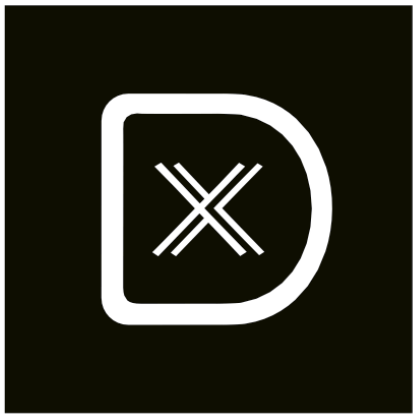


DEXTF

A decentralized traded fund

Sandro Cavallari,
PhD Candidate

Marco Cora,
CFA

Federico Cristina,
CFA

Filippo Fanin,
CFA

March 26, 2018

Version 0.88

Abstract

A purely peer-to-peer version of asset management would allow investment management services to be offered directly from one party to another without going through a financial institution. Given the volatility and the asymmetric information associated with digital-assets, investors would have strong benefit from professional portfolio management techniques. Unfortunately the current investment/fund infrastructure is not able to cater for Crypto-Investors. In this paper, we provide four necessary but not independently sufficient conditions required to support a Digital-Assets Management infrastructure and we propose DeXtf, a protocol where Investors and Portfolio Managers interact, peer-to-peer, in a secure, scalable and efficient way. Eventually, DeXtf will became the platform that allow the transition from a traditional fund of cryptos to a real *crypto-fund*.

INDEX TERMS: BLOCKCHAIN, ASSET MANAGEMENT, CRYPTO-FUND, FUND.

Contents

1 Introduction 4

2 Comparison 7

3 Market Opportunity 11

4 DeXtf Mechanics 15

4.1 Baskets Rebalancing 16

4.2 DeXtf, XTF Tokens and Consensus 19

5 Considerations 20

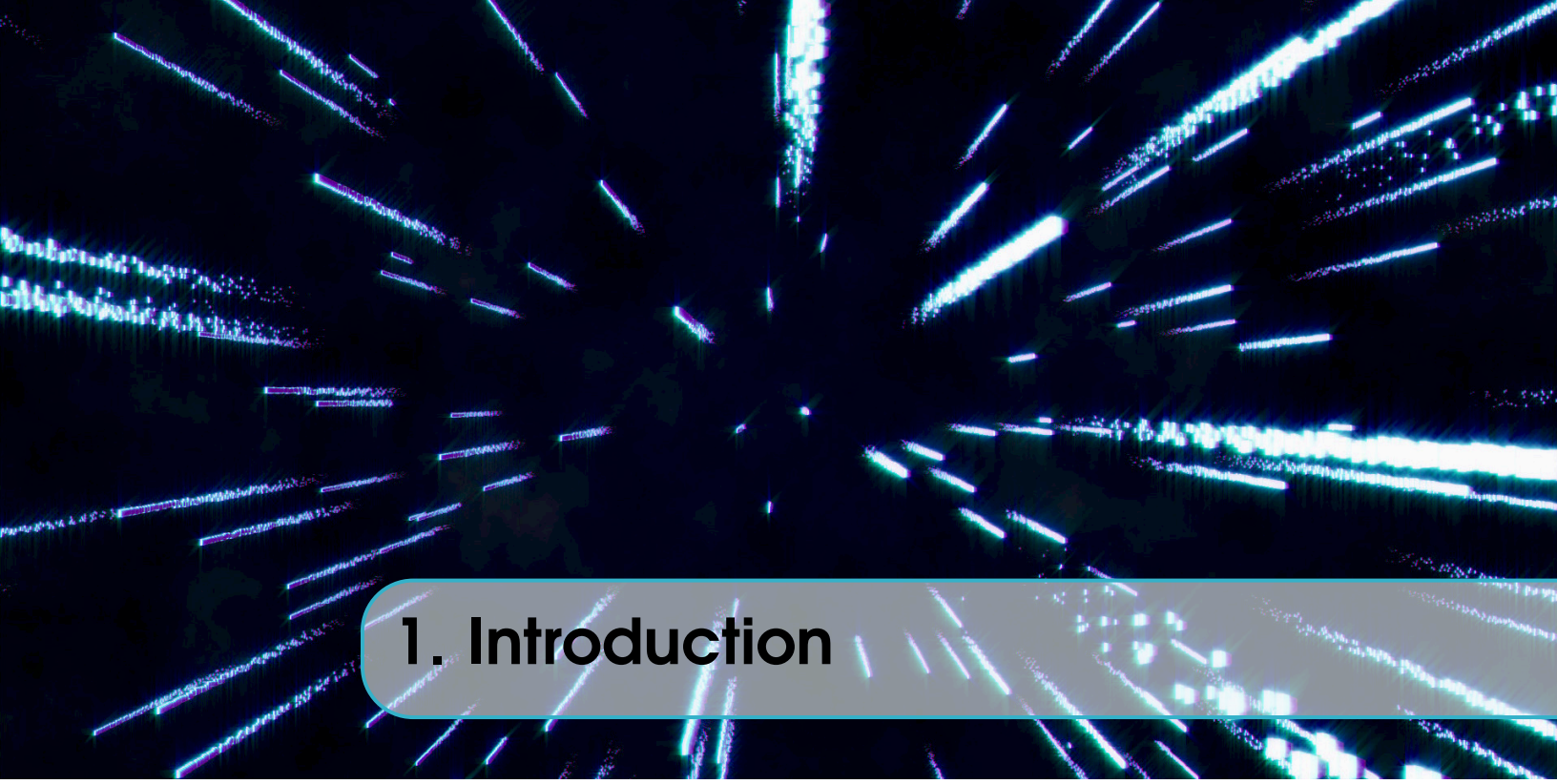
5.1 DeXtf Smart-Custody protocol 20

5.2 Mechanics Considerations 21

6 Appendix 1 - Type of Funds 24

7 Appendix 2 - Custody 27

Bibliography 30



1. Introduction

Given the recent rise of interest in Blockchain technology and crypto-currencies, there is a growing need for professional portfolio management services and well-established investment techniques. In this paper, we present **DeXtf**, a Decentralised Traded Fund protocol that uses a novel *decentralised custody structure* to directly connect investors with portfolio managers in a peer-to-peer fashion.

In this section, we will explain our reasons to work on such a project and discuss the major features required for a protocol to support the Management of Digital Assets successfully. In Sec. 2 we will compare the existing Blockchain projects in this space, in Sec. 3 we will analyse the market opportunity for DeXtf and, finally, in Sec. 4 and 5 we will propose our solution along with some considerations. Moreover, we will clarifying some concept in two appendixes Sec. 6 and Sec. 7.

We started to become interested in crypto-currencies in 2013; it started as a hobby then flourished as a significant part of our portfolios. With the proliferation of the number of investment opportunities and the increase in the size of the investment, we started to look at how to improve our portfolios and incorporate diversification, asset allocation and other basic and well-tested investment techniques. With the growth of this market, it became obvious to us that there is a need for both: professional portfolio management skills as well as a good understanding of the underlying information technology. What started as a need for our own portfolios soon enough became a more structured project: what was useful for us could have been useful for others and we realised that a professional asset management offering could have scaled to a broader range of customers.

In our previous careers, we have been involved in managing and setting up various funds and the first step in this process is always to choose an efficient and appropriate infrastructure.

We looked at the conventional fund infrastructure and at some new Blockchain projects that are trying to re-imagine the fund industry. while looking for a suitable platform we realised that there are **four necessary requirements**:

1. **Rebalancing**: we needed a structure that allows Fund Managers to re-balance portfolios without giving them full control over the underlying assets;
2. **Custodising**: the structure must be able to take direct custody of the assets and hold them on the Blockchain, on behalf of the clients without intermediaries;
3. **Pricing**: we needed to deal with the problem of pricing of both the underlying and the fund;
4. **Execution**: we wanted a platform that allows cheap *real-time* subscription, redemption and transferability.

We further believe that these requirements are **all non-sufficient**: we believe that an unified solution to all these problems is crucial for a Blockchain technology to: first, be able to disrupt the investment in digital-assets, subsequently affect the traditional Asset Management industry. Having done extensive research in Sec. 2, we believe that there is currently no integrated solution that can support our needs. These problems are all tackled in various Blockchain projects, but they are all addressed individually and independently. By looking at these projects we recognised that they all seem to be stuck in a trade-off among the requirements, solving the rebalancing problem seems to come at the cost of having a weak protection for custody, having a real-time execution seems to come at the cost of being able to price the structure correctly.

We started to look at the conventional-assets management infrastructure. This has many problems (of efficiency, transparency, duplication, etc.) that apply equally to conventional as well as crypto assets, but still, most of the current fund try to fit the conventional model to the new digital-asset class which has different needs as it has "unique operational and technological features"[1]. For example, conventional-assets are registered by centralised trusted third parties (with the exception of some outdated bearer certificates): if an incident destroys or a malicious actor modifies the custodian's database of an equity share ownership: the rightful owner can demonstrate her ownership (through past statements, proofs of payments, etc.) and have the company destroy the previous certificate and re-issue a new one. This is not possible for digital assets, if an incident destroys the keys or a malicious actor steals them, the underlying assets cannot be recovered. Effectively most of the solutions proposed so far are akin to centralised exchanges where the private keys are held by third parties and in case of failure or miss-behaviour of such third parties the most likely outcome is the loss of funds.

We believe that for digital-assets, "first-party custodianship [is] the only responsible form of safeguarding client assets"[2]. Another interesting point to note is that: it is ironic that "despite all the new technology surfacing, crypto[-asset] funds can be even more expensive to set up and run than traditional funds. This can be seen in some of the fees they are

[1] `https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3055979`

[2] `https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3055979`

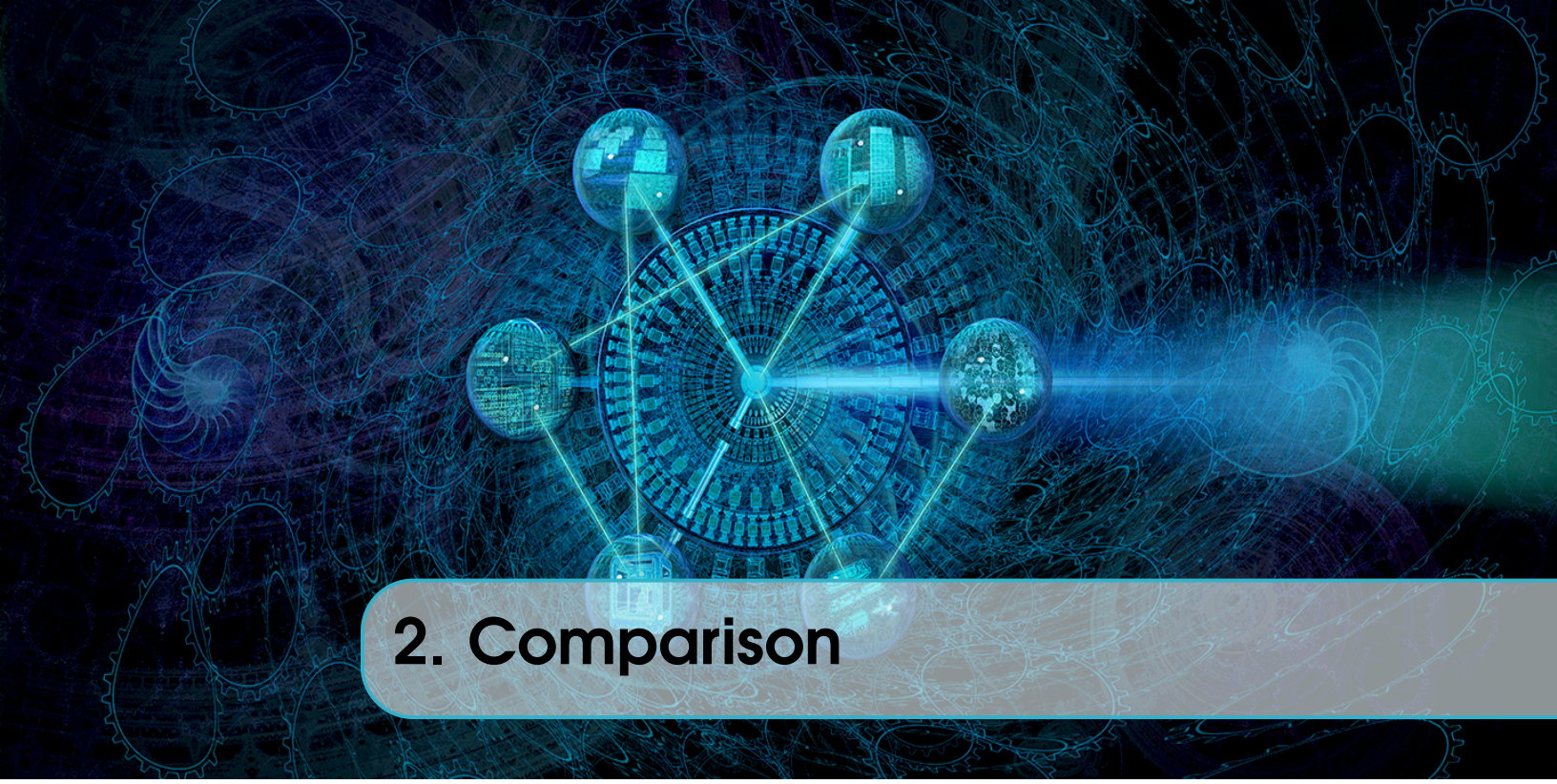
charging, where is not uncommon to see higher fee structures for crypto[-asset] funds than traditional asset funds"[3].

In practice, adapting the conventional asset-management model generate a *fund of cryptos*; whereas, in order to upgrade the asset management infrastructure to properly take care of digital-assets, we need a **crypto-fund**, rooted and ingrained in the Blockchain. We looked at the world of Blockchain and at those projects working in the fund management industry. Here, we noticed that the current ventures look at the four requirements above as independent. The underlying unspoken assumption underpinning many of these projects is that they can focus on one requirement at a time and solve the others later. We believe this will not work (the problems cannot be solved sequentially because they are not independent) and instead, we realised that a novel approach was required: one focusing on a mechanism that could solve all of them at the same time.

To this end, we decided to design our own solution: **DeXtf** combines cutting hedge ledger and transaction technology based on the Blockchain with arbitrage ideas developed in traditional fund business.With DeXtf, Investors are bridged peer-to-peer with Fund Managers, **eliminating the need for all the intermediaries** (Transfer Agents, Fund Administrators, Custodians, etc.) and service providers (Accountants, Auditor, etc.). It truly represents the democratisation of Asset Management: it will allow boutique players to market their expertise directly to investors and to set-up a new structure with limited capital and time. In so doing, it will cut most of the typical costs of the Asset Management industry and will enable Investors to take direct control over their goods, appraise managers fairly and transparently, and have their asset managed in the most efficient way.

We believe that DeXtf will open the doors to a larger pool of people's wealth to be invested in digital assets, as part of the optimal allocation of their portfolios. This, in turn, will drive demand for these assets, and drive further investment in Blockchain related application and services, thus accelerating the arrival of the economy we are envisioning.

[3] `https://www.coindesk.com/buying-bitcoin-investment-funds-will-blockchain/`



2. Comparison

In this chapter, we review some of the other solutions that have been proposed in the past years to the needs of digital asset management. Tab. 2.1 report an overview of the most similar projects. It has to be noted that Tab. 2.1 is built using information collected from the white papers and blog-post of the relative companies so it may not be a perfect representation of the project.

Before discussing each project in details we would like to summarise the issues that we found with them and why we start to work on an alternative. All but one of the others projects avoid the issues related to **custody**, they are all assuming that investors will be willing to give their private keys to them. We think that, while this may be ok for small sums, it will not be acceptable for big investors and for institutional players. These entities will simply not be willing to handle millions of dollar worth of digital-assets to third parties given the bearer nature of such assets. Another key issue is practicality: the only project that has made the issue of custody a key focus, it has proposed a contract that should be able to safely and independently interact with the real world. We believe that the technology is simply not yet advanced enough and hence some form of backdoor will always be required and this will bring back the issue of custody.

Furthermore, they all have problems with **pricing**: given that the crypto-market trades 24h, there is no commonly agreeable closing price. This means that the operator of the infrastructure will need to choose (and take responsibility for) the appropriate price for Net Asset Value (NAV). This could bring on these small companies issues of compliance, controls, and audit with the associated operational and managerial complexities. Moreover, Blockchains (at time of writing) are "isolated" from each other so they are not able to observe external information, hence in order to obtain the prices these project will have to factor in either Oracle (which will increase the fragility of the infrastructure) or they will have to rely on Auditors and Reconciliation (which bringing back the same old institutions).

Table 2.1: Comparison w.r.t competitors. Note that, • indicate the full implementation of a features, ○ indicate only a partial implementation.

	DeXtf	Melonport	Blackmoon	ICONOMI	Nousplatform
Decentralized platform	•	•	•		•
Decentralized custody	•	•		○	
Rebalancing	•	○	○	○	○
Autonomous pricing	•				
Remove asset pricing	•				
Focus on compliance	•		•	○	

Most of them take direct control of the assets so they should not have problems with the **rebalancing** in normal market condition, but may face issues in nonstandard market conditions. For example, in periods of extreme volatility where most of the funds want to pay off they could have issues with market liquidity, the priority of trades and trading costs.

Finally, most of them focus on traditional mutual fund structures. This creates a trade-off in terms of **execution**: Close-End Fund structures are able to trade in real-time 24h thus providing 24h price discovery as well as 24h liquidity to investors, but they will trade at a premium/discount thus creating issues w.r.t. properly establishing the true return on an investment. Open-End Fund, instead, price their NAV regularly and allow redemption and subscription at that official price, but this comes at the expense of liquidity that is provided to investors only after the NAV has been calculated (daily, weekly or montly). On top of that, this will make the structures opaque to investors in between NAV calculations.

We will now talk about the various projects.

ICONOMI[1] is the first mover in the space of *digital-asset management*. They provide a user-friendly interface that allows investment, creation and management of index-like structures. ICONOMI is a great instrument for an investor who can easily buy multiple digital-asset at the same time and have mutual fund functionalists through their digital asset array data-structure. On the other hand, their platform is not decentralized and seems to be based on a proprietary database. With respect to the key problems highlighted above, custody could be an issue as they provide this service directly: while they claim the assets are protected trough multi-signature, the reliability of signatories can be a concern. Rebalancing, instead, given direct control on the assets, should not be a problem even if, in non-standard market conditions, may become an issue. Pricing will be difficult as the choice of the pricing source and the calculation of NAV is left to ICONOMI who will need to make some price-sensitive choices (for example to include or not Korean exchanges which at time of writing are pricing most assets at 30-50% premium vs the rest of the world). Execution on the underlying funds will be ok, but the funds will be subject to the limitations of either the Open-End Funds (no premium-discount on price but only tradable after the NAV is calculated) or the Close-End Funds (tradable at any time but subject to significant premium/discounts).

[1] `https://www.iconomi.net/`

Shortly after ICONOMI, **Melonport**[2] started another platform for digital-asset management. Melonport aims is to provide a fully decentralized platform focusing on mutual funds which in principle will address the issue of custody. It is building a modular platform where users can program their own funds. At present it is not clear how easy would be for users to program their own modules, but the architecture-level choices will impose some constraints on the implementations of some functionalists. While their goal is to provide a smart contract able to directly interact with the exchanges to trade and manage the funds, this could be difficult to put in place given the current state of technology. We consider Melonport the most related project to DeXtf, the key differentiation is that Melonport aims at creating a contract that will interact with the real world independently under control of a Portfolio Manager and for the benefit of Investors. We don't think the technology is developed enough to allow this with complete independence of the contract from Melonport, this will imply that there will always be a backdoor required to modify the code every time there is a new feature in the real world (new regulations, new exchanges, new practices, new forks, new type of orders, new tokens with different features, etc.). This backdoor, even if it's there for a good purpose, will always be there also for malicious users. Our framework instead, as discussed later on, assumes a much simpler contract that enforces only very few type of instructions in a very predictable sub-set of the real world while leaving most of the complexity of interacting with exchanges, regulators and new tokens to arbitrageurs. We don't have many details on how the project aims at solving the four key problems we highlighted in the previous section but in principle, it seems that they don't want to rely on third-party custody which would solve this issue. If they manage to write a smart contract that can interact with exchanges directly, then they will also solve the rebalancing problem. Since they are going to create either a Close-End or Open-End fund they will have the same issues as ICONOMI with respect to pricing and execution.

Blackmoon[3] is a platform which aspires to provide access to both digital-assets as well as fiat-assets. Blackmoon is particularly interesting for their focus on compliance (which we agree will be a key feature in the near future) and aims to provide a trustworthy way to tokenize real-world assets on Blockchain and manage them as a traditional fund. This approach is interesting because it provides more transparency to the Investors, who will be enabled to know in real-time the fund's composition and because it will provide a standard tokenization process to the Fund Managers. This focus makes them unique (and hence very interesting) but highlights the requirement for strong legal expertise to bridge the Blockchain world with the real one. We don't consider Blackmoon as a competing project but more of a complementary project: the more real-world assets will be tokenized (and the more this process happens in a compliant and legally correct way), the bigger our target market becomes. As ICONOMI they will have to give a clear indication to investors on the safety of their custody solution and as long as they choose the framework of Close-End or Open-End funds they will have the same issues as the two projects above with respect to pricing and execution. Since they seem to have direct custody, they should not have issues

[2] `https://melonport.com/`

[3] `https://blackmooncrypto.com/`

with rebalancing if not in nonstandard market conditions.

Recently lunched, **Nousplatform**[4] set the goal of providing a digital-asset management platform for any type of fund, from Venture Capital funds to Open/Close-ended fund. Nousplatform aims to provide a complete toolkit to create and manage a fund based on smart contract. They suggest that the entire platform is built using a blockchain rather than a database and aim at supporting both conventional-assets as well as digital-assets. From the paper, it seems that they still assume to take over direct custody of the assets (with all the above-mentioned issues pertaining to digital-assets). Furthermore, while they mention that they are working on an ETF implementation they gave no indication as for the mechanism of rebalancing that they have in mind. Finally, they also gave no indication yet on the mechanism of Pricing and computation of NAV.

There are few other projects which are in the space of managed investments in digital-assets but they all seem to sell tokens to either raise money for their funds or share fees for their asset management companies. In this group, we looked at **CryptF, NaPoleonX, Crypto20, Mirocana**. Some of these projects seem very worthy of attention and potential investments and we consider them complementary to our as they will all be able to benefit from a full asset management implementation on the blockchain.

[4] `https://nousplatform.com/ico`

3. Market Opportunity

Table 3.1: Notations used.

Symbol	Definition	Symbol	Definition
NAV	Net Asset Value	DAM	Digital Asset Management
ETF	Exchange Traded Fund	FM	Fund Manager
AR	Arbitrageur	IN	Investor
CL	Clearer	TR	Trustee
RB	Rebalancing Basket	EB	Effective Basket
P_{XTF}	XTF Unit Market Price	P_{EB}	Effective Basket Market Price
P_{RB}	Rebalancing Basket's Market Price	NA	No-Arbitrage Zone
AM	Arbitrage Mechanism	TA	Transfer Agent
PoC	Proof of Collateral	DPoS	Distributed Proof of Stake

The short-term market opportunity is to offer an infrastructure to provide professional digital-asset management services to investors in cryptos. At the time of writing, there is a total capitalization of roughly USD 600bn. Most of these are held by first mover crypto-investors who want full control on their portfolios and assets and who enjoy the process of managing, buying and dealing with Blockchains. We can safely assume that there is a growing group of people that want exposure to this asset class in their personal portfolios, but they are stopped by the complexity. If we assume that there is an initial 10% interested in a solution that allows them to invest in multiple digital-assets, without having to have many wallets or many accounts on different exchanges, with a single KYC/AML process, without having to understand the details and peculiarity of each single assets we have a potential market of roughly $USD\ 60bn$. This is a safe assumption given the exponential increase in interest for the asset class. Anyone who recently tried to open an account with

an exchange can testify to the difficulty and time required. Also, it is well known that the reason for this is the huge interest from new investors who are trying to get access to the crypto-asset class. In the near future, this interest will be increased by family offices and institutional investors who will want exposure to this new asset class without giving control over their private keys to third-party advisors. If we assume a base fee of 1% this leads to an initial market opportunity of USD 600m per year.

The long terms market opportunity is to dis-intermediate the current conventional asset management infrastructure which evolved over time in a huge, heavily regulated and highly complex ecosystem. Its processes are lengthy, costly and it needs numerous and specialised intermediaries as well as trusted counterparts. All of which add expenses and inefficiencies to Investors (IN) and Portfolio Managers (PM). The traditional model has multiple intermediaries between IN and PM. When an Investors sends an instruction to subscribe or redeem a fund, it typically employs a **Transfer Agent**[1] (TA) whose role is to record transactions, issue or cancel certificates, process investors' mailings and deal with other investors' problems. A fund investment, furthermore, requires a **Fund Administrator**[2] who is responsible for calculating the NAV, prepare reports for investors, pay the fund's expenses, settling daily purchases and sales of securities, calculating dividends, preparing and filing reports and calculating performance measures. Finally, the IN needs to enlist the help of a **Custodian**[3] to hold his assets for safekeeping. On top of these intermediaries the structure requires **Accountants**[4] to calculate the formal accounts for the fund, **Auditors**[5] to confirm that the calculations and the processes are performed correctly and **Reconciliation Service Providers** as all the entities above will keep individual and independent copies of all information which will differ from each other.

As shown in Fig. 3.1, a Deloitte's paper [1] on the Luxembourg fund industry (2nd largest in the world for total AUM but largest for cross-border volume), estimates total yearly waste at around EUR 1.2bn. They also estimate that roughly a quarter of all orders are processed manually (by over 14,000 employees in the grand-duchy) and through fax with all the obvious impacts on confidentiality, security, speed, and efficiency. The US fund industry is similar in size and the rest of the world industry is around half this size. This is currently yielding a total of over EUR 3bn annually in unnecessary costs. This scenario is the direct cost imposed on the system, and hence mostly passed on Investors and residually on Portfolio Managers, but does not include the fees charged by the various intermediaries.

We estimate the below:

1. **Waste** = USD 3bn per year;
2. **Transfer Agents + Fund Administrators**: According to [2], $10-30$bps over a 15tr USD industry = USD $8-24$bn per year;

[1] `https://www.investopedia.com/terms/t/transferagent.asp`
[2] `https://en.wikipedia.org/wiki/Fund_administration`
[3] `https://www.investopedia.com/terms/c/custodian.asp`
[4] `https://www.investopedia.com/terms/a/accountant.asp`
[5] `https://www.investopedia.com/terms/a/auditor.asp`

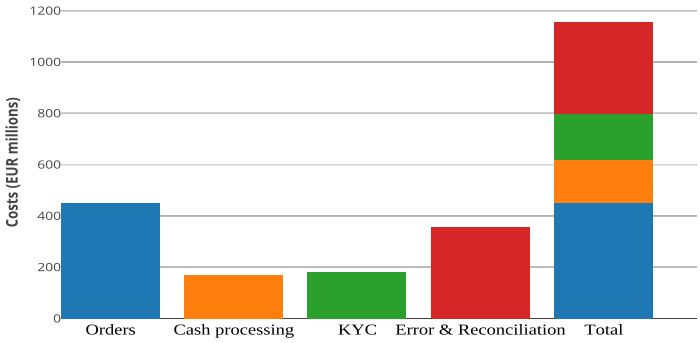


Figure 3.1: Costs of fund distribution in Luxembourg

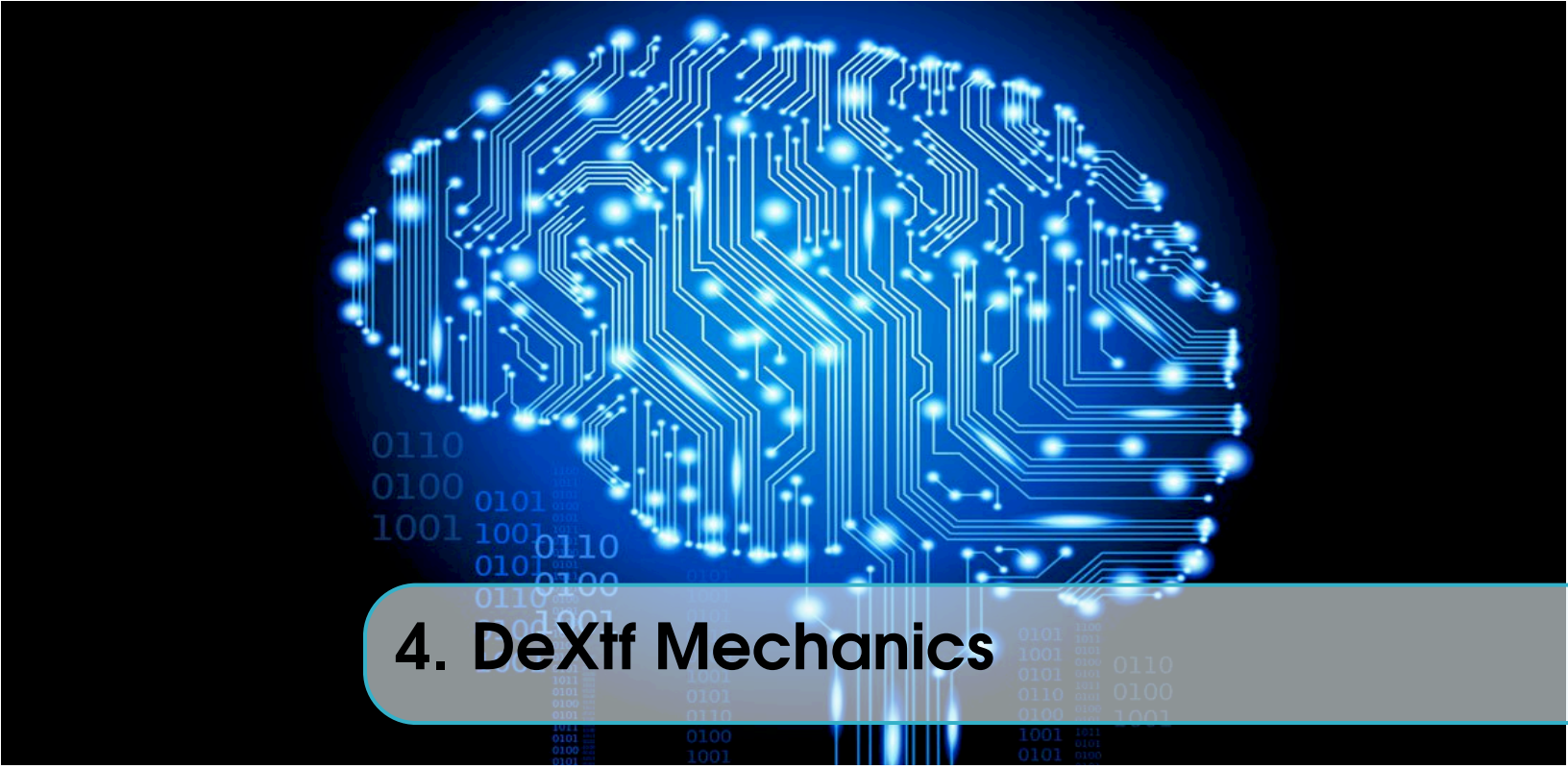
3. **Custodians**: $5-10$ bps = USD $4-8$bn;
4. **Audit**: USD $15,000-30,000$ per fund over $25,000-30,000$ funds = USD 400m$-$1bn[6];
5. **Reporting Services**: USD $500-10,000$ per report, 1 report per client per jurisdiction;
6. **Reconciliation**: It is difficult to estimate the reconciliation cost since each country has different legislation. For this reason we left out those cost form our estimation;

This leads to a conservative estimate of USD 15bn to 35bn annually which excludes all the indirect economic impact: today the minimum size required to participate in the industry is very large, this leads to oligopolies which are well known to lead to sub-optimal resources allocation but also thwarts entrepreneurship, new ideas, and innovation. By combining smart-contracts and recording of transactions in its ledger; the Blockchain is able to replace any kind of intermediary whose role is simply to maintain a registry, ensures trust or execute transactions between parties. The services provided by the financial intermediaries discussed above can be substituted easily by a Blockchain solution. Transfer Agent and Registry services are the easiest to eliminate by moving to the Blockchain. Fund Administrators' roles can also be implemented on the Blockchain using smart-contract solutions. Custody services are the cornerstone of the intermediary business because it's the service that requires the most level of trust. The Blockchain, with its tamper-resistant ledger and strict enforcement of rule-based smart-contract, can ensure a higher level of trust compared to a traditional Bank. Accounting, Reconciliation, and Audit service are only required if there are multiple silos and no golden copy. In a complex structure, these services are important to guarantee that the assets are properly accounted for, that there are no missing assets and the various silos are aligned. By moving the custody on the Blockchain these roles will be redundant as accounting becomes a simple observation problem and the single golden copy ensures consistency among information. Finally, Reporting and Monitoring will also be eased as a permission Blockchain can easily be probed by regulators and investors, instead of reported by intermediaries. In practice with a full implementation of a Fund Infrastructure on the Blockchain, Fund Managers and Investors will be able to interact with each other directly in

[6] `https://www.statista.com/topics/1441/mutual-funds/`

a peer-to-peer manner.

With DeXtf we codify fund transactions and agreements in a shared protocol which guarantees execution based on conditions that can be mutually and independently assessed by the parties. Fund Managers will be able to directly distribute their expertise without costly and inefficient intermediaries. Investors will be able to subscribe and redeem directly and instantaneously, to identify themselves for regulatory purposes and to prove directly to third parties ownership of assets and level of wealth. We believe most if not all of the assets will be tokenised in the near future, many Blockchain projects, as well as standard banking projects, are working in this direction. Once stocks, bonds, real estate, ships, infrastructure etc. will be tokenised they will all get the positive features of the distributed ledgers (speed, immutability, control, etc.) but will all be subject to the constraints that digital-assets have with respect to the traditional asset management framework and will all require a solution that encompasses the four problems highlighted in the introduction section.



4. DeXtf Mechanics

In order to build a successful Digital Asset Management protocol, it is fundamental to provide a **safe, real-time, easy-to-use subscription, redemption and exchange** functionality, while ensuring a **trustworthy custody**. Our approach to solving the problems highlighted in Sec. 1 relies on a similar mechanism that underpins ETFs. We model our protocol in such a way that our fund's tokens would be directly linked to the underlying, thus eliminating the need for third-party custody and the risks associated with it. We named our custody policy as **DeXtf Smart-Custody**. To the one hand, thanks to our smart-custody, the Investors is able to keep control of the owned assets. To the other hand, due to links between the investors' assets and the fund's tokens, it is possible to efficiently manage a portfolio by an *arbitrage mechanism* (AM) which will be specifically regulated by smart-contracts.

While ensuring transparency and security, in our consideration, the smart-contract eco-system impose some limitations. Until the digital-asset and the artificial intelligence ecosystems are mature enough, it would be unreasonable to think of a *"sophisticated"* smart-contract able to safely interact with the real world independently. Moreover, this would assume the presence of well defined and static digital-assets infrastructure already compliant with national and international regulations. The sophisticated smart-contract should be able to input and manage various type of orders, satisfy compliance requirements, calculate its NAV and know asset prices. We believe that, at present state of technology, no system is going to be able to safely perform all the above tasks. Such a system will always have some back-door access for the developer to constantly update it and this will be a significant risk for the assets. Our solution is to push the complexity outside of the contract and to use a *"compressed"* smart-contract which only enforces strictly, predictably and transparently an AM. As it can be proven by the successes of the traditional ETF market, the AM addresses the *pricing*'s requirement very well. The systems only need to assume that prices will move asynchronously and the existence of Arbitrageurs, who

will interact with the external world and deal with all the above-mentioned complexity on behalf of the fund's contracts. As we will discuss in Sec. 4.1, the arbitrage mechanism can also solve the *rebalancing* requirements. In order to provide the DeXtf smart-custody, we needed a protocol able to lock funds on multiple different chains; while at the same time we needed a system that could enforce micro-transaction across multiple counterparts in order to facilitate rebalancing. As explained in Sec. 4.2 and 5.1, those micro-transaction are enabled by a **layer 2 scaling protocol** implementation through *Hashed Timelock Contracts* (HTLC). This new layer allows Investors and Arbitrageurs to bond digital assets to a selected XTF fund, while the Portfolio Manager can optimise the portfolio performances issuing rebalancing orders in a secure and transparent way.

Our infrastructure assumes the following elements:

1. **DeXtf Token**: the main tokens in the chain, they are required to use the system (i.e. create a new fund, issue rebalancing orders, initiate an AM and subscribe/redeem, etc.);
2. **XTF Token**: the funds' token. Each fund will be represented by a relative XTF token, created by the fund managers. These are fully tokenized assets, their private keys will be owned by the investors and will allow the investors to transfer the tokens;
3. **Fund Managers** (FM): The fund managers, also known as Portfolio Managers, own a special private key of the fund's contract (XTF smart-contract) that gives them the right to issue rebalancing instruction to the contract. This will change the composition of the underlying basket that the contract will accept for the AM (see below);
4. **Investors** (IN): A normal user that intend to invest in one or more XTF funds;
5. **Arbitrageurs** (AR): The arbitrageurs are normal users, they can be FM, IN or neither of the above. AR will spend DeXtf tokens to start an AM which allows them to create and destroy units of an XTF fund by contributing or receiving their content in kind (see Sec. 4.1);
6. **Trustee** (TR): The Trustees are delegated witnesses who have to sign DeXtf transactions, guard against double-spend attacks, keep track of the XTF balances and create Blocks; As under-explained, they will be elected trough a Distributed Proof of Stack process to create and sign a new block of transactions;
7. **Rebalancing Basket** (RB): this is chosen by the FM. When a re-balancing instruction is issued, the XTF will change the basket that it accepts for an AM to take place (see below);
8. **Effective Basket** (EB): is the effective basket custodised by the XTF. It is determined by the actions of the AR and will tend, over time, to RB.

4.1 Baskets Rebalancing

In this section, we are going to describe how, through the usage of arbitrage mechanism, it is possible to rebalance an XTF fund. Firstly, we prove how we provide a safe and real-time redemption, subsequently, we show how the XTF tokens creation process is used to align the Effective and Rebalancing basket.

Destruction Arbitrage Mechanism

Let's denote the XTF market price as P_{XTF}, the Effective Basket price as P_{EB} and the Rebalancing Basket price as P_{RB}. If $P_{XTF} < P_{EB}$; an Arbitrageur is encouraged to redeem XTF tokens and sell the obtained assets to generate profit. Fig. 4.1 shows a typical XTF token destruction scheme where: at step number ① the AR can buy the XTF-token on the market. Subsequently, given the price advantage, he will push the acquired tokens to the DeXtf smart-contract (step ②) calling the redemption function. At step ③, during the redemption process, the smart-contract will destroy the XTF-tokens and release an equivalent amount of underlying assets. Lastly, it is up to the AR to sell the obtained assets to the market to generate its own profit (step ④).

This procedure will have three **desirable effects**:

1. by purchasing the XTF on the open market the P_{XTF} will increase;
2. by selling the obtained underlying assets on the open market the P_{EB} will decrease;
3. the entire process does not change the relative composition of the Liabilities nor of the EB.

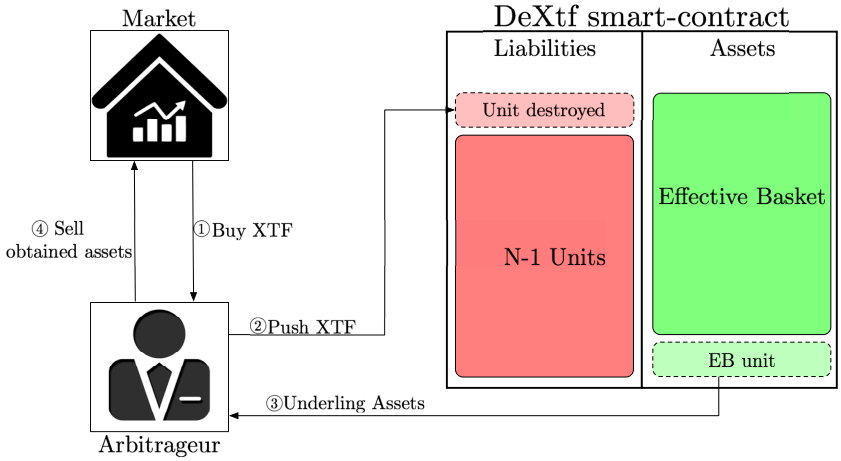


Figure 4.1: Example of destruction arbitrage process.

In Ex. 1, we demonstrate the functionality of a destruction AM. Please note that once the AM finishes, the relative composition of the Effective basket is **not changed** ($EB_1 = EB_2$).

Example 1: Destruction AM. Note that $\#_1$ indicate the status of an entity at time t_1 while $\#_2$ indicate the status at time t_2.

$\text{Liability}_1 = 100$ XTF
$\text{Assets}_1 = 10\ \text{Coin}_a + 20\ \text{Coin}_b$
$\text{EB}_1 = \frac{\text{Assets}_1}{100} = 0.1\ \text{Coin}_a + 0.2\ \text{Coin}_b$
An AR sees an opportunity and initiate a destruction AM; suppose he sends back 10 XTF Units to the contract which release 10 EB units = 1 Coin_a + 2 Coin_b
At time t_2, once the AR is terminate, we have the current situation:
$\text{Liability}_2 = 90$ XTF
$\text{Assets}_2 = 9\ \text{Coin}_\text{a} + 18\ \text{Coin}_\text{b}$
Thus $\text{EB}_2 = \frac{\text{Assets}_2}{90} = 0.1\ \text{Coin}_a + 0.2\ \text{Coin}_b$

Creation Arbitrage Mechanism

As illustrated in Fig. 4.2, when $P_{XTF} > P_{RB}$, an Arbitrageur can buy the equivalent of the RB on the market, push it to the DeXtf smart-contract, which will create a new XTF Units and issue it to the Arbitrageur.

Similar to the destruction AM, also this functionality will have three **desirable effects**:

1. by purchasing the RB on the open market the P_{RB} will increase;
2. by selling the XTF on the open market the P_{XTF} will decrease;
3. the Effective Basket will be altered and will start to converge towards the RB.

Moreover, the creation AM generate a new Unit of the XTF and add it to its Liabilities, meanwhile, it also receives an RB and adds it to its Assets. This **process changes the composition of the EB** which will start to re-balance towards the RB. This process produces the desired effects, while re-balancing the EB in a transparent way w.r.t. the smart-contract. For a better clarification, please analyse Ex. 2.

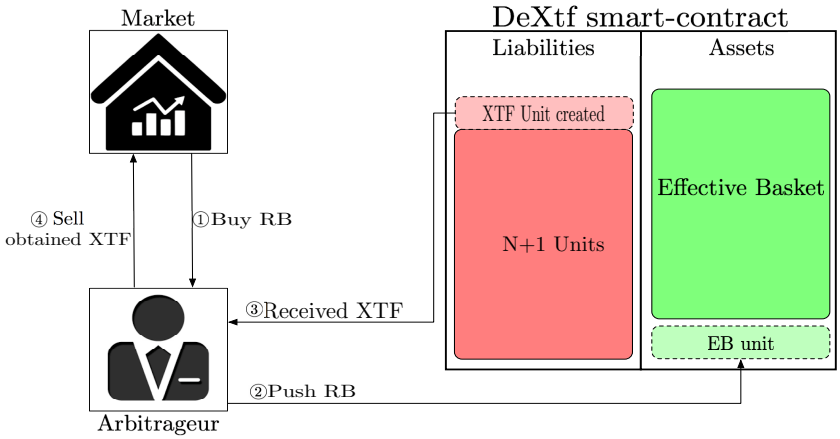


Figure 4.2: Example of creation arbitrage process.

Example 2: Creation AM.

$\text{Liability}_1 = 100$ XTF
$\text{Assets}_1 = 10\ \text{Coin}_a + 20\ \text{Coin}_b$
$\text{EB}_1 = \frac{\text{Assets}_1}{100} = 0.1\ \text{Coin}_a + 0.2\ \text{Coin}_b = \text{RB}_1$
Suppose that at time t_2, the FM issues an re-balancing instruction with
$\text{RB}_2 = 0.122\ \text{Coin}_a + 0.145\ \text{Coin}_b$
Driven by it own interest an AR execute a creation AM:

Buys $10\text{RB}_2 = 1.22\ \text{Coin}_a + 1.45\ \text{Coin}_b$ on the market

Pushes the 10RB_2 to the smart-contract, which issues back 10 XTF Units.

As we can see, differently from the destruction mechanism this process will alter the smart-contract baskets:

$\text{Liability}_2 = 110$ XTF

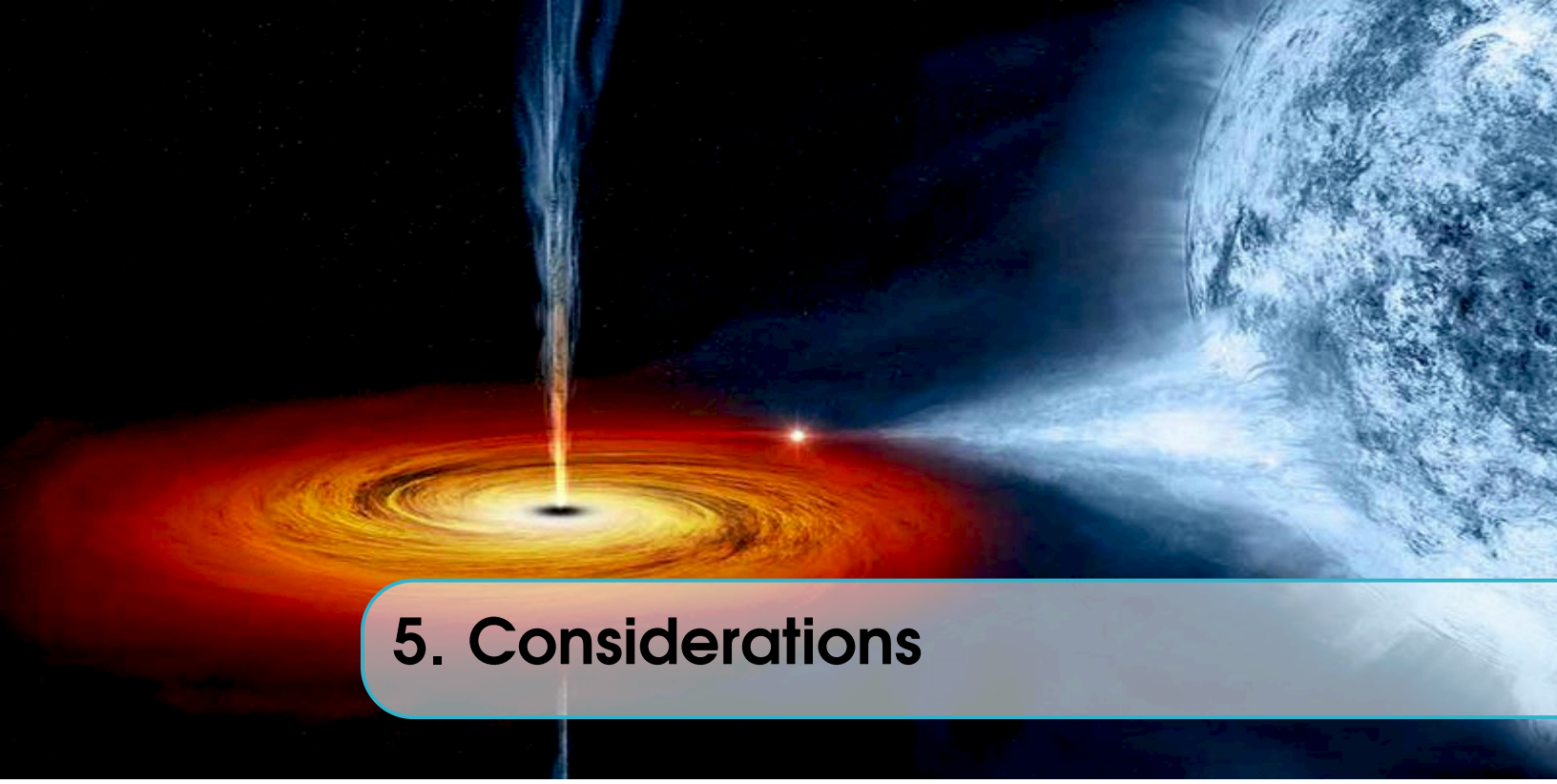
$\text{Assets}_2 = 11.22\ \text{Coin}_a + 21.45\ \text{Coin}_b$

Thus $\text{EB}_2 = \frac{\text{Assets}_2}{110} = 0.102\ \text{Coin}_a + 0.195\ \text{Coin}_b$

4.2 DeXtf, XTF Tokens and Consensus

Digest:

89E0FFD1AB8AB70223F76C8928ECC10E
21E26A68D5FB162DDCA13F81356419FE



5. Considerations

5.1 DeXtf Smart-Custody protocol

Digest:

A90D2C84EC36B7D9486B3F0F443F98C5
61404A919C04F722ABB5A7729D2C3CAB

5.2 Mechanics Considerations

Non technical Investors and Subscription/Redemption

Subscription and Redemption in DeXtf are just two special use-cases of Creation and Destruction AM: in order to subscribe to an XTF Fund an Investor just needs to assemble an RB and bond it to the protocol which in turn will create and assign new XTF Units. Similarly, an investor who wants to Redeem her Units in an XTF can simply push the XTF Token to the protocol and receive proceeds in kind (alternatively can divest in a simpler way by selling the XTF to another Investor).

This process may seem difficult for the average non-technical Investor who may want to have a simpler experience. To cater for these investors, the protocol allows for the Arbitrageurs (or for the PM) to act as Transfer Agents[1] in exchange for a small (market-set) fee. The Arbitrageurs would be able to receive an amount in various currencies (crypto or fiat if they have the right licence) and DeXtf will enable them to assemble the correct basket for the Investor, bond it to the network, transfer the bond to the Investor who will finally receive an XTF unit. Similarly, the AR will be able to receive XTF tokens from any Investor, destroy the tokens, receive the redemption in kind and pay the investor back in currency (crypto or possibly fiat). DeXtf will allow Arbitrageurs to bond a certain amount of capital (PoC_{AR}) to be used as a guarantee for the role of Transfer Agent and Investors will be able to access this information through the Proof of Collateral and decide what amount they require for comfort.

In a second stage, the development of platform as KyberNetwork[2] would solve this problem in a secure and programmable way. Thanks to dedicated interfaces it would be possible to assemble or disassemble an XTF unit automatically ex through Kyber decentralised exchange.

External Information and DeXtf

The **XTF-Contracts do not need to be aware of the rest of the world** in order to function. They do not need to know their own prices nor the prices of their underlying. This eliminates the need for Oracles and Relayers with the associated complications and risks.

Arbitrage Incentives

Like for traditional ETFs, we assume that Arbitrageurs will exist and that they will follow their own best interest and arbitrage the price differences between the RB and the XTF away. We are aware that the attractiveness of an AM is inversely proportional to the time that the AM transaction takes (the longer the time the more the Arbitrage is a statistical AM and the risk must be factored in). We will monitor the evolution of atomic swaps carefully as

[1] `https://www.investopedia.com/terms/t/transferagent.asp`
[2] `https://kyber.network/`

these will make the AR a true risk-less arbitrage but at the beginning, we are implementing a short block time to minimize the risk in the AM. Given current volatility in alt-coins (in excess of 100%) a 1h time for a transaction (6 confirmations for bitcoin, for instance) will create a price dispersion of $\frac{100\%}{\sqrt{(365*24)}} = 1.07\%$. Given the altcoins will be not perfectly correlated with the XTF the move in the XTF will partially offset this.

No-Arbitrage Zone (NA)

There is an NA if $P_{EB} < P_{XTF} < P_{RB}$. We believe this should not create significant issues as the composition of RB and hence the ordering of P_{RB} is under the control of the FM who can change the RB in order to trigger arbitrages if necessary. The FM can also control the width of the NA. All financial instruments are subject to no-trade zones and all ETFs are subject to no-arbitrage zone. This is due to bid-offer spreads and the conventional market long history shows that is able to cope with this kind of situations well.

Continuous destruction of until full redemption

In a scenario where an exogenous shock decreases P_{XTF} significantly (i.e. a flash crash), all Arbitrageurs will start destroying units. Can this lead to a full redemption and closure of the XTF? In order to destroy units, AR must first buy XTF on the market which should raise its price. The only case where the XTF can be fully redeemed is the theoretical case where someone is manipulating the price of XTF and keep it artificially low but this could only be done by a large Investor who would be better served by simply redeeming its units rather than depressing the price. Furthermore, this investor will lose money by constantly fighting the market to keep the price low.

Double Spending attacks

DeXtf runs on Ethereum and is protected by its nodes and DLT.

KYC/AML, compliance and regulatory extensions

DeXtf will fully support:

- KYC / AML
- Account freezing
- Account seizing
- Proof of wealth
- Account hypothecation

Alting Arbitrage

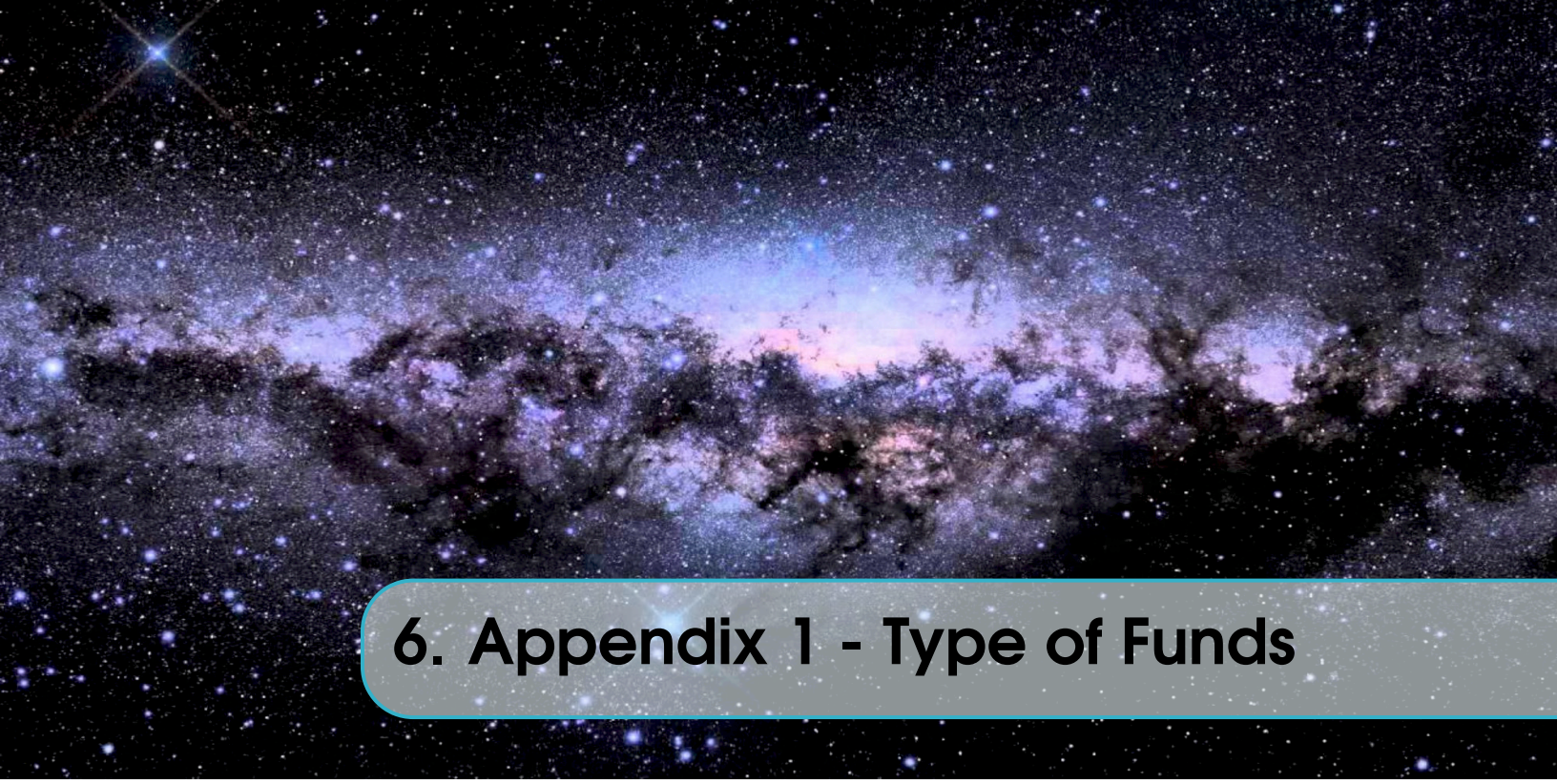
We are going to implement a mechanism to temporarily Alt the XTF creation/destruction process to stop manipulations that can lead to malicious behaviours.

Proof of Collateral and support for Hypothecation, Proof of Wealth

The Proof of Collateral implemented in DeXtf protocol can be used to prove ownership over a certain amount of Wealth. We are working on extensions of the Smart-Custody protocol that will allow:

- any user to prove to other users a certain level of wealth. The Enquirer will be able to issue a request for a proof of wealth of at least X and the users will be able to allow the enquirer to receive such proof (without disclosing the details of the content of the portfolio nor the total value of the wealth if above the threshold)
- any user to add a Lien[3] on her assets. This enables many different uses (i.e. Hypothecation and Rehypothecation). The protocol will be able to provide an unencumbered level of wealth as well as an encumbered level of wealth

[3] `https://www.investopedia.com/terms/l/lien.asp`



6. Appendix 1 - Type of Funds

Close End Fund

This is the original design of mutual funds. A Close End Fund is a collective investment scheme based on issuing a fixed number of shares which are not redeemable from the fund. Similarly, managers don't create new shares when an investor wants to participate.

The shares of the fund are instead purchased and sold on the open market. The price of the units is then determined by market forces and usually differs (often significantly) from the Net Asset Value of the underlying.

A premium might be caused by the market's confidence in the investment managers' ability or the underlying securities to produce above-market returns. A discount might reflect the charges to be deducted from the fund in future by the managers, uncertainty from high amounts of leverage, concerns related to liquidity or lack of investor confidence in the underlying securities.

Although they predate Open End Funds, they offer some advantages:

- offer real-time intra-day liquidity as they can be bought and sold at any time during the day without having to wait for the calculation of the NAV and the settlement of the money transfer
- do not have to deal with the expense of creating and redeeming shares, they tend to keep less cash in their portfolio, and they need not worry about market fluctuations to maintain their "performance record"

- in case of market panic, needing to raise money for redemptions, the manager of an Open-End Fund may be forced to sell stocks he would rather keep, and keep stocks he would rather sell, because of liquidity concerns

The costs associated with these advantages is the premium/discount to NAV which creates convoluted incentives for investors as the investment's return don't directly reflect the performance of the Fund.

Open End Fund

Open End Funds are collective investment schemes that can issue and redeem shares at any time. An investor will generally purchase shares in the fund directly from the fund itself in exchange for a monetary subscription. The manager will create new units and issue these units to the investor. On the other side when an investor wants to realize her investment they will ask a redemption to the manager who will calculate the NAV, liquidate a portfolio of the fund and pay back the inventor.

The principal advantage of Open-End Fund is that the price at which shares in an open-ended fund are issued or can be redeemed will vary in proportion to the net asset value of the fund and so directly reflects its performance.

The cost is that they don't have liquidity in between NAV calculation and may be more expensive (both directly and indirectly, see above) for investors than Close End Funds.

Exchange Traded Fund - ETF

An Exchange Traded Fund (ETF) is an investment fund traded on stock exchanges. An ETF holds assets and operates with an arbitrage mechanism designed to keep its price close to its Net Asset Value (NAV).

ETFs have both properties of Open and Close End Funds: as an Open-End Fund, ETF distributors can buy newly issued shares but they do it only directly from or to Authorized Participants (AP) in creation units, which are large blocks of ETF shares, exchanged in-kind with baskets of the underlying securities. AP may wish to invest in the ETF shares for the long-term, but they usually act as market makers on the open market, using their ability to exchange creation units with their underlying securities to provide liquidity of the ETF shares and help ensure that their intra-day market price approximates the net asset value of the underlying assets. Other investors, such as individuals using a retail broker, trade ETF shares on this secondary market, just like a Close-End Fund.

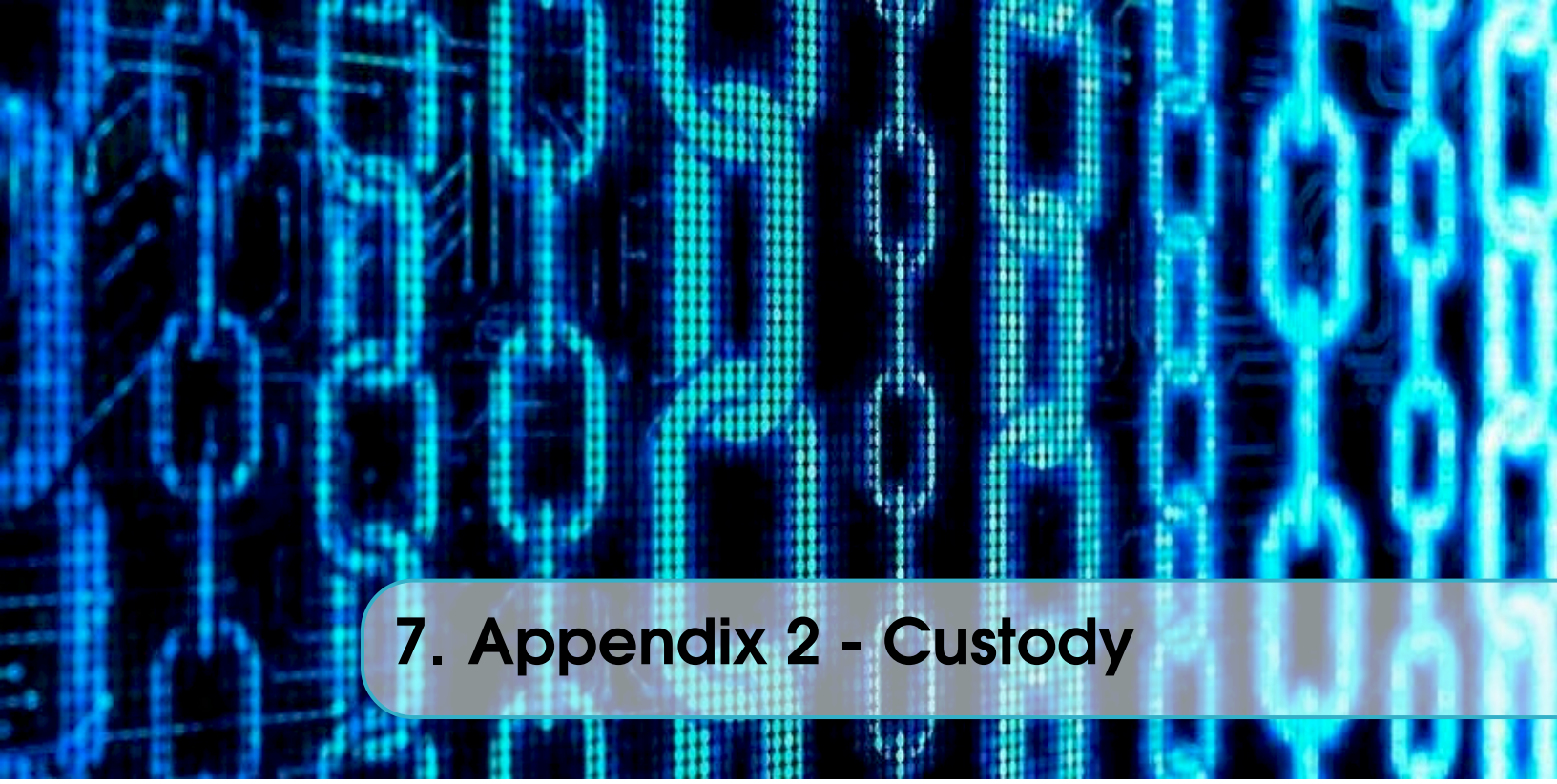
An ETF combines 2 features:

- like Open End Fund, ETF prices are close to the price of the underlying
- like Close End Fund, they can be freely traded intra-day like a Closed-End Fund

Today ETFs are one of the most popular investment vehicles on the market. The ability to create and destroy units gives ETFs an arbitrage mechanism intended to minimize the potential deviation between the market price and the net asset value of ETF shares. If there is strong investor demand for an ETF, its share price will temporarily rise above its NAV per share, giving arbitrageurs an incentive to:

1. buy the ETF's underlying shares basket in the open market;
2. deliver them to the ETF manager in exchange for ETF shares;
3. sell ETF shares in the open market.

The additional supply of ETF shares reduces the market price per share, generally eliminating the premium over the NAV. A similar process applies when there is weak demand for an ETF: its shares trade at a discount from NAV.



7. Appendix 2 - Custody

Conventional Custody

Custody is, in essence, a service consisting in holding (and normally administering) securities on behalf of third parties. It has its roots in physical safekeeping, in the days when securities existed only in paper form, investors needed a safe place to keep these certificates of value. That safe place could either be their own premises (which however then needed to be adequately protected) or those of a safekeeping service provider (banks with their vaults were a natural choice at that time). Nowadays, custody is offered by a variety of institutions, primarily by brokers, commercial banks, and investment banks. Today the US is the largest custody market in the world and according to US regulation, a person who owns securities and who is not a member of an exchange holds the securities through a registration chain which involves one or more custodians. This is due to the current impracticality of registering traded securities in the name of each individual holder; instead, the custodian or custodians are registered as the holders and hold the securities in a fiduciary arrangement for the ultimate security holders.

The roles of custodians (which may or may not be enforced by securities regulation) are to:

1. facilitate the exercise of share ownership rights;
2. act as information intermediary communicating between issuers and securities holders;
3. be the repository of the assets.

With high trading volumes, the movement of massive amounts of physical securities could cause delays and errors that would result in more delays. Severely delayed settlement of securities transactions could give rise to liquidity problems in the financial markets. Physical certificates could also increase the probability of fraud and forgeries. Therefore, at

the urging of national authorities and central banks, some markets set up central securities depositories (CSDs) many decades ago, to immobilize the securities certificates for the whole market, so that physical movements would be eliminated.

Advances in technology enabled other markets to dematerialize, whereby securities would only exist in electronic form. Whether by immobilization or dematerialization, securities are transferred from one holder to another in CSDs by "book-entry settlement" between securities account holders, which are commonly called members or participants. These institutions operate as central providers for the entire market and are expected to treat all users equitably. Some markets set up CSDs only after having suffered through "paper crises", or after adopting best practice recommendations by important international organizations. The immobilization or dematerialization of physical securities in CSDs should, in theory, eliminate the need for any investor to use custodians or brokers to safe-keep physical securities. Under immobilization or dematerialization, safekeeping is reduced to a reconciliation activity, whereby the custodian's task is to ensure that its holdings at the CSD are equivalent at all times to the number of securities owned by its customers. Yet investors continue to use custodians, for several reasons:

1. Ineligibility: most investors and market participants are not eligible to become a member of the CSD. Some CSDs only want members that are regulated, financially sound, have robust operational capabilities and have the ability to continuously invest in technology that ensures straight-through processing. These membership criteria are ostensibly to minimize the probability of disruption but also to protect current members power.
2. Intermediation solution: even when investors and market participants could be a direct member of the CSD, they might still decide to buy the services of a custodian with economies of scale and expertise in the procedures of the CSD. These procedures are complex and involve various risks.
3. Specialisation and banking services: the custodian bank provides services that are most efficiently performed by the same entity that holds the securities for investors and other financial intermediaries. These services fall into two broad categories: specialized reporting for a specific customer segment, such as investment funds, and banking services, such as intraday liquidity provision and securities financing, which most CSDs do not provide because it involves credit exposure.

Providing custody services involves risks and hence custodians' customers also take risks on their service providers. The risks for both parties fall into three general categories: operational, financial and legal. In the wider context of financial market stability, there is also a systemic risk that can be caused by the operational or the financial failure of a custodian that is a large financial institution. There are extensive regulatory controls governing bank custodians. These, unfortunately, are not fully coherent globally and this creates the opportunity for arbitrage and an amplification of the systemic risk.

- **Operational Risks**
  - Actions on to the assets not performed correctly or in line with the investor

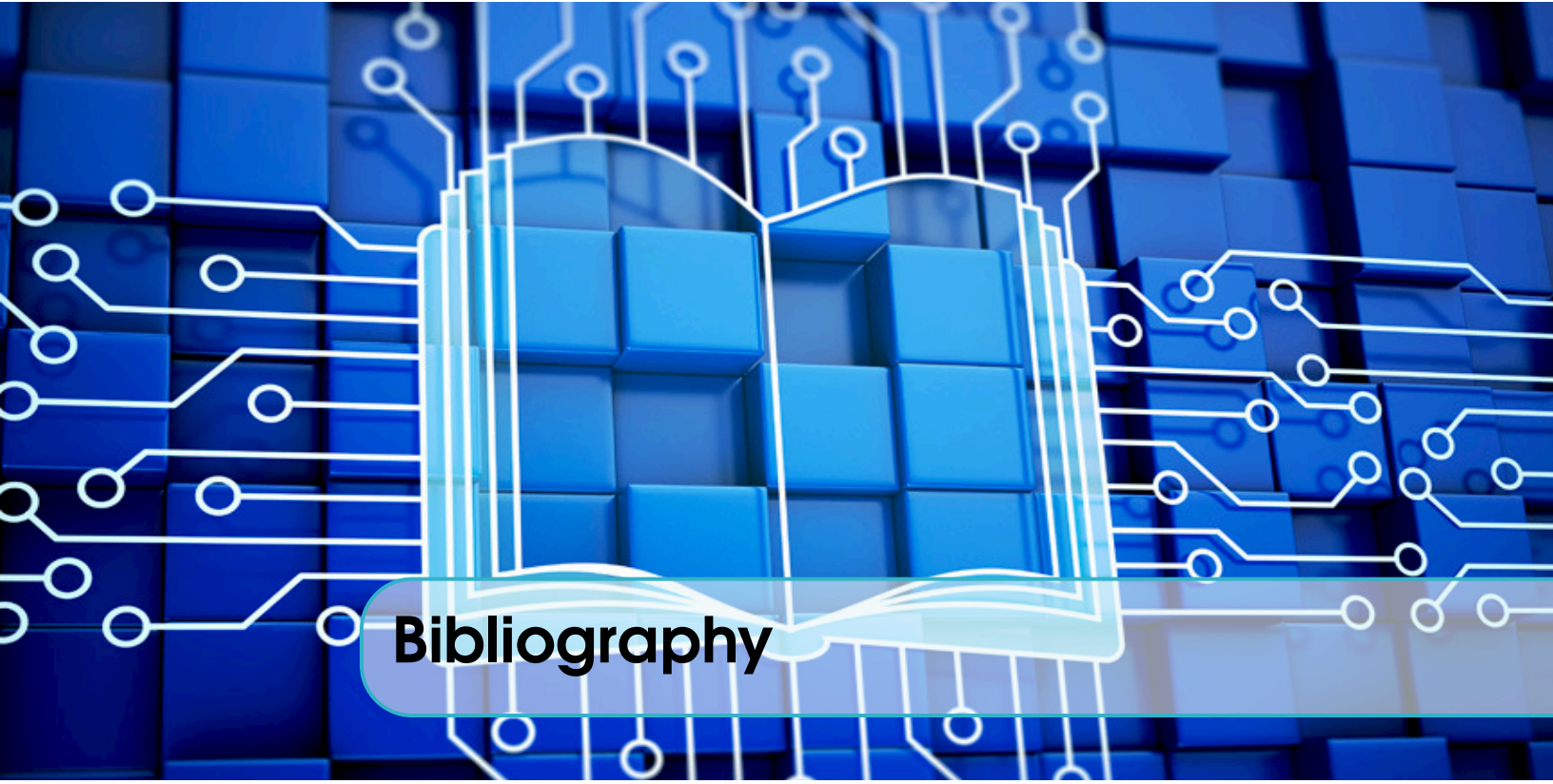
wishes.
  - Settlement: delivery versus payment exposes to delays and in cases of inadequate follow-up of mistakes, loss of capital.
  - Valuation and accounting errors.
- **Credit Risk**
  - The bank may be doing other activities (lending to clients or to third parties) that may lead to the inability to fulfil its obligations.
  - Security Lending.
  - Cash that is deposited enters the bank's balance sheet and is no different than a traditional bank account and subject to the same credit risk.
  - Securities typically do not enter the banks' balance sheet but their restitution will be subject to delays and lengthy processes in case of bank failure.
- **Legal Risk**
  - Contestability of rights over collateral.
  - Inapplicability of the preferred law governing the collateral.

Currently, Assets are stored on multiple individual ledgers of records in different institutions, subject to different laws and requirements. Multiple records are needed to guarantee the possibility of independently reference previous actions thus every FI ends up with its own independent "book of record". This ensures errors and unnecessary duplication as well as the proliferation of centralizing intermediaries which provide reconciliation services.

DeXtf On-chain Custody

The DeXtf Blockchain will locks in a tamper-resistant distributed way the assets. The XTF token issued under DeXtf will "own" the assets directly. The structure eliminates the need for different Information Silos and hence of reconciliation and aggregation services.

It will also, most importantly, eliminate the need for trusted counterparties and the associated operational, credit and legal risks.



Bibliography

[1] Benjamin Collette, Simon Ramos, and Patrick Laurent, “Blockchain and the impact on fund distribution,” Tech. Rep., Jun. 2016. [Online]. Available: https://www2.deloitte.com/lu/en/pages/technology/articles/impacts-blockchain-fund-distribution.html

[2] Barry Benjamin, Kevin O’Connell, Nicholas D’Angelo, Scott Esposito, and Gena Wilson, “Evolution of the mutual fund transfer agent: Embracing the challenges and opportunities,” Tech. Rep., Jul. 2015. [Online]. Available: https://www.pwc.com/us/en/asset-management/investment-management/publications/assets/pwc-mutual-fund-transfer-agent-evolution.pdf