers". This can refer to external events (i.e. triggers), such as a corporate action, or other inputs used by smart contracts, such as security prices.

Transactions may be entered upon the occurrence of such external events, and are not necessarily generated by a transaction local to the distributed ledger.

Example: a trusted authority, such as ISDA, shall be required to indicate that a credit event is indeed triggered for a given debtor. Such an event would trigger a payoff on CDS contracts living on a distributed ledger.

SMART CONTRACTS FOR ASSET MANAGEMENT

Fund distribution use-case: in this example, all required information lives on *TheFundsChain* platform (the fund ledger): investors' holdings and distribution agreements. Distribution agreements are modelled as smart contracts computing trailer fees to be paid to distributors, e.g. quarterly. Holdings are split beforehand by distribution channel. This is possible since every order is earmarked with all distributing intermediaries. The smart contract outcome is to generate payments to distributors and possibly, an invoicing document stored on the ledger. Since all information, by construction, has already been validated by all parties and the contract behavior is already agreed upon, no further reconciliation is necessary.

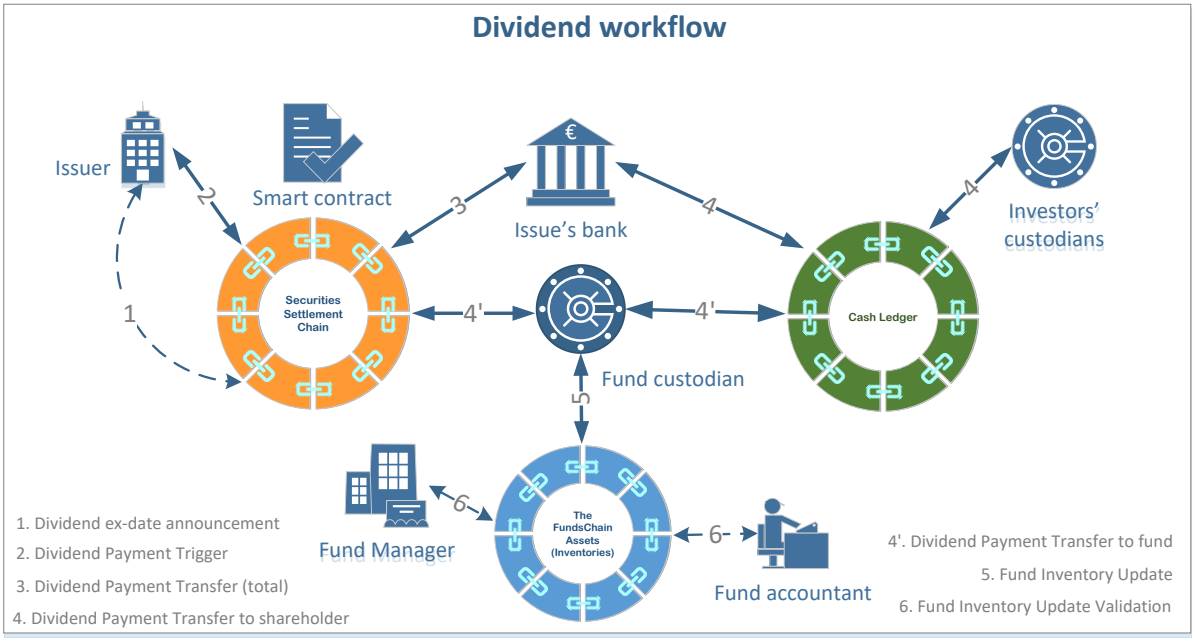
Fund custodian use-case: in this example, three specialized ledgers coordinate the processing of a dividend payment thanks to smart contracts (see figure next page). Let us assume that a fund owns a given stock. This stock could be modelled as a smart contract on a securities ledger, coded to enable dividends to be paid upon the issuer's decision (first trigger). On the payment date (second trigger), the contract executes a cash transfer to shareholders by connecting to a cash ledger. The dividend event is propagated to *TheFundsChain* platform which eventually validates the transaction upon reception of the corresponding event from the cash ledger. As a result, the fund's inventory gets updated.

Likewise, transaction validation might require some external oracle. Example: if one assumes a separate cash ledger, be it implemented as a distributed ledger or not, validating a subscription to a fund share would require that the cash ledger informs the mutual funds ledger that the corresponding cash transfer has in effect been carried on. In this example, a typical design issue within the scope of *TheFundsChain* workgroup would be to determine whether the contract should require the actual cash transfer from the investor, or could carry on with a mere guarantee from its sponsoring bank.

Handling oracles may be fully automated, but could as well require some manual or controlled input from a trusted operator. Example: the issuer of a mutual fund may specify the ex-dividend date for a given fund's share.

With *TheFundsChain*, we may think of oracles such as:

- cash transfer confirmations from a cash ledger (i.e. an external payment system, not necessarily DLT-based);
- security prices and more generally, market data;
- security definitions from an external securities ledger, and more generally, master data definitions formalized as smart contracts;
- confirmations of collateral posts from a collateral ledger;
- settlement confirmations from an external securities ledger;
- ISIN code input upon fund registration;
- ...



Investors services deployed as smart contracts

Smart contracts are extremely versatile. Bilateral or multilateral private agreements may be set up. Furthermore, and beyond acting as the workhorse feature supporting financial transactions, smart contracts could support many services consumed by fund managers.

Example: a fund manager and a fund accountant agree on specific rules to price financial instruments on a given fund's inventory. This "contract" would allow to validate the result of the computation and then authorize its dissemination to other participants or to external systems. A more evolved version of this contract, which would encompass fees and accounting provisions, could in turn produce NAV's.

In this paper, we develop further on this approach and argue that genuine, long-term savings are contingent to a minimal set of standards to maintain a level-playing, competitive environment for such services.

Smart contracts challenges.

Smart contracts also come with challenges of their own. In particular, the execution of trusted code over a distributed network requires some consensus-seeking procedure – just like data updates. Platforms which have overlooked scalability issues when designing the consensus protocol that supports smart contracts will not be able to match the industry's expectations. For instance, the Ethereum platform requires all voting nodes to execute the smart contract code to validate their outcome.

Main initiatives in the financial sector

Possible DLT applications to the financial industry are numerous, especially for all activities that involve burdensome manual reconciliation processes such as trading OTC derivatives, issuing and keeping track of financial instruments, payments or settlements. It is therefore not surprising to see so many initiatives covering capital markets.

Banks have been the most active in investigating and investing in blockchain technology, either with in-house projects or through consortium approaches, thus taking a significant advance over other actors of the financial industry.

Blockchains developed by banks, and more generally, sell-side actors, focus on banking core business lines: payment, OTC trading and securities settlement. It came as no surprise that one of the first demonstration of a concrete use case for smart contracts was about derivative contracts (ISDA agreement). It is admittedly a great use case, which the buy-side may also benefit from, but it probably does not take into account other specific buy-side use cases requirements. For instance, a fund manager might be interested in checking its portfolio constraints before establishing such a trade.

That is one more reason why this paper strongly argues for an independent assessment of DLT potential by the Asset Management industry. Perhaps most crucially, the industry as a whole should get onboarded as early as possible in the standardization process.

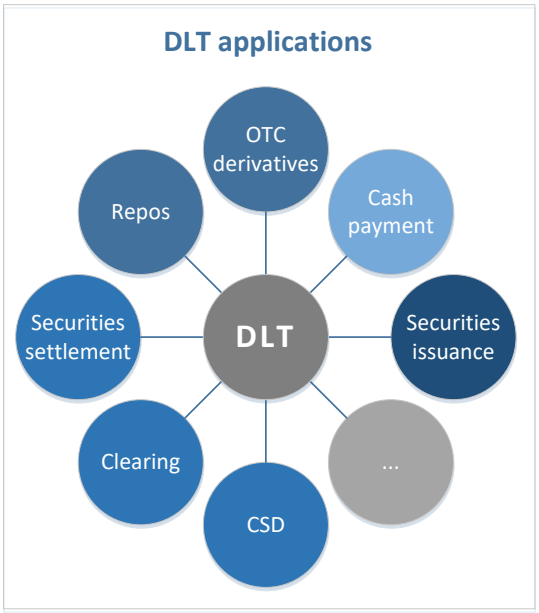
R3 AND THEFUNDSCHAIN

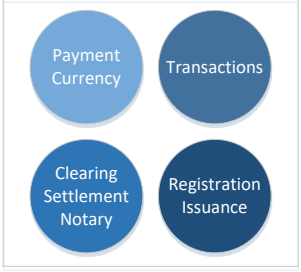
DLT scenarios for securities settlement and derivatives confirmation are currently the most advanced ones in terms of experimentation and prototyping at banks. As a matter of fact, the banking community has heavily invested to rapidly take the lead on this matter. The R3 consortium has been created to reunite their efforts and promote the technology. As such, the platform developed by R3, **Corda**, is based on a sound understanding of banking operations and has so far been focused on sell-side applications.

TheFundsChain **initiative is complementary** to the great work started by R3, and will certainly benefit from R3's pioneering efforts.

As argued in this paper, we firmly believe that given the potential of DLTs, every sector in the financial industry should make its own judgement and possibly develop its own bespoke blockchain fitting its unique requirements. The "wait and see" strategy is definitely not an option.

We are thus convinced that several complementary initiatives will develop. Such initiatives will clearly have to cooperate, as different ledgers will have to interconnect in order to leverage the full potential of DLT.





PART TWO DLT IMPACT ON THE ASSET MANAGEMENT INDUSTRY

ACTORS & BUSINESS PROCESSES

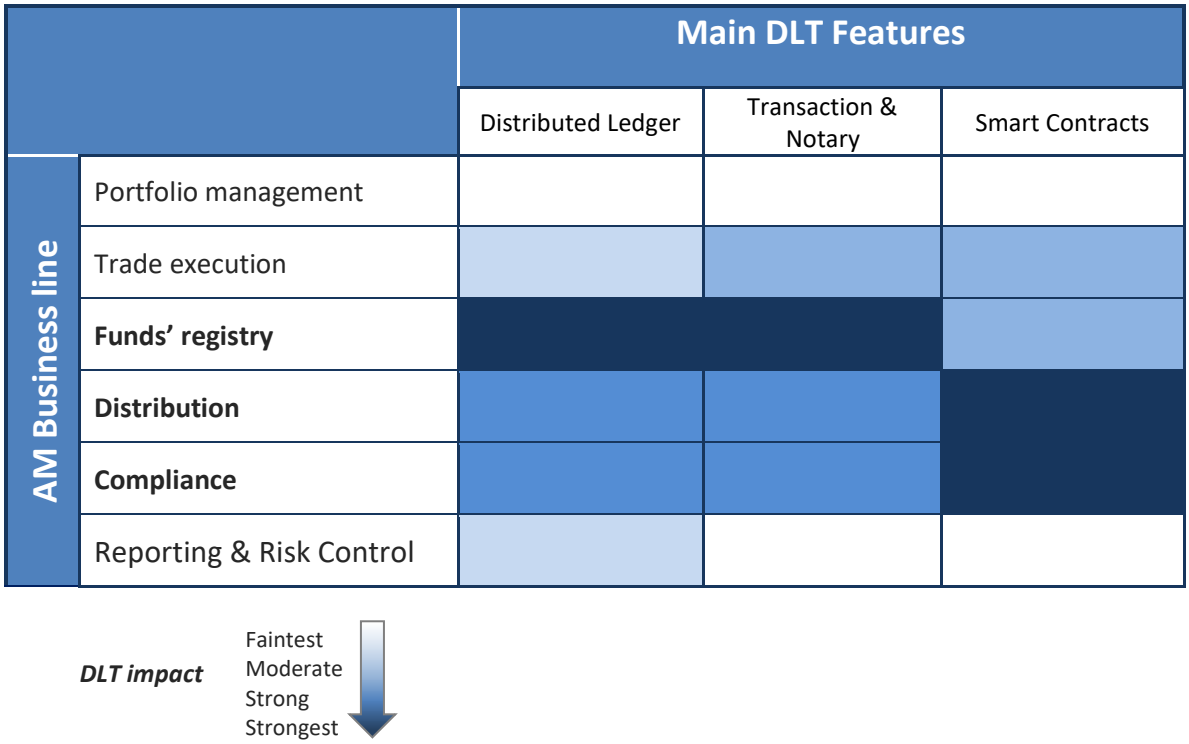
SCENARIOS

DLT & Asset Management

Expected impact for the Asset Management industry

Given the core functionalities of DLT, what could be the use cases for the Asset Management industry?

Our take is summarized in the following heat map.



Portfolio management

DLT is in essence a back-office enabler: data driven algorithms for decision-making will probably not leverage on this technology. Most likely, portfolio management will benefit from other technological innovations to assist in crunching data, designing and back-testing portfolios. In this area, we are naturally more inclined toward big data or artificial intelligence applications rather than distributed ledgers.

Trade Execution

The implementation of portfolio management decisions will probably be impacted by DLT as trade confirmation and management is an obvious use case, especially for illiquid, exotic OTC derivatives. Deploying a DLT covering these processes is currently the main objective pursued by banks. We expect that the Asset Management industry will benefit, as a side effect, from DLT designed by banks and brokers but will not be at the forefront of innovation.

Operating fund registries & associated processes

The best use case for the AM industry is most certainly the implementation of a distributed ledger designed to keep track of units of mutual funds. The identification of holders comes as a natural consequence. This view is now largely consensual among the industry actors we have been interviewing.

Most funds are distributed through intermediaries, which channel investors toward products. Even in the case of direct sales – for instance, to institutional investors – all orders are currently processed through the investor's bank – its custodian.

On the infrastructure side, the registry of a fund's units is usually outsourced to specialized participants[3], such as a CSD or registrar and a transfer agent, depending on local jurisdictions. This situation has created both operational and core-business issues. Operational issues arise from the fact that different participants maintain and update their own registry. Business issues from the degradation of information along the intermediation chain, resulting in reduced direct marketing capabilities for fund managers. As a matter of fact, fund managers seldom have a good knowledge of their customers. DLT would address both types of issues thanks to a single shared registry.

Distribution

Distributing funds can be a complex business, with multiple arrangement set up with a vast array of intermediaries, with which fund managers negotiate various rebate arrangements (trailer fees). On top of such indirect sales channels, fund managers favor direct sales to large institutional investors.

Managing the complex partnerships ruling fund distribution is a resource-intensive process. The association of a distributed ledger to earmark orders and investors' holdings, and of smart contracts to coordinate the invoicing and payment of trailer fees could be a very powerful tool. Leveraging these new capabilities to support direct sales is also a possibility to be considered.

Besides, the current distribution landscape relies on several independent order management platforms used to execute clients' orders. These platforms currently compete for STP and technical excellence. By realigning the focus on client knowledge, DLT would level the STP and technical playing field, in effect pushing distribution platforms to move up the value chain.

Regulatory Compliance

Distributors and fund managers overall share the responsibility to carry on regulatory checks with their investors, with some nuances depending on the jurisdiction. Indeed, funds distribution is a heavily regulated business (KYC, AML). Industry actors must already comply with many rules driven by the regulator's mandate to protect end investors. The expected trend is toward ever more stringent rules (Know Your Transactions, ...).

A distributed ledger keeping track of investors' holdings could drastically simplify existing processes, as well as enabling the stricter rules to come at a low marginal cost. As will be discussed later in this paper, implementing such a ledger implies that participants share some information about end investors, in order to simplify KYC and AML checks.

Eventually, keeping directly at hand a full audit trail of investors orders would allow to check that the various intermediaries involved have indeed performed their duties, for instance in terms of suitability.

[3] In some uncommon cases in which shares are issued under a registered form, the registry is directly operated by the fund management company (the issuer).

Other processes

Reporting & Risk Control

Moving to the assets side, funds' assets and transactions follow a complex life-cycle, from fund manager's decision to market execution to fund accountant validation. As such, multiple reconciliation processes are carried on between middle-offices, custodians, brokers and fund accountants. Furthermore, there are additional burdens to reconciliation issues: all subsequent inventory-dependent processes, such as reporting and risk calculation, suffer from the limitations of the existing setup, which delays and often degrades the information flow.

Many industry actors mitigated such issues by handing over such processes to a single service provider, in effect limiting, but not annihilating, reconciliation issues. In this paper, we express this idea by considering that data ownership creates a barrier to entry for service providers.

A distributed ledger providing an instant up to date shared view of funds inventories would greatly simplify all such processes and ultimately reduce both costs and risk. Regulators would also benefit from such data quality enhancement and could in some cases be granted direct access to certain data to perform their own reporting.

NAV validation and dissemination

NAV production would be an interesting fallout of such harnessing of the full life cycle of funds inventories. NAV is indeed produced by a dedicated service provider acting as accountant on behalf of the fund. Depending on local market practices, NAV may have to be cross-validated by fund managers before eventually being disseminated to various platforms. Note that the regulator may also take place in this process, thus acknowledging the official status of the NAV.

Given the diversity of valuation rules in use for the many asset classes one may encounter on a fund's inventory, a fully automated DLT version of this process is probably rather far on our journey. However, even with limited automation, sizeable improvements could be gained from a transparent exposure of valuation rules and pricing parameters.

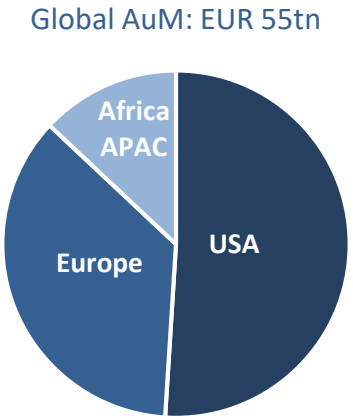
NAVs would anyhow be an important information living on a funds DLT – either produced locally or captured as external information – since they constitute a key input to the subscription/redemption process.

Cost savings

What could be the savings generated by a successful implementation of DLT for the Asset Management industry?

Obviously, a clear-cut figure is impossible to produce. However, adopting a top down approach (see box) and a conservative rough estimate of a 5% overall operating costs reduction, we reckon that annual cost savings brought by DLT could be **up to EUR 10 bn**, industry-wide.

To illustrate our estimate, a fund manager with a turnover of about EUR 600 m and operating costs of EUR 450 m would be able to save EUR 11 m a year.



ESTIMATING SAVINGS

We based our assessment on a global estimate of assets under management of EUR 55tn (Europe representing roughly 35% of that total). In order to determine the global costs associated with this figure, we may estimate the average total expenses ratio on investors holdings to about 0.5% of that total and average operating costs of about 75%, thus giving us a total expenses figure of about EUR 200bn (industry aggregate).

We estimate that the full potential of cost savings brought by DLT to be approximately 5% of that total, that is EUR 10bn, or 2 basis points.

This is a quite conservative estimate, especially when compared to other figures presented in similar studies.

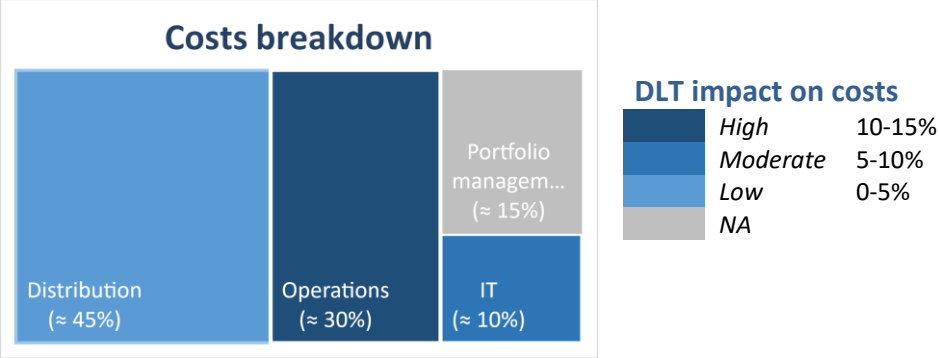
We feel this result is consistent with our general approach of an incremental implementation that will take several years before fulfilling its full potential and with hard to estimate investment costs.

Costs & Savings break down

In terms of costs breakdown, we took the following assumptions regarding the average operating costs structure of an asset manager.

- 40-50%: distribution (e.g. trailer fees)
- 25-35%: operations (including compliance costs)
- 10-15%: IT
- 15-20%: portfolio management

Given our previous analysis of the impact of DLT on buy-side business lines, we estimated that the highest impact is to be expected on funds' registry, distribution and compliance. Cost reduction would indeed mainly affect operations, IT and to a lower extent, distribution costs. The heat map below indicates how savings would be split across cost items.



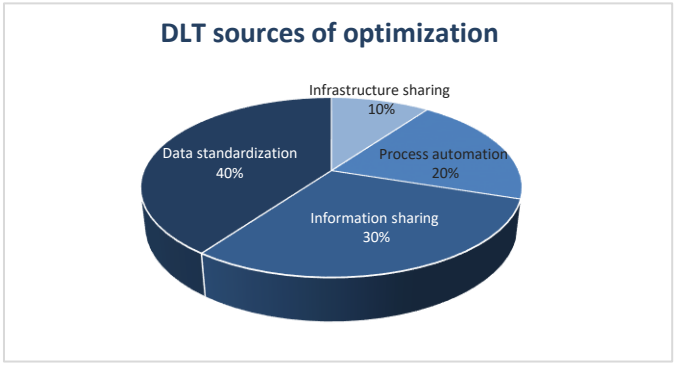
Such savings represent about 2 bps of additional performance that could be passed on to end investors. Clearly, asset managers would not be the only one impacted, and distributors as well as investor services providers would also be able to cut on their operating costs.

To best describe our central scenario, we would say that business carries on *almost* as usual, at a lower level of energy.

Another way to look at costs savings is to break them down by source of optimization, considering the industry as a whole.

We thus reckon four different sources of optimization, with the following estimated split.

- **40%** come from the required advances carried on by the community of industry actors in terms of data and protocols standardization. Such progress could have been achieved without DLTs, but the unique potential of such a distributed platform at last provides a strong enough incentive toward harmonization.
- **30%** come from information sharing and the expected positive fallouts in terms of process efficiency and outsourcing. Most obvious examples to be cited here are reconciliation processes and regulatory processes. An important positive impact to be also expected here is the improvement of data quality.
- **20%** come from process automation. As standardization and information sharing progress, new opportunities are looming ahead for automation.
- **10%** come from savings on IT infrastructure. Indeed, gradually deploying more business processes on a DLT platform equates to a larger part of on-premises computing power being moved to a "cloud" of shared nodes.



MYTH BUSTER #3
DLT REDUCE WHATEVER COSTS

DLT comes with the promise of more efficient processes – post-trade processes in general, and more precisely, reconciliation and regulatory compliance processes.

However, our conviction is that a genuine, long term reduction of costs is more likely to be generated by fair competition than by efficiency gains.

Technological upgrade scenarios – no matter how much potentially disruptive technology gets deployed – are more likely to merely reshuffle cards between actors: some being "disrupted", and some others predating most benefits.

Winner-takes-all scenarios are indeed a recurring story with new technologies that generate huge network effects. DLT is no exception. The problem here is that such a platform may only result from a collaborative effort carried on by participants, not from a single actor operating on its own. Therefore, viable scenarios necessarily rule out dominant positions and should overcome most salient conflicts of interests between actors.

Our vision – and most advocated scenario for a target operating model for the industry – is one of a shared infrastructure hosting the building blocks required for a vibrant investment services marketplace to emerge. The term building block should be interpreted here as the minimal set of data structures and operational services required to efficiently conduct operations without impeding innovation and competition.

In such a competitive landscape, basic information – about products, investors, orders, holdings… – becomes a shared ownership, while service providers compete to cleverly exploit the shared information. In addition to relieving actors from running reconciliation processes, we strongly believe that a large portion of operational efficiency gains will come from such information sharing.

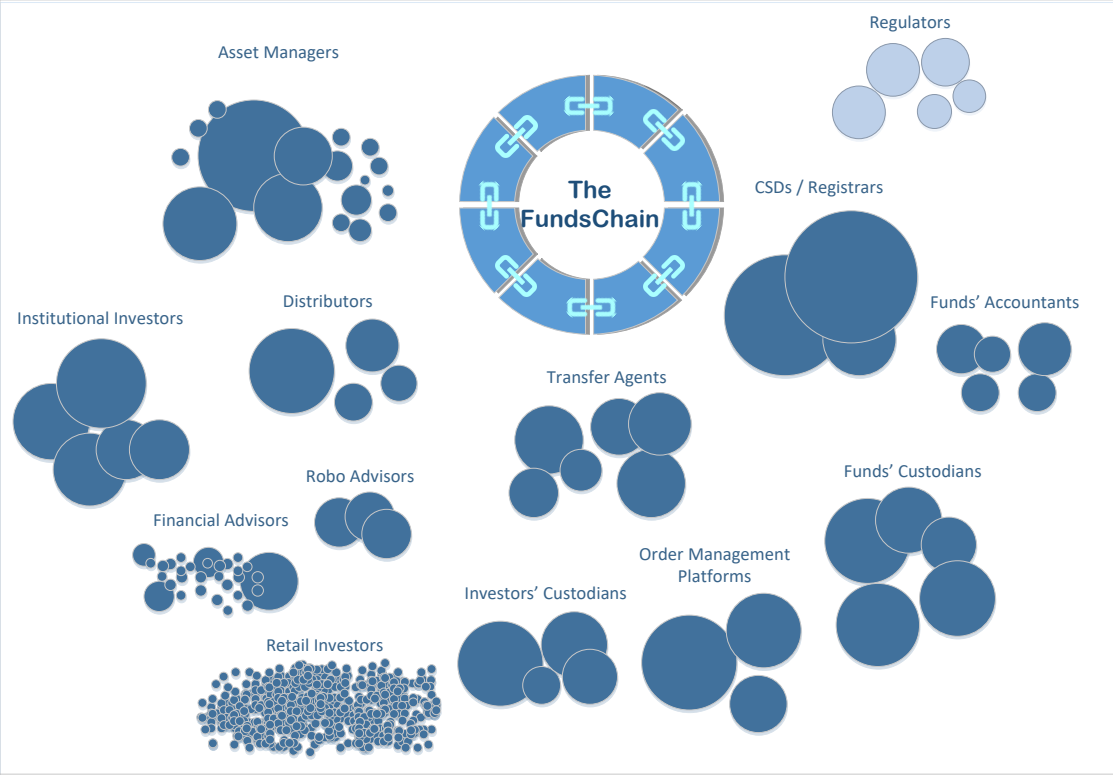
ACTORS & PROCESSES

In order to better understand the current issues and how DLT could address them, let us start by looking at the main participants and processes involved.

Actors

The Fund management industry is a complex ecosystem involving different kind participants. A fund is basically a financial instrument that consists of a portfolio of investments (its assets) and units representing ownership in this portfolio (liability side). These assets are managed by a fund manager. At the other end of the chain, investors (retail and institutional) purchase and sells units of the fund, usually through distributors.

Focusing on the liability side of this business, the other main participants are the following ones.



In between the investor holding units of a fund and the asset manager in charge of that fund there are several participants mostly involved in the distribution and the administration of the fund with sometimes some overlap between those two functions.

Distribution

The distribution chain can be relatively short (a bank selling funds from its asset management arm through its retail network or its internet site) or long (a fund manager has an agreement with a distribution platform which is accessed by independent financial advisors). International distribution obviously adds an extra layer of complexity.

The main participants to distinguish are:

- the distributor (even if the whole chain includes several actors);
- financial advisors who have a privileged relationship with the investor and actually own the relationship;
- robo-advisors (algorithms providing tailored investment recommendations to investors);
- order management platforms sometimes used to route orders for execution.

Fund administration

Several participants can be involved in the fund administration.

- The investor's custodian in charge of safeguarding its assets: financial instruments and cash.
- The Transfer Agent (TA) collects orders from the distribution network and transmits them to the relevant participants for execution.
- The Fund's custodian in charge of the creation/redemption of the fund's units (and cash management of the fund).
- Fund accountant: in charge of computing the NAV.
- Fund registrar / CSD, in charge of keeping track of the total number of units in circulation and of the individual holdings of the investors' custodians (notary function).

What about regulators?

Regulators should favor the emergence of DLT to the extent that it could enhance transparency and investors protection in securities markets. We think that regulators could strongly benefit from DLT as they could take an active part within the network of participants. A regulator could indeed become a special participant to the distributed ledger platform, with specific access granted to audit trails, and thus gain access to relevant data available on the ledger.

Regulators could even act as validating participants in certain transactions, with a potential veto power whenever applicable (we describe this concept of role-based consensus mechanism in part III). The regulator could for instance block certain transactions involving identified participants (AML, assets freeze...), or enforce certain restrictions such as a temporary short-selling ban, or a temporary restriction on funds' redemption in case of a liquidity run.

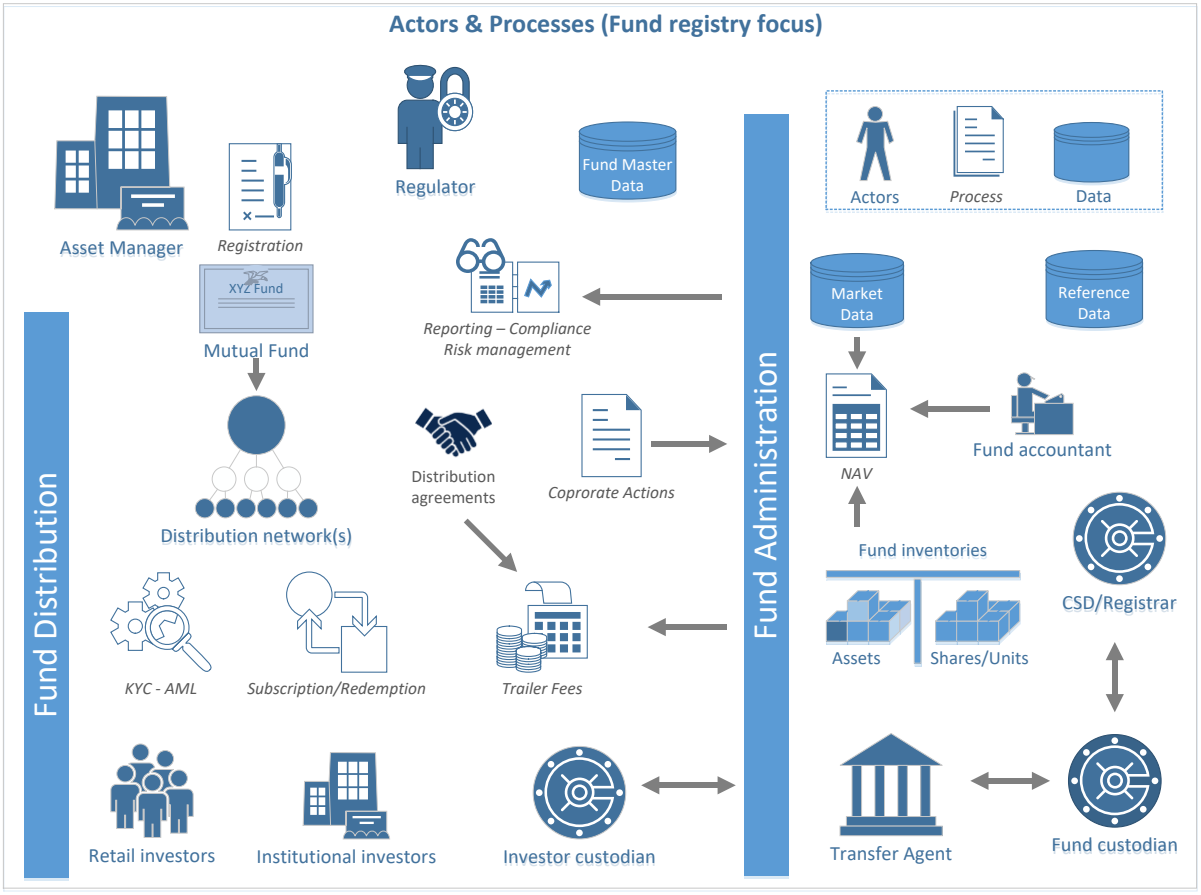
In the context of MiFID II, a regulator could check that suitability tests have been adequately performed and that the target market defined for a given investment vehicle actually corresponds to the customers buying it.

On the assets side of mutual funds, a regulator having access to the funds' assets inventory could directly check that the fund respects its constraints in terms of eligible assets, use of derivatives...

In addition, in the case of funds newly issued on a DLT, regulators could take part in an automated registration process, validating the issue of a new fund and enabling the publication of reference documents, such as prospectus.

Processes

The figure below details the various participants involved in most of the processes related to fund registry. Some of the participants may act upon different capacities (the financial advisor in some case can also be the investor's custodian) depending on cases and jurisdictions. The main point is that the processes involve multiple actors each maintaining their own ledger and that the asset manager has a very poor knowledge of its customers, if not none at all.



Main relevant processes where DLT could help

		
Fund design	*Fund managers relying on a complex distribution chain often have limited knowledge of their customers' base.* ⚠ **Marketing issue** ⚠ **Compliance issue** (suitability / target market in MiFID II jargon)	A fund registry based on a distributed ledger could allow to better know customers, holding periods, investing behaviors… ⇨ That could be achieved without full clients' details disclosure (*data encryption, flexible granular access to data*)
Fund issuance	*Fund managers need to produce and maintain legal and marketing documents. Fund Managers need to keep funds reference data up to date* ⚠ **Fund documentation** ⚠ **Reference data**	A distributed ledger could include up to date legal and marketing documents accessible to all relevant parties. Similarly, reference data would be shared among parties. ⇨ Need to design a consistent distributed ledger including reference data
Subscription/Redemption	*Keeping track of subscription and redemption orders as well as positions is a challenge. Reconciliation issues are numerous. Compliance checks are not optimal.* ⚠ **Complex order management / execution** ⚠ **Reconciliation issues** (difficulty to keep track of flows and holdings) ⚠ **Compliance (KYC and AML)**	A distributed ledger could keep track of the flows and holdings: all participants would share the same information. ⇨ Need to design a consistent distributed ledger including investors' reference data to leverage on the compliance requirements
C A	*Corporate actions involve several participants (Fund manager, fund's custodian, CSD/registrar, investors' custodian).* ⚠ **Reconciliation issues**	A distributed ledger would allow the relevant participants to share the same up to date information. ⇨ **Smart contracts** would streamline corporate actions processes
Distribution	*Keeping track of subscription and redemption orders as well as positions is a challenge. Reconciliation issues are numerous. Trailer fees calculation is not straightforward. Compliance checks are not optimal.* ⚠ **Reconciliation issues** (difficulty to keep track of flows and holdings) ⚠ **Commercial agreements / trailer fees calculation**	A distributed ledger could keep track of the flows and holdings: relevant participants would share the same input needed for trailer fees computation. ⇨ **Smart contracts** would allow to organize commercial agreements and compute trailer fees
NAV	*NAV is an essential information to be used for subscription / redemption. Depending on local jurisdictions, several participants can be involved in the computation, validation and dissemination of NAV.*	A distributed ledger would make validated NAVs available to all the relevant parties. ⇨ **Smart contracts** would allow to streamline NAV

SCENARIOS FOR THE FUNDS MARKETPLACE

In this section we look at a number of plausible scenarios for the industry, in a more or less distant future. Some are radically disruptive and could drastically transform the industry. Others introduce milder changes. We analyze in turn the odds, impact and expectations associated with these scenarios.

The central scenario advocated by *TheFundsChain* initiative attempts to keep a balance between innovation and the need to pave a workable path toward change. Indeed, our belief is that DLT may and should be used to streamline existing processes, rather than sinking existing institutions into oblivion.

Did you say disruption ?

Disruption (literally: an interruption of normal activities and by extension, a radical change with actors occupying a given business niche) is the meme developed by the ever-growing buzz around blockchain and DLT. Having conducted a number of interviews with the main actors of the Asset Management industry, we came to the conclusion that almost everyone may well come along with a new "disrupting" scenario envisioning a dominant role for itself.

Surprisingly too, a strange fascination for catastrophic scenarios also makes people contemplate the idea of their own disruption... We felt the need to develop and study the rationale for such scenarios.

Indeed, we think it is essential for industry actors to stay aware of potentially radical changes lying ahead. As important for us is to figure out how overrated a number of such hypothesis are.

TheFundsChain vision is one of bold ambition, but also pragmatism: we argue that much of the disruptive talk should now be considered more as an obstacle to transformation.

To better describe the target platform envisioned, we thus coined the much unappealing term of "**distributed back-office**", thereby denoting a series of incremental changes in technology, which most actors in business would accommodate by gradually adapting their business model to this new paradigm.

In the present paper, our contribution to the question introducing the BCE Paper, *DLT: Revolution or Evolution?* is a firm Evolution answer. We call such a scenario "incremental".

Allegedly, DLT is all about disintermediation. After all, the whole financial industry is composed of intermediaries. Let us assume a perfectly automated world where fiduciary responsibility as well as expertise would be fully handed over to algorithms, say for instance, a blockchain – perhaps on steroids – and a handful of smart contracts – some of the very smart sort. In this world, not much would remain of the financial industry... Of course, we exaggerate the threat on purpose to demonstrate the fascinating power of such irrational thinking, all the more when it comes under the guise of visionary prediction.

However, it is now widely acknowledged that DLTs offer a truly *transformational* potential. Even the "milder" scenarios we propose in this section clearly transform in depth the daily operations of most asset management actors. They do not disrupt their core business, though.

MYTH BUSTER #4
DLT DISRUPTS INTERMEDIARIES

A sentence usually followed by either one of:

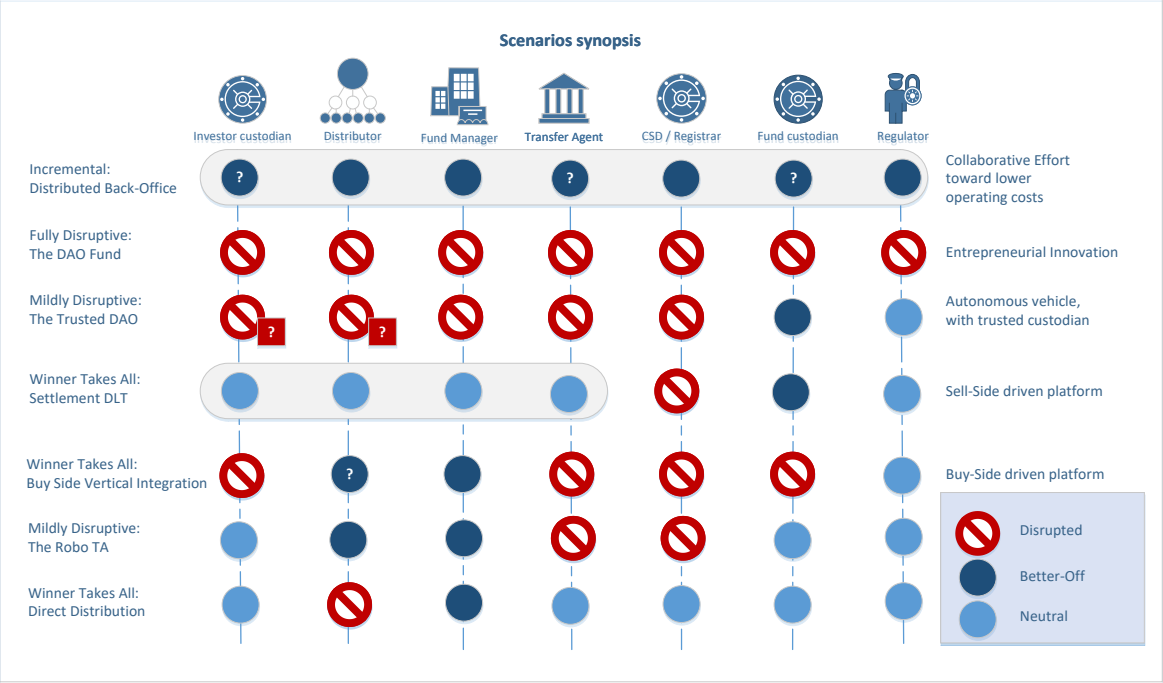
- "Let's launch our own fund, directly managed by investors!"
- "Let's distribute directly our funds to investors and get rid of costly distribution networks!"
- "Let's drop our costly infrastructure, now that ownership registries manage themselves!"
- "Let's us build an infrastructure we fully control: who controls the pipes controls the flows".

See the issue in this? Every single actor is naturally tempted by a "Winner-Takes-All" scenario of its own design. This leads to a counter-productive approach, slowing the pace of change as "disrupted" actors are naturally reluctant.

Moreover, such scenarios, even if they eventually succeed, are sub-optimal in the sense that they would only solve local issues, whereas an inclusive approach would lead to a global optimum, in its economic sense.

In this paper, we argue that putting actors out of business is not an automatic outcome of the technological transition to DLT. More than that, it may not even be a desirable outcome, all things being considered.

We cannot rule out that such milder scenarios could act as "enablers" and lead the industry toward more radical changes in a distant future. In particular, it is worth inquiring what kind of intermediaries the industry might simply drop out, and which new ones could be introduced. The diagram below gives an idea on how "disruptive" a scenario might be.



Fully Disruptive Scenario: how likely?

The DAO Fund: the autonomous vehicle

Imagine a ubiquitous "investment machine" automatically taking care of all asset custody processes. This machine would overcome jurisdictional boundaries. It wouldn't need to be "registered" anywhere. Investors would directly purchase token units to virtual investment vehicles, the same way they purchase bitcoins or ethers. Investors would vote on investment recommendations carried on by the machine and will be able to follow their assets' value.

Moving on further, one could easily imagine new incentives for individual investors to take part in this vote. For instance, the voting procedure could make the investment process fun (a marketing technique known as "gamification") by scoring the value of investor's decisions. Successful decision-makers with an established track record would get rewarded.

If the reward is materialized by more weight in the investment voting process, talented (or merely lucky) investors would naturally be promoted to "virtual" fund managers, thus removing the need for an appointed manager.

The utopia described here (or dystopia, depending on your point of view), is almost already a reality. The Ethereum DAO (a kind of investment "fund" running almost like the one described above) has been pursuing a very similar objective, successfully raising USD 150 million.

In such a scenario, most actors from the traditional financial industry would disappear ("be disrupted"). Perhaps fund managers could reinvent themselves as pure "asset pickers", "asset allocators" or pure investment advisors.

Perhaps banks would be keen on becoming "Wallet Custodians" to keep the secret holdings of their customers. A new breed of distributors would have to emerge as pure "Fund promoters".

Besides, such autonomous investment vehicles would remain mostly unregulated, and investors would probably remain anonymous. Who would be left to care about identifying them anyway?

There is just a missing detail, but a fundamental one: trust.

Indeed, the dark side of such a scenario is that precisely, there is nobody to regulate the machine. Investors would remain totally unprotected by any kind of legal enforcement authority and would be fully exposed to scams, heists and unfair valuation methods.

Another issue is that such a fully automated, "immutable" machine would be totally impervious to innovation and change. The developers behind the machine (its protocols and inner workings) would also gain an unprecedented advantage over any other actor.

Recent issues with the Ethereum DAO (see box) show that such projects have still a long way to go. This scenario cannot be totally ruled out, though, especially on the longer period.

In the specific context of passive asset management strategies, a derived scenario (see box on the right) could be an interesting way to further cut down the costs of managing such funds. We called this variation on the theme of automated investment vehicles "The Trusted DAO Fund", in other words a DAO Fund with a trustee. Still there is a limit to cost reductions, as designing and licensing the proper indices would remain at the core of this business.

This comparison is useful regarding the real disrupting potential of such a scenario: indeed, pundits have been announcing for decades the imminent demise of classical active fund managers, disrupted by passive management and ETFs. Time has shown that both styles could evolve side by side.

SHORT STORY: THE ETHEREUM DAO HEIST

A bug in the Ethereum DAO Smart Contract allowed cyber-thieves to steal away around USD 50 million.

The whole story ended up with a major decision by the platform developers to fork the Ethereum blockchain. In plain English, this means the admission that there is always some sort of administrator of last resort, similar to a central bank acting as a lender of last resort (in the context of currencies).

This episode has indeed strongly comforted ourselves with our approach toward DLTs – or, for that particular matter, smart contracts: as a matter of fact, we do not see assets or smart contracts on the blockchain as completely independent objects living out there in cyberspace.

"THE TRUSTED DAO": STILL EFFECTIVE LESS RADICAL

In this variant of the "DAO Fund", we keep most properties of the utopia, but we dare to add a trusted party to keep the fund's asset under custody. This trusted party, like any fund administrator, would be responsible for a fair valuation of the assets, that is, publishing to investors a NAV they can put their trust in.

When looking at this setup, we realize immediately that it is not very different from a regular fund with a passive investment strategy (e.g. index-linked funds), apart from the investor's voting process, which is after all, optional.

Essentially, the "Trusted DAO" simply differs from its radical cousin by adding trust. This makes a major difference in terms of risks taken by investors.

This scenario simply shows how the segment of passive investment strategies could be further driven toward lower costs using DLT, by automating most processes along the value chain.

To move on further, the implication of investors in the strategy (voting, rewards, gamification) would allow for some new, enticing products. After all, the investment rationale for such "democratic investment" may be easily compared to investment in index-linked products: the wisdom of the crowd would simply replace the wisdom of the market.

Winner-Takes-All Scenarios

Settlement DLT: the dawn of CSD's

Until recently, DLT has essentially drawn attention to one single specific pain point of the financial industry: trade settlement.

The main incentive to deploy DLT in this context is to maintain a single shared view of transactions: cross-validation occurs for every single transaction, which alleviates banks from maintaining costly reconciliation processes at their back-offices. Payment validation would occur almost in real time, *a priori* no more requiring a central authority dedicated to clearing trades.

Another key aspect in this scenario is the implicit maintenance of a securities ownership registry: the advent of a full-fledged DLT registry indeed removes the need for a Central Securities Depositary. In such a scenario, banks would be the clear winners. The DLT platform would allegedly operate at much lower costs than the clearing and CSD platforms their operations currently finance. Exchanges, CSDs and clearing houses would probably not disappear altogether, though. Today, these actors already clearly act as technology providers. This "platform caretaker" role would probably endure, but technological leadership could be fiercely disputed by new entrants. Furthermore, as it is most likely that cash transfers remain managed by a separate platform (this one being a DLT or not), some trusted party would be required to act as an "oracle" to eventually validate transactions.

In addition, the distributed nature of the DLT platform would bring down IT infrastructure costs.

Banks would benefit most from this technological advance: drastically reduced back-office operations, real-time settlements and lower transaction costs are strong arguments to eagerly push for such a change.

Dealers and market making businesses would experiment a large change of technology, but otherwise, their main business function – liquidity providers – would remain largely unaffected, while securing and accelerating settlement processes would probably allow for lowered instant exposures to market or execution risks.

Eventually, buy-side actors, such as fund managers and the related asset management ecosystem, would barely benefit from this change. Moving around assets across their portfolios would at best incur lower transaction costs, but their core business operations (and issues) would remain essentially unchanged under this scenario.

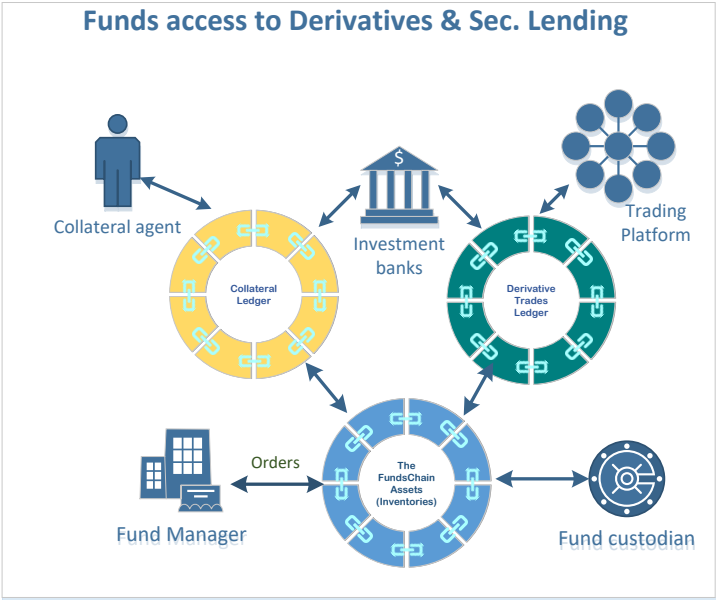
DLT for OTC derivatives & Securities Lending

Pure agents have to reinvent themselves – liquidity pools stay

DLT applications to Over-The-Counter trades (privately agreed upon contracts) investigate another acute pain point: the process of confirming the terms of a trade between parties. Such process would be radically overhauled by technology.

Sell-side actors would be the clear winners as DLT alleviates the need for post-trade reconciliations.

Another positive side-effect would be reduced costs to abide by heavy regulations on such activities, such as EMIR.



To move on further, the complex process of properly assessing and exchanging collateral (aka margin calls) could be much simplified, possibly without the need for a trusted third-party holding collateral in escrow.

As such, DLT comes with the promise of a deep transformation of the OTC ecosystem, reshuffling the economics of intermediation businesses currently running pure agency models, such as trading venues operators or collateral handling agents.

Again, the winners are sell-side actors, essentially the trading desks operated by investment banks. Buy-side actors would have to adjust their trading software, and would continue business as usual in all other respects. In a way much similar to what could be experienced on securities markets, derivative exchanges would be able to maintain a role as trusted "oracles" and main liquidity pools.

Eventually, we shall insist on some economic hard-facts: true game changing factors in such a scenario are not technological choices, but long-term cost reductions and the possibility for new entrants to start competing with incumbent actors thanks to lower barriers to entry. In other words, such a scenario would require, to be realistic, that it is followed by a sizeable share of liquidity pool owners, and is not limited to a cozy club of top-notch trading platforms.
The latter fact actually applies to a much wider range of DLT applications, as it is rooted in the distributed – hence, collective – nature of this technology.

Buy-side vertical integration: exeunt fund admins & transfer agents

Let us adopt now a buy-side point of view, in which fund managers collectively run an automated fund administration platform. Such a move would indeed put traditional fund administrators out of business, by offering essential services such as transfer agent, registrar or CSD, funds' asset custody, asset valuation and accounting.

This would be a clear win for the buy-side community at the expense of other infrastructure actors. The expected reduction of administration fees could well justify the significant investments thrown into such a technological venture. However, there are several preliminary hypotheses to check when assessing this scenario. Dismissing infrastructure players would, as a result, conduct the buy-side community to vertically integrate the lower end of the value chain. Our analysis strongly suggests this particular "winner-takes-all" scenario to be highly improbable.

Firstly, we doubt that this situation is in fact desirable.

For years, fund managers have been outsourcing most of the administrative burden to specialized "investors services" actors. Such a move is indeed rational when economies of scale are generated by specialization. For such incumbents, specialized actors, massive gains on reconciliation processes and infrastructure management alone would provide a sufficient incentive to invest. The path to automation will no doubt be long and patchy, but cost reductions would rapidly kick-in, even with limited automation. It thus comes as no surprise that bank subsidiaries specialized in securities services, which have already reached a high level of market concentration and economies of scale, are on the brink of massively investing on DLT technology to optimize their custody processes.

On the other hand, a similar move from fund managers, with the objective of putting out of business some cost-inducing actors (see box), would only be workable if the substituted platform proves to be more cost-efficient.

DISINTERMEDIATION: A MATTER OF POINT OF VIEW

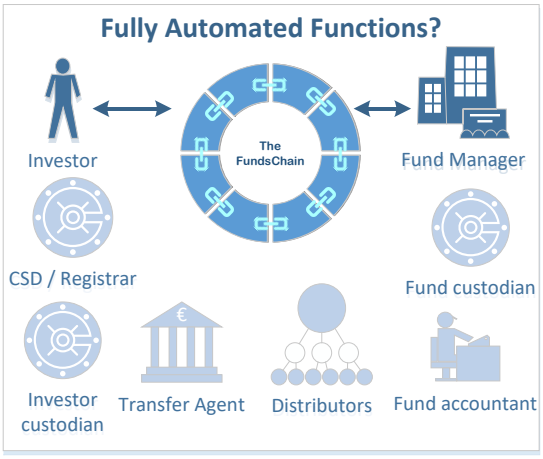
As a comparison with the Bitcoin platform, we observe that "disintermediation" is a matter of point of view: this platform has indeed essentially reshuffled roles by replacing established banks by providers of "bitcoin Wallets" and "bitcoin marketplaces", allowing users to exchange their token money against old fashioned hard currencies. In a similar way, the "central bank authority" has been somewhat replaced by a small community of developers who indeed control the pivotal protocol of the platform.

Therefore, we must be particularly vigilant in our approach, and thoroughly analyze the potential side-effects of technology in terms of new entrants.

Moreover, by pushing some actors out of business, disintermediation naturally leads to more vertical integration for the remaining, actors. This is not necessarily a desired outcome.

For instance, it is not obvious at all that fund management companies would be keen on re-insourcing the roles and responsibilities associated with managing the market infrastructure, even with more automated and secured processes. Indeed, over the past decades, asset managers have been consistently delegating more and more administrative processes and responsibilities to specialized actors (or asset servicers, typically integrated within large banking groups), thus creating economies of scale.

However, successfully re-insourcing infrastructure processes, assuming this is possible under local regulation, would mean that DLT brings back-office automation to unprecedented levels. Notwithstanding the technical challenges, reaching such efficiency levels would certainly be a long and costly investment. All the more, this investment would only produce long-term benefits, with only limited possibilities for quick wins.
Return on investments exhibit a very different profile depending on who moves first and takes the leadership. This makes a major difference between incumbent players (the asset services) and potential new players (fund manager).



To further strengthen our point, and taking a closer look at the assets side of funds, we shall not overlook the complexity of keeping the books on a largely diversified set of assets: bonds, equities, derivative & securities lending contracts, other funds, commodities or even illiquid assets such as real estate, private equity... As a matter of fact, the role of a fund's custodian, is much more complicated than merely confirming trades. For instance, automating corporate actions would require as many "smart contracts" as business events, meaning supporting a huge effort in IT developments. The sheer diversity of available asset classes largely protects custodians from new entrants.

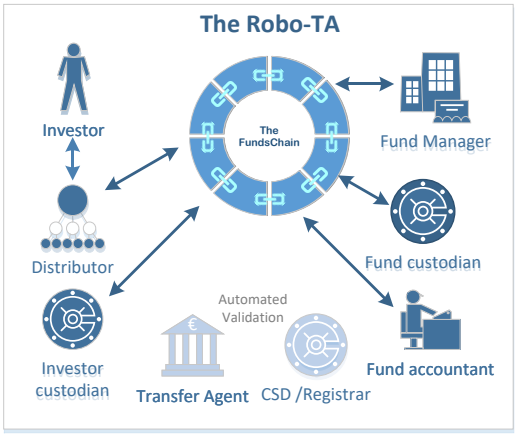
We thus believe that the replacement of a full-fledged infrastructure at the sole initiative of fund managers and at the expenses of asset servicers would present a formidable challenge, whereas competing initiatives carried on by asset servicers could offer a better risk-reward trade-off. Disintermediating the role of the fund's custodian constitutes the heart of this challenge. Thus, we don't expect the funds management community to take the lead on such a risky road.

This doesn't mean however that fund managers should not play an active role. Our next scenario, "The Robo-TA", suggests that by narrowing the scope, the DLT business case becomes much more compelling.

Analyzing this scenario illustrates our approach rather well. Indeed, even though we discard this "winner takes all" scenario as highly unrealistic, we immediately see opportunities for a fruitful collaboration to take place between service providers and service consumers. Again, we shall stress that, in order to truly generate long term savings, such a collaboration should take place on fair terms regarding the selection of service providers, that is, technology should not be used as a mean to further lock-in service consumers.

A variation: The Robo-TA

Full vertical integration seems quite a bit too ambitious. Let us examine a perhaps more realistic scenario, which would not have to cope with the extreme complexity of fully overhauling asset management services, and custody services in particular. By limiting the disruption scope to a narrower set of processes, more realistic scenarios may be formed.



Indeed, considering the liabilities side of funds only, DLT would prove excellent in unraveling the intricate pipe works of transfer agents, registrars and CSDs.

Handling orders on funds would indeed constitute a fairly attainable target, as there is no need to tackle the daunting diversity of funds' assets.

Processing corporate actions on funds, which constitute a limited set of events, would be a further move toward automation. In this scenario, fund managers benefit most from process simplification. Custodians and accountant would be only marginally affected. Indeed, from an infrastructure point of view, this business is already running rather smoothly. This is however not the case from a fund manager and distributor' viewpoint.

If we carry on the same analysis as with the previous "Vertical integration" scenario, the situation is indeed reversed: business stakes are much higher for fund managers – as it addresses real pain points on the high end of their value chain – than for asset servicers. Investment levels in such a project are lower, and there are actual opportunities for fund managers to reap incremental benefits.

Transfer Agents (TAs) and Registrar would not disappear overnight, though. But their role would be marginalized. TAs would thus evolve into pure "oracle gatekeepers", in charge of validating cash transfers with an external cash ledger. In the ultimate evolution of this scenario, this role becomes fully automated and held by a utility. Registrars and CSDs would become pure "notaries" and, ultimately, depending on how regulatory frameworks evolve, might even disappear.

It remains to be seen if technology and regulation may actually lead to such an ultimate vision. More realistically though, CSDs and Registrars could endure as technology providers and platform caretakers, while TAs would keep a role as gateways to external platforms; Indeed, Transfer Agents would remain key in maintaining the full interoperability of the infrastructure and would be able to process orders from investors, platforms or jurisdiction not directly connected to the DLT, in a sense not very much different from their current prime TA business.

Direct Distribution: distributors fade away. Or do they really?

Moving up the value chain, let us now investigate how disruptive DLT could be regarding the distribution of funds. A DLT platform operating funds would primarily be able to process orders in a decentralized way. A natural consequence would be the subsequent creation of a single venue for a (potentially) large universe of products.

Such a platform would indeed disrupt players on the fund distribution turf, which leverage on technology and STP capabilities only (e.g. order management platforms). It would also probably affect agents specialized in calculating trailer fees or hauling clients' holdings data (e.g. wealth management platforms).

DLT & DIGITAL IDENTITY

The idea of a digital identity for retail customers is not in itself, part of the DLT setup. Rather, we see this development as a companion technology for DLT, an enabler to get farther on.

Experiments, such as the Open Identity Exchange UK initiative, are ongoing. It will probably take some time before Digital ID becomes mainstream, but the concept is undoubtedly getting traction.

Indeed, ***universal*** *Digital ID* takes everything to the next level when it comes to streamlining customer relationship and regulatory checks.

Retail investors would be instantly identified and checked. It would then be up to the distributor to submit an adequate KYC and suitability questionnaire and then route this new investor to some smart "robo-advisor". Further, an account could be created online instantly to invest in. Alternatively, the machine could connect seamlessly to the investor's account. The latter might well be the most impacting feature of Digital ID, as it would definitely disconnect fund distribution from traditional banking and probably make way for a new breed of "pure players" in the field of funds distribution.

The impact of such a technology could be quite important, as it is a "front office" technology, directly affecting the investor's experience when looking for investment opportunities. Indeed, businesses would have to evolve rapidly in line with this technology, or fear oblivion.

Digital ID is obviously useful in many other respects. It may develop on its own, quite independently from DLT.

On the other hand, DLT may develop without Digital ID and carry on with its own identification model: after all, if retail investors remain channelled through distributors, a bespoke Digital ID scheme could be adopted by platform participants, without relying on some universally available Digital ID.

However, DLT would eventually require Digital ID to reach its ultimate level of development on the retail segment.

Investor access

We assume here an indirect model, in which the core platform (a *permissioned* blockchain) remains inaccessible to retail investors. We could have imagined a more radical distribution scheme with direct access to the public. However, we think the latter model prone to security issues, and overall, of limited added value. Indeed, we believe that investors will seek advice from a trusted, if not completely independent, third party. Because of inherent conflicts of interest, we think it would still be difficult for fund managers to develop an advisory role on the retail segment.

Therefore, we chose not to pursue the direct retail distribution scenario in a first approach. Future developments however, might focus on such an extended approach.

Under more realistic assumptions however, institutional investors could gain direct platform membership access and send their investment orders directly. In all cases, *TheFundsChain* platform would operate with full traceability, making direct and indirect sales easier to follow-up. Further extending the platform capabilities, one may even envision a full-digital RFP process to be organized on the distributed ledger.

Competing on investment advisory services

Further, any platform participant would be able to provide investors an access to products, thus becoming in effect a distributor. Fund referencing thus becomes a commodity. Pushing this line of reasoning up to the limits leads us to a distribution scheme, in which for instance, asset managers could directly propose their products online to customers. Deploying such distribution platforms would come at a low additional cost. Other online distributors would of course apply as participants to operate a similar service on a wide range of products. Distributors would thus purely compete on the quality of their advice given to investors.

The equalizer

Are traditional distributors disrupted after all? We found out that most fears about radical disruption are actually fueled by the promises of scenarios similar to "The DAO Fund", which we deemed as quite unrealistic, at least in the foreseeable future.

As a matter of fact, we see DLT more as an "equalizer" than a truly game-changing technology for distributors. In our opinion, threats to traditional distribution networks will more likely come from robo-advisors and universal digital identity initiatives (see boxes aside).

However, even mere "equalization" would bring its own wind of change, under the form of fiercer competition and lower barriers to entry for new entrants. Overall, DLT comes with a genuine opportunity to drastically improve operations and address the pain point of abiding by ever more stringent regulations. Traditional players would thus be able to operate more efficiently, but so would new players as well. Most certainly, such "equalization" would result in higher pressure on margins. On the other hand, incumbent players, particularly banking and insurance networks, enjoy a large customers base valuing their reputation as financial advisors. Reputation and advisory skills shall remain key, as they always have. As a result, DLTs are not part of the problem for distributors, but part of the solution.

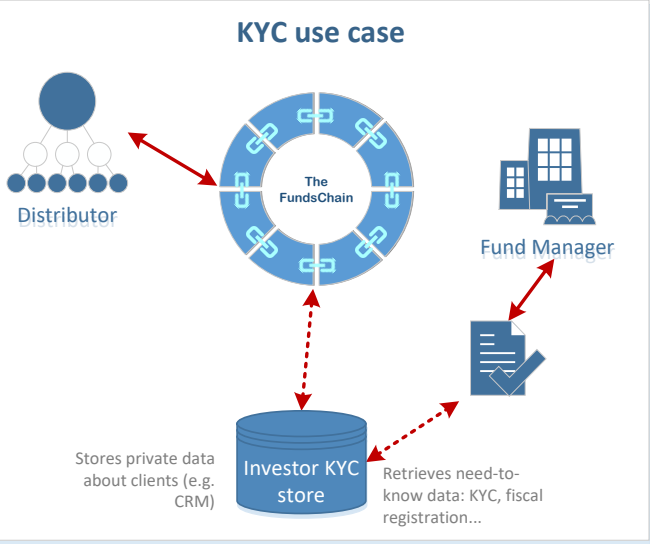
AN ASIDE: ROBO-ADVISORS

Fears for being disrupted by fintech innovation often bring confusion about the actual source of potential disruption. The advent of automated financial advice, dubbed "robo-advisors" is probably the most impacting innovation regarding funds distribution. However promising and disruptive it is, this technology remains largely unconnected to DLT. Distributed ledgers are indeed a boon for back-office operations, but definitely not a cure for every ailment of the funds management industry.

Nevertheless, such robo-advisors could enjoy the improved data quality available on *TheFundsChain* platform to describe funds. Probably not more.

Identity management

The DLT promise is indeed to reduce distribution costs, by streamlining the subscription process and simplifying compliance checks such as KYC, AML, and their subsequent extensions such as CTF (Countering Terrorism Financing). In this context, the advent of "universal" Digital Identification schemes (aka Digital Passport) is much promising. However, and consistently with our incremental thinking, we believe that DLT adoption in the field of funds distribution does not have to wait for some future universal Digital ID scheme to emerge (see previous box).



Nevertheless, end investors would still have to be uniquely identified on the distributed ledger.

This would indeed be a kind of Digital ID, but local to this system: people could use it to invest in funds, but not in their daily life. One should get prepared to interoperate with multiple public Digital ID schemes, which will undoubtedly emerge in the future.

For instance, the UK might issue a public Digital ID scheme used by its domestic banks to identify investors. Such an "external ID" could be used by the platform, alongside say, Danish social security numbers, to back our local ID with real-life credentials.

Investors sponsorship

Distributors play a key role here, acting as "trusted oracles" to the platform: by endorsing one of its customers on the platform, the distributor implicitly acknowledges that a number of identity verifications, as well as some suitability and "honorability" checks have been carried on.

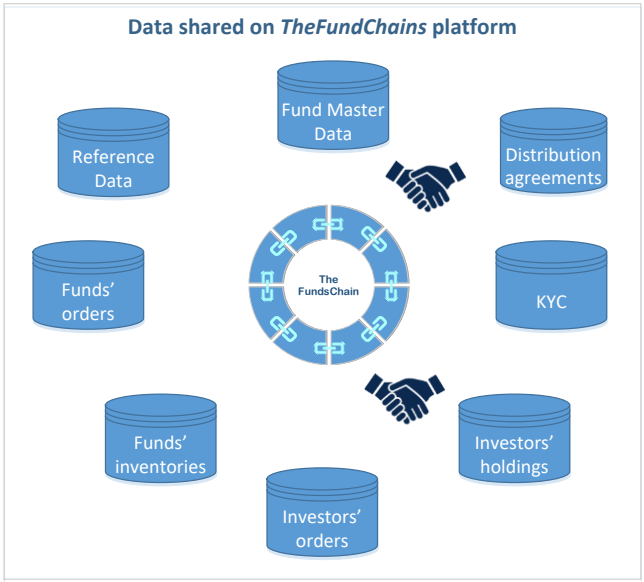
Such a platform-specific identity management scheme would allow participants to share a minimal set of information on end-investors allowing other participants to verify that the required checks have been carried on (thanks to a "KYC store", shown on the diagram above), with possible variations across jurisdictions.

International distribution

Further, one should not have to rely on a unified regulatory framework regarding investor protection and AML, and the various "smart contracts" involved would have to adapt to domestic regulatory constraints. The design of such contracts would obviously leverage on the E.U harmonization efforts in this field, but this shall not be a prerequisite.

Incremental Transformation Scenario

TheFundsChain platform: The Distributed back-office



So far, we have examined more or less disruptive scenarios, each designed with the clear intent to disrupt the other parties contributing to the value chain. In the present section, we show how, by properly organizing such different objectives, one may define a realistic scenario, which would benefit most parties [4]. This proposition to the industry constitutes the central scenario for *TheFundsChain* platform.

Our domains of interest lay on both sides of a fund's balance sheet: full inventories on the assets side as well as fully detailed investors' holdings on the liabilities side. We have stated earlier that the liabilities side should probably be addressed first.

This scenario assumes that securities services, especially fund assets custody and investors registry, are still mainly operated by specialized corporations, which would take care of the infrastructure details. Fund managers would still be able to reap major benefits, as the inventories of their funds would be shared. Indeed, defining proper governance for data available on the distributed ledger would unlock significant savings for funds managers.

Transactions would be shared likewise: custodians, registrars or CSDs would keep their notary function and TAs would still be involved in the validation of orders. As a matter of fact, all trusted parties involved in the fund management process would remain useful contributors to the overall trustworthiness of the system albeit on different terms and conditions, while collectively achieving tremendous efficiency gains.

With such a scenario, a more balanced economic equilibrium is reached thanks to the advent of shared inventories (assets) and investors holdings (liabilities), which would still be "owned" by funds' issuers.

This scenario thus provides an edifying example of how a mutual benefit may be generated from a properly shared resource, in the present case, accurate, real-time information about funds inventories and investors holdings. On the contrary, situations resulting from unilateral developments of locally efficient solutions are customarily lame and sub-optimal (e.g. custodians would only contend with optimizing their processes; funds managers would do the same).

This scenario is *not* disruptive in the sense that no major participant is put out of business. However, this does not mean that business goes as usual: corporations embracing DLT would undergo deep changes in their operations. Our intent in this paper is to sketch a scenario in which such changes could be tackled incrementally.

[4] Peripheral players currently extracting rents from purely technical interfaces or data consolidation would not run a profitable model, though

The three pillars supporting *TheFundsChain* platform

1. A focus on global asset management business

As stated before, our conviction is that DLT should produce a number of specialized platforms, inter-operating with each other. This conviction is rooted in the very nature of DLT, but it is also a practical necessity to conduct incremental changes to existing infrastructures. As such, *TheFundsChain* platform focuses on supporting all business processes related to funds management. To sum up, *TheFundsChain* platform is a distributed back-office and distribution platform ultimately offering a validated view of a fund's transactions and balance sheet.

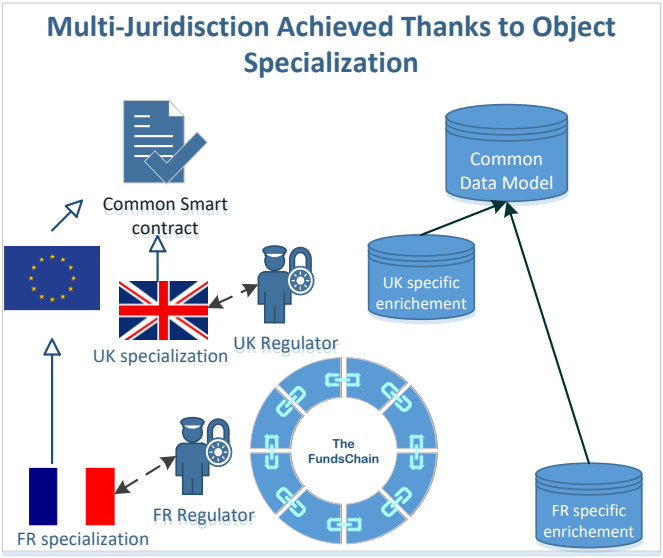
- It is not a Payment platform;
- it is not an Exchange;
- it is not a Securities lending platform;
- it is not a Derivatives trading platform.

Rather, our concept is to interoperate with those, be they DLT-based or not.

2. A fully regulated environment

When examining the role of regulators, we found out that DLT is particularly efficient in the context of regulated trades[5]. The scope being global, this means that the platform should devise flexible mechanisms to support local regulations. The intent is to streamline cross-border funds distribution, while maintaining the highest standards in terms of investor protection. As such, our objective is to study, promote and develop:

- regulators onboarding;
- flexible support for cross jurisdictions transactions;
- streamlined local regulatory compliance services;
- highest security standards for investors.



3. A new landscape to compete over services

TheFundsChain is essentially a decentralized system. On top of a set of "core services" belonging to the community of participants, new value-added services could be developed by participants, mostly relying on the smart contract feature. Such services could remain proprietary in order to gain a competitive edge, or on the contrary, be published for other participants to use.

Such a framework of *certified* services (aka "smart contracts"), together with the concept of data shared ownership, create a favorable environment for participants to compete over services.

In our opinion, this "competitive" feature is the truly disruptive aspect of this scenario.

The table below shows examples for such services. The services themselves are not new: the innovation lies in the potential for automation and seamless integration of many services, thus in effect creating – on the longer term – a full-fledged information system for asset management. Such a target would potentially allow new entrants, such as entrepreneurial asset managers or smaller service providers to thrive on various specific businesses related to managing funds.

[5] This statement extends beyond applications to finance.

Services Offered & Used by actors (Smart Contracts published on the platform)			
	Assets	**Liabilities**	**Other**
Distributor		**Distribution Agreements** Trailer Fees Calculation Trailer Fees Invoicing & Payment **Built-in KYC/AML checks**	Gateway to B-to-C channels (e.g. web) **Legal documentation** Funds Selection & Advisory (e.g. gateway to robo-advisors) Marketing documentation
Fund Manager	**Front-To-Back Position Keeping** (implied custodian & accountant matching) **Order Management** (implied broker & custodian matching)	**Built-in KYC/AML checks** **Trailer fees Provisioning (re. fees payment)** Auto currency hedge | benchmark hedge on investors orders Sales follow-up & reporting	**Fund Registration** **Data Management** Market Data Automated fund management strategies (e.g. index linked, …)
Custodian	**Asset orders execution** [via external ledger] (implied broker execution matching) Investment Constraints Check **Regulatory Compliance Check** Sec. Lending/Borrowing [via external ledger]		
Registrar & CSD		**Detailed registry of investors holdings** (implied notary service) **Aggregate registry of distributors holdings (re. trailer fees calculation)**	CRM connectivity
Transfer Agent		**Investors Transaction Validation** Liaise with external platforms	Digital ID services
Accountant	**Fund Valuation (NAV)** NAV validation & dissemination (implied fund manager matching) Management fees calculation & provisioning		Liaise with auditors
Other	Performance Reporting Risk Exposure Calculation Market Research	CRM (investors targeting)	Due diligence research

TheFundsChain as a platform

Let us recall the core features made available to platform members. As previously indicated, the set of services (and information) would be extensible, in a decentralized way.

- **Global funds book-keeping**

The platform publishes a set of core services to handle transactions on funds. Transactions may affect the assets side (capturing and settling the investment decisions of fund managers) as well as the liabilities side (capturing and settling investors subscriptions and redemptions).

- **Global funds master data**

Services are built on top of distributed master data, which are collectively administered, enriched under shared ownership agreements or privately extended to suit specific needs. Core master data objects are funds, investors and financial instruments listed on funds' inventories. We also set plans to handle distribution agreements.

- **Assets & Liabilities**

TheFundsChain is much more than a mere journal of transactions: it provides a reconciled view on inventories and investors' holdings[6] (i.e. a fully detailed balance sheet).

- **Identifiable investors and intermediaries**

Investors' orders are fully traceable. This means that every single investor is personally known by at least one platform participant (most likely, the distributor). Not everybody has to know about the name and address of every single investor: it suffices to know that there is a trusted sponsoring member which knows about the investor. For other, unconcerned parties, investors would remain anonymous numerical keys. Transactions also keep track of the full chain of intermediaries, thus allowing for an accurate calculation of various fees (upfront or trailer fees).

Opportunities for actors

We have presented the objectives and main features of *TheFundsChain*. Let us now try to figure out how this scenario impacts industry actors. Actual impact on the long run is difficult to predict, as much will depend on how the collective platform will set a balance between "commoditized" services and proprietary value-added services. Our vision is that more and more services will over time become utilities, and that actors specialized in asset servicing would have to compete on a narrower and narrower field of value-added services. We have summarized our projections in the table below.

DISINTERMEDIATION OF THE CUSTODIAN AND REGISTRAR ROLES

Custodian use-case. A useful reminder – perhaps obvious – is that keeping the books up to date requires much more expertise and technical sophistication than keeping a cash ledger, for securities are subject to many events (e.g. corporate actions). In many ways, securities are to be handled like living things: they are born, generate revenues, give birth to other entities, and eventually die… It gets even more complex when enlarging the scope of instruments to derivatives and securities lending contracts.

Reducing the administrative burden of such book-keeping is quite a challenging objective. It is hard to believe, even remotely, in a fully automated custodian robot.

As a result, we don't consider the custodian role to be endangered by the adoption of DLT. Again, we expect an evolution in practices and automation level, but no disruption.

Registrar use-case. Let us consider the role of CSDs (Central Securities Depositaries) and Registrars. Depending on the jurisdiction, they play a similar role of notary on behalf of mutual funds issuers, keeping the book of investors holdings, in a more or less detailed fashion. An early, straightforward, conclusion would be that DLT makes such actors redundant.

However, it so happens that such complex things rarely work by themselves. No matter how "smart" the "contracts" may be. Contrary to closed-universe crypto-asset platform, running a DLT platform for mutual funds shall require trusted "oracles", that is external events to be introduced into the platform by trustworthy actors.

Indeed, DLT would render things an order of magnitude simpler as parties would more easily agree on the outcome of such events. This would be already quite an achievement if, for instance, simple corporate actions such as paying a dividend, could be seamlessly propagated across portfolios.

Low-cost trusted notaries. CSD, registrars, custodian and more generally, fund administration functions are already trusted to perform this "notary" task. They may well continue doing so, much more efficiently.

As a conclusion, we expect that fund administration costs would plummet significantly, even though the platform doesn't pursue an objective of full disintermediation.

[6] We provide a more extensive, technical discussion of the transactions vs balances issue in our third part.

Offered Services: Value-Added vs Utilities			
	Standard	Value-Added	Trend
Distributor	Trailer Fees Calculation Distribution Platform	Funds Selection	**Toward pure advisor** **Toward robo-advisors** [through gateways] **Pure technical providers fade out**
Fund Manager	Compliance Checks	Direct Distribution	**Toward pure fund manager** **Leaner organizations**
Custodian	Oracle gatekeeper (orders, corporate actions, cash ledger)	Smart contracts on a wider set of assets Hedging investor's orders	**Toward pure notary (reg. depend.)** **Thrive as smart Contract vendor**
Registrar & CSD	Oracle gatekeeper (investors custodians, corporate actions)	Digital ID Services	**Toward pure notary (reg. depend.)** **Toward pure oracle gatekeeper**
Transfer Agent	Oracle gatekeeper (investor orders, cash ledger)	Link to external platforms (i.e. Prime TA services reloaded)	**Toward pure oracle gatekeeper (Robo-TA)**
Accountant	NAV Fees calculation Oracle gate keeper (market data)	-	-
Other	Performance Reporting Market Data (Oracle) Benchmarks & Survey (aggregator)	Performance Attribution Risk Computation Reports & Analysis	**Toward pure analyst** **Pure data aggregators fade out**

Challenges ahead

We advocate for such a "distributed back-office" as a pragmatic, flexible, yet ambitious scenario for the funds marketplace. Moreover, we see as a strength the fact that the proposed platform acts merely as an equalizer, focusing on bringing down operations costs without assuming the sudden demise of a particular breed of business actors. Indeed, with this scenario, disruptive features are not built-in the technology, but would rather result from the market forces at work.

No gain will come without pain, however. The organization of such a collective effort, as well as implementation complexities come with many pitfalls on the way ahead. Our next section, Part III, contributes to demystify a number of these challenges.

PART THREE

DESIGNING DLT FOR THE ASSET MANAGEMENT INDUSTRY

TECHNOLOGY INSIGHT

OVERVIEW

As previously stressed in parts I and II of this paper, permissioned distributed ledger technology is the preferred route for the financial industry. Moreover, we observed that DLTs come in many flavors and variations, while only some of them provide an adequate level of functionality to cope with the industry's expectations. *TheFundsChain* initiative is not bound to a particular technology or brand. We argue that now is the time to figure out which capabilities such a technology should deliver in order to address existing business issues.

In this third and last part of our paper, we would like to shed some light on the set of features required from the DLT powerhouse, and compare it with first generation blockchains.

The DLT Decalogue

The list below follows our requirement-based approach. We outline the 10 most needed requirements for the DLT itself. In the following, we'll develop on why they are important requirements.

1. **True Distributed Database: the platform must deliver a genuine distributed database service**

This comprises *at least* scalable data storage and integrity management as well as some querying facilities. In addition, such a potentially huge database would require efficient storage algorithms, that is:

2. **Efficient peer-to-peer storage: every participant only holds a fraction of the total storage**
3. **Flexible consensus: consensus protocols must be configurable, dynamically**

E.g. transactions rules (involved parties) may change, depending on the product or the investor's location.

4. **Privacy over distributed data: distributed data remain essentially private**

Security is paramount in our context. However, the platform needs more than to be hacker-proof: it should ensure absolute data privacy whenever needed. This leads to an important additional technology requirement:

5. **Advanced cryptography: technology to provide (and revoke) role based authorizations**
6. **Decentralized Key Exchange: classical single key authority scheme would defeat the purpose**

Ensuring both security and privacy requires an efficient key management mechanism. To suit the decentralized nature of the platform, this mechanism should avoid relying on a central single authority.

7. **Avoid the genesis block curse: it may be sometimes useful to store account balances or to reboot the chain**
8. **Flexible and scalable smart contracts execution**

Smart contracts are merely rules executed by involved parties, which output is validated by consensus. Again, the consensus protocol should be both scalable and dynamically configurable. Besides, all data objects are potentially concerned – e.g. master data – and not only tradable assets living on the ledger.

9. **Third-party identification: participants know each other, not each other's customers**

Investors must be recognizable on the platform, but their identity is not necessarily universally shared. Nonetheless, it should be easy for any participant to share the knowledge of its own customers with some other party.

10. **Cross-blockchain interoperability: routing transactions from a chain to another**

No single blockchain will probably fulfil all requirements for all financial products. Such dedicated chains will have to cooperate. Interoperable protocols are thus required.

TECHNOLOGY INSIGHT

Distributed Database Technology

Scalability. The workhorse technology underlying *TheFundsChain* platform should be highly scalable. The following figures give us an idea of the main sizing parameters for a target platform supporting fund management businesses worldwide.

- **Participants:** 5 000

The number of participants to the shared DLT infrastructure, potentially involved in a consensus protocol.

- **Investment vehicles:** 100 000

Number of investment products referenced (e.g. fund shares).

- **Managed identities:** 100 000 000

Number of end investors identified (order of magnitude).

- **Financial instruments universe:** 5 000 000

Instruments refer to securities and derivative contracts managed by fund managers. This number encompasses: stocks (50 000), bonds (2mn+) and various derivative instruments (2mn).

- **Subscription/redemption orders:** 25 million per year
- **Transactions:** 250 million per year

Gross estimate: 20% of total executed orders, globally (source: BIS)

- **Financial value stored as holdings:** 55 trillion €

More than 5 000 times the size of holdings on the Bitcoin platform as of Q2 2016.

Scalability and Consensus latency

Fund management is no high-frequency trading business, yet processing about 5 000 subscription/redemptions per hour is largely out of reach, for technologies like Bitcoin. Further, keeping the inventories up to date shall require a large amount of transactions on the assets side to be validated, albeit perhaps not necessarily in real-time.

TECHNOLOGY INSIGHT: THE BOOK OF NUMBERS

The sector is composed of a large number of actors, but remains highly concentrated in terms of assets. There are more than 3 000 fund management companies across Europe. Globally, the top 400 fund managers concentrate almost all the global AUM. Asset servicing companies are much more concentrated with about 25-30 globally significant actors.

As of 2015, there were about 60 000 fund vehicles (UCITS and AIF) in Europe, and about 10 000 in the US. Extrapolating to Asia and Latin America, we might fairly estimate the global number of investment vehicles to be close to 100 000.

Regarding securities, we may find about 50 000 listed stocks worldwide. The universe for bonds investment is much wider, at about 2 million.

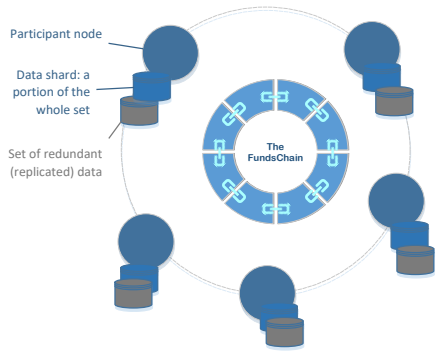
Orders on funds: European estimate is 5.5 million orders per year (estimate derived from BCE settlement data).

Efficient storage

The set of data aforementioned, with its full historical record, represents a tremendous amount of data, most likely counted in the tens of terabytes. This is to be compared to a petty 75 gigabytes for the bitcoin transaction record. Simplistic replication protocols distributing the **full** dataset across **all** participants are obviously not workable.

The problem is not intractable, though: several technologies fare much better by providing a sensible replication trade-off when distributing ("sharding") data across database nodes. Consider for instance, a database of 50 TB shared across 5 000 nodes with a replication factor of 5, i.e. the community maintains 5 copies: each participant would manage on average a 50 GB database, which is quite reasonable.

Data sharding with redundancy across the network



Consensus Protocols

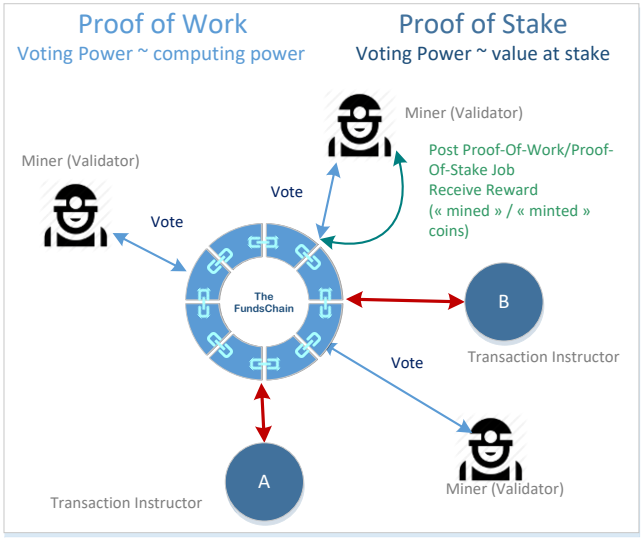
Back to basics: fault-tolerant consensus. The idea of a distributed database ruled by a consensus protocol is not new. As a matter of fact, this principle underpins most advanced distributed database systems which nowadays run the Internet. However, such systems work on a different set of hypothesis than DLT, namely, they do not assume that some participant may maliciously attempt to corrupt data or subvert the consensus mechanism to their own advantage. Such systems are usually designed to efficiently distribute an infrastructure across sites operated by a single corporation. Most industrial scale systems today use some variant of the Paxos algorithm, a well-known, efficient consensus-seeking method between trusted parties, also known as *fault-tolerant consensus*.

Byzantine Generals Problem. Obviously, this is not sufficient to handle situations in which parties do no trust each other. In other word, when one assumes that some participant might *lie*, reaching a consensus is a much more complicated task. The theoretical problem itself, called the "Byzantine Generals" problem[7], has even been proven to be impossible to solve in its purest form[8].

Most DLT platforms try to overcome this theoretical intractability thanks to additional simplifying assumptions. Bitcoin, for instance, did so by relaxing the constraint on a deterministic outcome of the consensus protocol, which explains in turn, why transactions take on occasion a very long time to settle. This system is indeed not able to guarantee that a transaction is validated within a given time limit: there is always a (low) probability that the validation protocol hangs about for a very long time. One should keep in mind that every single original DLT comes with its own assumptions and choices of design regarding the inner workings of the consensus protocol.

Regarding *TheFundsChain* platform, and more generally any platform built to support a large volume of transactions, we think it essential to rely on a design with a time-bounded algorithm: an event which would be deemed as almost impossible when considering thousands of transactions suddenly becomes likely to occur when considering millions.

Voting. Many variations also exist regarding the voting power of each participant to a consensus. Early platforms adopted a biased algorithm to favor well-behaving participants. For instance, Bitcoin deliberately chose to bias vote toward their respective computing power, requiring voters to compete to solve a "Proof of Work" problem. This "proof" is a complicated numerical puzzle to be solved by consensus participants. Ordinary Bitcoin users cannot generally compete with the vast computing resources deployed by participants who specialize in the transaction validation business: the "miners". Alternatively, some other platforms did choose to bias consensus using a measure of their respective financial interest in the platform, that is a "Proof of Stake", which is faster to determine. In both cases, the objective is to tip the scales of the validation protocol toward participants which actively contribute to the platform.



Voting bias is indeed a desired behavior for fully open, public platforms. The underlying idea is to favor – and possibly, reward – active contributors and deter cheating participants. It is important in an open environment to discourage so-called "Sybil attacks", that is attempts made by one or several participants to bias the consensus toward their own interest. The "Proof-of-X" family of protocols is precisely designed to make such attacks too costly.

[7] A parable presenting how several separate armies should coordinate an attack plan, while knowing that some among them might be traitors. Originally, the problem what researched to design fault-tolerant IT systems.
[8] Fischer, Lynch & Paterson – 1985. Also known as "the FLP result"

A noteworthy consequence of this approach is that the parties entering a transaction seldom participate to the validation consensus.

Obviously, things work differently on a permissioned ledger: even though the system must remain secure, participants have a genuine business interest in the platform and such artefacts are not really needed. Furthermore, in most use-cases, all parties involved in a transaction are willing to take part in the consensus.

Another key feature of public platforms is that the notion of *reward* is a built-in feature of the consensus protocol: again, this feature is fundamental to build a self-sustaining closed ecosystem which run its own economy. Examples of such platforms abound, all following the Bitcoin philosophy.

Obviously, such considerations are not necessary and even not desirable for our target platform – or any DLT intended to seriously *serve* the financial industry – *serve* and not *disrupt*. Besides, a consensus protocol is a flexible concept: there is no reason to believe we are stuck with methods such as "Proof-of-Work".

First of all, there is no real need for a smart algorithm to bias the consensus toward one particular category of participants.

Most simple consensus we may think of is one in which fully-trusted participants would share equal voting powers. If not equal, their voting powers are at least predefined. Participants which are not eligible to "full-trust" would simply be non-voting participants. This very simple (and fast) mechanism constitutes what we call a "federation consensus". Obviously, it is too simple to capture the subtleties of financial transactions.

MYTH BUSTER #5
BUILT-IN REWARDS

Generating rewards for consensus resolution services as a concealed way of paying operating costs appears as an intricate, and at the same time very limited way to make business on the platform.

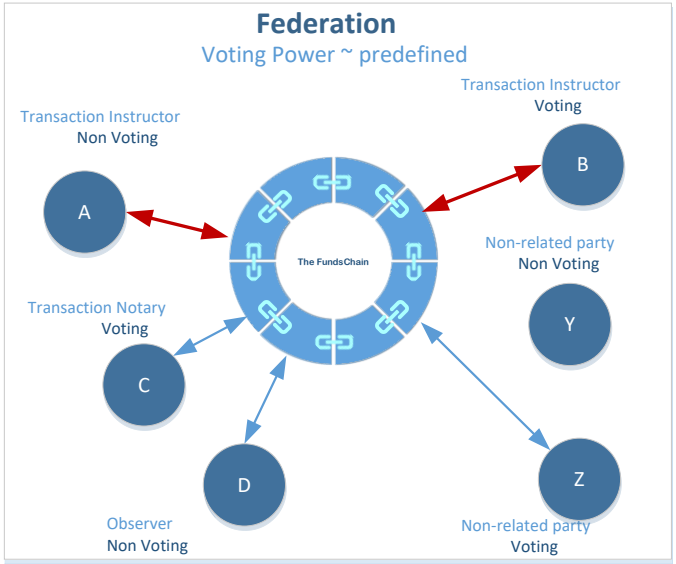
It is however essential as an incentive to participate to the closed economies simulated by platforms such as Ethereum or Bitcoin.

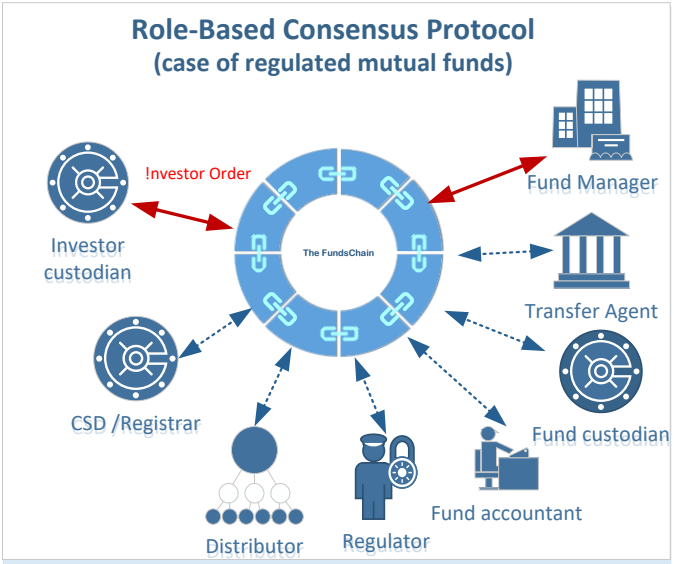
As a matter of fact, such rewards paid in internal token-currency dilute other owners of tokens. Only a platform minting its own currency may be able to pass on transaction fees in such an almost invisible dilution.

TheFundsChain platform, or for that matter, any DLT processing securities or financial instruments, does not constitute a closed ecosystem, and in particular, does not have to (and should not) mint its own currency.

Likewise, protocols generating built-in rewards are useless in our context.

A more complex, but also much promising method is context-dependent voting. The idea is to define voting power according to the role of a participant in a transaction. This is what we call "role-based consensus". The idea is to allow a different set of validating participants for every transaction and to define voting power accordingly. In particular, we believe that the introduction of a "veto vote" ability built-in the consensus protocol supports our idea of an onboarded regulator and could help with a number of regulatory issues, such as AML or temporary freezes on funds.



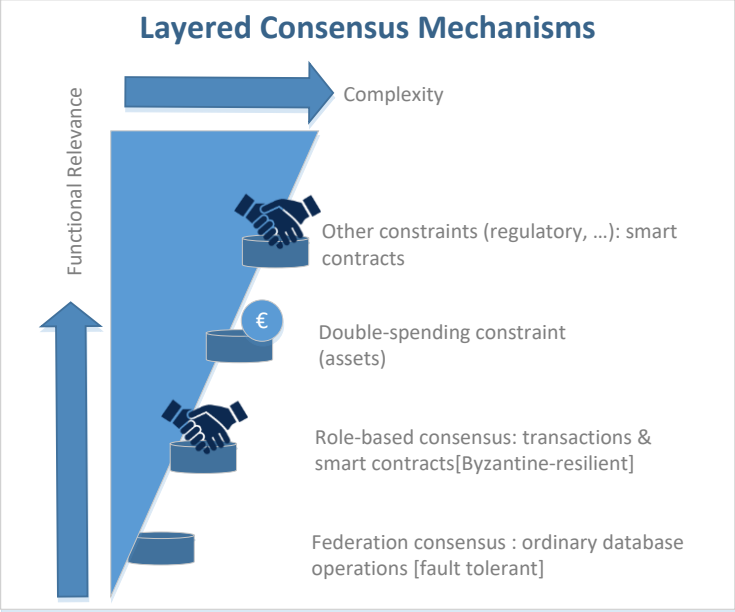


Multi-layered consensus

We have seen that the complexity of a consensus protocol drastically raises with the number of requirements (fault-tolerant, Byzantine-resilient, ...).

A promising way of engineering efficient protocols is to address such requirements separately, defining consensus at multiple levels. This is indeed an interesting option, since it would allow to build a system bound to evolve, gradually plugging newly required consensual checks.

For instance, one could imagine that sponsoring a new end-investor is materialized by a new entry added to some "KYC store" database object. All participants would somehow have to acknowledge this change to their data structures. However, only some of them would be entitled to enter a validation of the information related to, say, investor's suitability. Furthermore, no other than the sponsor would be entitled to validate the "private" description of this investor.



Some existing platforms, available for testing, already propose mechanisms designed along these lines, that is addressing separately the Fault-Tolerance consensus problem on the one hand and the Byzantine Generals consensus problem and double-spending check on the other hand. More complex consensus rules may be added further, for instance with business rules based on the role of participants.

Such technology leads to much better performances and flexibility to build real-life business applications.

What do participants vote for?

Voting to reach a consensus is essentially a matter of ensuring that distributed data remain consistent and that no single change occurs which could corrupt the whole system. We have mentioned earlier several approaches to determine *who* is involved in a consensus. But even though a number of participants may be relevant in validating a data entry, not all of them, if any, might be entitled to know about the full details.

For instance, whenever a fund manager declares a new product entry, this information must be acknowledged by other participants. However, only a subset of this product description is intended for sharing. For instance, the fund manager may have dedicated this fund to one of its clients, which should remain unknown to other participants.

Fortunately, there is no need for voters to be aware of the full data being voted for.

In other words, it is possible to design a consensus mechanism in which voting participants do not get the full knowledge of validated data. This concept, known as "zero-knowledge proof", is now widespread among DLTs. With such a mechanism at hand, it is possible to validate and store data on the distributed ledger that remain *private*.

Yet, due to the physical distribution of data across the network, the encrypted bits may be peppered over many different places. In other words, the new fund entry created above lives on the network of database nodes (most likely with several copies) and not on only the fund's issuer own copy of the distributed ledger. Privacy is achieved through encryption and no longer by ring-fencing data centers from the outside[9]. Such considerations should apply to any change applied to the information stored on the chain (i.e. a "transaction" in the database sense), and not necessarily only to *business* transactions related to the purchase or sale of a digital asset. Examples abound, especially when considering that master data also live on the distributed ledger: updating investor's data, issuing a new product...

[9] The permissioned ledger setup would however limit the exposure of such "secrets in the open".

The double spending issue

Now when it comes specifically to transactions recording a change of ownership in a given asset (e.g. a subscription of some units in a mutual fund), it is essential that the consensus performs further verifications, namely that this asset is actually available for trading. For instance, when the asset in question is some amount of currency, the consensus verifies that it has *not already been spent* in some other transaction. This non-double spending check is another essential cornerstone that must be built in any DLT consensus protocol. Again, it does not need to be enforced on *all* changes, but only changes in asset ownership. A double spending check is intuitive for cash trades. It is getting more intricate when the ledger has to support trades for which it is possible to sell something one does not own (one borrows it) or to buy something with money you don't have (e.g. deferred settlement).

Regarding this kind of "enhanced" double-spending check, we refer the interested reader to the contribution *TheFundsChain* recently made to the ESMA consultation[10] in which we attempt to enlarge the concept asset, transaction and double-spending to address deferred settlement (with netting) and margin finance use-cases.

Platform operating costs

Without built-in reward in place, platform operating costs would be charged as a separate process, as well as the various fees associated to the usage of the services made available on the platform.

We'd rather advocate for such a separate invoicing mechanism than for some internally minted token-currency. Indeed, keeping the cost-charging aside keeps the financing scheme for the platform flexible and up to its participants to determine, without specific assumption on the inner workings of the underlying technology. Fees would possibly be based on service consumption, or any other business agreement (fixed or holdings-based fees). This does not mean that the calculation, invoicing and payment of fees cannot be handled by the platform and automated. Rather, we do not think it desirable to introduce such features within the core technology – i.e. the consensus protocol. As a result, we stand against "mining costs" and other "gas" tokens. Such assumption vastly simplifies the engineering of fast and efficient consensus. Smart contracts do, on the contrary, provide sufficient flexibility to support such features.

The table below summarizes the concepts discussed in this section.

Consensus protocol feature	
Fault-tolerant consensus	Required
Relaxed-Byzantine problem consensus	Required; a time-bound method is desirable
Transaction privacy	Required
Double spending check	Required on asset ownership changes only
Proof-of-Work voting bias	Not required
Proof-of-Stake voting bias	Not required
Built-in contest for a reward ("mining")	Not desirable
Built-in currency minting	Not desirable
Role-based Voting bias	Desirable

DEFERRED VS REAL TIME SETTLEMENT

Publicly observable distributed ledgers have shown it was possible to proceed with transactions in near real-time. Indeed, the transfer of ownership may be considered settled once a transaction is validated.

However, real-time settlement may not be always desirable. This is for instance a most unwanted features for all applications to margin finance.

In the context of mutual funds, most investor' orders are settled at T+1 on purpose. For funds holding illiquid assets, investment and disinvestment transactions may be even more delayed.

Smart contracts may be used to solve this kind of issue, with scheduled settlement events to activate the smart contract agent in due time.

[10] https://www.esma.europa.eu/file/19557/download?token=1oGKSa7O

Privacy

Security is not privacy. Pioneering blockchains have deliberately chosen to expose every transaction to all participants. For instance, everyone may consult the global bitcoin ledger of anonymous transactions. The same remark applies to most publicly observable platforms. However secure, such platforms do not operate privately.

In the context of *TheFundsChain* platform, this choice should indeed be reverted: parties involved in a transaction have to be identifiable, though not necessarily by every participant, while participants not involved in a transaction should not be able to extract any useful information about their competitors'.

In other words, **the DLT platform should enforce data privacy** whenever required. However, there is a minimal set of information to be fully shared in order for the platform to carry on its regular consensual validation job.

It should be noted that, besides technical considerations applying to an eligible target DLT technical platform, *TheFundsChain* has already started the painstaking exploration and contouring of such a minimal public information set for the main business objects that shall "live on the chain".

Seal vs encryption. DLT rely heavily on cryptography and more precisely, on the ability to generate a cryptographic seal, i.e. a way of ensuring that any information put in store is not tampered with. Putting it differently, the so-called "immutable" property of a blockchain is another word to say "hard to tamper with".

This specific cryptographic tool is not related in any way to privacy, that is, keeping some data secret or restricted to a subset of participants. In order to ensure privacy, it is necessary to resort to other cryptographic tools. An interesting finding is that data distributed across the blockchain, or data payload, may be composed of a public part and a restricted part. The restricted part may be further encrypted to ensure privacy. A number of DLTs currently implement this kind of privacy.

However, this is not enough to fulfil our requirements. Indeed, commonly used encryption schemes (e.g. public/private key schemes, aka asymmetric cryptography) are designed in such a way that party A may communicate a secret to party B, which in turn can verify that this secret indeed originates from party A. In short, public key encryption manages secret exchanges between two parties only. This is a very limiting situation in a business context in which several parties, but not all platform participants, have to collaborate privately. Not to mention that regulators may demand special access to otherwise private data. Fortunately, recent research in the field of cryptography comes with a solution (see box).

TECHNOLOGY INSIGHT: DATA PRIVACY

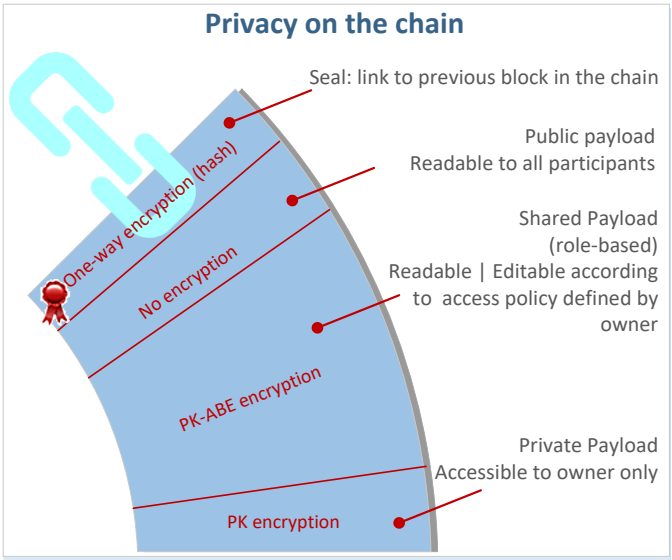
Recent research conducted in the field of cloud storage has been able to overcome the limitation of classical asymmetric encryption to two communicating parties only. New algorithms can generate keys and encrypted messages, which embed access granting rules, or "attributes".

Such new algorithms, known as PK-ABE (Public Key - Attribute Based Encryption) thus define various roles for participants, which may be allowed or denied access to a given encrypted payload. This technology is still quite new, like DLT. We believe that coupling both would lead to an extremely valuable "new alloy", with a broad range of applications.

An example application to *TheFundsChain* platform could be to define roles such as fund manager, distributor, CSD, regulator, … We would then define fund's specifications to be public, investor's details to remain privately held by the distributor, while some information about investors (e.g. KYC) would remain accessible to the fund manager.

We consider PK-ABE technology as an essential building block for our target DLT. In particular, PK-ABE enables the concept of data shared ownership and provide some solid ground for our framework of delegated services.

Like any new technology, PK-ABE comes with issues of its own regarding security. A noteworthy one is certainly the so called "collusion attack", or the possibility that several participants with limited access share their keys to guess keys with a higher access level. *TheFundsChain* is currently closely watching this new field of algorithms.



Platform & Data Access Policy

Platform access. Taking the distributed ledger private – or "permissioned"– means that a minimum membership governance is required. We envision a situation much similar to clearing platforms, albeit probably with a more extended population of members. As a matter of fact, ***TheFundsChain*** **platform should not be restricted only to fund managers, banks** and their various specialized subsidiaries, but also opened to independent asset managers and distributors.

Access policy would have to be maintained by a board of platform caretakers. The definition, role and governance of such a "membership authority" remain to be defined by the community, as much debating about the target organization still lies ahead. For instance, an interesting, but debatable, issue is whether to open the platform to non-financial institutions such as corporate institutional investors, thus making direct distribution a reality on this segment.

Sponsored membership. We see a similar debate about membership regarding possible access and role granted to software, data and services vendors. If not granted direct access, such actors could still offer services on the platform through sponsoring members. Levying fees on such indirect access could be a source of ancillary revenues for fund managers or asset servicers. For example, we might consider the case of a data vendor specialized in funds due diligence research. This vendor would be able to develop a value-added service available on the platform, possibly in partnership with an incumbent member, in order to enrich product master data publicly available on the platform.

As a non-member actor, this vendor would have to deploy the service by renting the access to a sponsoring member, as a guarantee that the service operates securely and safely.

Nonetheless, in order to guarantee smooth and secure operations, **retail investors would most likely not be granted access**. Retail investors would typically invest through distribution platforms. It should be noted that *any platform participant could technically act as a distribution platform*. End-investor sponsorship must therefore be closely controlled by adequate checks implemented with smart contracts.

Taking care of the caretakers. Our approach assumes a supervised evolutionary process, based on a community of reputable caretaking participants, operating under regulator's scrutiny. Without doubt, the platform might experience issues, even perhaps be hacked, despite hardened security measures. This should not, however, be perceived as a blocking issue and more as an attention point to all participants.

Indeed, in situations such as a hack, heist or other disruption, participants react, fix the issue, possibly backtrack fake transactions or stolen assets. The platform is indeed *curated*, meaning that the rule of law applies here. A restricted membership setup also comes with responsibilities: every participant holds a responsibility in keeping its access to the platform tight (a situation in many ways comparable to accessing the SWIFT interbank network).

Introducing the concept of a "board of caretakers" obviously raises concerns about the long-term cost-efficiency and fairness of a platform thus in effect ruled by a few dominant players. This is not an unavoidable situation, though, as new self-governing possibilities have emerged alongside DLTs.

When looking at DLTs from a higher point of view, and without a particular focus on financial transactions or crypto-currency applications, we may observe that non-financial actors are currently developing practical e-governance concepts applying to governments, corporations and organizations in general.

Thinking out the box, the "board of caretakers" could be implemented as a much transparent and dynamic organization, possibly ruled by voting and decision-making procedures, and embedded in the inner workings of the platform. This is the deep meaning of the term "DAO" that we sometimes see associated with DLTs. As an example, we could imagine that new applications for membership are subject to a vote by existing members. This is much arguable, though, as a policy ruling the construction of a new field for open competition.

However, the pragmatic vision we advocate with *TheFundsChain* platform is that such a "DAO setup" would be too much of a burden to begin with. Given enough time, though, the concept might well become a viable option. Indeed, setting up truly automated and efficient self-governance procedures is a daunting task, which would probably divert a significant portion of the development effort. Therefore, we believe that further field experience is required, in order to step back and define new, improved governance policies taking advantage of the technology.

The key management challenge. To guarantee a secure access, members shall be provided with adequate credentials, or certificates. Besides, sharing non-public data among a subset of participants (say, a fund manager and its fund administration services providers) would require a number of keys to be generated in order to properly reflect the adequate data access policy (i.e. granting and revoking access).

In a typical security & privacy management scheme, all such keys would be generated and then distributed to participants by a central key authority. An illustration to the financial world of such an authority is SWIFT. The point is that this would just create a new central authority that everyone would have to trust (and pay for…). This would offset a number of the benefits gained from largely distributing data and sharing resources.

Fortunately, technology advances in the field of key exchange protocols provide new ways for truly distributed key management to operate without such a central authority (see box). In our opinion, it is thus extremely important to consider and study the deployment of such technology in the context of permissioned DLT with support for data privacy.

TECHNOLOGY INSIGHT: KEY DISTRIBUTION AUTHORITY

From an engineering standpoint, the equivalent of such a "board of a caretakers" is what is called a key distribution authority, which is in charge of verifying the identity of parties and producing authentication credentials that may be trusted by others. This is for example the role of "Certificate Authorities" on the Internet, or within the financial community, the SWIFT organization.

However, some recent technological breakthroughs in the area of security - originally not related to DLT – allow to envision more decentralized possibilities. Indeed, the original "Web of Trust" concept (first coined some 20 years ago already) and more generally, Distributed Public Key Infrastructures, have been a research topic for years and have been slowly maturing. The distributed nature of DLT has somewhat recently revived the attractiveness of such complex security schemes.

Again, we believe that such developments are indeed much valuable in order to form a truly open target platform, but that their governance and organizational implications would create a diversion of the overall coordination effort needed to define a unified and interoperable platform.

For the time being, we should contend with keeping in mind the possibility of a truly decentralized security infrastructure, while concentrating efforts on core business issues.

Immutability: vulnerability, the genesis block curse and rebooting the chain

Vulnerability: immutable, unbreakable and all that jazz

Immutability simply refers to the cryptographic seal added as a fingerprint to every single transaction on assets, and more generally, to any change applied to the distributed data that would require such fingerprinting mechanism. The seal must be very strong to ensure that forging a transaction is nigh impossible. However, nothing is unbreakable. Or remains so for long.

Just to mention one reason for this, the length of keys used to compute the seals (or any other encryption purpose) must grow with the evolution of computing power. An alternative to keys growing longer is the formulation of a new numerical problem upon which to base cryptographic computations.

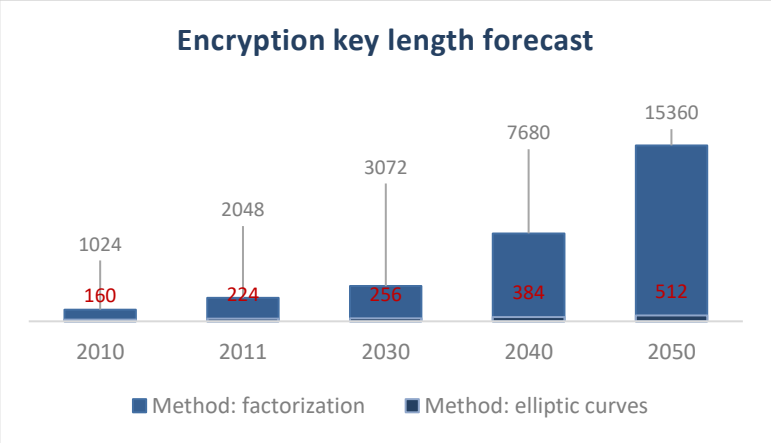
The "elliptic curves" method, which wide adoption remains quite recent, has to this extent provided some relief regarding this ever-growing trend (see graph next page). But even though this issue were considered solved, another one would soon arrive. Computer security is just like the never-ending story of the shield and the sword.

The astute construction of blockchains – and for that matter, all DLTs - gives us some reason to be more optimistic: seals are chained every time a new block of transactions is validated, hence, breaking a seal should be done before the next block is validated – for instance, Bitcoin spawns a new block every 10 minutes or so. With current computation technology, a brute force attack to break a seal is impossible in such a short time.

However, there are more possibilities than brute force attacks. The recent hacking of the Ethereum platform exploited other vulnerabilities, at another level of the system (smart contracts). To put it differently, every complex system comes with its weak points.

For all practical matters, we should thus think about the whole system as being highly secure for a period of time only. An "immutable" system recording all transactions since the epoch would necessarily hit a point in time when its security is compromised.

We also have to remember that asset management, and investment in securities in general, is a long-term business, in which a decade is not considered a long time horizon. One should thus anticipate and take provision for future security enhancements, such as key size or key computation method change, and more generally any kind of modification required to keep up with the security arms' race.

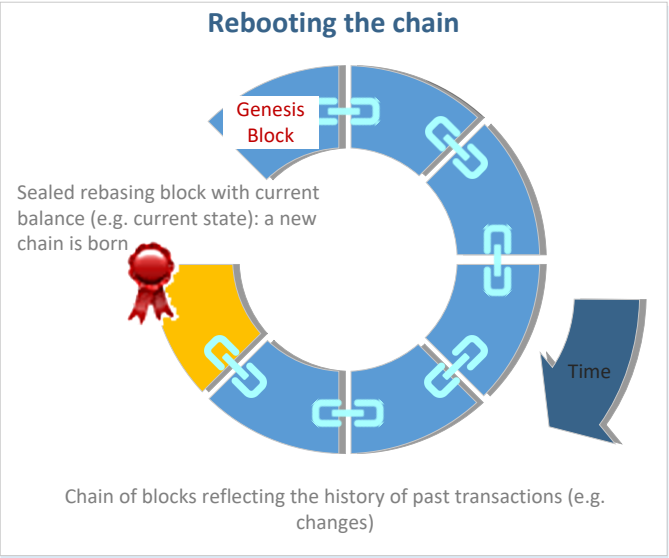


Rebooting the chain: security upgrades

Applying a security upgrade to an "immutable" system would require either to define a point in time from which encryption and security change, or to compute once again ("rehash") the whole chain of cryptographic seals since the very beginning – a new chain for the whole transactions history. We call this situation "rebooting the chain".

We clearly see that a full rebuild is simply not an option for a real life platform operating a global production.

Designing a workable procedure to mark a new starting point for the chain is thus a strong operational constraint.



Rebooting the chain (again): retrieving account balances.

The Bitcoin platform requires no more than a single debit/credit transactions journal to operate its crypto-currency transactions. Moreover, Bitcoin designers chose to keep data structures as simple as possible, and thus not to model explicitly account balances. Account balances result from the sum of past transactions. Most obviously. Or is it really?

A DLT platform such as *TheFundsChain* platform would have a much more complex information model, for which the debit/credit model is not always adequate. However, regarding the financial transactions tracked by the platform (issuing or transferring funds units, or, on the assets side, purchasing or selling securities), the model is quite relevant.

Now this begs some interesting questions about practical issues:

- Genesis block issue: do we need to keep the full history since the very first transaction?
- Querying capabilities & performance issues: do we have to browse through the whole history every time we need to get a balance?

Clearly again, dealing with a "Genesis Block" is simply not a sustainable constraint, as it severely hampers the system's scalability, especially given the timespan considered. Nobody wants to scan 20 years of transactions on a fund to get such an elementary figure as the number of issued shares. Nobody wants to audit a transaction validated 50 years ago either.

However, this "youthful mistake" has now been widely acknowledged by DLT developers. Some DLT platforms should be now able to "reboot the chain", starting with a (validated) initial account balance and regenerating a new sealed chain of transactions from this point onwards. At the moment, however, none to our knowledge has been able to perform such a maintenance action without temporarily halting business operations.

Such an operation should be benign enough to be carried on a regular basis, for a number of reasons:

- keeping no more than the depth of audit trail than necessary;
- allowing to query balances in a more efficient way;
- allowing to deliver strongly impacting platform upgrades.

TECHNOLOGY INSIGHT: KEEP YOUR BALANCE

The transaction vs balance issue is actually a data modelling question and should not have anything to do with DLT itself. To make a transaction system workable, it is indeed tempting – as most current systems do – to keep a persistent image of current positions and a systematic calculation of balances.

This issue is almost as old as the accounting technique itself and a number of industry-proven solutions have been deployed since database systems started to perform accounting tasks, such as: rebasing the system at some predefined period-ends, or updating a latest balance entry together with every transaction…

Therefore, if DLT effectively provides truly flexible data modelling capabilities – e.g. beyond a single debit/credit ledger – there is no reason to believe that retrieving an account balance should be particularly constrained by the technology itself. As a first estimate, we suggest to carry on with a monthly persistence of balances. Most importantly, such a move would keep the "genesis curse" at bay. In addition, such a "monthly closure" could trigger a number of smart contracts, for instance to process the payment of trailer fees.

More on smart contracts

We have presented earlier the concept of smart contracts and what they could be useful to. In this section, we elaborate more on the conceptual and technological aspects of this feature.

Smart contracts as defined by the work of N. Szabo (1993), reflect an abstract and very general concept relating to performing automatically agreed upon contractual terms. Another recurring term, *the Ricardian contract* (Riggs 1996), refers to a design pattern used to capture the intent of an agreement established between the contracting parties, effectively capturing legal prose into parameters and software logics. Both provide some conceptual support to establish a definition of what a smart contract living on a DLT should be.

In order to be useful to the community, such "contracts" should either represent at least one of the following aspects:

- operational procedures to be enforced by the platform (e.g. rules to establish the amount subscribed on a fund, given a valuation calendar and a series of NAVs);
- actual business contracts established between parties (e.g. the terms of a distribution agreement for a fund).

In practice, a smart contract lives on the chain as a certified software agent, meaning that the code and interface of such an agent are sealed by cryptographic means to provide a unique signature identifying the contract. Such a signature may be used for instance to find the right contract on a directory of published services.

Triggers. This *agent* is activated by events, which may be internal or external to the distributed ledger. The outcome of its execution may be a calculated result (e.g. management fees), a data manipulation carried on the distributed ledger (e.g. issuing a new product), another event to be consumed by other contracts (e.g. "KYC OK, let's proceed") or some output provided to an external system (e.g. payment acknowledgement).

We believe there is a strong requirement on the underlying smart contract technology regarding the diversity of supported events: indeed, while some DLTs may well be demonstrating cascades of internal events to pipeline related transactions, we have so far been unable to figure out similar demonstrations of time-triggered events, e.g. a daily cut-off, a monthly or quarterly reckoning of trailer fees.

Parameters. In addition, most contracts would need some input to be worked upon. Input might be provided by another triggering transaction, by other objects living on the ledger or provided by a trusted oracle.

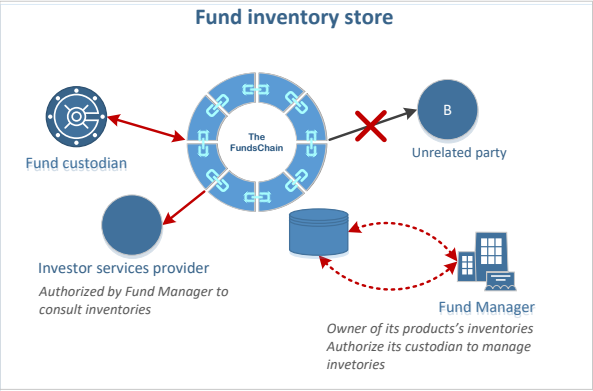
For instance, NAVs could be considered a legit object living on the ledger, readily available for contracts to use. Conversely, security prices would rather be provided by an oracle to an "inventory valuation" contract. In this example – which is a very complex use-case - the details of how such an oracle would work remain open to discussion. More generally, market data acquisition and licensing issues on a shared platform still constitute a challenge.

Enforceability. The execution of such a contract is subject to consensus validation, just like transactions – albeit possibly with some variations on the consensus protocol. This means that its outcome may be considered enforceable. By enforceable, we mean that the execution of this certified software agent, whose output has been validated by a consensus of participants, constitutes an admissible evidence to settle disputes between participants, possibly through an internal arbitration process. To put it differently, smart contracts conveniently enforce marketplace conventions and rules. Legal enforceability is another matter.

Disputes calling on courts may indeed rely on smart contract audit trails to support a case. However, the outcome of such a case would heavily depend on how the terms of the smart contract did *interpret* any relevant law and regulation.

The execution of a smart contract is not required to be instantaneous (i.e. response follows inquiry) and could follow a full-fledged workflow of possibly asynchronous events. The software agent thus maintains an internal state of its active workflows.

Service delegation patterns. Sharing information is not only a requirement for transaction validation: it is also required to properly hand over administrative tasks to specialized providers. Consider for instance, the creation of new shares upon a valid subscription order: creating new shares is nominally under the responsibility of the fund's issuer. On an operational basis however, this action is most often delegated to the fund's administrator. This example exhibits the need for the platform to support delegation schemes whenever a consensus is required. A noticeable finding is that ubiquitous data sharing makes such delegation much more flexible and exposed to competition, as "data ownership" no more constitutes a barrier. Consider for instance that an asset manager could delegate a funds custody to one provider and reporting services to another one. Eventually, large integrated groups would be able to more easily leverage on the information shared by their subsidiaries.



PROCESSING NAV

NAV is a key information as it is basically the price of the fund used for subscription/redemption. There are basically three steps involving various actors : the computation of NAV (most of the time performed by the fund accountant which is often its custodian), the validation of the NAV (the asset manager being responsible for publishing a reliable NAV might want to validate the figure computed by the accountant) and the actual publication which again, depending on local regulations and business practices, should be disseminated to various participants of the platforms as well as to the general public : investors, regulators, transfer agent, order management platforms…

The main takeaway from this short description is that the platform should be able to accommodate different workflows and processes to eventually publish NAV. Rules to compute NAV could be defined in a smart contract between the asset manager and its supplier. Such a smart contract would need to access the fund's assets' inventory, as well as reference and market data to compute a market value. The fund custodian, when different from the fund accountant, would have to authorize such access to its client's data. The source of the data used for asset valuation would be defined in the smart contract and could result from a special commercial relationship between the contract vendor and the data provider or be specifically designated by the fund manager. The consensus protocol to validate the NAV could strictly be bilateral involving the fund manager and its supplier, or multilateral if other parties need to be included because of business or legal requirements. Eventually, the validated NAV would be disseminated to the relevant participants (fund manager, regulator, transfer agent, distribution platforms…).

Identity Management

Identifying platform participants

When roughly sizing the target platform, we have assessed a rather larger number of platform participants: in the thousands or tens of thousands, assuming a global coverage of the market. Our central scenario assumes that participants may be trusted, up to a point. At least, their corporate identity is no secret. Therefore, it is rather natural to imagine, as part of the distributed ledger, a directory services for participants. Such a database is indeed required to expose the participants' public keys. We can think of it as something very similar to the SWIFT BIC directory service. So similar, in fact, that it could actually be a distributed ledger version of the SWIFT directory service. Why reinvent the wheel?

Identifying end-investors

The real challenge begins with the identification of end-investors, and more generally, any non-member, sponsored actor of the platform, such as a data vendor for instance. There is no similar convenient standard yet, which could be readily reused. Indeed, there is still a long way to go until a global universal Digital ID scheme is eventually available. The platform should thus carry on with identity management by itself, relying on its trusted members (e.g. distributors) to collect whatever identification means they find adequate within a given jurisdiction. For instance, if the UK comes to develop early a Digital ID for Britons, such an ID could be directly put to use by the platform to seamlessly identify a Briton investor. On the other hand, investors from countries with no such ID scheme should not be barred from investing. The platform should thus support several external identification schemes.

How does it work without Digital ID?

The distributor – e.g. a bank – could simply collect and scan the required documents from their clients, then store this information on the distributed ledger with a fully private encryption status, or perhaps, for regulator's eyes only. Such identification data should obviously be supplemented with information supplied by the distributor itself. Likewise, questionnaires filled by end-investors to assess product suitability would be stored as well. This may sound reminiscent of good old back-office paperwork, but one should be reminded that the weak point of any identification scheme is where one first enters the identity: distributors would thus act as oracles to the platform – a point of contact with the real world. As a matter of fact, a full-fledged universal Digital ID scheme would only be a commoditized version of such an oracle: the weak point would simply be moved to another entity in charge of first declaring identities. Obviously, it is all the better when such utilities do exist to provide oracles. We have to contend with a less efficient version of investor identity oracles when they don't.

Such an identity store, or KYC store as we call it at *TheFundsChain*, would constitute a trove of data, which should obviously be kept away from competitors' eyes, thanks to the data privacy capabilities offered by the ledger. Such capabilities are thus of a critical importance. From now on, all what other participants would know about a particular end-investor would be an anonymous public key.

Such a setup set raises a number of interesting questions to be debated by *TheFundsChain* contributors.

- Could end-investors gain control over their personal data? For instance, it should be possible to ensure an individual that her personal details have in effect been destroyed after she has closed her investments and account at the distributor's. This point obviously comes with related regulatory concerns.
- Could other actors enrich the partial information about end-investor they are allowed to know? Would such enrichments remain private? For instance, fund managers might want to augment the information made available by distributors with they own client segmentation or more generally, additional information from their own CRM.

Compliance checks with smart contracts

Invoking smart contracts to act on behalf of a data owner paves the way toward a true data shared ownership. Indeed, it is a key feature to a platform where services are competing with each other. It also provides a convenient way to perform KYC checks without knowing the full details about an end-investor. For instance, as a part of the distribution agreement, the fund manager could use a specialized service which is granted access to the distributor's client information, but only exposes the information the fund manager needs to know. Such a certified contract would carry on the required verifications and return only the summarized information the fund manager actually needs to know, without revealing details.

A LAST WORD: A FLEXIBLE GLOBAL PLATFORM WITH LOCAL IMPLEMENTATIONS

Our business and technological analysis of distributed ledgers and of the asset management industry requirements both highlight the need for flexibility. This is an essential component for a bespoke DLT designed for the Asset Management industry. This contrasts with some quite rigid features of original blockchains, which literally "engraved" business rules in their inner workings.

This flexibility will ensure that the platform will be able to evolve and fix bugs, develop further enhancements or adopt new technologies in the future.

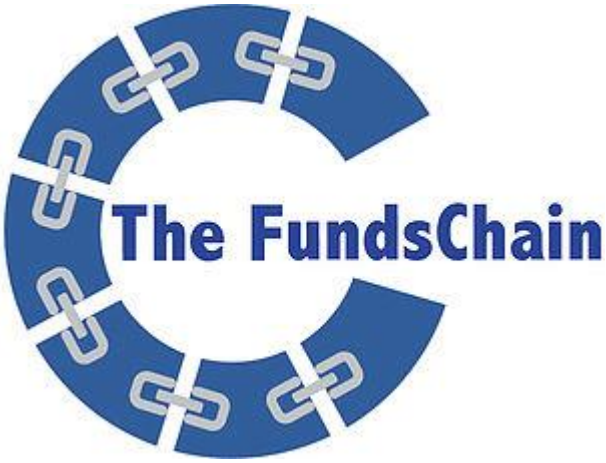
It should also favor competition by allowing participants to design and offer new services leveraging the platform and to organize business and commercial relationships among them as they see fit. Flexibility will also ensure that platform participants follow all relevant regulations or local practices.

As stated before, DLT is above all a powerful technology that should favor innovation and not raise legal issues or regulatory uncertainty. One of the key requirements for the platform to be developed will be to support cross-jurisdiction business. A fund manager based in the UK for instance should be able to manage all its funds on *TheFundsChain* platform whether they are registered in the UK, Luxemburg or Ireland.

Eventually, the platform should be able to address any basic requirement associated with fund management: proceed with subscription/redemption orders, record transactions, provide up to date inventories, compute and automate trailer fees based on existing commercial agreements and inventories, publish NAV...

The platform should also provide sufficient flexibility so that such basic functions can be assigned and delegated to different participants depending on local jurisdiction, business practices or commercial agreements. How to process NAV is an interesting example in this delegation context (see box above).

A successful local implementation would require a very granular definition of basic functions and privileges regarding data access and transactions validation roles. Such flexibility will result from **context-dependent consensus protocols**, **advanced data privacy capabilities** as well as from **truly versatile smart contracts**.



For more information, contact:

Romain Devai *romain.devai@thefundschain.com*

Frédéric Bidon *frederic.bidon@thefundschain.com*

Olivier Bramat *olivier.bramat@thefundschain.com*

Visit **www.thefundschain.com**